A partial result about the factorization conjecture for finite variable-length codes

Clelia De Felice*

Dipartimento di Informatica ed Applic., Università di Salerno, 84081 - Baronissi (SA), Italy

Received 27 September 1990
Revised 22 October 1991

Abstract

We construct a family of finite maximal codes over the alphabet \{a, b\} which verify the factorization conjecture on codes proposed by Schützenberger. This family contains any finite maximal code with at most three occurrences of the letter b by word.

1. Introduction

This paper gives a partial answer to the conjecture of factorization of finite maximal codes proposed by Schützenberger (see [2, 3]).

The theory of variable-length codes was born in Shannon's early works on information transmission in the 1950s. It was subsequently developed in an algebraic direction by Schützenberger and his school, and is now a part of theoretical computer science related to automata theory, formal power series and languages theory [24, 25]. For a complete survey of the theory of codes see [2].

Codes C are naturally defined as subsets of A* such that any word w in A* has at most one factorization into words of C. One important aim of the theory of codes is to give a structural description of the codes in a way that allows their construction. This is easily accomplished for prefix (suffix) codes, i.e. codes such that none of their words is a left (right) factor of another one. This is also verified for finite maximal biprefix codes [9, 10] i.e. finite maximal codes both prefix and suffix. However no systematic method is known to construct all finite codes and particularly all finite maximal codes.

Correspondence to: Clelia De Felice, Dipartimento di Informatica ed Applic., Università di Salerno, 84081 - Baronissi (SA), Italy.

*This work was supported by contract n. 3166 ESPRIT-EBRA ASMICS and by project 40% MURST 'Algoritmi, Modelli di Calcolo e Strutture Informative'.

0012-365X/93/$06.00 © 1993—Elsevier Science Publishers B.V. All rights reserved
In this context, Schützenberger has proposed several conjectures. A first one, still open today, is inspired by a problem of information theory and states that any finite maximal code is commutatively equivalent to a prefix code (i.e. they have the same commutative image) [19]. A more general conjecture has been formulated in terms of noncommutative polynomials of \( \mathbb{Z}\langle \text{A} \rangle \): any finite maximal code \( C \subseteq \text{A}^* \) is factorizing, i.e. there exist finite subsets \( P, S \) of \( \text{A}^* \) such that \( C-1 - P(\text{A}-1)S \) (\( C \) denotes the characteristic polynomial of \( C \)). The major contribution to this conjecture is due to Reutenauer [21,22]. He proved that for any finite maximal code \( C \) equality \( C-1 = P(\text{A}-1)S \) holds with \( P, S \in \mathbb{Z}\langle \text{A} \rangle \). We call \( (P, S) \) a factorization of \( C \). Then, if the factorization conjecture would be true, there would exist a 'privileged' factorization \( (P, S) \) of \( C \) with \( P, S \in \mathbb{N}\langle \text{A} \rangle \).

In a natural way codes having multiple factorizations were investigated. Boë created a particular family of factorizing codes \( C \) with a unique factorization [4,5]. Other families of factorizing codes were constructed in the framework of another Schützenberger's conjecture. This conjecture dealt with the notions of decomposability and degree of codes [25]. If \( C_1 \) is a code over the alphabet \( \text{A} \) and \( C_2 \) a code over the alphabet \( \text{C} \), then the image of \( C_2 \) into \( \text{A}^* \) is again a code over \( \text{A} \) named the composed code. The degree is a parameter associated with codes. The codes of Boë are synchronous, i.e. they have degree 1. Perrin constructed a family of prefix factorizing codes all indecomposable and asynchronous (with degree > 1) [18]. Moreover Vincent [27] found a method to construct asynchronous indecomposable factorizing codes neither prefix nor suffix. Finally a characterization of codes having multiple factorizations can be found in [6-8].

On the other hand algorithms exist to construct some families of codes, finite maximal codes over the alphabet \( \{a, b\} \) which have few letters \( b \) by word: they are 1-codes or 2-codes, a \( n \)-code being a finite maximal code with \( n \) letters \( b \) or less by word. This shares some properties with a special class of binomial trees corresponding to particularly efficient algorithms [1].

1- and 2-codes are factorizing and algorithms to construct them are all obtained by using a class of factorizations of the cyclic group \( \mathbb{Z}_n \) (see [20] for 1-codes and [11,12] for 2-codes). A factorization of the finite cyclic group \( \mathbb{Z}_n \) is a pair \( (I, J) \) of subsets of \( \mathbb{N} \) such that any \( m \in \mathbb{Z}_n \) can be uniquely written as \( m = i + j \mod n \) with \( i \in I, j \in J \) [15]. The structure of the factorizations of \( \mathbb{Z}_n \) is unknown except for the class used for 1- and 2-codes. This class was also described by Hajós [13,16]. The study of the degree and the decomposability of \( n \)-codes with \( n \leq 3 \) can be found in [6-8].

Then some natural questions arise in this framework. Can any factorizing code be constructed by using only this class of factorizing codes? Does there exist a similar relation between a finite maximal code and a factorization of cyclic group? Does there exist a recursive transformation which turn a finite maximal code into a factorizing code?

We answer positively to the first question for 3-codes and we conjecture that this result remains true in the general case.

We solve the factorization conjecture for 3-codes. Moreover we prove that for any factorization \( (P, S) \) of a 3-code, then \( P, S \) are characteristic polynomials. It is known
that this result does not hold for any finite maximal code [23]. Thus the demonstration techniques presented in this paper can certainly not be extended to any finite maximal code. An open research direction consists in seeing whether they can be extended to finite maximal codes which admit only one factorization.

We construct a class of n-codes which are factorizing and which can be obtained recursively starting by a (n - 1)-code. More precisely, for any \( P \in \mathbb{Z}\langle A \rangle \) denote \( P_r \) the polynomial such that any word in \( \text{supp}(P_r) \) has \( r \) occurrences of the letter \( b \) and \( P = P_0 + \cdots + P_r \). Let \((P,S)\) be a factorization of \( C \) with \( P = P_0 + \cdots + P_n \). Suppose that \((P_0 + \cdots + P_r) (A - 1) S + 1 \geq 0\), for any \( r \in \{0, \ldots, h\} \). We prove that \( C \) is factorizing. As for 3-codes, Hajós factorizations of \( \mathbb{Z}_n \) are used in this construction.

These results can be generalized to arbitrary alphabets \( A \) having cardinality greater than two.

This paper is divided in six parts. In Section 2 we recall several previous definitions and results. In Section 3 we prove some technical lemmas. In Section 4 we show a preliminary and general result for a factorization of a finite maximal code and we construct our family of factorizing codes. From a remark we can infer that for every 3-code \( C \), every factorization \((P,S)\) verifies one of the following two properties: (1) \( \text{supp}(P) \subseteq a^* \) (or \( \text{supp}(S) \subseteq a^* \)); (2) \( \text{supp}(P), \text{supp}(S) \subseteq a^* \cup a^* \). In Section 4 the first case is examined and in Section 5 the second. In Section 6 these codes are constructed. An extended abstract is already published [28].

2. Definitions and previous results

Let \( A \) be a finite alphabet and \( A^* \) the free monoid generated by \( A \). We denote \( 1 \) the empty word and we set \( A^+ = A^* \setminus 1 \). For any word \( w \in A^* \) we denoted by \(|w|\) the length of \( w \) and for any letter \( a \in A \) by \(|w|_a\) the number of the occurrences of the letter \( a \) in \( w \). Moreover \( w^r \) denotes the reverse of \( w \) i.e. the word \( w \) read from right to left.

A subset \( C \) of \( A^* \) is a code over \( A \) if for any \( c_1, \ldots, c_n, c'_1, \ldots, c'_m \in C \) the equation

\[
 c_1\cdots c_n = c'_1\cdots c'_m
\]

implies

\[
 n = m \quad \text{and} \quad \forall i \in \{1, \ldots, n\} \quad c_i = c'_i.
\]

\( C \subseteq A^+ \) is a prefix code if \( C \cap C A^+ = \emptyset \). Suffix codes \( C \) are defined symmetrically such that \( C \cap A^+ C = \emptyset \). A biprefix code is a code both prefix and suffix.

A code \( C \subseteq A^+ \) is said maximal (over \( A \)) if it cannot be strictly included in another code over \( A \). Given a finite maximal code \( C \subseteq A^+ \), each letter \( a \in A \) has a unique power \( a^n \) in \( C \). A systematic exposition of the theory of codes can be found in [2].

As usual \( \mathbb{Z} \) denotes the ring of the integer numbers, \( \mathbb{N} \) the semiring of nonnegative integers. For any semiring \( K, K\langle A \rangle \) (resp. \( K\langle A \rangle \)) denotes the semiring of series (resp. polynomials) with noncommutative variables \( \alpha \in A \) and coefficients in \( K \) (see [3, 14] for a complete survey of this theory). \( K[A] \) denotes the semiring of the commutative polynomials generated by \( A \) over \( K \). For a series \( S, (S, w) \) denotes the
coefficient of the word $w$ in $S$. Any (finite) subset $X$ of $A^*$ will be identified with its characteristic (polynomial) series $X = \sum_{x \in X} x$. The support $\text{supp}(S)$ of a series $S$ is equal to $\{w \in A^* | (S, w) \neq 0\}$.

Let $P \in K\langle A \rangle$. $P^r$ denotes the reverse of $P$, i.e. the polynomial $P$ read from right to left. Let $h \in \mathbb{N}$. $P$ is $h$-homogeneous if $p \in \text{supp}(P)$ implies $|p|_h = h$. Let $h$ be the maximum number of occurrences of $b$'s in the words of $\text{supp}(P)$. For any $r \in \{0, \ldots, h\}$, $P_r$ denotes the $r$-homogeneous polynomial such that $P = P_0 + \cdots + P_h$. Given two polynomials $P, S \in \mathbb{Z}\langle A \rangle$, we write $P < S$ when $(P, w) < (S, w)$ for all $w \in A^*$.

As in [12] we denote $\mathbb{N}_1 = \mathbb{N} \setminus \{1\}$ the semiring of the finite $\mathbb{N}$-sets (multisets) of nonnegative integers. For any $M \in \mathbb{N}_1$, we denote by $a^M$ the polynomial $\sum_{n \in \mathbb{N}} (M, n) a^n e^{\mathbb{N}\langle A \rangle}$. The computation rules are

$$a^0 = 0, \quad a^0 = 1, \quad a^{M \cup N} = a^M + a^N, \quad a^{M+N} = a^M a^N$$

The symbols $\cup$ and $+$ mean union and addition for multisets.

The notion of factorizing code shows the interplay between codes and polynomials. A code $C$ over $A$ is factorizing if there exist two subsets $P, S$ of $A^*$ such that $C-1 = P(A-1)S$.

Finite maximal prefix (resp. suffix) codes $C \subseteq A^*$ are factorizing since $C-1 = P(A-1)$ (resp. $C-1 = (A-1)S$) with $P$ (resp. $S$) be the set of proper left (resp. right) factors of words in $C$.

As a special case, note that if $C$ is a factorizing code with $P, S$ finite, then $C$ is a finite maximal code; conversely, if $C$ is a finite maximal factorizing code, then $P, S$ are finite sets [2]. However it is not known whether any finite maximal code is always factorizing:

**Conjecture 2.1** (Schützenberger [2, 3]). Any finite maximal code is factorizing.

Schützenberger investigated deeply the structure of the characteristic polynomial of a finite maximal code and proved the well known theorem of the commutative factorization of this polynomial [2, 3, 26]. Reutenauer proved a noncommutative version of it [22] and as a consequence he gave a characterization of the finite maximal codes. Let $C \subseteq \mathbb{N}\langle A \rangle$ with $(C, 1) = 0$. $C$ is weakly factorizing if there exist two polynomials $P, S \in \mathbb{Z}\langle A \rangle$ such that $C-1 = P(A-1)S$. We call $(P, S)$ a factorization of $C$.

**Theorem 2.2** (Reutenauer [21, 22]). $C$ is a finite maximal code if and only if $C$ is weakly factorizing.

**Remark 2.3** ([21]). If $P, S \in \mathbb{N}\langle A \rangle$ are such that $P(A-1)S + 1 \geq 0$, then $P(A-1)S + 1$ is the characteristic polynomial of a finite maximal code and $P, S$ have coefficients $0, 1$.

For finite maximal codes over the alphabet $\{a, b\}$ having a few times the letter $b$ inside their words, Conjecture 2.1 is true. We call $n$-codes any finite maximal code.
The factorization conjecture

Theorem 2.4 ([11, 20]). Any 1- or 2-code \( C \subseteq \{a, b\}^+ \) is factorizing. Moreover, for any factorization \( (P, S) \) of \( C \) with \( P, S \in \mathbb{Z}\langle A \rangle \), then \( P, S \) are characteristic polynomials.

The second part of this result does not hold in general [23].

The aim of this paper is the construction of a family of factorizing codes which contains 3-codes. This construction is related to a class of factorizations of the finite cyclic groups.

Let \( \mathbb{Z}_n \) be the cyclic group of integers modulo \( n \), and \( R, T \) two subsets of \( \mathbb{N} \). The pair \( (T, R) \) is a factorization of \( \mathbb{Z}_n \) if

\[
\forall i \in \mathbb{Z}_n, \exists! r \in R, \exists! t \in T : i = r + t \mod n
\]

A method is given in [17] to construct all the factorizations of \( \mathbb{Z}_n \) where the sum is as in \( \mathbb{N} \), without modulo \( n \). We call Krasner factorizations these particular factorizations and 1-codes are constructed by using them [20].

Hajós gave a method for constructing a more general class of factorizations of \( \mathbb{Z}_n \) which we call Hajós factorizations [16]. This class of factorizations can be characterized in the following way.

Proposition 2.5 ([13]). Let \( R, T \in \mathbb{N}_1 \). \((R, T)\) is a Hajós factorization of \( \mathbb{Z}_n \) if and only if there exist a Krasner factorization \( (I, J) \) of \( \mathbb{Z}_n \) and \( M, L \in \mathbb{N}_1 \) such that

\[
a^R = a^I (1 + a^M (a - 1)) \geq 0, \quad a^T = a^J (1 + a^L (a - 1)) \geq 0
\]

Moreover \( M, L, R, T \in \mathbb{N} \).

2- and 3-codes are constructed by using Hajós factorizations of \( \mathbb{Z}_n \) ([12], Section 6). The problem of finding all the factorizations of a finite cyclic group is still open.

In this paper we suppose \( A = \{a, b\} \) as in Theorem 2.4. However we can generalize these results to arbitrary alphabets \( A \) containing at least two distinct letters \( a, b \). A characterization of the degree and the decomposability of \( n \)-codes with \( n \leq 3 \) can be found in [6–8]. It is obtained by an algebraic characterization of respectively, codes with multiple factorizations and decomposable codes (over arbitrary alphabets) (see [6–8]).

From now on, we suppose all the codes to be finite and maximal, we briefly call them codes.

3. Some technical lemmas

In this section we prove two lemmas needed for our main results.

In the first one we consider two inequations and we prove that some homogeneous polynomials appearing inside them have nonnegative coefficients. We will prove
(Theorem 4.2) that for any factorization \((P,S)\) of \(C\) some of the homogeneous components of \(P\) and \(S\) have nonnegative coefficients thanks to this lemma.

In the second one we consider other inequations. Two parameters are associated with them: a polynomial \(a^H \in \mathbb{N} \langle a \rangle\) and a nonnegative integer \(z\). We prove that \(z\) is a bound for the coefficient \((a^H, a')\) of the word \(a'\) on \(a^H\), where \(t \in \mathbb{N}\). In Theorem 5.1 we will prove our result about 3-codes. The proof is by contradiction. We will get a contradiction by showing that \((a^H, a')\) is greater than \(z\), for a particular \(t \in \mathbb{N}\).

**Lemma 3.1.** Let \(X, Y, Z, T\) be polynomials in \(\mathbb{Z} \langle A \rangle\). Suppose that \(X\) is \(k\)-homogeneous, \(Y\) is \(h\)-homogeneous, \(T\) is \((k-1)\)-homogeneous and \(Z\) is \((h-1)\)-homogeneous, where \(h, k > 0\).

(i) If \(x, y \in A^*\) are such that \(|x|^a = k\) and \(|y|^a = h\) then we have
\[
(X \cdot Y, x \cdot y) = (X, x) \cdot (Y, y).
\]

(ii) If \(X \cdot Y\) has coefficients \(0, 1, \ldots\) then \(X\) and \(Y\) (or \(-X\) and \(-Y\)) have coefficients \(0, 1, \ldots\).

(iii) Suppose \(X, Y\) have coefficients \(0, 1, \ldots\). If \(X(a-1)Y + TbZ \in \mathbb{N} \langle A \rangle\) then
\[
T \in \mathbb{N} \langle A \rangle \setminus 0 \quad \text{and} \quad X = \sum_{t \in \text{supp}(T)} t a^t \cdot (L_t \subseteq \mathbb{N})
\]
or
\[
Z \in \mathbb{N} \langle A \rangle \setminus 0 \quad \text{and} \quad Y = \sum_{k \in \text{supp}(Z)} a^k \cdot b \cdot (M_k \subseteq \mathbb{N}).
\]

**Proof.** (i) By definition we have
\[
(X \cdot Y, x \cdot y) = \sum_{x' \cdot y' = x \cdot y} (X, x') \cdot (Y, y')
\]
The nonzero terms in this sum are such that \((X, x') \neq 0\) and \((Y, y') \neq 0\). In this case, by the hypotheses we have \(|x'|^a = k = |x|^a\) and \(|y'|^a = h = |y|^a\). So, by \(x \cdot y = x' \cdot y'\) we get \(x = x'\) and \(y = y'\).

(ii) It suffices to prove that \(X, Y\) (or \(-X\) and \(-Y\)) \(\in \mathbb{N} \langle A \rangle\).

Assume the contrary, there exist \(G, R \in \mathbb{N} \langle a \rangle\) with \(\text{supp}(G) \cap \text{supp}(R) = \emptyset\). Suppose that the first case holds. By (i) we have
\[
\forall y \in \text{supp}(R) \quad (X Y, x \cdot y) = (X, x) \cdot (Y, y) = (X, x) \cdot (-R, y) < 0
\]
which is a contradiction. By a similar argument we get the conclusion in the other cases.

(iii) Let \(R, G, V, Q \in \mathbb{N} \langle A \rangle\) be polynomials such that \(Z = V - Q\) and \(T = R - G\) with \(\text{supp}(R) \cap \text{supp}(G) = \emptyset = \text{supp}(V) \cap \text{supp}(Q)\). Moreover let \(X', Y'\) be subsets of \(A^*\).
such that
\[ X = \sum_{x \in X} xba^Lx, \quad Y = \sum_{y \in Y} a^M_y by, \]
with \( L_x, M_y \) finite subsets of \( \mathbb{N} \).

Let us prove that \( X' \subseteq \text{supp}(R) \) or \( Y' \subseteq \text{supp}(V) \). Assume the contrary, let \( x \in X' \setminus \text{supp}(R), y \in Y' \setminus \text{supp}(V), \alpha = \min L_x, \beta = \min M_y. \) By hypothesis we must have
\[ (X(a-1)Y + TbY + XbZ, xba^{a+\beta} by) \geq 0 \]
On the other hand we have \((X(a-1)Y, xba^{a+\beta} by) < 0.\) Moreover \((T, x) \leq 0.\) So, by (i) we have
\[ (TbY, xba^{a+\beta} by) = (T, x) (Y, a^{a+\beta} by) \leq 0. \]
By a similar argument \((XbZ, xba^{a+\beta} by) \leq 0.\) Then we have
\[ (X(a-1)Y + TbY + XbZ, xba^{a+\beta} by) < 0 \]
which is a contradiction.

So \( X' \subseteq \text{supp}(R) \) or \( Y' \subseteq \text{supp}(V) \). Let us suppose that the first case occurs, the argument is similar in the other one. Let \( g \in G \setminus \{0\}, y = a^m by' \in Y. \) By hypothesis we must have
\[ (X(a-1)Y + TbY + XbZ, gby) \geq 0 \]
On the other hand, by (i) we have \((XbV, gby) = (X, gba^m) (V, y')\) and by definition we get
\[ (XaY, gby) = \sum_{t+n=m-1} (X, gba^t) (Y, a^t by'). \]
Then, by \( X' \subseteq \text{supp}(R) \) we get \((XbV, gby) = (XaY, gby) = 0.\) Moreover by (i),
\[ (TbY, gby) = (T, g) (Y, y) = (-G, g) (Y, y) < 0. \]
So we have
\[ (X(a-1)Y + TbY + XbZ, gby) < 0 \]
Consequently \( G = 0 \) and the conclusion follows. \( \square \)

Lemma 3.2. (i) Let \( P, a^H \in \mathbb{N}\langle a \rangle \) be polynomials. Suppose that there exists \( n \in \mathbb{N} \) such that \( P + a^H(a^n - 1) \geq 0 \). Then for any \( t \in \mathbb{N} \) we have
\[ (a^H, a^t) \leq \sum_{j \equiv t (\text{mod } n)} (P, a^j). \]

(ii) Let \( I, H \subseteq \mathbb{N} \). Suppose that there exists \( n \in \mathbb{N} \) such that \( I = \{0, \ldots, n-1\} (\text{mod } n) \) and \( a^t = a^t + a^H(a^n - 1) \geq 0. \) Then \( I' = \{0, \ldots, n-1\} (\text{mod } n). \)

(iii) Let \( H, I \subseteq \mathbb{N}; \alpha \in \mathbb{N}. \) Then \( a^I + a^H(a^n - 1) \geq 0 \) implies \( a^I + a^H(a^n - 1) \geq 0. \)

(iv) Let \( a^H \in \mathbb{N}\langle a \rangle \). Suppose that there exist \( x, n \in \mathbb{N} \) such that
\[ a^t = \alpha \left( \frac{a^n - 1}{a - 1} \right) + a^H(a^n - 1) = \frac{a^n - 1}{a - 1} (x + a^H(a - 1)) \geq 0. \]
Then for any $t \in \mathbb{N}$ we have $(a^H, a^t) \leq z$. If $z=1$ then $a^H$ has coefficients $0, 1$ and $I' = \{0, \ldots, n-1\} \pmod{n}$. If $H \subseteq \mathbb{N}$ then
\[
\frac{a^H - 1}{a-1} (1 + a^H(a-1)) \geq 0.
\]

**Proof.** (i) The proof is by induction on $\text{card}(\text{supp}(a^H))$. If $H = \emptyset$ then the conclusion follows. Otherwise let $h = \min(\text{supp}(a^H))$. Since $P + a^H(a^n - 1) \geq 0$ and $(a^{H+n}, a^h) = 0$ then $(a^h, a^h) \leq (P, a^h)$.

Let $a^H = a^H - (a^H, a^h) a^h$ and $P' = P + (a^H, a^h) a^h (a^n - 1)$. We have $a^{H'}, P' \in \mathbb{N} < a$.

Moreover
\[
P + a^H(a^n - 1) = P' + a^{H'}(a^n - 1) \geq 0
\]
and
\[
\sum_{j \equiv t \pmod{n}} (P, a^j) = \sum_{j \equiv t \pmod{n}} (P', a^j), \quad \text{for any } t \in \mathbb{N}.
\]

Since $\text{card}(\text{supp}(a^{H'})) < \text{card}(\text{supp}(a^H))$ we can apply to $a^{H'}$ and $P'$ the induction hypothesis. We obtain
\[
\forall t \in \mathbb{N}, t \neq h \quad (a^{H'}, a^t) = (a^{H'}, a^t) \leq \sum_{j \equiv t \pmod{n}} (P', a^j) = \sum_{j \equiv t \pmod{n}} (P, a^j).
\]

Then the conclusion follows.

(ii) The proof is by induction on $\text{card}(H)$. If $H = \emptyset$ then the conclusion follows. Otherwise let $h = \min H$. Since $(a^t + a^H(a^n - 1), a^h) \geq 0$ and $(a^H(a^n - 1), a^h) < 0$ then we have $(a^t, a^h) > 0$.

Let $a^H = a^H - a^h$, $a^t = a^t + a^h (a^n - 1)$. We have $H_1, I_1 \subseteq \mathbb{N}$ and $I_1 = \{0, \ldots, n-1\} \pmod{n}$. Moreover $\text{card}(H_1) < \text{card}(H)$ and $a^t = a^t + a^H(a^n - 1) = a^h + a^H(a^n - 1) \geq 0$.

We apply to $H_1$ and $I_1$ the induction hypothesis and we obtain $I' = \{0, \ldots, n-1\} \pmod{n}$.

(iii) By contradiction suppose that there exists $t \in \mathbb{N}$ such that $(a^t + a^H(a^n - 1), a^t) < 0$. Then we have
\[
1 \geq (a^H, a^t) > (a^t + a^{H+n}, a^t) \geq 0.
\]

So $(a^H, a^t) = 1$, $(a^t + a^{H+n}, a^t) = 0 = (a^t, a^t) = (a^{H+n}, a^t)$. On the other hand, by hypothesis we have
\[
(za^t + a^H(a^n - 1), a^t) \geq 0.
\]

Since $(a^H(a^n - 1), a^t) = -1$ then we have $(z a^t, a^t) \geq 1$. Thus $(a^t, a^t) > 0$, which is a contradiction.

(iv) The conclusion follows straightforwardly by (i), (ii) and (iii).

**Remark 3.3.** It is known that a pair $(T, R)$ of subsets of $\mathbb{N}$ is a factorization of $\mathbb{Z}_n$ if and only if
\[
a^T a^H = \frac{a^n - 1}{a-1} (1 + a^H(a-1)) \geq 0.
\]

$H$ is the set of the holes of $(T, R)$ [13].
4. Partial results about the conjecture

In this section we obtain some partial results about the factorization conjecture. In particular we construct our family of factorizing codes (Theorem 4.3). As a byproduct we obtain our result for 3-codes having a factorization \((P, S)\) with \(\text{supp}(P) \subseteq a^*\) or \(\text{supp}(S) \subseteq a^*\).

**Remark 4.1.** Let \(C \in \mathbb{N}[A]\), \(P, S \in \mathbb{Z}[A]\) be polynomials such that \(C - 1 = P(A - 1)S\). The set \(C_r = \{w \in \text{supp}(C) | |w|_b = r\}\) is given by the sum of the terms of degree \(r\) with respect to the variable \(b\) in the polynomial \(P(A - 1)S + 1\), i.e.

\[
C_0 = P_0(a - 1)S_0 + 1 = a^*, \quad \forall r > 0 \quad C_r = \{w \in \text{supp}(C) | |w|_b = r\} = \sum_{i+j=r} P_i(a-1)S_j + \sum_{i+j=r-1} P_ibS_j
\]

**Theorem 4.2.** Let \(C\) be a finite maximal code. Let \(P = \sum_{k=0}^h P_i, S = \sum_{k=0}^h S_i\) be a factorization of \(C\). Then the following statements hold either for \((P, S)\) or for \((-P, -S)\):

(i) \(P, S\) have coefficients 0, 1.

(ii) either

\[
P_{k-1} \in \mathbb{N}[A] \setminus \{0\} \quad \text{and} \quad P_k = \sum_{r \in \text{supp}(P_{k-1})} pba^{L_r}
\]

or

\[
S_{k-1} \in \mathbb{N}[A] \setminus \{0\} \quad \text{and} \quad S_k = \sum_{r \in \text{supp}(S_{k-1})} a^{M_r}bs.
\]

**Proof.** By Remark 4.1, \(C_{k+h+1} = P_kbS_h\) and \(C_{k+h} = P_k(a-1)S_h + P_{k-1}bS_h + P_kbS_{h-1}\) have coefficients 0 or 1. So we get the result by Lemma 3.1(ii) and (iii) applied to \(X = P_k, Y = S_h, T = P_{k-1}, Z = S_{h-1}\).

**Theorem 4.3.** Let \(C\) be a code. Let \(P = \sum_{k=0}^h P_i, S = \sum_{k=0}^h S_i\) be a factorization of \(C\).

(i) Suppose \(P\) (resp. \(S\)) \(\in \mathbb{Z}[A]\). Then for any \(r \in \{0, \ldots, h\}\) (resp. \(\{0, \ldots, k\}\))

\[
C' = P_0(A - 1)(S_0 + \cdots + S_r) + 1 = \sum_{i \in \{0, \ldots, r-1\}} C_i + P_0bS_r
\]

(resp. \(C' = (P_0 + \cdots + P_r)(A - 1)S_0 + 1 = C_0 + \cdots + C_{r-1} + P_rbS_0\)

is a code. Moreover \(P, S\) have coefficients 0, 1.

(ii) Suppose that for any \(r \in \{0, \ldots, h\}\) we have \(P(A - 1)(S_0 + \cdots + S_r) + 1 \geq 0\). Then \(P, S\) have coefficients 0, 1.

**Proof.**

(i) By Theorem 4.2, \(P_0, S_0\) or \(-P_0, -S_0\) have coefficients 0, 1. Suppose that the first case holds (the argument is similar in the other case).

We prove the conclusion by induction over \(h\). For \(h = 0\) we have nothing to prove. Suppose the statement is true for any nonnegative integer smaller than \(h\), \(h \geq 0\). By
Theorem 4.2(ii) we have $S_{h-1} \in \mathbb{N} \langle A \rangle$. So $C'_h = P_0 b S_{h-1} \in \mathbb{N} \langle A \rangle$. Moreover, by Remark 4.1 we have

$$C_0 = P_0 S_0 (a-1) + 1 \in \mathbb{N} \langle A \rangle;$$

$$\forall r \in \{1, \ldots, h-1\} \quad C_r = P_0 (a-1) S_r + P_0 b S_{r-1} \in \mathbb{N} \langle A \rangle$$

Set $S' = S_0 + \cdots + S_{h-1} \in \mathbb{Z} \langle A \rangle$. We have

$$C' = P (A - 1) S' + 1 = \sum_{i=0}^{h-1} C_i + C'_h \in \mathbb{N} \langle A \rangle$$

with $(C', 1) = 0$. By Theorem 2.2, $C'$ is a code and supp$(S')$ has $h-1$ letters $b$ or less by word. By induction hypothesis the conclusion follows.

(ii) If $r=0$ the statement holds thanks to (i). Then the conclusion follows by induction over $h$ and by using Theorem 4.2(i). $\Box$

**Theorem 4.4.** Let $C$ be a code and $P, S$ a factorization of $C$. $C$ is a $n$-code where $n > 1$, if and only if there exist $h, k \geq 0$ such that supp$(S)$ has $h$ letters $b$ or less by word, supp$(P)$ has $k$ letters $b$ or less by word and $h + k + 1 = n$.

**Proof.** Straightforward, by Remark 4.1. $\Box$

5. 3-Codes

Let $C$ be a 3-code. By Theorem 4.4, a factorization $(P, S)$ of $C$ verifies one of the following three properties: (i) $P \in \mathbb{Z} \langle a \rangle$, (ii) $S \in \mathbb{Z} \langle a \rangle$, (iii) $P = P_0 + P_1$, $S = S_0 + S_1$. Suppose that case (i) (resp. (ii)) holds. By Theorem 4.3, $P, S$ have coefficients 0, 1. We examine case (iii) in Theorem 5.1.

**Theorem 5.1.** Let $C$ be a 3-code and $(P, S)$ a factorization of $C$. Then $P, S$ have coefficients 0, 1.

**Proof.** Let $C$ be a 3-code and $(P, S)$ a factorization of $C$. By Theorem 4.4, $(P, S)$ verifies one of the following three properties: (i) $P \in \mathbb{Z} \langle a \rangle$, (ii) $S \in \mathbb{Z} \langle a \rangle$, (iii) $P = P_0 + P_1$, $S = S_0 + S_1$. By Theorem 4.3(i), in case (i) or (ii) the conclusion follows.

Suppose that case (iii) holds. By Theorem 4.2 we can suppose that there exist finite subsets $I, J, L_i (i \in I), M_j (j \in J)$ of $\mathbb{N}$, with $P_0 \in \mathbb{N} \langle A \rangle$ and $a^j = \text{supp}(P_0)$ such that

$$P_i = \sum_{i \in I} a^i b a^i, \quad S_1 = \sum_{j \in J} a^{M_j} b a^j$$

and with at least an $i \in I$ such that $L_i \neq \emptyset$ (otherwise $C$ would be a 2-code).

In order to prove the theorem we have to prove that $S$ is in $\mathbb{N} \langle A \rangle$, i.e. that $S_0 \in \mathbb{N} \langle A \rangle$. Assume the contrary, let $Q = \{ j \in \mathbb{N} \mid \exists x_j > 0: (S_0, a^j) = -x_j \} \neq \emptyset$. 


By Remark 4.1 we have the three inequations $C_r \geq 0$, where $r \in \{0, 1, 2\}$. By every inequation we will infer some facts which will lead to a contradiction.

Let $n$ be the positive integer such that $a^n \in C$. We have

$$C_0 = a^n = P_0 S_0 (a - 1) + 1 \geq 0.$$  

So, $1 = (P_0, 1) = (a^j, 1)$.

Let us consider $C_2 \geq 0$:

$$C_2 = \sum_{i \in I} a^i b a^L (a - 1) a^M b a^j + \sum_{j \in J} P_0 b a^M b a^j + \sum_{i \in I} a^i b a^L b S_0 \geq 0.$$  

Let $i \in I$ be such that $L_i \neq \emptyset$ and let $j \in Q$, $v = \min L_i$. Let us evaluate the integer $(C_2, a^i b a^v b a^j)$. We have

$$0 \leq (C_2, a^i b a^v b a^j) \leq \left( \sum_{j \in J} P_0 b a^M b a^j, a^i b a^v b a^j \right) + (S_0, a^j)$$

we have

$$\left( \sum_{j \in J} P_0 b a^M b a^j, a^i b a^v b a^j \right) \geq (S_0, a^j) > 0.$$  

Then we have

$$Q \subseteq J, \forall j \in Q \quad v \in M_j \neq \emptyset. (4.1)$$

Remember that $1 \in \text{supp}(P_0) = a^j$. Let us consider $C_1 \geq 0$:

$$C_1 = \sum_{i \in I} a^i b a^L (a - 1) S_0 + P_0 b S_0 + \sum_{j \in J} a^M (a - 1) P_0 b a^j \geq 0.$$  

Fix $i = 0$ in $C_1 \geq 0$. By

$$0 \leq b a^L (a - 1) S_0 + b S_0 - \sum_{j \in J} a^M b a^j \leq b (a^L (a - 1) S_0 + S_0)$$

we get $b (a^L (a - 1) S_0 + S_0) \geq 0$. This inequation implies $L_0 \neq \emptyset$ since $S_0 \notin \mathbb{N} \langle a \rangle$. So we have

$$L_0 \neq \emptyset, a^L (a - 1) S_0 + S_0 \geq 0 \quad (4.2)$$

Now $P_0, S_0 (1 + a^L (a - 1)) \in \mathbb{N} \langle a \rangle$ imply

$$P_0 S_0 (1 + a^L (a - 1)) = \frac{a^n - 1}{a - 1} (1 + a^L (a - 1)) \in \mathbb{N} \langle a \rangle.$$  

By Lemma 3.2(iv) $P_0 S_0 (1 + a^L (a - 1))$ has coefficients 0, 1. So

$$P_0$$

has coefficients 0, 1. (4.3)

In the following we will set $P_0 = a^j$ and $-(S_0, a^j) = x_j$, for any $j \in Q$. 
We come back to $C_2 \geq 0$. By fixing $i=0$ and $j \in Q$ in this inequation we get
\[ 0 \leq ba^M(a-1)a^M + ba^M(a-1) - 2ja^Lb^L \leq a^M(a-1)b^L. \]
So we have
\[
\forall j \in Q \quad a^{L_0 + M_j}(a-1) + a^{M_j} - \gamma j a^{L_0} \geq 0
\]
\[ \text{i.e.} \quad \gamma j a^{L_0} + a^{L_0 + M_j} \leq a^{L_0 + M_j} + 1 + a^{M_j} \quad (4.4)
\]
Consequently
\[
\forall \alpha \in \mathbb{N} \quad a^{L_0 + M_j}(a-1) + a^{M_j} + \alpha a^{L_0} \geq 0.
\]
Moreover, let $v = \min L_0$. We get
\[
1 \leq \gamma j = \gamma j(a^{L_0}, a^v) \leq \gamma j(a^{L_0} + a^{L_0 + M_j}, a^v)
\]
\[
\leq (a^{L_0 + M_j} + 1, a^v) + (a^{M_j}, a^v) = (a^{M_j}, a^v) \leq 1.
\]
These inequations imply
\[
\forall j \in Q \quad \gamma j = 1, \min M_j > 0 \text{ and } v \in M_j.
\]

Let $j \in Q, \alpha \in \mathbb{N}$. Define $a^H = a^{M_j} + \gamma\alpha^{L_0} + a^{L_0 + M_j}(a-1)$. By (4.5) we have that $a^H$ is in $\mathbb{N}(a)$. Moreover (4.6) imply
\[
(a^H, a^v) = (a^{M_j}, a^v) + \alpha(a^{L_0}, a^v) = 1 + \alpha
\]
(4.7)

Now, by fixing $i \in I$ and $j \in Q$ in the inequation $C_1 \geq 0$ we get
\[
0 \leq a^{M_j}(a-1)a^I - a^I + \sum_{i \in I} (a^{L_0}(a-1)S_0, a^I) a^I \leq a^{M_j}(a-1)a^I + \gamma a^I
\]
for any positive integer
\[
\alpha > \max_{i \in I} ((a^{L_0}(a-1)S_0, a^I) - 1).
\]

So, by (4.2) for any $j \in Q$ there exists $\alpha \in \mathbb{N}, \alpha > 0$ such that
\[
0 \leq \frac{a^n - 1}{a^I - 1} (1 + a^{L_0}(a-1)) (x + a^{M_j}(a-1)) - x \left( \frac{a^n - 1}{a^I - 1} + a^H(a^n - 1) \right)
\]
(4.8)

where $a^H = a^{M_j} + a^{L_0 + M_j}(a-1) + \alpha a^{L_0}$.

By (4.5) we have $a^H \in \mathbb{N}(a)$. By (4.7) we have $(a^H, a^v) = 1 + \alpha$. On the other hand, by Lemma 3.2(iv) (applied to (4.8) with $t = v$) we have $(a^H, a^v) \leq \alpha$. This contradiction concludes the proof. □

6. Structure of 3-codes

In this section we characterize the structure of 3-codes. Let $C$ be a 3-code and $(P, S)$ a factorization of $C$. By Theorem 5.1, $P, S$ have coefficients 0 or 1. By Theorem 4.4,
(P, S) verifies one of the following three properties:

(i) $P \in \mathbb{N}\langle a \rangle$,
(ii) $S \in \mathbb{N}\langle a \rangle$,
(iii) $P = P_0 + P_1, S = S_0 + S_1$.

It exists [12] an algorithm to construct all the 3-codes that verify (i) or (ii) and more generally factorizing codes $C - 1 = P(A - 1)S$ such that $P \subseteq a^*$ and $S \subseteq \{a, b\}$ (or symmetrically $S \subseteq a^*$ and $P \subseteq \{a, b\}$). The algorithm uses Krasner factorizations and Hajós factorizations of $\mathbb{Z}_n$ as described in Proposition 2.5.

**Theorem 6.1** ([12]). $C$ is a 3 code with $a^n \in C$ that verifies (i) (resp. (ii)) if and only if $C$ (resp. the reverse $C^*$ of $C$) satisfies the equation

$$C - 1 = P_0(A - 1)(S_0 + S_1 + S_2) = a' \left( (A - 1) \left( a' + \sum_{j \in J} a^M b a^j + \sum_{w \in S} a^M b w \right) \right)$$

where $(I, J)$ is a Krasner factorization of $\mathbb{Z}_n$ and for any $w \in S_2$,

$$M_j, M_w \subseteq \mathbb{N}; \quad a'(1 + u^{a-1}(a-1)) > 0, \quad a'(1 + a^M(a-1)) > 0.$$

**Example 6.2** ([7]). $C = \{a^4, b, ba, a^2ba, a^6b, aba^2b, ba^3b, a^2ba^3b, b^2a^2b, ba^3ba^2b, ba^2b^2a^2b, a^2ba^3ba^2b, a^2ba^4ba^2b\}$ is a 3-code given by

$$C - 1 = a^{0,2} (A - 1) (a^{0,11} + a^{12,3} b + a^{10,3,4} b a^2 b)$$

Let $C$ be a 3-code that verifies (iii). Let $n$ be the positive integer such that $a^n \in C$. By Remark 4.1 and by Theorem 4.2, we can suppose that there exist finite subsets $I, J, L_i (i \in I), M_i (t \in T)$ of $\mathbb{N}$ such that

$$P_0 = a^I, \quad S_0 = a^J, \quad P_1 = \sum_{i \in I} a^i b a^I, \quad S_1 = \sum_{i \in I} a^M b a^I$$

(otherwise we turn $C$ into its reverse $C^*$).

The following theorem characterizes the factorizations $(P, S)$ of a 3-code which verifies (iii). More precisely it characterizes the pairs $(P_1, S_1)$ in a factorization of these codes. Indeed we can see that $(P_0, S_0)$ is a Krasner factorization of $\mathbb{Z}_n$. Consequently we have a description of the structure of the corresponding codes.

**Theorem 6.3.** Let $(P, S)$ be a pair of polynomials in $\mathbb{N}\langle A \rangle$ such that

$$P = a' + \sum_{i \in I} a^i b a^I, \quad S = a^J + \sum_{i \in I} a^M b a^I$$

where $(I, J)$ is a Krasner factorization of $\mathbb{Z}_n$ and $T, L_i (i \in I), M_i (i \in T)$ are subsets of $\mathbb{N}$.

Then, we have $P(A - 1)S + 1 \in \mathbb{N}\langle A \rangle$ if and only if $(P, S)$ verify the following conditions:

1. $\forall i \in I a^{L_i} = a^{L_i} (a - 1) a^J + a^J > 0$,
2. $T \subseteq \bigcup_{i \in I} R_i$. 


(3) \( \forall t \in T \) set \( I_t = \{ i \in I \mid t \in R_i \} \). Then we have
\[
a^{M_i} (a-1)a^i + a^t \geq a^{M_i} (a-1)a^i + a^t \geq 0,
\]

(4) \( \forall i \in I, t \in T \) if \( t \not\in J \) then \( a^{L_i} (a-1)a^{M_i} + a^t \geq 0 \), if \( t \in J \) then \( a^{L_i} (a-1)a^{M_i} + a^{M_i} + a^t \geq 0 \).

**Proof.** Let \((P, S)\) be a pair of polynomials in \( \mathbb{N} \langle A \rangle \) such that
\[
P = a^t + \sum_{i \in I} a^t b a^{L_1}, \quad S = a^t + \sum_{i \in I} a^t b a^t
\]
where \((I, J)\) is a Krasner factorization of \( \mathbb{Z}_n \) and \( T, L_i (i \in I), M_i (t \in T) \) are subsets of \( \mathbb{N} \).

By Theorem 2.2, Theorem 5.1 and Theorem 4.4, \( C = P(A-1)S + 1 \geq 0 \) if and only if \( C \) is a 3-code that verifies (iii). Then \( C_i \geq 0 \), where \( i \in \{0, 1, 2, 3\} \).

Suppose \( C = P(A-1)S + 1 \geq 0 \). Let us prove that \( a^t a^t (1 + a^{M_i} (a-1)) \geq 0 \), for any \( t \in T \). As in Theorem 5.1 we can prove that there exists \( x \in \mathbb{N}, x > 0 \) such that \( a^t (x + a^{M_i} (a-1)) \geq 0 \). Indeed, for any \( i \in I \) set \( x_i = (a^{t_i} (a-1)a^t_i + a^t_i, a^t_i) \). By Remark 4.1, we have
\[
C_i = \sum_{i \in I} a^t b a^{L_1} (a-1)a^t_i + \sum_{i \in T} a^t b a^{L_1} + a^t b a^t \geq 0.
\]
Then for any \( h \in \mathbb{N} \) we have
\[
0 \leq (C_1, a^h b a^h) = \left( a^{M_i} (a-1)a^t + \sum_{i \in I} a^t_i, a^h \right) \leq (a^{M_i} (a-1)a^t + x a^t, a^h)
\]
where \( x \) is any positive integer such that \( x > \max_{i \in I} x_i \).

Consequently \( a^t a^t (x + a^{M_i} (a-1)) \geq 0 \). So, by Lemma 3.2(iv), \( a^t a^t (1 + a^{M_i} (a-1)) \) has coefficients 0, 1.

Let us prove (1). Assume the contrary, there exist \( i \in I, h \in \mathbb{N} \) such that \( (a^{L_i} (a-1)a^t + a^t, a^h) < 0 \). Consequently we have
\[
0 \leq (C_1, a^h b a^h)
\]
\[
= \left( \sum_{i \in I} a^t b a^{L_1} (a-1)a^t_i + a^t b a^h \right) + \left( \sum_{i \in T} a^t b a^{L_1} a^t_i b a^h \right)
\]
\[
< \left( \sum_{i \in T} a^t b a^{L_1} a^t_i b a^h \right)
\]

This inequation implies \( h \in T \) and \( (a^{M} (a-1)a^t, a^i) > 0 \). So, by \( (a^t, a^t) > 0 \) we have \( a^t (1 + a^{M_i} (a-1)), a^t \) \( \geq 1 \). On the other hand \( a^t a^t (1 + a^{M_i} (a-1)) \) has coefficients 0, 1. Thus we get
\[
\exists j \in J \setminus 0, q \in \mathbb{N} : q + j = i, (a^t (1 + a^{M_i} (a-1)), a^q) < 0.
\]
Remember that \( a'(x + a^{M_n}(a-1)) \geq 0 \). So, by \( a'(x + a^{M_n}(a-1), a^q) \geq 0 \) and \( x > 0 \) we get \( (a'(x-1), a^q) > 0 \), i.e. \( q \in I \). Consequently we have \( a'(a'-1) = (a^q-1)/(a-1) \) and 
\[ q + j = i + 0 \in I + J \] with \( j \neq 0, i \neq 0 \) i.e. a contradiction.

By Proposition 2.5, \( a^{R_i} = a^{k_i(a-1)}a^j + a^j \) has coefficients 0, 1.

Let us prove (2). Let \( t \in T \) be such that \( M_t \neq 0 \) and \( m = \min M_t \). We have

\[ 0 \leq (C_1, a^m b a^i) = \left( \sum_{i \in I} a^i b a^i, a^m b a^i \right) + \left( \sum_{i \in J} a^{M_t}(a-1)a^i, a^m b a^i \right) \]

Thus (2) follows. By fixing \( t \in T \) in \( C_1 \geq 0 \) we get (3). By fixing \( i \in I \) and \( t \in T \) in \( C_2 \geq 0 \) we get (4).

Conversely, suppose that \((P, S)\) verify (1), (2), (3) and (4). Then it is clearly evident that \( C_i \geq 0 \), where \( i \in \{0, 1, 2, 3\} \). Thus \( \mathbb{C} = P(A-1)S + 1 \in \mathbb{N} \langle A \rangle \).

Inequalities in (1) and (3) show that \( I_\alpha (i \in I) \) and \( M_\alpha (t \in T) \) are particular sets related to the Hajós factorizations of \( \mathbb{Z}_\alpha \) (see Proposition 2.5). The description of the structure of these sets and their relation with 2-codes can be found in [12].

**Theorem 6.4 ([12]).** \( C \) is a 2-code with \( a^* \in \mathbb{C} \) if and only if \( C \) or the reverse \( C^- \) of \( C \) satisfies the equation

\[ C - 1 = a'(A-1) (a^j + \sum_{j \in J} a^{M_j} b a^j) \]

where \((I, J)\) is a Krasner factorization of \( \mathbb{Z}_\alpha \) and for any \( j \in J \),

\[ M_j \in \mathbb{N}, \quad a^i(1 + a^{M_j}(a-1)) \geq 0. \]

By this theorem we can see that any 3-code can be constructed starting from a 2-code. For instance, the 3-code \( C \) [7] defined by

\[ C - 1 = (a^{[0,1]} + a^2 b a^{[0,3,4]}) (A-1) (a^{[0,2]} + b + a^{[0,1]} b a^2) \]

can be constructed starting from the 2-code

\[ C^- - 1 = a^{[0,1]} (A-1) (a^{[0,2]} + b + a^{[0,1]} b a^2). \]

The 3-code \( C \) defined by

\[ C - 1 = (a^{[0,2]} + b) (A-1) (a^{[0,1]} + ba) \]

can be constructed starting from the 2-code

\[ C^- - 1 = (a^{[0,2]} + b) (A - 1) a^{[0,1]}. \]

**Example 6.2 (continued).** The 3-code \( C \) can be constructed starting from the 2-code

\[ C - 1 = a^{[0,2]} (A - 1) (a^{[0,1]} + a^{[2,3]} b). \]
Acknowledgements

I would like to thank C. Reutenauer for the many encouragements throughout the course of this work.

This work was partially supported by the Istituto Nazionale di Alta Matematica (Roma, Italy), by P.R.C. Math. et Inf. (Paris, France) and by contract ESPRIT-EBRA ASMICS n° 3166.

References