## INFORMATIQUE THÉORIQUE ET APPLICATIONS

## A. Restivo <br> S.SALEMI <br> T. Sportelli <br> Completing codes

Informatique théorique et applications, tome 23, $\mathrm{n}^{\mathrm{o}} 2$ (1989),
p. 135-147
[http://www.numdam.org/item?id=ITA_1989__23_2_135_0](http://www.numdam.org/item?id=ITA_1989__23_2_135_0)
© AFCET, 1989, tous droits réservés.
L'accès aux archives de la revue «Informatique théorique et applications » implique l'accord avec les conditions générales d'utilisation (http://www.numdam. org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

## Numdam

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

# COMPLETING CODES (*) 

by A. Restivo ( ${ }^{1}$ ), S. Salemi ( ${ }^{1}$ ) and T. Sportelli ( ${ }^{1}$ )

Communicated by J.-E. PIN


#### Abstract

The problem to characterize those finite codes that can be embedded in a finite maximal code is investigated.

The main results, which give some necessary conditions for the embedding, are obtained by using factorizations of cyclic groups.

Résumé. - Nous étudions le problème de caractériser les codes finis qui peuvent être inclus dans un code maximal fini.

Les résultats principaux, qui donnent des conditions nécessaires pour linclusion, sont obtenus en utilisant les factorisations des groupes cycliques.


## 1. INTRODUCTION

The theory of (variable length) codes takes its origin in the theory of information and comunication devised by C. Shannon in the 1940s. It has been later developed in an algebraic direction by M. P. Shutzenberger and his school in connection to automata theory, combinatorics on words, formal languages and semigroup theory. A complete treatment of the theory of codes until very recent developments may be found in [1].

An important notion in this theory is that of maximal code: a code is maximal if it is no proper subset of any other code in the same alphabet. It is not difficult to see that any code is included in a maximal one. However there exist finite codes which are not included in any finite maximal code. An example containing only four words was given in [9] as the smallest member of an infinite family of codes which do not have a finite completion. The same example had been given by A. Markov in [7].

[^0]One of the main open problems on codes is to characterize those finite codes that can be embedded in a finite maximal code, i. e. that have a finite completion. It is not even presently known whether this prperty is effectively decidable.

In this paper we investigate this problem.
In section 2 the basic definitions and some non trivial completion procedures are presented. In particular we derive that any two-element code has a finite completion and we conjecture the same result for three-element codes.

In section 3 we show the relationship between this problem and an old conjecture of Schutzenberger concerning the optimality of prefix codes. The construction of a finite completion for a special code recently introduced by P. Shor would give a counterexample to this conjecture. Actually the results of this paper suggest that Shor's code does not have a finite completion.

In section 4 factorizations of cyclic groups are introduced as a tool to study the problem of code completion. We obtain only partial results. In particular some necessary conditions for a code to have a finite completion are given, generalizing previously published results. A conjecture on factorizations of cyclic groups is also proposed, which indirectly supports the validity of Schutzenberger's conjecture.

Let us finally remark that the results and the problems rised in this paper show the deep interconnections between algebraic and information theoretical arguments.

## 2. DEFINITIONS AND PRELIMINARY RESULTS

Let $A$ be a finite alphabet and $A^{*}$ the free monoid generated by $A$. As usual the elements of $A$ are called letters, the elements of $A^{*}$ words and by $|u|$ is denoted the length of the word $u \in A^{*}$. The empty word is denoted by 1 and the set of non empty words of $A^{*}$ by $A^{+}$.

Thus $A^{+}=A^{*}-1$. If $X$ is a subset of $A^{*}, X^{*}$ denotes the subsemigroup generated by $X$ and $X^{+}=X^{*}-1$.

A set $X \subseteq A^{*}$ is a code if

$$
x_{1} x_{2} \ldots x_{m}=y_{1} y_{2} \ldots y_{m}
$$

for

$$
n, m \neq 1, \quad x_{1}, x_{2}, \ldots, x_{n}, y_{1}, y_{2}, \ldots, y_{m} \in X \text { implies } n=m
$$

and

$$
x_{1}=y_{1}, \quad x_{2}=y_{2}, \ldots, x_{n}=y_{m} .
$$

In other words $X$ is a code if the submonoid $X^{*}$ generated by $X$ is free and of base $X$.
A code $X \subseteq A^{*}$ is maximal (in $A^{*}$ ) if it is not properly included in any other code $Y \subseteq A^{*}$.

A set $X \subseteq A^{*}$ is complete if for all $w \in A^{*}, A^{*} w A^{*} \cap X^{*} \neq \varnothing$.
Equivalently, $X$ is a complete set if every word of $A^{*}$ is factor of some word in $X^{*}$.
A set $X \subseteq A^{*}$ is thin if there exists at least one word $w \in A^{*}$ such that $A^{*} w A^{*} \cap X=\varnothing$. Finite sets and recognizable (by a finite automaton) sets are in particular thin sets.

The following foundamental result of M. P. Schutzenberger states the equivalence, for these codes, of the notion of maximality and completeness (see [1]).

Theorem 1 (Schutzenberger): A thin code is maximal if and only if it is complete.

Let $X \subseteq A^{*}$ be a code. Any maximal code $Y \cong A^{*}$ which contains $X$ is called a completion of $X$.

Proposition 1: Every code $X \subseteq A^{*}$ has a completion.
Proof: It is suffices to apply Zorn's lemma to the family:

$$
\mathscr{I}=\left\{Y \cong A^{*} / Y \text { code and } Y \supseteqq X\right\} .
$$

A code $X$ is a prefix code if no word of $X$ is prefix of another word of $X$. It is well known (see [1], cp. 2) that one can associate to a prefix code, over a $k$-letter alphabet, a $k$-ary tree in such a way that the leaves of the tree represent the words of the code. A $k$-ary tree is complete if all the nodes which are not leaves have exactly $k$ successors. As a consequence of theorem 1 , it is easy to verify that a thin prefix code is maximal if and only if the corresponding tree is complete.

For any finite subset $X$ of $A^{*}$ we denote by $d(X)$ the maximal length of words in $X$.

Proposition 2: Any finite prefix code $X$ has a finite completion $Y$ and, moreover, $d(Y)=d(X)$.

Proof: It suffices to complete the tree corresponding to $X$.

Of course proposition 2 holds true also for suffix codes which are obtained from the prefix ones by using the reverse operation.

Proposition 2 is no more true for general codes, as discovered in [9]: there exist finite codes which are not contained in any finite maximal code. The smallest example known is the code

$$
X=\left\{a^{5}, b a^{2}, a b, b\right\} \quad(\text { see [9] or [1], p. 64). }
$$

The main problem we here consider is to characterize those finite codes which have a finite completion. It is not even presently known whether this property is effectively decidable. The simplest example were the answer is unknown is the code

$$
X=\left\{a^{5} b, a^{2} b, b a, b\right\} .
$$

In section 4 we shall find that any completion of $X$ has words of length $\geqq 42$ and we conjecture that $X$ does not have a finite completion.

If we replase "finite" by "recognizable" a positive result has been obtained by Ehrenfeucht and Rozenberg [4].

Theorem 2 (Ehrenfeucht, Rozenberg): Every recognizable code has a recognizable completion.

The proof of this theorem gives also a procedure to complete a code. The procedure, which runs for any thin code, is the following. Let $X \subseteq A^{*}$ be a thin code which is not complete.

Then there exists a word $y \in A^{*}$ such that:
(i) $y$ is unbordered, i.e. $y A^{+} \cap A^{+} y=y A^{*} y$, and
(ii) $y$ is not completable in $X$, i.e. $A^{*} y A^{*} \cap X^{+}=\varnothing$.

One then considers the set $U=A^{*}-X^{*}-A^{*} y A^{*}$ and builds the code $Y=X \cup y(U y)^{*}$. It is not very difficult to verify that $Y$ is complete and therefore maximal. Moreover, if $X$ is recognizable, $Y$ is still recognizable.

Remark that this procedure gives, in any case, an infinite completion. Thus it does not give us any information about the main problem we have considered, i.e. whether a finite code is included in a finite maximal code.

Let us now introduce the notion of composition of codes (see [1], p. 71). Let $X$ and $Z$ be codes over the alphabet $A$ such that $X^{*} \subseteq Z^{*} \subseteq A^{*}$. Let $\beta$ be a bijection of a new alphabet $B$ onto $Z$ that can be extended to an isomorphism of $B^{*}$ and $Z^{*}$ (since $Z$ is a code). The set $Y=\beta^{-1}(X)$ is then a code over the alphabet $B$. We say that $X$ is composed of the codes $Y$ and $Z$ and we write $X=Y \circ Z$.

It is easy to prove that $X$ is a maximal code if and only if $Y$ and $Z$ are maximal codes.

Example 1: Let $A=\{a, b, c\}$ and $X=\{a, b, a c b\}$.
Consider the code $Z=\{a, b, c b\}$.
One has $X^{*} \subseteq Z^{*}$. Let $B=\{x, y, z\}$ and $\beta$ such that

$$
\beta(x)=a, \quad \beta(y)=b, \quad \beta(z)=c b .
$$

Then

$$
Y=\beta^{-1}(x)=\{x, y, x z\}
$$

and

$$
X=Y \circ Z=\{x, y, x z\} \circ\{a, b, c b\}
$$

In other words, $X$ is obtained by replacing in $Y$ the letters $x, y, z$ by the corresponding words of $Z$.

Let $X \subseteq A^{*}$ be a composed code, $X=Y \circ Z$, with $Z \subseteq A^{*}, Y \subseteq B^{*}, \beta$ the bijection of $B$ onto $Z$. Let $Z_{1} \subseteq A^{*}$ be a code containing $Z$, let $\beta_{1}$ be the extension of $\beta$ to a bijection of a new alphabet $B_{1} \supseteq B$ onto $Z_{1}$, and let $Y_{1} \subseteq B_{1}^{*}$ be a code containing $Y$. We then define a new code $X_{1}$ containing $X$, by composing $Y_{1}$ and $Z_{1}$ :

$$
X_{1}=Y_{1} \circ Z_{1}=\beta_{1}\left(Y_{1}\right) .
$$

The following proposition is a consequence of this construction.
Proposition 3: Let $X$ be a finite code obtained by composition of codes having a finite completion. Then $X$ has a finite completion.

From this and proposition 2 we obtain the following corollary. Let us first introduce the following terminology.

A code is called prefix-suffix composed if it is composed by prefix and suffix codes.

Corollary 1: Every finite code, which is prefix-suffix composed, has a finite completion.

We show the completion procedure by an example.
Example 1 (continued).
Consider the code $X=\{a, b, a c b\}=Y \circ Z . Z$ is a prefix code.
A completion of $Z$ is: $Z_{1}=\{a, b, c b, c a, c c\}$.

Let $B_{1}=\{x, y, z, s, t\} \supseteq B$ and let $\beta_{1}: B_{1} \rightarrow Z_{1}$ be the extension of $\beta$ defined as:

$$
\begin{gathered}
\beta_{1}(x)=\beta(x)=a \\
\beta_{1}(y)=\beta(y)=b \\
\beta_{1}(z)=\beta(z)=c b \\
\beta_{1}(s)=c a \\
\beta_{1}(t)=c c .
\end{gathered}
$$

The code $Y=\{x, y, x z\} \subseteq B_{1}^{*}$ is a suffix code and it has (in $B_{1}^{*}$ ) the following completion $Y_{1}$ :

$$
\mathbf{Y}_{1}=\{x, y, x z, s, t, y z, z z, s z, t z\} .
$$

The code

$$
X_{1}=Y_{1} \circ Z_{1}=\beta_{1}\left(Y_{1}\right)=\{a, b, a c b, c a, c c, b c b, c b c b, c a c b, c c c b\}
$$

is a finite completion of $X$.
From previous results one can derive a result for "small" codes. The next theorem considers codes $X$ with $\operatorname{Card}(X)=2$.

Theorem 3: Every two-element code is prefix-suffix composed.
Proof: Let $X=\{u, v\}$ be a code over the alphabet $A$. By well known results in the theory of free monoids (see for istance [1], p. 49), $X$ is a code if and only if $u$ and $v$ are not powers of the some word. We prove now the theorem by induction on the integer $K=|u|+|v|$. To left out the case of a trivial twoword code, the smallest $k$ we must consider is $K=3$; consequently, $X$ has either the form $X=\{a b, b\}$ or the form $X=\{a b, a\}$, with $a, b \in A$. So the statement is true for $K=3$.

Let us now suppose that it is true for $K<n$ and consider the code $X=\{u, v\}$ with $|u|+|v|=n$. If $X$ is not a prefix code, then one of its elements, say $u$, is prefix of $v: v=u w$. Consider the set $X^{\prime}=\{u, w\}$. $X^{\prime}$ is a code, otherwise $u$ and $w$ are powers of the some word and so also $u$ and $v$ are powers of the some word, against the fact that $\{u, v\}$ is a code. Moreover $|u|+|w|<n$ and then, by the induction hypothesis, $X^{\prime}$ is prefix-suffix composed. If $\beta$ is a bijection of a new alphabet $B=\{x, y\}$ onto $X^{\prime}$ defined as $\beta(x)=u, \beta(y)=w$, it is easy to verify that $X=X^{\prime} \circ Y$, where $Y=\{x, x y\} \subseteq B^{*}$ is a suffix code. Thus $X$ is prefix-suffix composed.

Corollary 2: Every two-word code has a finite completion.

The smallest known example, previously reported, of a code having no a finite completion, contains four words. It remains the case of codes with three words. Some partial results, similar to those in the proof of previous theorem, support the conjecture that such codes have a finite completion. In particular we propose the following conjecture:

Conjecture 1: Every three-word code is prefix-suffix composed.

## 3. SCHUTZENBERGER'S CONJECTURE AND SHOR'S CODE

The problem to characterize those finite codes that can be embedded in a finite maximal code is related to a conjecture formulated about thirty years ago by M. P. Schutzenberger. This is perhaps the main open problem in the theory of variable-length codes.

We need the following definition.
Two words $u, v \in A^{*}$ are said to be commutatively equivalent if, for any letter $a \in A$, the numbers of occurences of a in $u$ and $v$ are equal. The notion is extended to subsets of $A^{*}$, i.e. $X, Y \subseteq A^{*}$ are commutatively equivalent if there exist a one-to-one correspondence between $X$ and $Y$ exchanging commutatively equivalent words.

Conjecture (Schutzenberger): Any finite maximal code is commutatively equivalent to a prefix code (or, for short, is commutatively prefix).

Example 2: Let $A=\{a, b\}$ and consider the code

$$
X=\{a a, a b, a a b, a b b, b b\} .
$$

$X$ is neither a prefix code, nor a suffix code, but is commutatively equivalent to the prefix code

$$
Y=\{a a, a b, b a a, b a b, b b\} .
$$

This conjecture takes its motivation in a problem of information theory (see [8]). Let us consider a source of information defined by an alphabet $B$ and a Bernoulli distribution $\pi$ on the words over the alphabet $B$. Let us denote by $A$ the alphabet of the noisless channel through which a trasmission is realized by an encoding $\alpha: B \rightarrow A^{*}$. This defines a code $X=\alpha(B)$ over the alphabet $A$. If all the letters of $A$ have the some cost, the average cost of the trasmission is precisely the average length (with respect to $\pi$ ) $L(X, \pi)$ of the code $X$. The classical inequalities allow an inferior bound on $L(X, \pi)$, which
is the entropy of the source; and it is well known that the minimum may be reached within the class of prefix codes.

In a general case the letters of $A$ have inequal cost, i.e. there is a cost function $\gamma: A^{+} \rightarrow R$ which is extended to the elements of $A^{*}$ by additivity:

$$
\gamma\left(a_{1} a_{2} \ldots a_{n}\right)=\gamma\left(a_{1}\right)+\gamma\left(a_{2}\right)+\ldots+\gamma\left(a_{n}\right)
$$

In this case the average cost of the transmission is:

$$
L(X, \pi, \gamma)=\sum_{x \in X} p(x) \cdot \gamma(x)
$$

where $p(x)$ is the probability $\pi(b)$ of the symbol $b \in B$ coded by the word $x \in X$.

One can then ask the question whether, in this more general case, the minimum cost may still be reached within the class of prefix codes.

As one can easily verify, two commutatively equivalent codes have the same cost. By remarking that the minimum cost requires (at least in the case of a two letters alphabet) a maximal code, one derives that the solution of Schutzenberger's conjecture would give a positive anwer to the problem of optimality of prefix codes.

Recently Peter Shor [10] has constructed a (non maximal) finite code which is not commutatively prefix:

| $b$ | $a^{3} b$ | $a^{8} b$ | $a^{11} b$ |
| :--- | :--- | :--- | :--- |
| $b a$ | $a^{3} b a^{2}$ | $a^{8} b a^{2}$ | $a^{11} b a$ |
| $b a^{7}$ | $a^{3} b a^{4}$ | $a^{8} b a^{4}$ | $a^{11} b a^{2}$ |
| $b a^{13}$ | $a^{3} b a^{8}$ | $a^{8} b a^{6}$ |  |
| $b a^{14}$ |  |  |  |

It is not known whether Shor's code has a finite completion: if yes, then the Shutzenberger conjecture would be false. By using techniques of section 4 , we find that any completion of this code has words of length $\geqq 90$ and we conjecture that it does not have a finite completion.

## 4. CODES AND FACTORIZATIONS OF CYCLIC GROUPS

In this section we show that the problem of finite completion of codes is related to some problems concerning the factorizations of cyclic groups.

Let $Z_{n}$ be the group of integers modulo $n$, and let $P, Q$ be two subsets of $Z_{n}$. The pair ( $P, Q$ ) is a factorization of $Z_{n}$ (see [5]) if each element of $Z_{n}$ may be expressed uniquely as the sum, modulo $n$, of an element of $P$ and an element of $Q$. The factorization is elementary if one can take the sum as in the natural numbers (without modulo $n$ ).

Example 3: Consider the group $Z_{6}$. The pair

$$
P_{1}=\{0,2,4\}, \quad Q_{1}=\{0,5\}
$$

is a (non elementary) factorization of $Z_{6}$. The pair

$$
P_{2}=\{0,2,4\}, \quad Q_{2}=\{0,1\}
$$

is an elementary factorization of $Z_{6}$.
Remark 1: If $(P, Q)$ is a factorization of $Z_{n}$, it is obvious that $\operatorname{Card}(P)$ $\operatorname{Card}(Q)=n$. It follows that $Z_{p}$, with $p$ a prime number, admits only the trivial factorization $P=Z_{n}, Q=\{0\}$.

In [6] Krasner and Ranulac give a method to construct all the elementary factorizations of $Z_{\boldsymbol{n}}$. This method has been used in [9] to construct all finite maximal codes $X$ over the alphabet $\{a, b\}$ such that each word of $X$ contains at most once the letter $b$. Recently, C. De Felice [2] has extended this construction to codes such that each word has at most twice the letter $b$.

The structure of general factorizations still remains unknown to a large extent. The only known results concern particular groups. A subset $P$ of $Z_{n}$ is said to be periodic if there exists an element $t \in Z, t \neq 0$, such that $P=P+t$ $(\bmod n) . Z_{n}$ is said to be "good" if in every factorization $(P, Q)$ at least one factor is periodic. Otherwise it is called "bad". Unfortunately for our problems, there exist bad groups: the smallest example is $Z_{72}$. G. Hajos (see [5]) gives a method to construct all the factorizations of a good group. This problem remains unsolved for bad groups.

Let us now introduce the notion of unambiguous pair. Let $T, R$ be two subset of the set $N$ of natural numbers. The pair ( $T, R$ ) is unambiguous if, for any $t, t^{\prime} \in T, r, r^{\prime} \in R, t+r=t^{\prime}+r^{\prime}$ implies $t=t^{\prime}$ and $r=r^{\prime}$. If $(T, R)$ is an unambiguous pair and $(P, Q)$ a factorization of $Z_{n}$ such that $T \cong P$ and $R \cong Q$, we say that $(T, R)$ is embedded in $(P, Q)$.

Given an unambiguous pair $(T, R)$ and a group $Z_{n}$, the problem whether ( $T, R$ ) is embedded in a factorization of $Z_{n}$ is trivially decidable. The following remark will be usefull in the sequel.

Remark 2: If ( $T, R$ ) is an unambiguous pair, with $T, R \neq\{0\}$, as a consequence of remark 1 , it cannot be embedded in a factorization of $Z_{p}$ with $p$ a prime number.

The following problem appears more difficult.
Embedding problem: given an unambiguous pair ( $T, R$ ), decide whether there exist a group $Z_{n}$ and a factorization $(P, Q)$ of $Z_{n}$ such that $(T, R)$ is embedded in $(P, Q)$.

Example 4: Consider the unambiguous pair:

$$
T=\{0,5\}, \quad R=\{0,3,7\}
$$

$(T, R)$ can be embedded in the following factorization of $Z_{15}$ :

$$
P=\{0,5,10\}, \quad Q=\{0,1,3,4,7\}
$$

Example 5: Consider the unambiguous pair

$$
T=\{0,1\}, \quad R=\{0,2,5\}
$$

We are not able to decide the embedding problem for this pair. With a computer we have found that $(T, R)$ cannot be embedded in a factorization of $Z_{n}$ for $n \leqq 42$.

A solution to the embedding problem can be given only in some particular case: the general problem remains open (the difficult is perhaps related to the existence of "bad" groups). We are not even able to prove the existence of unambiguous pairs for which the embending problem has a negative answer. However we propose the following conjecture.

Conjecture 2: Consider an unambiguous pair of the form:

$$
T=\{0, p, k\}, \quad R=\{0,1\}
$$

where $p$ is a prime that does not divide $k$. Then $(T, R)$ cannot be embedded in a factorization of a cyclic group.

The pair of the example 5 satisfies the condition of the conjecture.
We now turn back our attention to codes and state their link with factorizations of cyclic groups.

In the sequel we shall consider codes $X$ over the alphabet $A=\{a, b\}$ which satisfy the supplementary condition that one letter, say $b$, is a code word, i.e. $b \in X$. For istance, Shor's code verifies this condition.

To each finite code in this family we associate a pair $(T, R)$ of sets of integer defined as follows:

$$
\begin{aligned}
T & =\left\{i \in N / a^{i} b^{+} \cap X \neq \varnothing\right\} \\
R & =\left\{j \in N / b^{+} a^{i} \cap X \neq \varnothing\right\} .
\end{aligned}
$$

Lemma: $(T, R)$ is an unambiguous pair. Moreover, if $X$ is a finite maximal code, $(T, R)$ is a factorization of $Z_{n}$, where $n$ is the integer such that $a^{n} \in X$.

Proof: Let us first prove that ( $T, R$ ) is unambiguous. Assume the contrary: there exist then four words

$$
a^{i} b^{h}, \quad a^{t} b^{k}, \quad b^{s} a^{j}, \quad b^{q} a^{r} \in X \quad \text { such that } \quad i+j=t+r .
$$

By recalling that $b \in X$, it is easy then to verify that the word

$$
b^{s+q} a^{i+j} b^{k+h} \in X^{*}
$$

has two different factorizations in elements of $X$, against the hypothesis that $X$ is a code.

Assume now that $X$ is a finite maximal code. Then it is well known that there exists an integer $n$ such that $a^{n} \in X$. Let $d$ be the maximal length of words in $X$. Since $X$ is maximal, by theorem 1 , for any natural $m$ the word $b^{d} a^{m} b^{d}$ is factor of some word of $X^{*}$. There exist then integers $q, t, r, k, j$ such that the following factorization holds:

$$
b^{q} a^{m} b^{k}=\left(b^{q} a^{r}\right)\left(a^{n}\right)^{\dot{j}}\left(a^{t} b^{k}\right)
$$

with

$$
b^{q} a^{r}, \quad a^{t} b^{k}, \quad a^{n} \in X \quad \text { and } \quad r+t+j n=m
$$

This means that for any $m$ there exist $r \in R$ and $t \in T$ such that $m=r+t(\bmod n)$. This concludes the proof.

Example 6: Consider the code

$$
X=\left\{a^{6}, a b a^{4}, b a^{4}, a b a^{2}, b a^{2}, a^{5} b, a b a^{3} b, b a^{3} b, a b a b, b a b, b\right\}
$$

The pair $(T, R)$ associated to $X$ is:

$$
T=\{0,5\}, \quad R=\{0,2,4\} .
$$

$(T, R)$ is a factorization of $Z_{6}$.
vol. $23, n^{\circ} 2,1989$

An immediate and remarkable consequence of the previous lemma gives a necessary condition for a code to have a finite completion.

Theorem 4: Let $X$ be a finite code over the alphabet $\{a, b\}$ such that $b \in X$. If $X$ has a finite completion, then the pair $(T, R)$ associated to $X$ can be embedded in a factorization of a cyclic group.

If the word $a^{n}$ belongs to $X$, then we know the group $Z_{n}$ in which ( $T, R$ ) has to be embedded. The following corollary, which generalizes some results obtained in [3], gives a method to construct codes having no finite completion.

Corollary 3: Let $X \subseteq\{a, b\}^{*}$ be a code such that $a^{n}, b \in X$. If the associated pair $(T, R)$ cannot be embedded in $Z_{n}$, then $X$ has no finite completion.

In particular, by using remark 2, we obtain the following interesting statement.

Corollary 4: Let $(T, R)$ be a non trivial unambiguous pair and let $p$ be a prime number such that

$$
p>\max \{t+r / t \in T, r \in R\} .
$$

The set

$$
X=a^{P} \cup a^{T} b \cup b a^{R}
$$

is a code that has no a finite completion.
Example 7: Let $p=5, T=\{0,1\}, R=\{0,2\}$. The code $X=\left\{a^{5}, a b, b a^{2}, b\right\}$ has no a finite completion. This is precisely the smallest known example of code having no a finite completion, reported in section 2.

If $X \cap a^{*}=\varnothing$, the situation is completely different, since the group $Z_{n}$, in this case, is not given and we are not able to solve the embedding problem. This is the case of Shor's code. The pair associated to Shor's code is

$$
T=\{0,3,8,11\}, \quad R=\{0,1,7,13,14\} .
$$

It is not known whether this pair can be embedded in a factorization of a cyclic group. By computer we have found that it cannot be embedded in $Z_{n}$ for $n \leqq 90$. This means that any completion of Shor's code has words of length $>90$.

Let us remark that the pair associated to Shor's code contains the pair

$$
T=\{0,3,8\}, \quad R=\{0,1\}
$$

which satisfies the condition in conjecture 2 . As a consequence we conjecture that Shor's code has no a finite completion and then that it cannot produce a counterexample to the Schutzenberger's conjecture.

As another example, consider the code reported in section 2 as the simplest example of code for which is unknown whether it has a finite completion. The associated pair is given in example 5 and it also satisfies the condition in conjecture 2 . This suggest that it has no a finite completion. Actually our arguments and computer verifications prove only that any completion of this code has words of length $>42$.

## REFERENCES

1. J. Berstel and D. Perrin, The Theory of Codes, Academic Press, 1985.
2. C. De Felice, Construction of a Family of Finite Maximal Codes, Report of L.I.T.P., 1987.
3. C. De Felice and A. Restrvo, Some Results on Finite Maximal Codes, R.A.I.R.O. Informatique Théorique, Vol. 19, No. 4, 1985.
4. A. Ehrenfeucht and G. Rozemberg, Each Regular Code is Included in a Maximal Regular Code, R.A.I.R.O. Informat. Theor. Application, Vol. 20, 1986, pp. 89-96.
5. Fuchs, Abelian Group, Pergamon Press, 1960.
6. Al. A. Markov, An Example of an Indipendent System of Words which Cannot be Included in a Finite Complete System (Russian), Mat. Zametki, Vol. 1, 1967, pp. 8790.
7. M. Krasner and B. Ranulac, Sur une propriété des polynomes de la division du cercle, C.R. Acad. Sci. Paris, T. 204, 1937, pp. 397-399.
8. D. Perrin and M. P. Schutzenberger, Un problème élémentaire de la théorie de l'information, Coll. Internat. du C.N.R.S., n ${ }^{\circ}$ 276, Théorie de l'Information, 1977.
9. A. Restivo, On Codes Having no Finite Completion, Discrete Math., Vol. 17, 1977, pp. 309-316.
10. P. Shor, A Counterexample to the Triangle Conjecture, J. Comb. Theory A, Vol. 38, 1985, pp. 110-112.

[^0]:    (*) Received November 1986, revised April 1987.
    $\left(^{1}\right)$ Dipartimento di Matematica ed Applicazioni, Università di Palermo, Via Archirafi 34, Palermo (Italy).

