

NGUYEN HUONG LÂM

DO LONG VAN

On a class of infinitary codes

RAIRO. Informatique théorique et applications, tome 24, n° 5 (1990),
p. 441-458

http://www.numdam.org/item?id=ITA_1990__24_5_441_0

© AFCET, 1990, tous droits réservés.

L'accès aux archives de la revue « RAIRO. 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/>

ON A CLASS OF INFINITARY CODES (*)

by NGUYEN HUONG LÂM and DO LONG VAN (1)

Communicated by J. E. PIN

Abstract. – *The notion of infinitary codes has been introduced and studied in [2]-[7]. We consider in this paper a special class of these codes called strict codes i.e. codes which involve infinite product of words.*

Résumé. – *La notion de codes infinitaires a été introduite et étudiée dans [2]-[7]. Nous considérons dans cet article une classe spéciale de tels codes appelés codes stricts i.e. des codes qui concernent un produit infini de mots.*

1. PRÉLIMINARIES

Let A be a finite or countable alphabet. Each symbol of A is called a *letter*. As usual, we denote A^* the free monoid generated by A whose elements are called *finite words*. For each word w of A^* , we denote $|w|$ the length of w . The unit of A^* is the empty word denoted by ε , $|\varepsilon|=0$. We denote $A^{\mathbb{N}}$ the set of all functions $u: \mathbb{N} \rightarrow A$ from the set \mathbb{N} of the natural numbers into the alphabet A . Such a function u is also written in the form of infinite sequence of letters,

$$u = u_1 u_2 \dots$$

with $u_i = u(i)$ ($i = 1, 2, \dots$) and called an *infinite word* over A . We say by convention that the length of every infinite word is $\omega = \text{card } \mathbb{N}$.

(*) Received June 1988, revised September 1989.

(1) Institute of Mathematics, P. O. Box 631 Bo Ho, Hanoi, Vietnam.

The set $A^\infty = A^N \cup A^*$ whose elements we call simply words can be equipped with a product defined by

$$\alpha \cdot \beta = \alpha \quad \text{if } \alpha \in A^N \quad \text{and} \quad \alpha \cdot \beta = \alpha\beta \quad \text{if } \alpha \in A^*$$

where $\alpha\beta$ is the concatenation of α and β . Clearly, this product makes A^∞ a monoid. In the sequel, for the sake of simplicity, we shall write $\alpha\beta$ instead of $\alpha \cdot \beta$. We call *infinitary* (*finitary*, *purely infinitary*) language any subset X of A^∞ (resp. A^* , A^N). Given an infinitary language X , we denote $X_{\text{fin}} = X \cap A^*$, $X_{\text{inf}} = X \cap A^N$. Also, the following notations are used:

X^* : the submonoid of A generated by X .

X^ω : the set of all the infinite words of the form $u = x_1 x_2 \dots$ with $x_i \in X_{\text{fin}} - \{\varepsilon\}$. Obviously $A^\omega = A^N$.

$$X^\infty = X^* \cup X^\omega$$

$$X_{(n)} = \{(x_1, x_2, \dots, x_n) / x_1, \dots, x_{n-1} \in X_{\text{fin}}, x_n \in X\}, \quad n = 1, 2, \dots$$

$$X_* = \bigcup_{n \geq 1} X_{(n)}$$

$$X_\omega = \{(x_1, x_2, \dots) / x_i \in X_{\text{fin}}, i = 1, 2, \dots\}$$

$$X_\infty = X_* \cup X_\omega$$

A word α is said to admit an X_* -factorization (resp. X_∞ -factorization) if $\alpha = x_1 x_2 \dots$ with $(x_1, x_2, \dots) \in X_*$ (resp. X_∞). Obviously α admits an X_* -factorization (resp. X_∞ -factorization) if and only if $\alpha \in X^*$ (resp. X^ω).

Let X, Y be two subsets of A^∞ , we denote

$$Y^{-1}X = \{\alpha \in A^\infty / \exists \beta \in Y : \beta\alpha \in X, \beta \in A^N \Rightarrow \alpha = \varepsilon\}$$

$$XY^{-1} = \{\alpha \in A^\infty / \exists \beta \in Y : \alpha\beta \in X, \alpha \in A^N \Rightarrow \beta = \varepsilon\}$$

$$XY = \{\alpha\beta / \alpha \in X, \beta \in Y\}$$

$$X^2 = XX.$$

When Y is a singleton, $Y = \{\alpha\}$, we write simply $\alpha^{-1}X, X\alpha^{-1}$ instead of $\{\alpha\}^{-1}X, X\{\alpha\}^{-1}$

An infinitary language X is said to be an *infinitary code* if each word of A^∞ admits no more than one X_* -factorization. The concept of infinitary codes was introduced in [3] and for them an extension of Sardinas/Patterson criterion was proved in [5] which provides a procedure to verify whether a given infinitary language is a code. We now recall it.

To every subset X of A^ω we associate a sequence of subsets $U_n(X)$ defined by

$$U_1(X) = X^{-1} X - \{ \varepsilon \}$$

$$U_{n+1}(X) = X^{-1} U_n(X) \cup U_n^{-1}(X) X, \quad n \geq 1$$

THEOREM 1.1: (Generalized Sardinas/Patterson criterion [5]). *A subset X of $A^\omega - \{ \varepsilon \}$ is a code if and only if for all $n \geq 1$, $U_n(X)$ does not contain the empty word ε .*

Our aim in this paper is to study a special class of infinitary codes obtained by replacing in the definition of codes the condition “every word has no more than one X_* -factorization” by a stronger one. More precisely, we have

DEFINITION 1.2: An infinitary language X is said to be a strict infinitary code if each word of A^ω admits no more than one X_ω -factorization.

Throughout this writing, without otherwise stated, a strict code means a strict infinitary code. L. Staiger [11] has introduced and considered infinitary finite-length codes, these are not other but strict codes, which are finitary.

By definition, the class of strict codes is contained in the class of codes. The following example shows that the inclusion is proper.

Example 1.3: Consider the subset $X = \{ a, ab, bb \}$ over the binary alphabet $\{ a, b \}$. An application of Theorem 1.1. shows that X is a code. It is not a strict code because the word ab^ω for example admits two different X_ω -factorizations (a, bb, bb, \dots) and (ab, bb, bb, \dots) .

The rest of the paper consists of two sections. In Section 2 we establish a relationship between strict codes and codes and also some criteria for strict codes, which are analogous to that of Sardinas/Patterson. In Section 3 a criterion for strict codes similar to that of Schützenberger for finitary codes is given. It is noted that in the case of infinitary codes the freeability alone is not enough for a submonoid of A^ω to have a code as base (see [4], [6]).

2. TESTS OF STRICT CODES

Given a new symbol c not belonging to the alphabet A . To each subset X of A^ω we associate a subset \bar{X} of $(A \cup \{ c \})^\omega$ defined by

$$\bar{X}_{\text{fin}} = \{ x_1 c x_2 / x_1 x_2 \in X_{\text{fin}} \}$$

$$\bar{X}_{\text{inf}} = X_{\text{fin}}^\omega \cup X_{\text{fin}}^* X_{\text{inf}} \cup \{ x_1 c x_2 / x_1 \in X_{\text{fin}}, x_1 x_2 \in X_{\text{inf}} \}$$

The following theorem establishes a connection between codes and strict codes.

THEOREM 2.1: *For any subset X of A^∞ , X is a strict code if and only if \bar{X} is a code.*

Proof: If \bar{X} is not a code then we have a word $\bar{\alpha}$ admitting two different \bar{X}_* -factorization $(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_{n-1})$ and $(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_{m-1})$ with $m, n \geq 0, \bar{x}_1 \neq \bar{y}_1, i. e.$

$$\bar{x}_1 \bar{x}_2 \dots \bar{x}_{n+1} = \bar{y}_1 \bar{y}_2 \dots \bar{y}_{m+1} = \bar{\alpha} \tag{1}$$

For every $\bar{\beta} \in (A \cup \{c\})^\infty$, denote β the word obtained from $\bar{\beta}$ by erasing all the occurrences of c . Then from (1), we have

$$x_1 x_2 \dots x_{n+1} = y_1 y_2 \dots y_{m+1} = \alpha \tag{2}$$

By the definition of \bar{X} , it is easy to check that $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m \in X_{fin}; x_{n+1}, y_{m+1} \in X^\infty$. Also, $\bar{x}_1 \neq \bar{y}_1$ and (1) imply that $x_1 \neq y_1$ which proves that X is not a strict code.

Conversely, let X not be a strict code. There exist then two different X_∞ -factorizations (x_1, x_2, \dots) and (y_1, y_2, \dots) with $x_1 \neq y_1$ of some word α of A^∞ . We always can suppose that $\alpha \in A^N$, since if $\alpha \in A^*$ and admits two different X_∞ -factorizations, so does α^ω . The words x_1, y_1 cannot both belong to X_{inf} , otherwise $x_1 = y_1$. If x_1 and y_1 are both in X_{fin} , assume that $|x_1| < |y_1|$ which implies $y_1 = x_1 z_1, z_1 \in A^+ = A^* - \{\varepsilon\}$. We put $\bar{x}_1 = x_1 c, \bar{y}_1 = x_1 c z_1, \bar{x}_2 = x_2 x_3 \dots, \bar{y}_2 = y_2 y_3 \dots$. Clearly $\bar{x}_1, \bar{x}_2, \bar{y}_1, \bar{y}_2$ are in \bar{X} and $\bar{x}_1 \neq \bar{y}_1$. From the equality

$$x_1 x_2 \dots = y_1 y_2 \dots = \alpha \tag{3}$$

it follows

$$\bar{x}_1 \bar{x}_2 = \bar{y}_1 \bar{y}_2$$

which shows that X is not a code.

Suppose $x_1 \in X_{fin}, y_1 \in X_{inf}$, from (3) it follows $y_1 = x_1 y$ with $y \in X^\infty \cap A^N$. We put $\bar{x}_1 = x_1 c, \bar{y}_1 = x_1 c y, \bar{x}_2 = x_2 x_3 \dots$. Then we have $\bar{x}_1 \bar{x}_2 = \bar{y}_1$ and thus \bar{X} is not a code. This completes the proof.

The use of Theorem 2.1 lies in the fact that instead of checking whether X is a strict code it suffices to verify whether \bar{X} is a code or not. For the latter can be applied Generalized Sardinas/Patterson criterion given in Theorem 1.1, and since \bar{X} is a rational and constructible language whenever X is

rational language, the Theorem 2. 1, provides an algorithm for testing whether a rational language is a strict code.

Example 2. 2: Let

$$A = \{ a, b \}, \quad X = \{ a, aba, ab^{\omega} \}.$$

Then

$$\bar{X} = \{ ca, ac, caba, acba, abca, abac \} \cup \{ acb^{\omega} \} \cup \{ a, aba \}^{\omega} \cup \{ a, aba \}^* ab^{\omega}.$$

We have

$$U_1(\bar{X}) = \{ ba, b^{\omega} \}, \quad U_2(\bar{X}) = \emptyset$$

Thus \bar{X} is a code and therefore X is a strict code.

Example 2. 3: Let

$$A = \{ a, b \}, \quad X = \{ aa, ba, baa \}.$$

Then

$$\bar{X} = \{ caa, acaaac, cba, bca, bac, cbaa, bcaa, baca, baac \} \cup \{ aa, ba, baa \}^{\omega}.$$

We have $U_1(\bar{X}) = \{ a \}$, $U_2(\bar{X}) = \{ ca, ac \} \cup \{ a \}$, $\{ aa, ba, baa \}^{\omega}$ and $\varepsilon \in U_2(\bar{X})$ because $X_{\text{inf}} \cap \{ a \} \{ aa, ba, baa \}^{\omega} \neq \emptyset$. Thus \bar{X} is not a code and therefore X is not a strict code.

Now if using directly the sequence of subsets $U_n(X)$ mentioned in Theorem 1. 1, we shall get a sufficient criterion for strict codes formulated as follows.

THEOREM 2. 4: *For any subset X of $A^{\omega} - \{ \varepsilon \}$ if $U_i(X) = \emptyset$ for some $i \geq 1$ then X is a strict code.*

Proof: Suppose on the contrary X is not a strict code, we shall prove that $U_i(X) \neq \emptyset$ for all $i \geq 1$. It is noted that if $U_i(X) = \emptyset$ for some i then $U_j(X) = \emptyset$ for all $j > i$.

If X is not a code then, by Theorem 1. 1 and the above remark, it is easy to see that $U_i(X) \neq \emptyset$ for all $i \geq 1$.

Suppose now X is a code not being a strict code. There exist then $(x_1, x_2, \dots) \in X_{\omega}$ and $(y_1, y_2, \dots) \in X_{\omega}$ with $x_1 \neq y_1$ such that

$$x_1 x_2 \dots = y_1 y_2 \dots$$

Clearly the proof will be completed if the following assertion is approved: For every $k \geq 1$ there exist a non-empty word $z \in U_k(X)$ and two integers

$i, j \geq 1$ such that holds one of the following cases:

- (a)
$$x_1 \dots x_i = y_1 \dots y_j$$

$$zx_{t+1} x_{t+2} \dots = y_{j+1} y_{j+2} \dots, \quad |z| < \omega$$
- (b)
$$x_1 \dots x_t = y_1 \dots y_j$$

$$x_{t+1} x_{t+2} \dots = zy_{j+1} y_{j+2} \dots, \quad |z| < \omega$$
- (c)
$$x_1 \dots x_1 z = y_1 \dots y_j$$

$$x_{t+1} x_{t+2} \dots = z, \quad |z| = \omega$$

We now prove it by induction on k .

If $|x_1| > |y_1|$ there exists then a nonempty finite word z such that

$$x_1 = y_1 z$$

$$zx_2 x_3 \dots = y_2 y_3 \dots$$

and so $z \in U_1(X)$.

If $|x_1| < |y_1| < \omega$, there exists then a nonempty finite word z such that

$$x_1 z = y_1$$

$$x_2 x_3 \dots = zy_2 y_3 \dots$$

and so $z \in U_1(X)$.

If $|x_1| < |y_1| = \omega$ then there is an infinite word z such that

$$x_1 z = y_1$$

$$x_2 x_3 \dots = z$$

and so $z \in U_1(X)$. Thus the assertion is true for $k=1$. Suppose now it is true for $k>1$, we prove it true for $k+1$. By the induction assumption there exists a nonempty word z of $U_k(X)$ such that one of the conditions (a), (b), (c), holds. We treat only the case when (a) holds, for the other cases the arguments are similar. We have $y_{j+1} \neq z$ because if not the equality $x_1 \dots x_i = y_1 \dots y_j z$ implies $x_1 \dots x_i = y_1 \dots y_j y_{j+1}$ which contradicts the fact that X is a code. So the following three cases are possible.

If $|z| > |y_{j+1}|$ then there is a nonempty finite word z_1 such that $z = y_{j+1} z_1$. So $z_1 \in U_{k+1}(X)$ and from (a) we have

$$x_1 \dots x_t = y_1 \dots y_{j+1} z_1$$

$$z_1 x_{t+1} x_{t+2} \dots = y_{j+2} y_{j+3} \dots$$

i. e. (a) holdk for z_1 , $i, j+1$.

If $|z| < |y_{j+1}| < \omega$ then there is a nonempty finite word z_2 such that $zz_2 = y_{j+1}$. So $z_2 \in U_k(X)$ and from (a) we have

$$x_1 \dots x_t z_2 = y_1 \dots y_{j+1}$$

$$x_{j+1} x_{j+2} \dots = z_2 y_{j+2} y_{j+3} \dots$$

i. e. (b) holds for z_2 , $i, j+1$.

If $|z| < |y_{j+1}| = \omega$ then there exists an infinite word z_3 such that $zz_3 = y_{j+1}$. So $z_3 \in U_{k+1}(X)$ and from (a) we have

$$\begin{aligned} x_1 \dots x_i z_3 &= y_1 \dots y_{j+1} \\ x_{i+1} x_{i+2} \dots &= z_3 \end{aligned}$$

i.e. (c) holds for $z_3, i, j+1$.

Thus the assertion is true for $k+1$. This completes the proof.

The converse fails, as it is shown in the following example.

Example 2.5: Let $X = \{aa, ba, baa(aa)^* \{ba, baa\}\}$. It is easy to verify that X is a regular strict code, but $U_1 = a(aa)^* \{ba, baa\}$ and for all $n > 0$, $U_1 = U_n \neq \emptyset$.

The converse of Proposition 2.4 holds if we restrict ourselves to finite languages, to wit

THEOREM 2.6: *For any finite subset X of $A^\omega - \{\varepsilon\}$, X is a strict code if and only if $U_1 = \emptyset$ for some $i \geq 1$.*

Remark: The Example 2.5 above also shows that the Theorem 2.6 does not hold for the regular languages, for which we develop another criterion in the sequel (Theorem 2.10).

Proof: It suffices to prove the “only if” part. To do this we make use of the following result of D. König which has an interest of its own.

LEMMA (König [8]): *Let $G = (V, E)$ be a directed graph whose set V of vertices is an infinite union of nonempty finite subsets $V_i, i = 1, 2, \dots$ such that for each $y \in V_{i+1} (i > 0)$ there exists $x \in V_i$ such that x and y are joined by an edge: $x \rightarrow y$ in E . Then there exists a finite path $x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_n \rightarrow \dots$ with $x_i \in V_i$ for $i = 1, 2, \dots$*

We now turn to proving Theorem 2.6. Suppose on the contrary that $U_i(X) \neq \emptyset$ for all $i \geq 0$ and X is a strict code. Put $V_i = U_i(X) i = 1, 2, \dots$. The vertices $\alpha \in V_i, \beta \in V_{i+1}$, for every i , are joined by an edge if and only if there is u of X such that $\beta = \alpha^{-1}u$ or $\beta = u^{-1}\alpha$. Since X is finite, so is each V_i . That each $\beta \in V_{i+1}$ is joined with some $\alpha \in V_i$ by an edge (α, β) for every i is obvious from the definition of subsets $U_i(X)$. Thus, from Lemma it follows that there exists an infinite path $\alpha_1 \rightarrow \alpha_2 \rightarrow \dots$ with $\alpha_i \in V_i$. We now construct by induction on k two sequences of words of $X: u_1, u_2, \dots$ and v_1, v_2, \dots with the property: for every $k > 0$ there exist $i(k)$ and $j(k) > 0$ such that either

$$u_1 \dots u_{i(k)} \alpha_k = v_1 \dots v_{j(k)} \tag{1}$$

or

$$u_1 \dots u_{i(k)} = v_1 \dots v_{j(k)} \alpha_k \tag{2}$$

For $k=1$, since $\alpha_i \in U_1(X)$ there exist u, v of X such that $u\alpha_1=v$ and $u \neq v$. We put $i(1)=j(1)=1$ and $u_{i(1)}=u, v_{j(1)}=v$. Suppose now for $k>0$ $u_1, \dots, u_{i(k)}, v_1, \dots, v_{j(k)}$ have been defined already such that (1) or (2) holds.

Since $\alpha_k \rightarrow \alpha_{k+1}$ is an edge, there exists then u of X such that either

$$\alpha_{k+1} = u^{-1} \alpha_k \Rightarrow u \alpha_{k+1} = \alpha_k \tag{3}$$

or

$$\alpha_{k+1} = \alpha_k^{-1} u \Rightarrow \alpha_k \alpha_{k+1} \tag{4}$$

We must have in (3) $u \in X_{\text{fin}}$ and in (4) $|\alpha_k| < \omega$, otherwise $\varepsilon = \alpha_{k+1}$ and X is no more a strict code (not even a code: Theorem 1. 1).

Four possible combinations are (1) & (3), (1) & (4), (2) & (3), and (2) & (4). We treat first the case of (1) & (3). Then

$$u_1 \dots u_{i(k)} u \alpha_{k+1} = v_1 \dots v_{j(k)}$$

Thus we can take $u_{i(k+1)} = u, i(k+1) = i(k) + 1$ and $j(k+1) = j(k)$.

For the case of (2) & (4), from (2) and (4) it follows

$$u_1 \dots u_{i(k)} \cdot \alpha_{k+1} = v_1 \dots v_{j(k)} \alpha_k \alpha_{k+1} = v_1 \dots v_{j(k)} u$$

It suffices to take $i(k+1) = i(k), j(k+1) = j(k) + 1, v_{j(k+1)} = u$. The other cases are treated similarly. Note that when treating the combinations, we take $i(k+1) = i(k)$ and $j(k+1) = j(k) + 1$ or $i(k+1) = i(k) + 1$ and $j(k+1) = j(k)$ iff (2) or (4) appears in them respectively. Thus the required sequences are constructed.

Now we distinguished two possibilities, both leading to contradictions

(i) $|\alpha_i| = \omega$ for some s .

We have, for instance, $u_1 \dots u_{i(s)} \alpha_s = v_1 \dots v_{j(s)}$ and $|v_1 \dots v_{j(s)}| = \omega$ and for all $i \leq i(s): |u_i| < \omega$ (otherwise $u_1 \dots u_{i(s)} = v_1 \dots v_{j(s)}$).

Furthermore, by construction from s on we have for all $k \geq s: i(k+1) = i(k)$ and $|u_{i(k)}| < \omega$ and $|\alpha_k| = \omega$ [(1) & (3) always happens]. Hence $u_1 u_2 \dots = y_1 \dots y_{j(s)}$: a contradiction with X is a strict code.

(ii) For all $s > 0$ $|\alpha_i| < \omega \Rightarrow u_i, v_j \in X_{\text{fin}}$ for all i, j .

If the sequence (u_i) is finite then there exists s such that for every $k > s$ $i(s) = i(k)$, hence there is $k, k > s$ such that $|u_1 \dots u_{i(k)}| < |v_1 \dots v_{j(k)}|$ (since

for all $k > s$ $i(k+1) = i(k)$ implies $j(k+1) = j(k) + 1$ that is (v_j) is infinite). That is to say we are in the case (1), it follows that $i(k+1) = i(k) + 1$: a contradiction with $i(s) = i(k+1)$. So (u_i) must be infinite. As X is a strict code $u_1 u_2 \dots \neq v_1 v_2 \dots$. There might be then integers m and $n \geq 1$ such that each of the words $u_1 \dots u_n, v_1 \dots v_m$ is not a prefix of the other which is impossible because of (1) and (2). Theorem is proved.

Example 2.7: Let $A = \{a, b\}$, $X = \{ba, bab, b(bab)^\omega\}$. We have $U_1(X) = \{b\}$, $U_2(X) = \{a, ab, (bab)^\omega\}$. Hence $(bab)^\omega \in U_i(X)$ for every $i \geq 3$. By Theorem 2.6 X is not a strict code. In fact, the word $(bab)^\omega$ has two different X_∞ -factorizations (bab, bab, \dots) and $(ba, b(bab)^\omega)$.

Now we give another modification of the Sardinas/Patterson algorithm. To any language $X \subseteq A^\infty$ we associate the following sequence of subsets of A^∞ :

$$V_1(X) = X^{-1} X - \{\varepsilon\}$$

$$V_i(X) = V_{i+1}^{-1}(X) X^\infty, \quad i = 1, 2, \dots$$

PROPOSITION 2.8: *For any subset X of $A^\infty - \{\varepsilon\}$, if $V_i(X) = \emptyset$ for some $i \geq 1$ then X is a strict code.*

Proof: Suppose on the contrary that X is not a strict code. There exist then two different X_∞ -factorizations (x_1, x_2, \dots) and (y_1, y_2, \dots) with $x_1 \neq y_1$ such that

$$x_1 x_2 \dots = y_1 y_2 \dots \tag{1}$$

We now show that $V_i(X) \neq \emptyset$ for all $i \geq 1$. Indeed, by (1) and $x_1 \neq y_1$ we can assume $|x_1| < |y_1|$ and then $x_1 z_1 = y_1$ for some $z_1 \neq \varepsilon$. Thus $z_1 \in V_1(X)$ and $V_i(X) \neq \emptyset$. It follows from (1) that

$$x_2 x_3 \dots = z_1 y_2 y_3 \dots$$

If $|z_1| = \omega$ then $z_1 = x_2 x_3 \dots \in X^\infty$. Hence $V_2(X)$ contains ε , for $\varepsilon = z_1^{-1} z_1 \in V_1^{-1}(X) X^\infty = V_2(X)$. Since $\varepsilon \in X^\infty$ it follows $\varepsilon \in V_i(X)$ for all $i \geq 2$, i.e. $V_i(X) \neq \emptyset$. If $|z_1| < \omega$ we put $z_2 = y_2 y_3 \dots$. Clearly, $z_2 \in X^\infty$ and $z_2 = z_1^{-1} (x_2 x_3 \dots) \in V_1^{-1}(X) X^\infty = V_2(X)$. Consequently, $\varepsilon = z_2^{-1} z_2 \in V_3(X)$. By the same argument as above, we have $\varepsilon \in V_i(X)$ for all $i \geq 3$ and therefore $V_i(X) \neq \emptyset$ for all $i \geq 1$. This concludes the proof.

The following example shows that the converse of Proposition 2.8, is not true.

Example 2.9: Consider any infinite prefix code X_0 in A^* , $X_0 = \{x_1, x_2, \dots\}$. Put $X_1 = \{x_1, x_1 x_2\}$, $X_2 = \{x_3, x_3 x_4, x_4 x_5\}, \dots$, $X_n = \{x_{n(n+1)/2}, x_{n(n+1)/2} x_{n(n+1)/2+1}, \dots, x_{n(n+1)/2+n-1} x_{n(n+1)/2+n}\}$, and put $X = \bigcup_{i \geq 1} X_i$. It is easy to see that $x_{n(n+1)/2+n} \in V_n(X)$ for all $n \geq 1$. The fact that

X is a strict code can be verified directly.

Nevertheless, the converse holds true for the case of regular languages. We recall that a language X of A^∞ is said to be *regular* if the family $\{\alpha^{-1} X / \alpha \in A^\infty\}$ is finite. We call the cardinality of this family *index* of X . It is noteworthy that every language recognizable by finite automata is regular and that the class of regular languages is closed under union, intersection, *, ω and ∞ .

The following theorem is a generalization of Lemma 15 in [4].

THEOREM 2.10: *If $X \subseteq A^\infty - \{\varepsilon\}$ is an infinitary regular language then X is a strict code if and only if $V_i(X) = \emptyset$ for some $i \geq 1$.*

Remark: The theorem 2.10 holds also for the infinitary finite (not necessarily regular) languages. The proof can be proceeded just as in case of Theorem 2.6, taking into account the fact that whenever X is finite $V_i \subset w_1 X^\infty \cup \dots \cup w_n X^\infty$, for every i , with some words $w_1, \dots, w_n \in A^\infty$.

Proof: In view of Proposition 2.8, it suffices to prove that if $V_1(X) \neq \emptyset$ for all $i \geq 1$ then X is not a strict code. Let the index of X^∞ be n . We choose $m > n$ and any word $u_m \in V_m(X)$. By definition, there exist $u_1 \in V_1(X), \dots, u_{m-1} \in V_{m-1}(X)$ such that $u_{i+1} \in u_i^{-1} X^\infty$ for $i = 1, 2, \dots, m-1$. Since X^∞ is a regular language of index n and $m > n$, there must be integers p and q such that $1 \leq p < q \leq m$ and $u_p^{-1} X^\infty = u_q^{-1} X^\infty$. Without loss of generality we can suppose $q = m$ and $d = m - p > 1$. We put for every $j \geq m : u_j = u_{p+t}$, where $t = j - m \pmod d$.

We state that for every $i \geq 1$ $u_{i+1} \in u_i^{-1} X^\infty$. Indeed, it is trivial for $1 \leq i \leq m-1$. Suppose $i \geq m$, for $i = m$ we have $u_{m+1} = u_{p+1} \in u_p^{-1} X^\infty = u_m^{-1} X^\infty$ (because $1 \leq d-1$). Suppose the statement is true for some $i \geq m$, we prove it holds true for $i+1$. Let $i = m + kd + t$ for some $k \geq 0, 0 \leq t \leq d-1$. If $t < d-1$, we have

$$u_{i+1} = u_{m+kd+t+1} = u_{p+t+1} \in u_{p+t}^{-1} X^\infty = u_{m+kd+t}^{-1} X^\infty = u_i^{-1} X^\infty$$

If $t = d-1$, we have

$$\begin{aligned} u_{i+1} = u_{m+(k+1)d} &= u_p = u_m \in u_{m-1}^{-1} X^\infty = u_{p+d-1}^{-1} X^\infty \\ &= u_{m+kd+d-1}^{-1} X^\infty = u_{m+kd+t}^{-1} X^\infty = u_i^{-1} X^\infty \end{aligned}$$

Now we put

$$x_i = u_i u_{i+1}$$

for $i = 1, 2, \dots$. Obviously $x_i \in X^\infty$. From the fact that $u_1 \in V_1(X) = X^{-1} X - \{\varepsilon\}$ it follows

$$u_0 u_1 = z_1$$

for some z_0, z_1 in X , $z_0 \neq z_1$.

Consider the product $z_0 u_1 u_2 u_3 u_4 \dots$. We can write it by two ways

$$z_0 (u_1, u_2) (u_2 u_4) \dots = (z_0 u_1) (u_2 u_3) (u_4 u_5) \dots$$

which yields

$$z_0 x_1 x_3 \dots = z_1 x_2 x_4 \dots$$

which shows that X is not a strict code. The proof is completed.

Remark 2.11: When X is finitary, we define the sequence of subsets $\bar{V}_i(X)$ by

$$\begin{aligned} \bar{V}_1(X) &= X^{-1} X - \{\varepsilon\} \\ \bar{V}_{i+1}(X) &= \bar{V}_i^{-1} X^*, \quad i \geq 1 \end{aligned} \tag{0}$$

and state

Claim: $V_i(X) \neq \emptyset$ for all i if and only if $\bar{V}_i(X) \neq \emptyset$ for all i .

Therefore we can replace in the formulation of Proposition 2.8 and Theorem 2.10 the subsets $V_i(X)$ by $\bar{V}_i(X)$ which are convenient for calculation.

We now outline the proof of Claim. By induction on i , we can easily establish the following two points:

- (i) $\bar{V}_i(X) \subseteq V_i(X)$ for $i = 1, 2, \dots$
- (ii) If $v_i \in \bar{V}_i(X)$ and there exist $x_1, x_2, \dots \in X$ and $y_1, y_2, \dots \in X$ such that

$$v_i x_1 x_2 \dots = y_1 y_2 \dots$$

then $\bar{V}_j(X) \neq \emptyset$ for all $j > i$.

(iii) Let n be the smallest integer such that $V_{n \text{ inf}} \cap X^\omega \neq \emptyset$. Then for $i = 2, 3, \dots, n$

$$\bar{V}_i(X) X^\omega = V_i \tag{1}$$

If $V_{i \text{ inf}} \cap X \neq \emptyset$ for all i then (1) holds for all i . Indeed, for all $i: 1 \leq i \leq n-1$

$$\begin{aligned}
 V_{i+1} &= V_i^{-1} X^\infty = V_{i \text{ fin}}^{-1} X^* \cup V_{i \text{ fin}}^{-1} X^\omega \cup V_{i \text{ inf}}^{-1} X^\omega \\
 &= V_{i \text{ fin}}^{-1} X^* \cup V_{i \text{ fin}}^{-1} X^\omega \tag{2}
 \end{aligned}$$

$$= (V_{i \text{ fin}}^{-1} X^*) X^\infty \tag{3}$$

(we write V_i instead of $V_i(X)$ for short).

Hence

$$V_{i+1 \text{ fin}} = V_{i \text{ fin}}^{-1} X^* \tag{4}$$

for $i=1, \dots, n-1$. Since $V_{1 \text{ fin}} = V_1 = \bar{V}_1$, comparing (4) with (1) we obtain $V_{i+1 \text{ fin}} = \bar{V}_{i+1}$, $i=1, \dots, n-1$. Hence, from (3) we get

$$V_{i+1} = (\bar{V}_i^{-1} X^*) X^\infty = \bar{V}_{i+1} X^\infty$$

Thus (iii) is proved.

Suppose now $\bar{V}_i(X) \neq \emptyset$ for every i then by (i) $V_i(X) \neq \emptyset$ for every i . Conversely, suppose $V_i(X) \neq \emptyset$ for all $i=1, 2, \dots$. If the number n mentioned in (iii) does not exist then (1) holds for all $i \geq 1$, therefore $\bar{V}_i(X) \neq \emptyset$ for all $i \geq 1$. If $n < \infty$ then (1) holds for $i=2, \dots, n$. From $V_{n \text{ inf}} \cap X^\omega \neq \emptyset$ and $V_n = V_{n-1}^{-1} X^\infty$ we must have some $w \in V_{n-1}$, $\alpha = x_1 x_2 \dots \in X^\omega$, $\beta = y_1 y_2 \dots \in X^\omega$ such that $w\alpha = \beta$ which gives $|w| < \omega$. Therefore, by (1), we can write $w = v_{n-1} z_1 \dots z_m$ for some $v_{n-1} \in \bar{V}_{n-1}$ and $z_1, \dots, z_m \in X$. Thus we get

$$v_{n-1} z_1 \dots z_m x_1 x_2 \dots = y_1 y_2 \dots$$

which implies that $\bar{V}_i \neq \emptyset$ for all $i \geq n-1$ (by (ii)). Claim is proved.

We now provide a procedure for calculating $\bar{V}_i(X)$. Let V be any finitary subset. For any $n \geq 1$ we define the subsets

$$\begin{aligned}
 Z_1 &= X^{-1} V \\
 Z_{n+1} &= X^{-1} Z_n
 \end{aligned}$$

and

$$\begin{aligned}
 T_1 &= V^{-1} X \\
 T_{n+1} &= T_n X \cup Z_n^{-1} X
 \end{aligned}$$

Put

$$T(V, X) = \bigcup_{i \geq 1} T_i$$

and we state that

$$\bar{V}_1 = X^{-1}X - \{\varepsilon\}$$

$$\bar{V}_{n+1} = T(V_n, X)$$

The last formulas become evident if we pay attention to the following relations

$$T_1 = V^{-1}X$$

$$T_2 = V^{-1}X^2 = (V^{-1}X)X \cup (X^{-1}V)^{-1}X = T_1X \cup Z_1^{-1}X$$

$$T_3 = V^{-1}X^3 = (V^{-1}X^2)X \cup [X^{-1}(X^{-1}V)]^{-1}X = T_2X \cup Z_2^{-1}X$$

etc.

As an example we apply this procedure to show that the languages X of $\{a, b\}^*$, $X = \{a^i b, (a^i b)^i b : i = 1, 2, \dots\}$ is a strict code. Such a verification cannot be done by using Proposition 2.4. We have

$$V_1(X) = \{x_i^{i-1}b / i \geq 1\}$$

It is easy to see that

$$Z_n = \{x_i^{i-n-1} / i \geq n+1\}$$

for $n \geq 1$, and

$$T_1 = V_1^{-1}(X)X = \emptyset$$

$$Z_n^{-1}X = \emptyset$$

for all $n \geq 1$. Consequently

$$T_{n+1} = T_nX \cup Z_n^{-1}X = \emptyset$$

for all $n \geq 1$. Therefore $V_2(X) = T(V_1, X) = \emptyset$. By Proposition 2.8, X is a strict code.

3. COMBINATORIAL CHARACTERIZATIONS

In this section we introduce the concept of ∞ -submonoid of A^∞ and study several properties of such ∞ -submonoids as well as their generator sets. As a main result, we prove a necessary and sufficient condition, analogous to that of Schützenberger [9], for an ∞ -submonoid of A^∞ to have a strict code as the minimal generator set.

Let M be a subset of A^∞ , M is said to be ∞ -submonoid of A^∞ if $M^\infty \subseteq M$. A subset $X \subseteq M$ is called an ∞ -generator set of M if $X^\infty = M$. From now on we shall call X simply a generator set of M . The generator set X is called *minimal* if it does not contain properly any generator set of M . The following proposition gives a characterization of the minimal generator set which is useful in the sequel.

PROPOSITION 3.1: *Let X be a subset of an ∞ -submonoid M of A^∞ , then X is minimal generator set if and only if*

- (i) $X^\infty = M$
- (ii) $X_{\text{fin}} X^{+\infty} \cap X = \emptyset$, where $X^{+\infty} = X^\infty - \{\varepsilon\}$

Proof: Let X be a minimal generator set. Clearly (i) holds. If $\alpha \in X_{\text{fin}} X^{+\infty} \cap X$, then after removing α from X , $X - \{\alpha\}$ remains a generator set of M which is in contradiction with the minimality of X . Thus (ii) holds.

Conversely, assume that (i) and (ii) hold and X is not a minimal generator set. There exists then a generator set Z properly contained in X . Choose $\alpha \in X - Z$. Since Z is a generator set, α is a product of elements of Z

$$\alpha = z_1 z_2 \dots$$

From $\alpha \notin Z$, we have $|z_1| < \omega$ and thus $z_1 \in Z_{\text{fin}} \subseteq X_{\text{fin}}$. Hence $\alpha \in X_{\text{fin}} X^{+\infty}$ which contradicts (ii). This completes the proof.

Given any submonoid M , we define on M_{fin} the relation “ $<$ ” as follows: $u < v$ if and only if there exists a word $w \in M_{\text{fin}} - \{\varepsilon\}$ such that $u = vw$. Clearly, the relation “ $<$ ” is only transitive but not equivalence one. An element u of M_{inf} is called *maximal* if there is no v satisfying $u < v$. The set of maximal elements of M_{inf} is denoted by $\text{MAX}(M_{\text{inf}})$. It is well known that every finitary submonoid N of A^* possesses a smallest generator set in the sense that it is contained in any generator set of N (see, for example, [10]) which we denoted by $\text{ATOM}(N)$ (see [7]). The following proposition shows that every ∞ -submonoid M has a smallest generator set and therefore it has a unique minimal generator set.

PROPOSITION 3.2: Every ∞ -submonoid M possesses a smallest generator set which is $Z = \text{ATOM}(M_{\text{fin}}) \cup \text{MAX}(M_{\text{inf}}) = M - (M_{\text{fin}} - \{\varepsilon\})(M - \{\varepsilon\})$.

Proof: First, we show that Z is contained in any generator set X . In fact, if $\alpha \in Z_{\text{fin}} = \text{ATOM}(M_{\text{fin}})$ then α is a finite product of elements of X_{fin} , and therefore, of M_{fin}

$$\alpha = x_1 x_2 \dots$$

Since α is an element of the minimal generator set of M_{fin} it follows that $n=1$ and thus $\alpha = x_1 \in X$. If $\alpha \in Z_{\text{inf}} = \text{MAX}(M_{\text{inf}})$, α cannot be a product of more than one nonempty word from X , otherwise α would belong to $(X_{\text{fin}} - \{\varepsilon\})X^{+\infty} \subseteq (M_{\text{fin}} - \{\varepsilon\})(M - \{\varepsilon\})$ that contradicts the maximality of α . Thus, we have $\alpha \in X$ and $Z \subseteq X$.

Now it suffices to show that Z is a generator set itself, i.e. every element of M can be expressed as a product of elements of Z . That every $\alpha \in M_{\text{fin}}$ or $\alpha \in M_{\text{fin}} \text{MAX}(M_{\text{inf}})$ is such a product is obvious. If now $\alpha \notin M_{\text{fin}} \cup M_{\text{fin}} \text{MAX}(M_{\text{inf}})$, there exists then an infinite chain

$$\alpha = \alpha_1 < \alpha_2 < \alpha_3 < \dots$$

where $\alpha_i \in M_{\text{inf}} - \text{MAX}(M_{\text{inf}})$, $i = 1, 2, \dots$ which means that

$$\alpha_i = u_{i+1} \alpha_{i+1}$$

for $u_i \in M_{\text{fin}} - \{\varepsilon\}$ and $i = 0, 1, 2, \dots$. Thus

$$\alpha = u_1 u_2 \dots \in M_{\text{fin}}^\omega = \text{ATOM}(M_{\text{fin}})^\omega \subset X^\omega$$

The proof is completed.

Now we come to a characterization of strict codes in terms of submonoids and ∞ -submonoids generated by them.

THEOREM 3.3: For any infinitary language X , X is a strict code if and only if

- (i) $X_{\text{fin}} X^{+\infty} \cap X = \emptyset$
- (ii) $(X^*)^{-1} X^* \cap X^\omega (X^\omega)^{-1} = X^*$

Proof: Suppose that X is a strict code. The fact that (i) holds is obvious by definition of strict code. Let $d \in (X^*)^{-1} X^* \cap X^\omega (X^\omega)^{-1}$. If $d = \varepsilon$ then $d \in X^*$. If $d \neq \varepsilon$ then there exist x from $X^* \cap A^*$ and y from X^* such that $xd = y$. Furthermore: $\exists \alpha, \beta \in X^\omega$ such that $d\alpha = \beta$. If $|d| = \omega$ that implies $d = \beta$ and thus we have $x\beta = y$, which in turn implies $d = \beta \in X^*$, since X is a strict

code. Now if $|d| < \omega$, as $(xd)\alpha = x(d\alpha)$ gives the same factorization of $x d \alpha$ over X , we have $d \in X^*$. Consequently, $(X^*)^{-1} X^* \cap X^\infty (X^\infty)^{-1} \subset X^*$. The reverse inclusion is obvious and therefore $(X^*)^{-1} X^* \cap X^\infty (X^\infty)^{-1} = X^*$.

For the converse, let (i), (ii) hold and suppose X is not a strict code. There exist then $x, y \in X_{\text{fin}}, \alpha, \beta \in X^\infty$ such that $x\alpha = y\beta$ and $|x| < |y|$ ($y \in X_{\text{fin}}$ according to (i)). Hence $x^{-1}y \in [(X^*)^{-1} X^* \cup X^\infty (X^\infty)^{-1}] - \{\varepsilon\}$, i.e. $x^{-1}y \in X^+$. It follows that $y \in X_{\text{fin}} X^+ \cap X$: a contradiction, which shows that X must be a strict code. The theorem is proved.

Let M be a subset of A^∞ , M is said to be *freeable* if $M^{-1}M \cap MM^{-1} = M$. The following theorem, analogous to a result of Schützenberger, characterizes the ∞ -submonoid generated by a strict code.

THEOREM 3.4: *Let M be a ∞ -submonoid then M is freeable if and only if its minimal generator set is a strict code.*

Proof: Let Z be the minimal generator set of M and suppose Z is not a strict code. There exist then $x, y \in Z, \alpha, \beta \in Z^\infty: x\alpha = y\beta$ with $|x| < |y|$ (hence $x \in Z_{\text{fin}}$). Therefore $y = xw$ implies $w \in M^{-1}M - \{\varepsilon\}$ and $\alpha = \omega\beta$ implies $w \in MM^{-1}$. Hence $w \in M - \{\varepsilon\}$. Consequently: $y \in Z_{\text{fin}} Z^{+\infty} \cap Z$, which is a contradiction with Z is a minimal generator.

Conversely, let Z be a strict code and let suppose that $\exists w \in (M^{-1}M \cap MM^{-1}) - M \neq \emptyset$. There exist then $u \in M_{\text{fin}}$ (since $w \neq \varepsilon$): $uw \in M$ and $v \in M: wv \in M$. If $|w| = \omega$ then $v = \varepsilon$ hence $v \in M$ that is a contradiction. If $|w| < \omega$ then from $u(wv) = (uw)v$ being the same factorization over Z we get $w \in Z^* \subset M$: a contradiction again. This completes the proof.

Finally, in the following theorem, we characterize the freeability of ∞ -submonoids via their special subsets. Note that the subset $M - M_{\text{fin}}^\infty$ need not be a submonoid in general.

THEOREM 3.5: *Let M be an ∞ -submonoid, then M is freeable if and only if*

- (i) M_{fin}^∞ is a freeable ∞ -submonoid
- (ii) The subset $M - M_{\text{fin}}^\infty$ is a freeable submonoid.

Proof: First, we recall some notions and results in our previous papers. A monoid M is called *regular* if $M_{\text{fin}}^\infty \cap M_{\text{inf}} = \emptyset$ and *quasi-free* if $M = X^*$ with X is a code. It has been proved that every quasi-free submonoid is freeable (see [2], [4]). The following statement is the Corollary 3.11 from [2] (see also [4]): A regular submonoid is quasi-free iff it is freeable.

Now if M is freeable then M is generated by a strict code $X: M = X^\infty = X_{\text{fin}}^\infty \cup X^*$. Since X is a strict code, then $X_{\text{fin}}^\infty \cap X^* = \emptyset$. Hence

$M - X_{\text{fin}}^{\omega} = M - M_{\text{fin}}^{\omega} = X^*$ is a submonoid generated by a (strict) code, consequently it is freeable. Further, $M_{\text{fin}}^{\omega} = X_{\text{fin}}^{\omega}$ is generated by a strict code X_{fin} , therefore M_{fin}^{ω} is a freeable ∞ -submonoid by Theorem 3.4. Thus the "only if" part is proved.

Suppose now (i) and (ii) hold. Put $\bar{M} = M - M_{\text{fin}}^{\omega}$ which is a submonoid by our assumption. Since $\bar{M}_{\text{fin}} = M_{\text{fin}}$ it follows that $\bar{M}_{\text{fin}}^{\omega} \cap \bar{M}_{\text{inf}} = M_{\text{fin}}^{\omega} \cap \bar{M}_{\text{inf}} = \emptyset$. This means that \bar{M} is a regular submonoid. In virtue of the statement aforementioned, \bar{M} is quasi-free, i.e. $\bar{M} = \bar{X}^*$ for some code \bar{X} . We have $\bar{M}_{\text{fin}} = M_{\text{fin}} = \bar{X}_{\text{fin}}^*$ and $\bar{M}_{\text{inf}} = \bar{X}_{\text{fin}}^* \bar{X}_{\text{fin}}$, hence $M = (M - M_{\text{fin}}^{\omega}) \cup M_{\text{fin}}^{\omega} = \bar{X}^* \cup \bar{X}_{\text{fin}}^{\omega} = \bar{X}^{\omega}$. On the other hand $X_{\text{fin}}^{\omega} \cap X^* = M_{\text{fin}}^{\omega} \cap \bar{M} = \emptyset$. Furthermore, by (i) and Theorem 3.4 M_{fin}^{ω} is generated by a strict code $\bar{X}: M_{\text{fin}}^{\omega} = \bar{X}$. Since $M_{\text{fin}}^{\omega} = \bar{X}_{\text{fin}}$ and the code X_{fin} and the strict code \bar{X} satisfy (i) and (ii) of Proposition 3.1, it follows that both X_{fin} and \bar{X} are the minimal generator set of M_{fin}^{ω} , so in view of Proposition 3.2 $X_{\text{fin}} = \bar{X}$. Thus X_{fin} is a strict code. Finally, note that a code X satisfying $X_{\text{fin}}^{\omega} \cap X^* = \emptyset$ whose finitary part X_{fin} is a strict code is a strict code itself. The proof is completed.

ACKNOWLEDGMENTS

The authors express their thanks to the referee who gave numerous valuable comments and suggested some improvements.

REFERENCES

1. J. BERSTEL and D. PERRIN, Theory of Codes, *Academic Press*, 1985.
2. DO LONG VAN, Contribution to Combinatorics on Words, Thesis, Humboldt University, Berlin, 1985.
3. DO LONG VAN, Codes avec des mots infinis, *R.A.I.R.O.-Informatique Théor. Applic.*, 1982, 16, p. 371-386.
4. DO LONG VAN, Sous-monoïde et codes avec des mots infinis, *Semigroup Forum*, 1983, 26, p. 75-87.
5. DO LONG VAN, Ensembles code-compatibles et une généralisation du théorème de Sardinas/Patterson, *Theor. Comp. Science*, 1985, 38, p. 123-132.
6. DO LONG VAN, Caractérisation combinatoire des sous-monoïdes engendrés par un code infinitaire, *Hanoi Preprint Series*, n° 6, 1984.
7. DO LONG VAN, Sur les ensembles générateur minimaux des sous-monoïdes de A^{ω} , *C.R. Acad. Sci. Paris*, 1985, 300, série I, p. 443-446.
8. D. KÖNIG, Theorie der endlichen und unendlichen Graphen, Leipzig, 1936; Sur les correspondances multivoques des ensembles, *Fundamenta Mathematicae*, 1926, 8, p. 114-134.

9. M. P. SCHÜTZENBERGER, Une théorie algébrique du codage, « Séminaire Dubreil », exposé n° 15, Algèbre et Théorie des Nombres, année 1955-1956; *C.R. Acad. Sci. Paris*, 1956, 242, p. 862-864.
10. L. N. SHEVRIN, On subsemigroups of free semigroups (Russian), *Dokl. Acad. Nauk SSSR*, 1960, 1, p. 892-894.
11. L. STAIGER, On infinitary finite-length codes, *R.A.I.R.O.-Informatique Théor. Appl.*, 1986, 20, p. 483-494.