Theoretical Informatics and Applications
Theoret. Informatics Appl. **35** (2001) 351–365

MAXIMAL CIRCULAR CODES VERSUS MAXIMAL CODES

Yannick Guesnet[1]

Abstract. We answer to a question of De Luca and Restivo whether there exists a circular code which is maximal as circular code and not as code.

Mathematics Subject Classification. 94A45.

Introduction

The theory of codes is closely concerned with the two notions of completeness and maximality. From this point of view, the equivalence between completeness and maximality has been established for famous families of codes as thin codes ([1], p. 67), thin circular codes [4], thin codes with finite deciphering delay [2] and thin codes with finite synchronization delay [3]. Recently, we have established this equivalence for the so-called class of code with finite interpreting delay [5, 7].

More precisely, let $\mathcal{F}$ be one of the previous families and let $X \in \mathcal{F}$, then X is complete if and only if X is maximal in $\mathcal{F}$. These families of codes even satisfy a stronger equivalence: X is maximal in $\mathcal{F}$ if and only if X is maximal in the general family of codes. The proofs of this powerful result lead on the particular case of thin codes.

In the case of dense codes, it is natural to wonder whether the equivalence still holds. Of course, as any dense code is complete, the question of the equivalence between completeness and maximality does not raise (for example, the restricted Dyck code is dense but not maximal). But what about the equivalence between the maximality in some family $\mathcal{F}$ and the maximality in the family of codes? When $\mathcal{F}$ is the family of bifix, prefix or suffix codes, we know that this equivalence does not obtain ([1], p. 145), but the question remains open for the other classes of codes of the literature.

This paper answer to a question of De Luca and Restivo in [4] whether there exists a circular code which is maximal as circular code and not as code. In fact

[1] LIFAR, Université de Rouen, Place Émile Blondel, 76821 Mont-Saint-Aignan, France; e-mail: Yannick.Guesnet@dir.univ-rouen.fr

we answer negatively by exhibiting a circular code which is maximal in the family of circular code and not maximal in the family of codes.

This paper is organized as follow:

The Section 2 is devoted to the preliminaries and definitions.

In Section 3, we give the construction of a circular code which is maximal as circular code but not maximal as code.

1. Definitions and preliminaries

We denote by A an alphabet, by A^* the free monoid it generates and by ε the empty word.

Given a word $w \in \Sigma^*$, the set of all factors (prefixes, suffixes) of w is denoted by $\mathrm{F}(w)$ ($\mathrm{P}(w)$, $\mathrm{S}(w)$). The set of the *proper prefixes* (*proper suffixes*) of w is equal to $\mathrm{P}(w) \setminus \{w\}$ ($\mathrm{S}(X) \setminus \{w\}$).

Two words u, v are *P-comparable* if they are comparable for the prefix order, that is $u \in \mathrm{P}(v)$ or $v \in \mathrm{P}(u)$. Similarly, u and v are *S-comparable* if they are comparable for the suffix order.

We denote by $|w|$ the length of the word w.

Now, we recall the definitions of some well-known codes:

A non empty subset $X \subset A^+$ is a code if for any $n, m \geqslant 1$ and for any $x_1, \ldots, x_n \in X$, $y_1, \ldots y_m \in X$ the following condition holds:

$$x_1 \ldots x_n = y_1 \ldots y_m \qquad \Rightarrow \qquad n = m,\ x_i = y_i \quad i \in [1, n]\,.$$

A non-empty set $X \neq \{\varepsilon\}$ is a *prefix* (*suffix*) code if none of its elements is prefix (suffix) of another one. A non-empty set $X \neq \{\varepsilon\}$ is a *bifix* code if it is prefix and suffix.

A code X is *circular* if for any $n, m \geqslant 1$, $x_1, \ldots, x_n \in X$, $y_1, \ldots, y_m \in X$, $p \in \Sigma^*$ and $s \in \Sigma^+$ the equalities

$$sx_2 \ldots x_n p = y_1 \ldots y_m, \qquad x_1 = ps$$

imply

$$n = m, \quad p = \varepsilon \quad \text{and} \quad x_i = y_i \quad \text{for} \quad i = 1, \ldots, n.$$

We denote by $\mathcal{F}_{\text{code}}$ ($\mathcal{F}_{\text{circ}}$, $\mathcal{F}_{\text{bifix}}$) the family of codes (circular codes, bifix codes).

A *dense* code X is a code such that $\mathrm{F}(X) = A^*$. A *thin* code X is a code which is not dense, that is $A^* \setminus \mathrm{F}(X) \neq \emptyset$. A code X is *complete* if X^* is dense, that is $\mathrm{F}(X^*) = A^*$.

Let $(\mathcal{F}, \mathcal{F}')$ be a pair of the preceding families of codes such that $\mathcal{F} \subset \mathcal{F}'$. Let $X \in \mathcal{F}$. We say that the set X is maximal in $\mathcal{F}'$ if it is not strictly included in an another element of $\mathcal{F}'$.

In the case where $\mathcal{F}$ is equal to $\mathcal{F}_{\text{circ}}$ and where $\mathcal{F}'$ is equal to $\mathcal{F}_{\text{code}}$, we have the following result:

Theorem 1.1. *Let X be a thin code belonging to $\mathcal{F}_{\mathrm{circ}}$. The three following properties are equivalent:*

(i) *X is complete;*
(ii) *X is maximal in $\mathcal{F}_{\mathrm{code}}$;*
(iii) *X is maximal in $\mathcal{F}_{\mathrm{circ}}$.*

The part (i) $\Longleftrightarrow$ (ii) is due to Schützenberger [8]. The part (ii) $\Longleftrightarrow$ (iii) is shown by De Luca and Restivo in [4].

The purpose of this paper is to show by an example that if we omit the hypothesis "X thin" then the relation (ii) $\Longleftrightarrow$ (iii) is no more true in general.

Let $X \subset A^*$ and let $w \in A^*$. An *X-interpretation* of w is a $(n+2)$-tuple

$$(d_0, d_1, \ldots, d_n, d_{n+1})$$

such that $d_0 \in \mathrm{S}(X) \setminus X$, $d_{n+1} \in \mathrm{P}(X) \setminus X$, $d_i \in X$ for $1 \leqslant i \leqslant n$ and $w = d_0.d_1 \ldots d_{n+1}$.

If $w = d_1 \ldots d_n \in X^*$, the X-interpretation $(\varepsilon, d_1, \ldots, d_n, \varepsilon)$ is a *trivial interpretation* of w.

Let $w \in A^*$ and let $u, w', v \in A^*$ such that $w = uw'v$. Let $(d_0, d_1, \ldots, d_n, d_{n+1})$ be an X-interpretation of w.

The X-interpretation $(d_0, d_1, \ldots, d_n, d_{n+1})$ *induces* an X-interpretation for w' iff there exist $s \in \mathrm{S}(X) \setminus X$, $p \in \mathrm{P}(X) \setminus X$ and $i, j \in \mathbb{N}$, $0 < i \leqslant j \leqslant n+1$ such that $s \in \mathrm{S}(d_{i-1})$, $p \in \mathrm{P}(d_j)$ and $w' = sd_id_{i+1} \ldots d_{j-1}p$ (see Fig. 1). The X-interpretation $(s, d_i, \ldots, d_{j-1}, p)$ is the X-interpretation of w' *induced* by $(d_0, d_1, \ldots, d_n, d_{n+1})$.

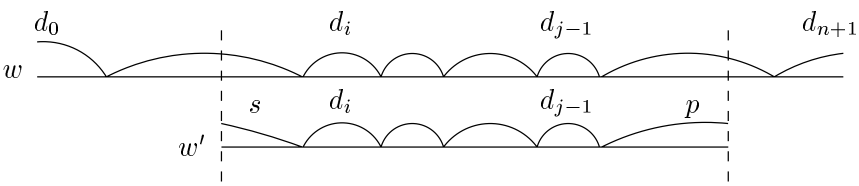

FIGURE 1. Induced interpretation.

When X is a code, we shall say, for short, that the triple (s, d, p) is an X-interpretation of w when $s \in \mathrm{S}(X) \setminus X$, $d \in X^*$, $p \in \mathrm{P}(X) \setminus X$ and $w = sdp$ (as X is a code, d has a unique X-factorization).

2. A maximal circular code which is not maximal as code

For any $u \in A^*$, we set

$$\begin{aligned} L_{ab}(u) &= b(ab)^+u, \\ R_{ab}(u) &= u(ab)^+a, \\ LR_{ab}(u) &= b(ab)^+u(ab)^+a. \end{aligned}$$

And finally we denote by $Extend_{ab}(u)$ the set

$$Extend_{ab}(u) = LR_{ab}(u) \cup L_{ab}(u) \cup R_{ab}(u) \cup \{u\}\cdot$$

The purpose of this section is the study of the set that is described below.

We set

$$\begin{aligned} U_1 &= \{ab\}, \\ U_n &= U_{n-1} \cup \\ &\quad \left\{ b(ab)^n u(ab)^n a \;\middle|\; u \in bA^*a \cap A^n, Extend_{ab}(u) \cap U_{n-1}^* = \emptyset \right\}, \qquad n \geqslant 2. \end{aligned}$$

Let

$$U = \bigcup_{n \geqslant 1} U_n.$$

The following of this paper is devoted to the proof of the above theorem, which is an answer to a question of De Luca and Restivo:

Theorem 2.1. *The set U is a circular code, maximal in $\mathcal{F}_{\mathrm{circ}}$ but not maximal in $\mathcal{F}_{\mathrm{code}}$.*

The proof of this result is divided in three part. First we prove that U is a bifix code which is not maximal in $\mathcal{F}_{\mathrm{bifix}}$. This prove that U is not maximal. Then we prove that U is a circular code. Finally we prove that U is maximal in $\mathcal{F}_{\mathrm{circ}}$.

2.1. U is not a maximal code

In this section, we prove that U is a bifix code. The non-maximality of U will follow directly. Afterwards we prove a lemma which will be helpful in the proofs of the next sections.

Lemma 2.2. *The set U is bifix.*

Proof. We first prove that U is a prefix code. By definition, the word ab is not prefix of another word in U (b is prefix of any word in U_n, $n \geqslant 2$).

It remains to prove that $U \setminus U_1$ is a prefix code ($U_1 = \{ab\}$). By contradiction, we assume that there exist $x, y \in U \setminus U_1$ such that $y \in \mathrm{P}(x)$, $x \neq y$. More precisely, let $u, v \in A^*$ and n, m be such that $n = |u|$, $m = |v|$, $x = b(ab)^n u(ab)^n a$ and $y = b(ab)^m v(ab)^m a$. We have $|x| > |y|$, thus $5n + 2 > 5m + 2$ that is $n > m$. Since $b(ab)^m b \in \mathrm{P}(y)$ $(v \in bA^*)$, we have $b(ab)^m b \in \mathrm{P}(x)$. Moreover, as $n > m$, we have $b(ab)^m b \in \mathrm{P}(b(ab)^n)$. That contradicts the fact that bb is not a factor of $b(ab)^n$.

Hence, the set U is a prefix code. In a similar way, it may be proved that U is suffix.

Therefore the set U is a bifix code. $\square$

Hence we have the first part of the proof of the Theorem 2.1.

Corollary 2.3. *The set U is not maximal in $\mathcal{F}_{\text{code}}$.*

Proof. Clearly $U \cup \{bb\}$ still remains a bifix code. $\square$

The following lemma (see Fig. 2), which is quite technical, will be helpful in the proof of Lemma 2.6.

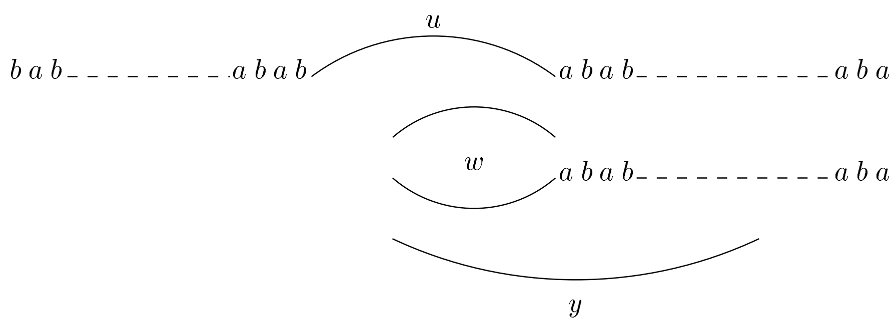

FIGURE 2. Lemma 2.4.

Lemma 2.4. *Let $x, y \in U \setminus U_1$. Let $u, v \in bA^*a$ such that $x = b(ab)^{|u|}u(ab)^{|u|}a$ and $y = b(ab)^{|v|}v(ab)^{|v|}a$. Assume that there exists a proper prefix w of y that satisfies the two following conditions:*

(i) $w \in \mathrm{S}(u)$*;*

(ii) *y and $w.(ab)^{|u|}a$ are P-comparable.*

Then we have $w = b(ab)^{|v|}v$.

Proof. Our proof will be done in two parts:

1. first, we prove that $w \in \mathrm{P}(b(ab)^{|v|}v)$;
2. then we prove that $b(ab)^{|v|}v \in \mathrm{P}(w)$.

The conclusion will follow directly.

1. First we shall prove that $w \in \mathrm{P}(b(ab)^{|v|}v)$. By definition of u, a is suffix of u, thus since $w \in \mathrm{S}(u)$, a is suffix of w.
   We have that y and $w.(ab)^{|u|}a$ are P-comparable. Hence we must study the two cases where $y \in \mathrm{P}(w.(ab)^{|u|}a)$ and $w.(ab)^{|u|}a \in \mathrm{P}(y)$. We shall prove that in this two cases we have $w.ab \in \mathrm{P}(y)$.

- Assume that $y \in \mathrm{P}(w.(ab)^{|u|}a)$ (Fig. 3). By definition of y, aba is suffix of y. Moreover w is a proper prefix of y thus wa is prefix of y. We have seen that a is suffix of w, thus aa is suffix of wa. Since by definition of y, aa is not suffix of y, the word wa is a proper prefix of y, hence we have $w.ab \in \mathrm{P}(y)$.

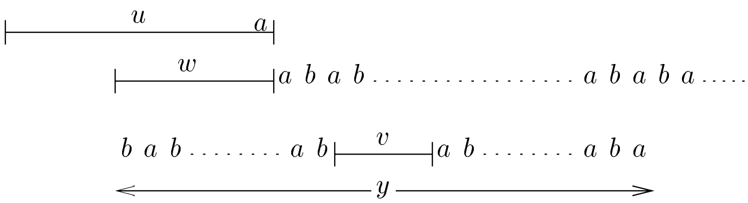

FIGURE 3. Lemma 2.4, $y \in \mathrm{P}(w.(ab)^{|u|}a)$.

- Trivially, if $w.(ab)^{|u|}a \in \mathrm{P}(y)$ then $w.ab \in \mathrm{P}(y)$.

We have $w.ab \in \mathrm{P}(y)$ and aab is a suffix of $w.ab$. Then, since aab is not a factor of $(ab)^{|v|}a$, the word $w.ab$ is a prefix of $b(ab)^{|v|}v.ab$ (it must be remembered that $y = b(ab)^{|v|}v(ab)^{|v|}a$), that is w is a prefix of $b(ab)^{|v|}v$.

2. Now, we shall prove that $b(ab)^{|v|}v \in \mathrm{P}(w)$.
   - Assume that $y \in \mathrm{P}(w.(ab)^{|u|}a)$.
   By definition of y, we have $b.(ab)^{|v|}.v.a \in \mathrm{P}(w.(ab)^{|u|}.a)$. Now a is a suffix of v, thus aa is a suffix of $b.(ab)^{|v|}.v.a$. As aa is not a factor of $(ab)^{|u|}.a$, we have $b.(ab)^{|v|}.v.a \in \mathrm{P}(w.a)$, that is $b.(ab)^{|v|}.v \in \mathrm{P}(w)$.
   - Assume that $w.(ab)^{|u|}a \in \mathrm{P}(y)$.
   As $b(ab)^{|v|} \in \mathrm{P}(y)$, we have $b(ab)^{|v|} \in \mathrm{P}(w)$ or $w \in \mathrm{P}(b(ab)^{|v|})$ but, since the word aa is a suffix of wa and aa is not a factor of $b.(ab)^{|v|}$, we have $b.(ab)^{|v|} \in \mathrm{P}(w)$. Since w is a suffix of u, we have $|w| \leqslant |u|$ and the condition $b.(ab)^{|v|} \in \mathrm{P}(w)$ implies $|v| < |w|$. We have $|v| < |w| \leqslant |u|$ and $w.(ab)^{|u|}a \in \mathrm{P}(y)$, thus

$$b.(ab)^{|v|}.v \in \mathrm{P}(w.(ab)^{|u|}).$$

   Therefore there exists $u' \in A^*$ such that $w.(ab)^{|u|} = b.(ab)^{|v|}.v.u'$. But $w.(ab)^{|u|}.a \in \mathrm{P}(y)$ and $y = b(ab)^{|v|}.v.(ab)^{|v|}a$, thus $u' \in \mathrm{P}((ab)^{|v|}a)$. Hence, if $u' = \varepsilon$ then $w.(ab)^{|u|} = b.(ab)^{|v|}.v$ and otherwise we have $b.(ab)^{|v|}.v.a \in \mathrm{P}(w.(ab)^{|u|})$. Therefore we have

$$b(ab)^{|v|}v.a \in \mathrm{P}(w.(ab)^{|u|}.a).$$

   Now aa is a suffix of $b.(ab)^{|v|}.v.a$ and aa is not a factor of $(ab)^{|u|}a$, thus $b.(ab)^{|v|}.v.a \in \mathrm{P}(w.(ab)^{|u|}.a)$ yields $b(ab)^{|v|}.v.a \in \mathrm{P}(w.a)$, that is $b(ab)^{|v|}.v \in \mathrm{P}(w)$.

Consequently, we have w prefix of $b(ab)^{|v|}.v$ and $b(ab)^{|v|}v$ prefix of w, thus we have $w = b(ab)^{|v|}.v$. □

By considering the reversed words, similar arguments lead to the following lemma:

Lemma 2.5. *Let $x, y \in U \setminus U_1$. Let $u, v \in bA^*a$ such that $x = b(ab)^{|u|}u(ab)^{|u|}a$ and $y = b(ab)^{|v|}v(ab)^{|v|}a$. Assume that there exists a proper suffix w of y that satisfies the two following conditions:*
(i) *$w \in \mathrm{P}(u)$;*
(ii) *y and $b(ab)^{|u|}.w$ are S-comparable.*
Then we have $w = v(ab)^{|v|}a$.

2.2. A property of the U-interpretations

The following lemma gives a powerful property that must be satisfied by any word in $U \setminus U_1$. This is the sinews of our main result.

Lemma 2.6. *Any word in $U \setminus U_1$ has no non-trivial U-interpretations.*

Proof. Let $x \in U \setminus U_1$. By definition of U, there exists $u \in A^*$, such that $x = b(ab)^{|u|}u(ab)^{|u|}a$ (we have $x \in U_{|u|}$). We set $n = |u|$.

By contradiction, we consider a non-trivial U-interpretation of x, namely $I = (d_0, d_1, \ldots, d_k, d_{k+1})$, $k \geqslant 0$.

First, we assume that I does not induce a U-interpretation for the factor $ab.u.ab$ of x, that is $ab.u.ab$ is a factor of a word in U.

More precisely, let $w \in U$ be the word equal to $b(ab)^{|v|}.v.(ab)^{|v|}a$ such that $w \in \{d_1 \ldots d_k\}$ or $d_0 \in \mathrm{S}(w)$ or $d_{k+1} \in \mathrm{P}(w)$ and such that $ab.u.ab$ is a factor of w.

Since aa is suffix of bua and aa is not a factor of $b(ab)^{|v|}$ and since bb is prefix of bua and bb is not a factor of $(ab)^{|v|}a$, we have $u \in \mathrm{F}(v)$. Moreover this implies $|u| \leqslant |v|$, hence, by definition of w and x, we have $x \in \mathrm{F}(w)$. But, as I is a non trivial interpretation, this case can not appear.

Now, we assume that I induces a U-interpretation $(s', d_{i+1}, \ldots, d_j, p')$, $0 \leqslant i \leqslant j \leqslant k$, $s' \in \mathrm{S}(d_i)$, $p' \in \mathrm{P}(d_{j+1})$, for the factor $ab.u.ab$ of x. We set $d' = d_{i+1} \ldots d_j$ (see Fig. 4) and we deal with the length of s'.

- $|s'| = 0$. In this case, if $p' = \varepsilon$ then we have $ab.u.ab \in U^*$. Hence $u \in U^*$ since ab is not a proper prefix nor a proper suffix of a word in U. Moreover, the words in $U \setminus U_{n-1}$ are of length greater than n (indeed they are of length greater than or equal to $5n+2$), therefore $u \in U^*$ and $|u| = n$ yields $u \in U^*_{n-1}$. Hence, since $x = b(ab)^{|u|}u(ab)^{|u|}a \in U_n$, this contradicts the definition of U_n.
  We have also $p' \neq b$. Indeed, otherwise the word aa is suffix of d'. Now, as the words in U are of length at least 2 and as no word in U has such a suffix, this case can not appear.
  Finally, $p' \neq ab$. Indeed, otherwise we have $ab.u \in U^*$, hence $u \in U^*$.

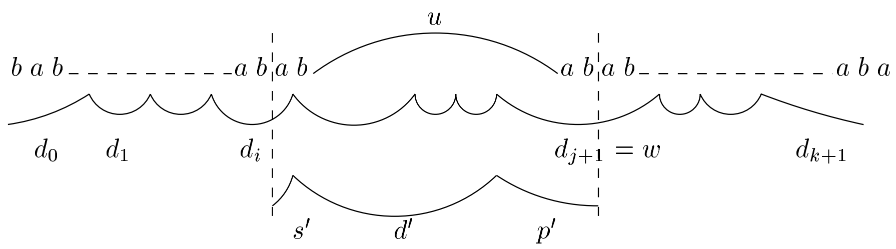

FIGURE 4. I induces a U-interpretation for the factor $ab.u.ab$.

As for the case where $p' = \varepsilon$, we have $u \in U_{n-1}^*$, which contradicts the definition of U_n.
Consequently, we have $|p'| > 2$, thus $p' \in \mathrm{P}(U \setminus U_1)$. Hence, if $j \neq k$ ($j = k$), there exists $v \in A^+$ such that the word d_{j+1} is equal to (is a prefix of) $b(ab)^{|v|}.v.(ab)^{|v|}a$. We set $w = b(ab)^{|v|}.v.(ab)^{|v|}a$. It must be remembered that p' is a prefix of d_{j+1}.
Since $s' = \varepsilon$, the prefix ab of $ab.u.ab$ is factor of d' (a is not in U), thus $p' \in \mathrm{S}(u.ab)$.
More precisely p' is a prefix of d_{j+1}, thus we have

$$p'(ab)^{-1}.(ab)^{|u|}a = d_{j+1} \dots d_{k+1}.$$

Therefore, if $j + 1 \neq k + 1$ then, since in this case we have $d_{j+1} = w$, we have $w \in \mathrm{P}(p'(ab)^{-1}.(ab)^{|u|}a)$, otherwise if $j + 1 = k + 1$ then we have $d_{j+1} = p'(ab)^{-1}.(ab)^{|u|}a$, thus, since in this case we have $d_{j+1} \in \mathrm{P}(w)$, we have $p'(ab)^{-1}.(ab)^{|u|}a \in \mathrm{P}(w)$.
Hence w and $p'(ab)^{-1}.(ab)^{|u|}a$ are P-comparable. Moreover, we have $p'.(ab)^{-1} \in \mathrm{P}(w)\backslash w$, $p'.(ab)^{-1} \in \mathrm{S}(u)$ thus, by Lemma 2.4, we have $p'.(ab)^{-1} = b(ab)^{|v|}.v$. That is $p' = b(ab)^{|v|}.v.ab$.
Therefore, $u.(ab)^{|v|-1}.a = d'.w \in U_{n-1}^*$ (we have $d' \in U_{n-1}^*$ since $|d'| \leqslant |u|$ and $w \in U_{n-1}$ since $|v| < |u|$). This contradicts the definition of u (we have $R_{ab}(u) \cap U_{n-1}^* = \emptyset$).

- $|s'| = 1$. With this condition, the word bb is a prefix of d'. By definition of U, this case cannot occur.
- $|s'| = 2$. As for the case $|s'| = 0$, by substituting u for $ab.u$, similar argument yields the similar contradiction.
- $|s'| > 2$. In this case $s' \in U \setminus U_1$. Thus, if $i \neq 0$ ($i = 0$), there exists $v \in A^+$ such that the word d_i is equal to (is a suffix of) $b(ab)^{|v|}.v.(ab)^{|v|}a$. We set $w = b(ab)^{|v|}.v.(ab)^{|v|}a$. Thus we have $(ab)^{-1}.s' \in \mathrm{S}(w) \setminus \{w\}$, $(ab)^{-1}.s' \in \mathrm{S}(u)$, $w \in \mathrm{S}(b(ab)^{|u|}.(ab)^{-1}.s')$ or $b(ab)^{|u|}.(ab)^{-1}.s' \in \mathrm{S}(w)$ hence, by Lemma 2.5, we have $s' = ab.v.(ab)^{|v|}a$.
  By considering the length of the corresponding word p', exactly one of the four following cases occurs.

– If $|p'| = 0$ then we have $ab.u.ab = ab.v.(ab)^{|v|}a.d'$, thus $b(ab)^{|v|}.u.ab = w.d'$. Hence we have

$$b.(ab)^+.u.ab \cap U_{n-1}^* \neq \emptyset,$$

since $ab \in U$ is not a suffix of words in $U \setminus U_1$, we have

$$b.(ab)^+.u \cap U_{n-1}^* \neq \emptyset.$$

This contradicts the definition of u.

– If $|p'| = 1$ then we have

$$b.(ab)^+.u.a \cap U_{n-1}^* \neq \emptyset.$$

As aa is not suffix of words in U, this case can not appear.

– If $|p'| = 2$ then we have

$$b.(ab)^+.u \cap U_{n-1}^* \neq \emptyset.$$

This contradicts the definition of u.

– If $|p'| > 2$, by a similar argument to the one in the case $|s'| = \varepsilon$, $|p'| > 2$, Lemma 2.4 yields

$$p'.(ab)^+.a \cap U_{n-1} \neq \emptyset.$$

Therefore we have $b.(ab)^+.u.(ab)^+.a \cap U_{n-1}^* \neq \emptyset$, this contradicts the definition of u.

Thus the interpretation I of x can not induces a U-interpretation for the word $ab.u.ab$.

Therefore, the words of $U \setminus U_1$ has no non trivial U-interpretation. □

2.3. U is a circular code

The following sections are dedicated to the proof of the Theorem 2.1. Before all it must be proved that U is circular. This is done by Proposition 2.7.

Proposition 2.7. *The set U is a circular code.*

Proof. Let $x_1, \ldots, x_n, x'_1, \ldots x'_m \in U$, $s \in A^+, p \in A^*$ be such that

$$x'_1 \ldots x'_m = sx_2 \ldots x_n p \quad \text{and} \quad x_1 = ps.$$

Without loss of generality, we can assume that $|s| \leqslant |x'_1|$ (otherwise we consider the equation $x'_2. \ldots .x'_m.x'_1 = ({x'_1}^{-1}.s).x_2 \ldots x_n.(p.x'_1))$.

If $x'_1 \in U \setminus U_1$, then, by Lemma 2.6, we have $s = x'_1$. Thus, by Lemma 2.2, we have $p = \varepsilon$, $n = m$, $x_i = x'_i$ for $1 \leqslant i \leqslant n$.

It remains to study the case where $x'_1 = ab$. Since $s \in \mathrm{P}(x'_1)$, exactly one of the two following cases occur:

- $s = a$. In this case, we have $m \geqslant 2$ ($m = 1$ implies $p = b$, now $ba \notin U$). If $n = 1$, since we have $x_1 = ps = a^{-1}.x'_1 \dots x'_m.a$, we have $x_1 \in U \setminus U_1$. The word x_1 has a non trivial U-interpretation $(b, x'_2 \dots x'_m, a)$, Lemma 2.6 assures that this case can not appear. If $n \geqslant 2$ then $x_2 \in U \setminus U_1$ and x_2 has a non trivial U-interpretation $(b, x'_2 \dots x'_k, p')$, with $k < m$, $p' \in \mathrm{P}(x_{k+1})$. With such a condition, according to Lemma 2.6 this case can not occurs.
- $s = ab$. In this case $p = \varepsilon$ (ab is not suffix of words in $U \setminus \{ab\}$ and we have $ps \in U$), hence by Lemma 2.2, we have $p = \varepsilon$, $n = m$, $x_i = x'_i$ for $1 \leqslant i \leqslant n$.

As a consequence, only the trivial interpretation holds. In other words, U is a circular code. $\square$

2.4. Some properties of U

The three following lemmas give us some properties that we hold when we add an element to U. They will be helpful to prove the maximality of U in $\mathcal{F}_{\mathrm{circ}}$.

Lemma 2.8. *Let $y \in A^+ \setminus U^+$ and $z \in U^*.\{y\}.U^*$. If the following condition holds:*

$$\exists k \geqslant 1, \qquad LR_{ab}(z) \cap U_k^+ \neq \emptyset,$$

then $U \cup \{y\}$ is not a circular code.

Proof. We have $LR_{ab}(z) \cap U_k^+ \neq \emptyset$ thus, by definition of $LR_{ab}(z)$, there exist $n, m \geqslant 0$ such that

$$b.(ab)^n.z.(ab)^m.a \in U_k^+.$$

Let $w = b.(ab)^n.z.(ab)^m.a$. Since $ab \in U$, the tuple $(b, (ab)^n, z, (ab)^m, a)$ induces a $(U \cup \{z\})$-interpretation $(b, ab, \dots, ab, z, ab, \dots, ab, a)$ of w.

By definition, we have $z \in U^*.y.U^*$. Let $u_1, \dots, u_i, u'_1, \dots, u'_j \in U$ with $i, j \geqslant 0$ such that $z = u_1 \dots u_i.y.u'_1 \dots u'_j$. The interpretation $(b, ab, \dots, ab, z, ab, \dots, ab, a)$ of w induces a $U \cup \{y\}$-interpretation of w which is equal to

$$(b, ab, \dots, ab, u_1, \dots, u_i, y, u'_1, \dots, u'_j, ab, \dots, ab, a).$$

Consequently the word w has a $U \cup \{y\}$-interpretation (s, d, p) with $ps \in U$ (we have $ps = ab$) and $p \neq \varepsilon$. By definition of U, we have $U_k \subset U$, thus $U_k \subset U \cup \{y\}$. Therefore we have $w \in (U \cup \{y\})^*$ and we have proved that this word has a non trivial circular $(U \cup \{y\})$-factorization. Consequently we have proved that $U \cup \{y\}$ is not a circular code. $\square$

Lemma 2.9. *Let $y \in A^+ \setminus U^+$ and $z \in U^+.\{y\}.U^+$. If the following condition holds:*

$$\exists k \geqslant 1, \qquad z \in U_k^+,$$

then $U \cup \{y\}$ is not a circular code.

Proof. We shall prove that $U \cup \{y\}$ is not a code. Let $z_1, z_2 \in U^+$ such that $z = z_1.y.z_2$. Since $z \in U_k^*$, we have $z_1.y.z_2 \in U_k^*$ (it must be remembered that $z \in U^+.\{y\}.U^+$). By definition, we have $y \notin U^*$, thus the word z has two distinct $U \cup \{y\}$-factorizations: one U-factorization induces by the condition $z \in U_k^*$ (by definition of U, we have $U_k \subset U$) and one $U \cup \{y\}$-factorization induces by the three $U \cup \{y\}$-factorizations of z_1, y and z_2. This proves that $U \cup \{y\}$ is not a code, hence it is not a circular code. □

Lemma 2.10. *Let $y \in A^+ \setminus U^+$ and $z \in (U \setminus U_1)^+.\{y\}.(U \setminus U_1)^+$. If the following condition holds:*

$$Extend_{ab}(z) \cap U^*_{|z|-1} = \emptyset,$$

then $U \cup \{y\}$ is not a circular code.

Proof. By definition of U, the words of $U \setminus U_1$ belongs to bA^*a. Hence, we have $z \in bA^*a$. It follows that if $Extend_{ab}(z) \cap U^*_{|z|-1} = \emptyset$ then, by definition of $U_{|z|}$, we have $b(ab)^{|z|}.z.(ab)^{|z|}a \in U_{|z|}$. By Lemma 2.8, the code $U \cup \{y\}$ is not a circular code. □

2.5. U is maximal in $\mathcal{F}_{\rm circ}$

We are now able to establish the main result of the paper. As a matter of fact, it remains to prove that U is maximal in $\mathcal{F}_{\rm circ}$. Indeed Corollary 2.3 stands that U is not a maximal code.

Proposition 2.11. *The set U is maximal in $\mathcal{F}_{\rm circ}$.*

Proof. Let y be a word in $A^* \setminus U^*$. In order to prove that U is maximal in $\mathcal{F}_{\rm circ}$, we shall prove that $U \cup \{y\}$ is no more a circular code.

If $LR_{ab}(y) \cap U^+ \neq \emptyset$ then let $z \in U^+$ such that $z \in LR_{ab}(y)$. Let $z_1, \ldots, z_n \in U$, $n > 0$ such that $z = z_1 \ldots z_n$. By definition of U, we have

$$z_i \in U_{\max\left\{\,|z_j|\,\middle|\,1 \leqslant j \leqslant n\,\right\}}, \qquad 0 < i \leqslant n.$$

Let $k = \max\left\{\,|z_j|\,\middle|\,1 \leqslant j \leqslant n\,\right\}$. We have $LR_{ab}(y) \cap U_k^+ \neq \emptyset$. By Lemma 2.8, the set $U \cup \{y\}$ is not a circular code.

Therefore we shall assume that $LR_{ab}(y) \cap U^* = \emptyset$.

Let x be a word in $U \setminus U_1$ and let $z = xyx$. We are now yield to examine the set $U \cup \{z\}$ in order to prove that the set $U \cup \{y\}$ is not circular.

By Lemma 2.10, if $Extend_{ab}(z) \cap U^*_{|z|-1} = \emptyset$ then $U \cup \{y\}$ is not circular. It remains to study the case where $Extend_{ab}(z) \cap U^*_{|z|-1} \neq \emptyset$. By definition of $Extend_{ab}(z)$, this implies that at least one of the four following conditions is satisfied:

(i) $LR_{ab}(z) \cap U^*_{|z|-1} \neq \emptyset$;
(ii) $z \cap U^*_{|z|-1} \neq \emptyset$;

(iii) $R_{ab}(z) \cap U^*_{|z|-1} \neq \emptyset$;

(iv) $L_{ab}(z) \cap U^*_{|z|-1} \neq \emptyset$.

In the sequel, we shall prove that, in each case, the set $U \cup \{y\}$ is not circular.

(i) If $LR_{ab}(z) \cap U^*_{|z|-1} \neq \emptyset$ then, by Lemma 2.8, the set $U \cup \{y\}$ is not circular.

(ii) In a similar way, if $z \cap U^*_{|z|-1} \neq \emptyset$ then, by Lemma 2.9, the set $U \cup \{y\}$ is not circular.

(iii) Assume that $R_{ab}(z) \cap U^*_{|z|-1} \neq \emptyset$. By definition of R_{ab}, there exist $n > 0$, $h \geqslant 0$ and $u_0, u_1, \ldots, u_h \in U_{|z|-1}$ such that $xyx(ab)^n a = u_0.u_1 \ldots u_h$.
First, since U is bifix, we have $u_0 = x$, that is

$$yx(ab)^n a = u_1 \ldots u_h \qquad \text{and} \qquad h \geqslant 1. \tag{1}$$

Let $0 \leqslant k < h$ be such that $y = u_1 \ldots u_k u'$, $u' \in \mathrm{P}(u_{k+1}) \setminus u_{k+1}$. Notice that the definition of u' is unique (k is the greatest integer satisfying the condition $y = u_1 \ldots u_k u'$ with $u' \in \mathrm{P}(u_{k+1})$).
By Lemma 2.6, the word $x \in U \setminus U_1$ has no non trivial U-interpretation, thus we have $x \in \mathrm{F}(u_{k+1})$. Hence, we have $u_{k+1} \in U \setminus U_1$ ($U_1 = \{ab\}$).
More precisely we have $u'x \in \mathrm{P}(U)$. By equation (1) and since $u_{k+1} \in A^*a$, there exists m such that $u_{k+1} = u'x(ab)^m a$.
Since $u_{k+1} \in U \setminus U_1$, there exist $w \in bA^*a$ such that

$$u_{k+1} = b(ab)^{|w|} w (ab)^{|w|} a.$$

Since $x \in A^*a$, we have $|w| = m$ and $u'x = b(ab)^m w$.
In order to prove that $U \cup \{y\}$ is not circular, we consider the word $z' = xzx$.
We shall prove that we have $(L_{ab}(z') \cup R_{ab}(z')) \cap U^*_{|z'|-1} = \emptyset$. Indeed, if this condition is satisfied, at least one of the two following situations occurs:

- Either

$$(LR_{ab}(z') \cup L_{ab}(z') \cup R_{ab}(z') \cup z') \cap U^*_{|z'|-1} = \emptyset$$

  and then by Lemma 2.10, the set $U \cup \{y\}$ is not circular.
- Or

$$(LR_{ab}(z') \cup z') \cap U^*_{|z'|-1} \neq \emptyset.$$

  Once again, by Lemma 2.8, the set $U \cup \{y\}$ is not circular.

We prove that $(L_{ab}(z') \cup R_{ab}(z')) \cap U^*_{|z'|-1} = \emptyset$ by considering the two following cases:

- We shall prove that $R_{ab}(z') \cap U^*_{|z'|-1} = \emptyset$. By contradiction, assume that $R_{ab}(z') \cap U^*_{|z'|-1} \neq \emptyset$.
  Let $u'' = u'xx$, by definition of z, we have $z' = xxyxx$, thus since $y = u_1 \ldots u_k u'$, we have $z' = xxu_1 \ldots u_k u''$ (see Fig. 5).
  We have $R_{ab}(z') \cap U^*_{|z'|-1} \neq \emptyset$, thus there exist $h' \geqslant 0$, $m' \geqslant 1$, $\alpha_0, \ldots, \alpha_{h'} \in U_{|z'|-1}$ such that $z'.(ab)^{m'} a = \alpha_0 \ldots \alpha_{h'}$. Since U is

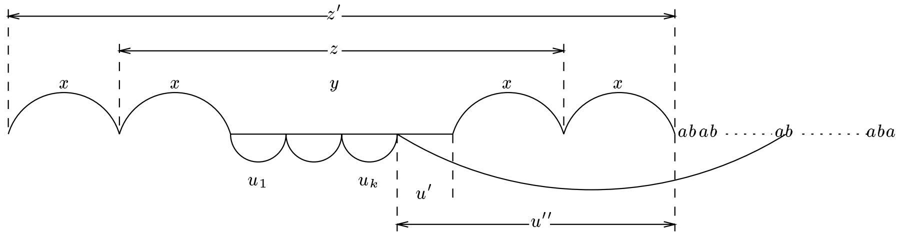

FIGURE 5. $R_{ab}(z') \cap U^*_{|z'|-1} \neq \emptyset$.

prefix, the equation

$$xxu_1 \dots u_k u'' = \alpha_0 \dots \alpha_{h'}.((ab)^{m'}a)^{-1}$$

yields $u'' \in U^*\mathrm{P}(U)$ (we have $\alpha_0 = \alpha_1 = x$, $u_i = \alpha_{i+1}$ for $1 \leqslant i \leqslant k$). Let $h'' \geqslant 0$, $\beta_1, \dots, \beta_{h''} \in U$, $\beta \in \mathrm{P}(U)$ such that

$$u'' = \beta_1 \dots \beta_{h''}\beta = u'xx.$$

Assume that $h'' > 0$. By definition of U, since $u' = b(ab)^{|w|}w$, we have $\beta_1 \in U \setminus U_1$ and there exists $r > 0$ such that $\beta_1 \in b(ab)^r bA^{r-2}a(ab)^r a$. Since $w \in bA^*a$, we have $r = |w|$ and $u' \in \mathrm{P}(\beta_1)$. Moreover, if $|u'| < |\beta_1| < |u'xx|$ then, since U is bifix, x has a U-interpretation (see Fig. 6), Lemma 2.6 states that this can not appear. Hence $|\beta_1| = |u'xx|$. However U is suffix, thus x can not be suffix of β_1. Hence we have $h'' = 0$, that is

$$u'' \in \mathrm{P}(U).$$

As $u'x = b(ab)^m w$ and $u'xx = u'' \in \mathrm{P}(U)$, the word $b(ab)^m wb$ (we have $x \in U \setminus U_1$, thus b is prefix of x) is a proper prefix of a word in U. Hence, by definition of U, there exists $w' \in bA^*a$ such that

$$b(ab)^m wb \in \mathrm{P}(b(ab)^{|w'|}w'(ab)^{|w'|}a).$$

As $w \in bA^*$, we have $|w'| = m$, thus $w = w'$. This implies $b(ab)^m wb = b(ab)^m wa$ which can not appear.
Thus we have $R_{ab}(z') \cap U^*_{|z'|-1} = \emptyset$.

- Now, we prove that $L_{ab}(z') \cap U^*_{|z'|-1} = \emptyset$. By contradiction, we assume that $L_{ab}(z') \cap U^*_{|z'|-1} \neq \emptyset$. With this condition, there exist $u'' \in \mathrm{S}(U)$, $k' \geqslant 0$ and $u'_i \in U$, $1 \leqslant i \leqslant k'$ such that $z' = u''u'_1 \dots u'_{k'}$. Since U is suffix, we have $u'_{k'} = u'_{k'-1} = x$. Now $z' = x.x.u_1 \dots u_k u'.x.x$, therefore we have $x.x.u_1 \dots u_k u' = u''u'_1 \dots u'_{k'-2}$. Hence, we have $u' \in \mathrm{S}(U^+)$.

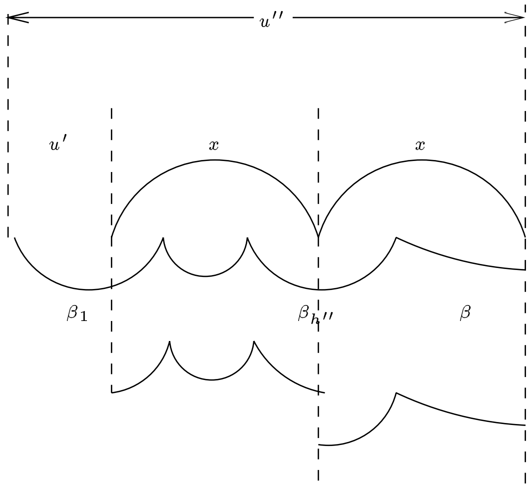

FIGURE 6. $h'' > 0$ induces a U-interpretation for x.

Let $s \in \mathrm{S}(U)$ and let $t \in U^*$ such that $u' = st$. The word $u'.x.(ab)^m a$ has a U-interpretation $(s, t.x.(ab)^m, a)$.
We have seen that $u'.x.(ab)^m a \in U$, thus by Lemma 2.6, this case can not appear.

We have proved that $(L_{ab}(z') \cap U^*_{|z'|-1}) \cup (R_{ab}(z') \cap U^*_{|z'|-1}) = \emptyset$, that is

$$(L_{ab}(z') \cup R_{ab}(z')) \cap U^*_{|z'|-1} = \emptyset.$$

Hence $U \cup \{y\}$ is not circular.

(iv) In a similar way, when $L_{ab}(z) \cap U^*_{|z|-1} \neq \emptyset$, we hold that the word $z' = xzx$ satisfies $(L_{ab}(z') \cup R_{ab}(z')) \cap U^*_{|z'|-1} = \emptyset$. Hence $U \cup \{y\}$ is not circular.

Consequently, the code U is maximal in $\mathcal{F}_{\mathrm{circ}}$. □

Therefore we have proved the Theorem 2.1: U is a circular code, maximal in $\mathcal{F}_{\mathrm{circ}}$ and not maximal in $\mathcal{F}_{\mathrm{code}}$.

Actually, there are only two families for which we know that the equivalence between the maximality in the family and the maximality in the family of codes is hold. This is the family of synchronous codes [6] and the family of uniformly synchronous codes [3]. However, these families are included in the family of thin codes. It is natural to wonder if there exists a family of codes, which intersects the family of dense codes, such that the two notions of maximality are equivalent.

REFERENCES

[1] J. Berstel and D. Perrin, *Theory of Codes*. Academic Press (1985).

[2] V. Bruyère, Codes, *Dissertation présentée pour l'obtention de grade légal de docteur en sciences*. Université de Mons-Hainaut (1991).

[3] V. Bruyère, On maximal codes with bounded synchronization delay. *Theoret. Comput. Sci.*, **204** (1998) 11-28.

[4] A. de Luca and A. Restivo, On some properties of very pure codes. *Theoret. Comput. Sci.*, **10** (1980) 157-170.

[5] Y. Guesnet, On codes with finite interpreting delay: A defect theorem. *Theoret. Informatics Appl.*, **34** (2000) 47-59.

[6] Y. Guesnet, *Codes et interprétations*, Thèse de doctorat. Université de Rouen (2001).

[7] Y. Guesnet, On maximal codes with finite interpreting delay. *Theoret. Comput. Sci.*, (to appear).

[8] M.P. Schützenberger, Une théorie algébrique du codage, in: *Séminaire Dubreil-Pisot 1955-56* Institut H. Poincaré (1956), Exposé n°15.

Communicated by Ch. Choffrut.
Received June, 2000. Accepted October, 2001.