Journal of Pure and Applied Algebra 36 (1985) 167–186
North-Holland

NONCOMMUTATIVE FACTORIZATION OF VARIABLE-LENGTH CODES

Christophe REUTENAUER
CNRS (LITP), Institut de Programmation, 4 place Jussieu, 75005 Paris, France

Communicated by S. Eilenberg
Received 17 January 1984

We prove a noncommutative version of a theorem of Schützenberger on the factorization of variable-length codes. As consequences, we obtain a positive answer to a weak form of the 'factorization conjecture, a complete characterization of maximal and finite codes and a noncommutative extension of an invariance property due to Hansel and Perrin.

1. Introduction

A (variable-length) *code* is a free subset of a free monoid; more formally, it is the basis of some free submonoid. The theory of these codes (not to be confused with error-detecting codes) was first developed by M.P. Schützenberger. A major problem in this theory is to factorize codes, that is, considering the characteristic formal power series of a code (in the noncommutative formal power series algebra), to find a factorization of that series, or of its commutative image.

Let A be some finite set and A^* the free monoid generated by A. Let C be a code and denote also by C its characteristic series, which is an element of the $\mathbb{Z}$-algebra $\mathbb{Z}\langle\langle A\rangle\rangle$ of noncommutative formal power series on A. Let $\varrho : \mathbb{Z}\langle\langle A\rangle\rangle \to \mathbb{Z}[[A]]$ be the canonical homomorphism. Schützenberger showed that, if C is a maximal and finite code, then there exists in the algebra of commutative polynomials, $\mathbb{Z}[A]$, a factorization of the form

$$\varrho(C) - 1 = PS(\varrho(A) - 1)(d + (\varrho(A) - 1)Q)$$

where

(i) $S = 1$ if and only if C is a *prefix* code.
(ii) $P = 1$ if and only if C is a *suffix* code.
(iii) d is the *degree* of C.

See [25] and also [14] and [1].

Our main result (Theorem 1 of Section 2) is a noncommutative version of this result: for such a code, there exists in the algebra of noncommutative polynomials

$\mathbb{Z}\langle A\rangle$ a factorization

$$C-1=P(d(A-1)+(A-1)Q(A-1))S$$

with the same conditions on P, S and d.

This result gives also a positive answer to a weak form of the *factorization conjecture* of Schützenberger: for such a code, there exist noncommutative polynomials X and Y, with coefficients 0 or 1, such that

$$C-1=X(A-1)Y. \tag{1}$$

Theorem 1 implies that such a factorization exists, at least with X, Y with integer coefficients.

Another result (Theorem 2 of Section 2) allows us to characterize completely maximal and finite codes: a subset C of A^*, not containing the empty word, is a maximal and finite code, if and only if there is a factorization of the form (1) for some polynomials X, Y in $\mathbb{Z}\langle A\rangle$.

For other work on the factorization conjecture, see Restivo [22], Césari [5], Perrin [18], Boë [3] and Perrin and Schützenberger [19]. In the latter is shown that, for any code C, the quotient

$$(\varrho(C)-1)/(\varrho(A)-1)$$

has nonnegative coefficients if and only if C is *commutatively equivalent to a prefix code* (i.e. there is some prefix code C' such that $\varrho(C)=\varrho(C')$), and that this is the case for *very pure codes*. The commutative equivalence was proved also for a special class of codes by Mauceri and Restivo [17]. A weaker form of this problem is the so-called *triangle conjecture*, which was studied by Perrin and Schützenberger [20], Hansel [12], Pin and Simon [21], De Felice [10] and finally by Shor [26], who showed that it is false in general. So the commutative equivalence is not true in general, but the problem remains open for finite and maximal codes (conjecture from Schützenberger).

In the last section, we give some applications of Theorem 1. The main one is a noncommutative version of a probabilistic invariance property due to Hansel and Perrin [13]: the Bernoulli measure of the set of *contexts* of a word with respect to a given maximal and finite code does not depend on that word. This result may be obtained as a corollary of an algebraic result on the set of contexts of a word (see Section 7, Corollaries 3 and 4).

For a general survey about codes, see the book of Berstel and Perrin [1].

The proof of Theorem 1 uses a double technique:

(1) The use of the structure of the minimal ideal of the syntactic monoid of C^* (the submonoid generated by C); this structure is given by the theorem of Suschkewitsch, and its use in coding theory was introduced by Schützenberger. It allows to establish equations of the form

$$A^*=YC^*X+Z$$

where X, Y, Z are finite subsets of A^* (eqs. (3.2) and (3.3)).

This equation is another weak form of the factorization (indeed, by inversion, (1) may be written as $A^* = YC^*X$). The proof of these equations uses a generalization of an idea of Boë [3], who studied some special class of codes.

(2) These equations are treated in the polynomial algebra and its field of fractions, using mainly the euclidean algorithm of Cohn [8] and the techniques he developped. We need also some arithmetical lemmas on polynomials with integer coefficients and on the factorization of polynomials which are equal to a scalar modulo the right ideal generated by $A-1$: Gauss' lemma, applications to continuant polynomials.

One byproduct of the proof presented here is a new proof of Schützenberger's factorization theorem [25]: the probabilistic and linear techniques of [25] are replaced by the use of the factoriality of $\mathbb{Z}[A]$, see [23] and Section 6.

A weak form of these results is already in [23] and [24].

2. Results

Let A be a finite alphabet and A^* be the free monoid generated by A. An element of A^* is called a *word*, and the neutral element of A is the *empty word*, denoted by 1. An element of A is called a *letter*. The length of a word w is denoted by $|w|$.

A *code* C is a subset of A^* such that for any words $u_1, \ldots, u_n, v_1, \ldots, v_p$ in C verifying

$$u_1 \cdots u_n = v_1 \cdots v_p$$

one has $n = p$ and $u_i = v_i$ for any i in $\{1, \ldots, n\}$.

In other words, any word in C^* (= the submonoid generated by C) has only one factorization in elements of C.

A code is called *maximal* if it is not a proper subset of any code.

A code C is *prefix* (resp. *suffix*) if no word in C is a left (resp. a right) factor of another word in C. Note that either of these conditions implies that C is a code, if $1 \notin C$ (see [1], [11], [15]).

Denote by $\mathbb{Q}\langle A\rangle$ (resp. $\mathbb{Q}\langle\langle A\rangle\rangle$) the algebra of noncommutative polynomials (resp. formal power series) generated by A over $\mathbb{Q}$. An element P of $\mathbb{Q}\langle A\rangle$ is a finite linear combination of words

$$P = \sum_{w \in A^*} (P, w)\, w, \qquad (P, w) \in \mathbb{Q}$$

while an element S of $\mathbb{Q}\langle\langle A\rangle\rangle$ is an infinite linear combination

$$S = \sum_{w \in A^*} (S, w)\, w, \qquad (S, w) \in \mathbb{Q}.$$

A series S is invertible in $\mathbb{Q}\langle\langle A\rangle\rangle$ if and only if its constant term is nonzero, that is, if $(S, 1) \neq 0$. A particular case is a series of the form $S = 1 - T$, where $(T, 1) = 0$. Then the inverse of S is

$$(1 - T)^{-1} = \sum_{n \geq 0} T^n.$$

This sum will also be denoted by T^*:

$$T^* = \sum_{n \geq 0} T^n.$$

A subset L of A^* will be identified with its *characteristic series*

$$L = \sum_{w \in L} w.$$

Note that if C is a code, then the sum

$$\sum_{n \geq 0} C^n$$

is the characteristic series of C^*; hence the star notation is unambiguous:

$$C^* = \sum_{n \geq 0} C^n = (1 - C)^{-1}.$$

Let C be a maximal and finite code. Let M be the *syntactic monoid* of C^* (that is, the quotient monoid of A^* by the biggest congruence for which C^* is a union of classes, see [11], [15]) and let

$$\varrho : A^* \to M$$

be the canonical monoid homomorphism. Note that, by definition of M and ϱ

$$C^* = \varrho^{-1}\varrho(C^*).$$

By Kleene's theorem ([1], [11], [15]), M is a finite monoid. Hence M contains an ideal $\mathcal{I}$ which is contained in any ideal of M: this ideal is called the *minimal ideal* of M. By Suschkewitsch's theorem ([6], [15]), $\mathcal{I}$ is equal to the disjoint union of the minimal right (resp. left) ideals of M; furthermore, for any minimal right (resp. left) ideal R (resp. L) of M, the intersection $R \cap L$ is a group; these groups are all isomorphic.

By a theorem of Schützenberger ([11], [15], [25]), C^* intersects all ideals of A^* (C being maximal). Hence $\varrho(C^*)$ intersects $\mathcal{I}$. In particular, there exists some minimal right (resp. left) ideal R (resp. L) of M such that $\varrho(C^*)$ intersects the group $G = R \cap L$. The intersection

$$H = G \cap \varrho(C^*)$$

is then a subgroup of G (being a subsemigroup of a finite group). By definition

$$d = [G : H]$$

is the *degree* of the code C. One shows that d does not depend on R and L. A code of degree 1 is called *synchronizing*.

Remark. The degree of C may defined in various ways. One elegant way is to consider infinite words, that is, mappings $\mathbb{Z} \to A$. Then, define the decomposition in C of such an infinite word (in an evident way). The degree of C is then the minimum

number of decompositions of the periodic infinite words ([2], [27]). It is always ≥ 1, C being maximal.

Our main result is

Theorem 1. *Let C be a finite and maximal code. Then there exist polynomials X, Y, Z in $\mathbb{Z}\langle A\rangle$ such that*

$$C-1=X(d(A-1)+(A-1)Z(A-1))Y$$

and

(i) *d is the degree of C,*

(ii) *C is prefix (resp. suffix) if and only if $Y=1$ (resp. $X=1$).*

Note that one has then in particular: $C-1=X'(A-1)Y'$ for some polynomials X', Y'. This last statement admits a converse, which is the following result. Note that this result also implies the 'if' part of condition (ii) in Theorem 1.

Theorem 2. *Let $C\in\mathbb{N}\langle A\rangle$ without constant term (i.e. $(C,1)=0$). Suppose $C-1=X(A-1)Y$ for some polynomials X, Y in $\mathbb{Q}\langle A\rangle$. Then C is a finite and maximal code. Furthermore, if $Y\in\mathbb{Q}$ (resp. $X\in\mathbb{Q}$), then C is a prefix (resp. suffix) code.*

We prove first Theorem 2. For this, define an algebra homomorphism $\pi:\mathbb{Q}\langle A\rangle\to\mathbb{Q}$ by $\pi(a)=1/\mathrm{card}(A)$ for each letter a in A.

Furthermore, for any series S in $\mathbb{Q}\langle\langle A\rangle\rangle$, define the *support* of S to be the following subset of A^*:

$$\mathrm{supp}(S)=\{w\in A^*\,|\,(S,w)\neq 0\}.$$

Proof of Theorem 2. Because $1-C=X(1-A)Y$ and because $1-C$ is invertible in $\mathbb{Q}\langle\langle A\rangle\rangle$ by assumption, X and Y are also invertible in $\mathbb{Q}\langle\langle A\rangle\rangle$, hence $(1-C)^{-1}=Y^{-1}(1-A)^{-1}X^{-1}$. Hence

$$(1-A)^{-1}=Y(1-C)^{-1}X.$$

Note that

$$(1-A)^{-1}=\sum_{n\in\mathbb{N}}A^n=A^* \quad\text{and}\quad (1-C)^{-1}=\sum_{n\in\mathbb{N}}C^n.$$

Thus

$$A^*=Y\Big(\sum_{n\in\mathbb{N}}C^n\Big)X. \tag{2.1}$$

This implies that any word in A^* may be written as $yc_1\cdots c_nx$ for some y in $\mathrm{supp}(Y)$, $c_1\cdots c_n$ in $\mathrm{supp}(C)$ and x in $\mathrm{supp}(X)$. Then take any word w in A^* and u a word longer than $\deg(X)$, $\deg(Y)$. One has

$$uwu=yc_1\cdots c_nx,$$

hence, by the choice of u, w is factor of $c_1 \cdots c_n$. Thus any word is factor of some word in the submonoid generated by supp(C); said otherwise: this submonoid intersects any ideal of A^*. In the terminology of [4], supp(C) is a *complete* subset of A^*. Hence, by [4], one has

$$\pi(\mathrm{supp}(C)) \geq 1.$$

But, because $C-1=X(A-1)Y$ and $\pi(A)=1$, one has also

$$\pi(C)=1.$$

Because the coefficients of C are nonnegative, we obtain

$$1=\pi(C)\geq\pi(\mathrm{supp}(C))\geq 1.$$

Hence $C=\mathrm{supp}(C)$. Thus C is a complete and finite subset of A^* with $\pi(C)=1$. Hence C is a maximal code, by [4].

Suppose now that $Y\in\mathbb{Q}$. Then by (2.1), any word is a left factor of some word in C^*, that is, C^* intersects any right ideal of A^*. By a theorem of Schützenberger ([1], [15]), C is therefore a prefix code. □

Remark. If in Theorem 2, one puts the additional hypothesis $X, Y\in\mathbb{N}\langle A\rangle$, then the proof is easier (and already known): indeed, (2.1) implies then that the coefficients of $\sum_{n\in\mathbb{N}} C^n$ are 0, 1: hence C is a code (and the coefficients of X, Y are 0, 1).

Recall that the 'factorization conjecture' of Schützenberger just tells that such a factorization (with $X, Y\geq 0$) always exists, when C is a finite and maximal code.

We give a corollary to Theorems 1 and 2, which characterizes completely finite and maximal codes.

Corollary. *Let C be a finite set of words not containing the empty word. Then the following conditions are equivalent:*

(i) *C is a finite and maximal code.*

(ii) *There exist polynomials P, S in $\mathbb{Z}\langle A\rangle$ such that*

$$C-1=P(A-1)S.$$

The following sections are devoted to the proof of Theorem 1.

3. Some equations

Let C be a finite and maximal code, $C\subset A^*$, M the syntactic monoid of C^* (the submonoid of A^* generated by C) and $\varrho: A^*\to M$ the canonical monoid homomorphism. Recall that M is finite, hence has a minimal ideal $\mathcal{I}$, that $\mathcal{I}$ intersects $M'=\varrho(C^*)$ and that $C^*=\varrho^{-1}(M')$.

By the theorem of Suschkewitsch, there is some minimal right (resp. left) ideal

R (resp. L) of M such that M' intersects the finite group $G=R\cap L$; then $H=M'\cap G$ is a subgroup of G, whose index is $d=[G:H]$, the degree of the code C.

Let $x_1,\dots,x_d,y_1,\dots,y_d$ be words in $\varrho^{-1}(G)$ such that each $\varrho(x_i)$ is the inverse of $\varrho(y_i)$ in G, that $\varrho(x_1)=\varrho(y_1)=e$ (the neutral element of G) and that the classes $H\varrho(x_1),\dots,H\varrho(x_d)$ (resp. $\varrho(y_1)H,\dots,\varrho(y_d)H$) are all the right (resp. left) classes of G mod. H.

Let j, $1\le j\le d$, and w a word. Then there exists one and only one i, $1\le i\le d$, such that $x_iwy_j\in C^*$. Indeed, the latter condition is equivalent to $\varrho(x_iwy_j)\in M'$, and because $\varrho(x_i)\in R$, $\varrho(y_j)\in L$, hence $\varrho(x_iwy_j)\in G$, it is still equivalent to $\varrho(x_iwy_j)\in H$. But $\varrho(x_iwy_j)\in H\Leftrightarrow e\varrho(wy_j)=\varrho(y_ix_iwy_j)\in\varrho(y_i)H$; this proves the claim.

We use now, to establish eqs. (3.2) and (3.3), some techniques already used in [14] and [25].

Define $S_i'=\{u\mid x_iu\in C^*\}$ and $P_j'=\{v\mid vy_j\in C^*\}$. Further, let $S_i=S_i'\setminus S_i'C^+$ and $P_j=P_j'\setminus C^+P_j'$ where $C^+=C^*\setminus 1$.

Note that each word u in S_i' is of the form $u=sc_1\cdots c_n$ for some proper right factor s of some word in C and some $c_1,\dots,c_n$ in C ($n\ge 0$); if further u is in S_i, then $n=0$ and $u=s$. It implies that S_i is finite. Similarly, P_j is finite.

Now, if a word w is in the product $S_iC^*P_j$, then $x_iwy_j\in C^*$. Conversely, if $x_iwy_j\in C^*$ and w is not factor of any word in C, then $w\in S_iC^*P_j$. This and the previous claim imply the existence of some finite set of words G_j such that

$$A^*=\bigcup_{1\le i\le d}S_iC^*P_j\cup G_j \qquad \text{(disjoint union)}. \tag{3.1}$$

But the product $S_iC^*P_j$ is *unambiguous*, that is, $smp=s'm'p'$ with $s,s'\in S_i$, $m,m'\in C^*$, $p,p'\in P_j$ implies $s=s'$, $m=m'$ and $p=p'$. Indeed, one has then $x_ismpy_j=x_is'm'p'y_j$, so one may conclude by unique factorization.

That unambiguity may be formulated otherwise: in $\mathbb{Z}\langle\langle A\rangle\rangle$, the product $S_iC^*P_j$ is a series with coefficients 0, 1. So, by (3.1) we obtain, in $\mathbb{Z}\langle\langle A\rangle\rangle$, for any j:

$$A^*=\sum_{1\le i\le d}S_iC^*P_j+G_j \tag{3.2}$$

where G_j is a finite subset of A^*.

Symmetrically, for any i:

$$A^*=\sum_{1\le j\le d}S_iC^*P_j+D_i \tag{3.3}$$

where D_i is a finite subset of A^*.

Now, when is C prefix, then for any words u,v

$$u,uv\in C^*\Rightarrow v\in C^*,$$

see [1], [11] or [15].

Hence, if C is prefix, $S_1'=C^*$ (because $x_1\in C^*$), thus

$$C \text{ prefix}\Rightarrow S_1=1. \tag{3.4}$$

Symmetrically

$$C \text{ suffix} \Rightarrow P_1 = 1. \tag{3.5}$$

4. Proof of Theorem 1

A polynomial $P \in \mathbb{Q}\langle A\rangle$ is called *primitive* if $P \neq 0$, $P \in \mathbb{Z}\langle A\rangle$ and if its coefficients have no nontrivial common divisor in $\mathbb{Z}$.

For each nonzero polynomial $P \in \mathbb{Q}\langle A\rangle$, there exists a unique positive rational number $c(P)$, the *content* of P, such that $P/c(P)$ is primitive. We shall write

$$P = c(P)\bar{P}.$$

Note that, for any nonzero polynomial P

$$P \text{ primitive} \Leftrightarrow c(P) = 1,$$

$$P \in \mathbb{Z}\langle A\rangle \Leftrightarrow c(P) \in \mathbb{N}.$$

Lemma 4.1 (Gauss lemma). (i) *If P, Q are primitive, then so is their product PQ.*
(ii) *For any nonzero polynomials P, Q, one has*

$$c(PQ) = c(P)\,c(Q) \quad \textit{and} \quad \overline{PQ} = \bar{P}\bar{Q}.$$

The proof of this lemma is similar to the proof in the commutative case; so we omit it.

We shall use the fact that $\mathbb{Q}\langle A\rangle$ possesses a 'universal field of fractions', U, such that $\mathbb{Q}\langle A\rangle$ is a subalgebra of U, see Cohn [8, chapter 7].

This (skew) field possesses the following property.

Proposition 4.2 (Cohn [9, corollary, p. 30]). *Let P_1, P_2, P_3, P_4 be nonzero polynomials such that $P_1 P_2^{-1} P_3 = P_4$ in U. Then there exist polynomials Q_1, Q_2, Q_3, Q_4 such that*

$$P_1 = Q_1 Q_2, \quad P_2 = Q_3 Q_2, \quad P_3 = Q_3 Q_4, \quad P_4 = Q_1 Q_4.$$

We use in fact the following arithmetical version of this result.

Corollary 4.3. *Let P_1, P_2, P_3, P_4 be nonzero polynomials in $\mathbb{Z}\langle A\rangle$ such that $P_1 P_2^{-1} P_3 = P_4$ in U. Then there exist polynomials Q_1, Q_2, Q_3, Q_4 in $\mathbb{Z}\langle A\rangle$ such that*

$$P_1 = Q_1 Q_2, \quad P_2 = Q_3 Q_2, \quad P_3 = Q_3 Q_4, \quad P_4 = Q_1 Q_4.$$

Proof. By Proposition 4.2, we have $P_1 = Q_1 Q_2$, $P_2 = Q_3 Q_2$, $P_3 = Q_3 Q_4$, $P_4 = Q_1 Q_4$ for some nonzero polynomials Q_1, Q_2, Q_3, Q_4 in $\mathbb{Q}\langle A\rangle$. Let $c_i = c(Q_i)$, $i = 1, 2, 3, 4$

Then by Lemma 4.1:

$$c(P_1)=c_1c_2,\quad c(P_2)=c_3c_2,\quad c(P_3)=c_3c_4,\quad c(P_4)=c_1c_4.$$

Thus $c(P_4)=c(P_1)c(P_3)/c(P_2)$. As by hypothesis $c(P_i)\in\mathbb{N}$, this relation implies the following factorizations in $\mathbb{N}$:

$$c(P_1)=d_1d_2,\quad c(P_2)=d_3d_2,\quad c(P_3)=d_3d_4,\quad c(P_4)=d_1d_4.$$

Furthermore, again by Lemma 4.1:

$$\bar{P}_1=\bar{Q}_1\bar{Q}_2,\quad \bar{P}_2=\bar{Q}_3\bar{Q}_2,\quad \bar{P}_3=\bar{Q}_3\bar{Q}_4,\quad \bar{P}_4=\bar{Q}_1\bar{Q}_4.$$

Thus, as $P=c(P)\bar{P}$:

$$P_1=d_1\bar{Q}_1d_2\bar{Q}_2,\quad P_2=d_3\bar{Q}_3d_2\bar{Q}_2,\quad P_3=d_3\bar{Q}_3d_4\bar{Q}_4,\quad P_4=d_1\bar{Q}_1d_4\bar{Q}_4.$$

This proves the lemma. □

We use now eq. (3.2). Let

$$S=\sum_{1\le i\le d}S_i,\qquad P=\sum_{1\le j\le d}P_j,\qquad Q=\sum_{1\le j\le d}G_j.$$

Thus by (3.2), we have $dA^*=SC^*P+Q$ or

$$dA^*-Q=SC^*P. \tag{4.1}$$

Furthermore, by (3.2), $A^*=SC^*P_1+G_1$ or $A^*-G_1=SC^*P_1$. But in $\mathbb{Q}\langle\langle A\rangle\rangle$, $A^*-G_1=(1-A)^{-1}(1-(1-A)G_1)$. Thus

$$(1-A)SC^*=(1-(1-A)G_1)P_1^{-1}.$$

(Note that $1\in P_1$, hence P_1 is invertible in $\mathbb{Q}\langle\langle A\rangle\rangle$.)

Hence, by (4.1),

$$d-(1-A)Q=(1-(1-A)G_1)P_1^{-1}P \quad \text{or}$$

$$P=P_1(1-(1-A)G_1)^{-1}(d-(1-A)Q).$$

(Again, note that $1\in P_1$ implies by (3.2) that $1\notin G_1$, hence $1-(1-A)G_1$ is invertible in $\mathbb{Q}\langle\langle A\rangle\rangle$.)

This relation holds in $\mathbb{Q}\langle\langle A\rangle\rangle$, hence in the universal field of fractions U' of $\mathbb{Q}\langle\langle A\rangle\rangle$, hence also in U (because U may be canonically embedded in U', see [8, ex. 7.6.4]). Hence, we may apply Corollary 4.3 to this relation and we derive the existence of polynomials E,F,G,H in $\mathbb{Z}\langle A\rangle$ such that

$$P_1=EF,\quad 1-(1-A)G_1=GF,\quad d-(1-A)Q=GH,\quad P=EH. \tag{4.2}$$

We shall use the following lemma, in which $(A-1)$ denotes the right ideal $(A-1)\mathbb{Z}\langle A\rangle$ of $\mathbb{Z}\langle A\rangle$.

Lemma 4.4. *Let $X,Y\in\mathbb{Z}\langle A\rangle$ and $\alpha\in\mathbb{Z}$, $\alpha\neq 0$, such that $XY\equiv\alpha \bmod(A-1)$. Then $X\equiv\beta$, $Y\equiv\gamma \bmod(A-1)$, for some $\beta,\gamma\in\mathbb{Z}$ with $\alpha=\beta\gamma$.*

This lemma will be proved in the next section.

By the lemma and eq. (4.2), we have $G = \pm 1 \bmod(A-1)$, hence $H = \pm d \bmod(A-1)$. Replacing eventually H by $-H$, we obtain

$$P = E(d + (A-1)R) \tag{4.3}$$

where $R \in \mathbb{Z}\langle A\rangle$.

We use now eq. (3.3) for $i=1$, and obtain $A^* = S_1 C^* P + D_1$. As $A^* - D_1 = (1-A)^{-1}(1-(1-A)D_1)$, we have by (4.3) and inversion

$$C - 1 = E(d + (A-1)R)(1-(1-A)D_1)^{-1}(A-1)S_1.$$

Applying Corollary 4.3, we derive the existence of polynomials X, Y, Z, T in $\mathbb{Z}\langle A\rangle$ such that

$$\begin{aligned} &E(d + (A-1)R) = XY, \qquad 1-(1-A)D_1 = ZY, \\ &(A-1)S_1 = ZT, \qquad C - 1 = XT. \end{aligned} \tag{4.4}$$

We may assume that $\pi(Y) \geq 0$, where π is as in Section 2. This implies, by Lemma 4.4,

$$Y = 1 + (A-1)Y', \qquad Z = 1 + (A-1)Z' \tag{4.5}$$

for some Y', Z' in $\mathbb{Z}\langle A\rangle$. Hence $(A-1)S_1 = T + (A-1)Z'T$ which shows that

$$T = (A-1)T', \quad T' \in \mathbb{Z}\langle A\rangle. \tag{4.6}$$

Now we compute X. For this, we use the *continuant polynomials* of Cohn [7]: let $x_1, \ldots, x_n$ be polynomials and define $p_i(x_1, \ldots, x_i)$ by

$$\begin{aligned} &p_0 = 1, \qquad p_1(x_1) = x_1, \\ &p_i(x_1, \ldots, x_i) = p_{i-1}(x_1, \ldots, x_{i-1})x_i + p_{i-2}(x_1, \ldots, x_{i-2}) \quad \text{for } 2 \leq i \leq n. \end{aligned}$$

For example,

$$p_2(x_1, x_2) = x_1 x_2 + 1, \qquad p_3(x_1, x_2, x_3) = x_1 x_2 x_3 + x_1 + x_3.$$

We shall simply write $p(x_1, \ldots, x_i)$ for $p_i(x_1, \ldots, x_i)$.

We use the following

Proposition 4.5 (Cohn [7, 4(iii)]). *Let U, V, U', V' be nonzero polynomials such that $UV' = U'V$. Then there exist polynomials $U_1, x_1, \ldots, x_n, V_1$ such that $\deg(x_1), \ldots, \deg(x_{n-1}) \geq 1$ and that either*

$$\begin{aligned} &U = U_1 p(x_1, \ldots, x_n), \qquad V' = p(x_{n-1}, \ldots, x_1)V_1, \\ &U' = U_1 p(x_1, \ldots, x_{n-1}), \qquad V = p(x_n, \ldots, x_1)V_1 \end{aligned}$$

or

$$\begin{aligned} &U = U_1 p(x_1, \ldots, x_{n-1}), \qquad V' = p(x_n, \ldots, x_1)V_1, \\ &U' = U_1 p(x_1, \ldots, x_n), \qquad V = p(x_{n-1}, \ldots, x_1)V_1. \end{aligned}$$

This proposition may be explained by the following identity

$$p(x_1, \ldots, x_n)p(x_{n-1}, \ldots, x_1) = p(x_1, \ldots, x_{n-1})p(x_n, \ldots, x_1), \tag{4.7}$$

see [7]. The technical condition on the degrees comes from the fact that the x_i's are the successive quotients of the euclidean algorithm of Cohn [7] applied to U and U' (x_n, which is the first quotient, may be scalar).

We shall use the following

Lemma 4.6. *Let $x_1, \ldots, x_n$ be polynomials. Then $p(x_1, \ldots, x_n)$ and $p(x_n, \ldots, x_1)$ either are both zero or have the same content.*

Furthermore, we use the following result, where $(A-1)$ denotes the right ideal $(A-1)\mathbb{Q}\langle A\rangle$ of $\mathbb{Q}\langle A\rangle$.

Lemma 4.7. *Let $x_1, \ldots, x_n$ be polynomials such that* $\deg(x_1), \ldots, \deg(x_{n-1}) \geq 1$ *and that both $p(x_n, \ldots, x_1)$ and $p(x_{n-1}, \ldots, x_1)$ are congruent to a scalar* $\bmod(A-1)$. *Then*

$$p(x_1, \ldots, x_n) \equiv p(x_n, \ldots, x_1)$$

and

$$p(x_1, \ldots, x_{n-1}) \equiv p(x_{n-1}, \ldots, x_1) \bmod(A-1).$$

These two lemmas will be proved in the next section.

By (4.4) and (4.5), we have the relation

$$E(d+(A-1)R) = X(1+(A-1)Y').$$

We apply Proposition 4.5, Lemma 4.4 and the previous lemmas to this relation and derive the existence of polynomials $U, K, L, M, N, V \in \mathbb{Q}\langle A\rangle$ such that

$$E = UK, \quad d+(A-1)R = LV, \quad X = UM, \quad 1+(A-1)Y' = NV,$$
$$KL = MN, \quad c(K) = c(N), \quad c(L) = c(M), \tag{4.8}$$
$$K \text{ and } N \text{ (resp. } L \text{ and } M\text{) are congruent to the same scalar } \bmod(A-1).$$

Recall that for any polynomial S, we denote by $\bar{S}$ the unique primitive polynomial such that $S = c(S)\bar{S}$.

As D_1 is a characteristic polynomial, $1-(1-A)D_1$ is primitive. Hence by (4.4), Y and Z are primitive. Thus, $NV = 1+(A-1)Y' = Y$ is primitive and, by Gauss' lemma, $c(N)\,c(V) = 1$; furthermore $1+(A-1)Y' = \bar{N}\bar{V}$. Hence by Lemma 4.4, $\bar{V} = \varepsilon + (A-1)V'$ with $\varepsilon = \pm 1$ and $V' \in \mathbb{Z}\langle A\rangle$.

On the other hand, $C-1$ is primitive, hence so is X, by (4.4). It implies, by (4.4), that $d+(A-1)R$ is primitive. Thus, by (4.8) and Gauss' lemma, $d+(A-1)R = \bar{L}\bar{V}$. This implies, by Lemma 4.4, that $\bar{L} = \varepsilon d + (A-1)L'$ for some L' in $\mathbb{Z}\langle A\rangle$.

But L and M are congruent to the same scalar $\bmod(A-1)\mathbb{Q}\langle A\rangle$, hence so are also $\bar{L}$ and $\bar{M}$ (as $c(L) = c(M)$). This shows that $\bar{M} = \varepsilon d + (A-1)M'$ with $M' \in \mathbb{Q}\langle A\rangle$; ac-

tually, as $(A-1)M'=\bar{M}-\varepsilon d\in\mathbb{Z}\langle A\rangle$ and as $A-1$ is primitive, we obtain $M'\in\mathbb{Z}\langle A\rangle$, by Gauss's lemma.

As X is primitive, we have $X=\bar{X}$, hence, by Gauss' lemma and (4.8), $X=\bar{U}\bar{M}$, so that

$$X=\bar{U}(\varepsilon d+(A-1)M'). \tag{4.9}$$

Using (4.4), (4.6) and (4.9), we obtain

$$C-1=\bar{U}(\varepsilon d+(A-1)M')(A-1)T'$$

where $\bar{U}, M', T'$ are in $\mathbb{Z}\langle A\rangle$ and $\varepsilon=\pm 1$.

This shows that

$$C-1=x(\varepsilon d(A-1)+(A-1)z(A-1))y$$

with $\varepsilon=\pm 1$, $x=\pm\bar{U}$, $y=\pm T'$, $\pi(x)\geq 0$ and $\pi(y)\geq 0$.

For any polynomial P, let

$$\lambda(P)=\sum_w (P,w)\,|w|\,\pi(w).$$

Note that $\lambda(PQ)=\lambda(P)\pi(Q)+\pi(P)\lambda(Q)$.

As $\lambda(C)>0$ and $\pi(A-1)=0$, we obtain $\varepsilon=1$ (because $0<\lambda(C-1)=\pi(x)\varepsilon d\pi(y)$), which proves the formula of Theorem 1.

Suppose now that C is prefix. Then $S_1=1$ by (3.4). Hence by (4.4), $ZT=A-1$, which implies by (4.6), $A-1=Z(A-1)T'$. Hence $y=\pm T'=\pm 1$, and because $\pi(y)\geq 0$, we obtain $y=1$.

Suppose that C is suffix: then $P_1=1$ by (3.5). Then $E=\pm 1$ by (4.2), hence by (4.8), $\pm 1=\bar{U}\bar{K}$, which implies $\bar{U}=\pm 1$. As $x=\pm\bar{U}$ and $\pi(x)\geq 0$, we obtain $x=1$.

This proves Theorem 1.

5. Proof of the lemmas

Before proving Lemma 4.4, we prove the following result.

Lemma 5.1. *Let X, Y, Z be polynomials such that $Y\neq 0$, $\deg(Z)\leq\deg(Y)$ and that $XY+Z$ is congruent to a scalar* $\bmod(A-1)\mathbb{Q}\langle A\rangle$. *Then so is also X.*

Proof. (1) If P is a polynomial and w a word, define the polynomial Pw^{-1} by $Pw^{-1}=\sum_u (P,uw)\,u$. Note that if P is a word, then $Pw^{-1}=u$ if $P=uw$ and $Pw^{-1}=0$ if P does not end with w. Note also that $\deg(Pw^{-1})\leq\deg(P)-|w|$, where $|w|$ is the length of w. Let P, Q be polynomials and w a word. Then there is some polynomial P' such that

$$(PQ)w^{-1}=P(Qw^{-1})+P', \qquad \deg(P')<\deg(P) \text{ or } P=P'=0. \tag{5.1}$$

Indeed, this is easily verified when P, Q are words, and extends by linearity to polynomials.

(2) Let

$$XY+Z=d+(A-1)T \tag{5.2}$$

where $d\in\mathbb{Q}$ and $T\in\mathbb{Q}\langle A\rangle$. Choose a word w with $(Y,w)\neq 0$ and $|w|=\deg(Y)$. Note that in this case $Yw^{-1}=(Y,w)=\alpha^{-1}$, say.

By (5.1), we have $(XY)w^{-1}=X(Yw^{-1})-X'$, $\deg(X')<\deg(X)$ (we may suppose $X\neq 0$) and $((A-1)T)w^{-1}=(A-1)(Tw^{-1})+e$, $e\in\mathbb{Q}$. Hence, because $(XY+Z)w^{-1}=(XY+(A-1)T)w^{-1}$, we have

$$(Y,w)X-X'+Zw^{-1}=(A-1)(Tw^{-1})+f$$

where $f=e+dw^{-1}\in\mathbb{Q}$. It implies

$$X=\alpha X'-\alpha Zw^{-1}+\alpha(A-1)Tw^{-1}+\alpha f \tag{5.3}$$

Put the right-hand side in the initial equality, obtaining

$$d+(A-1)T=\alpha X'Y-\alpha(Zw^{-1})Y+\alpha(A-1)(Tw^{-1})Y+\alpha fY+Z$$

so that

$$\alpha X'Y+Z-\alpha(Zw^{-1})Y+\alpha fY=d-\alpha(A-1)(Tw^{-1})Y+(A-1)T.$$

Note that $\deg(Z)\leq\deg(Y)$, so that Zw^{-1} is a scalar; hence we have an equation of type (5.2) with X' instead of X. By induction on $\deg(X)$, we conclude that X' is congruent to a scalar $\bmod(A-1)\mathbb{Q}\langle A\rangle$, hence so is X, by (5.3) and the fact that $Zw^{-1}\in\mathbb{Q}$. □

Proof of Lemma 4.4. By assumption, we have $XY=\alpha+(A-1)U$ where $\alpha\in\mathbb{Z}\setminus 0$ and $U\in\mathbb{Z}\langle A\rangle$. By Lemma 5.1, we obtain $X=\beta+(A-1)T$ for some β in $\mathbb{Q}$ and T in $\mathbb{Q}\langle A\rangle$. Hence $\alpha+(A-1)U=\beta Y+(A-1)TY$ which shows that $\beta\neq 0$ (because $\alpha\neq 0$) and that $Y=\gamma+(A-1)S$ for some γ in $\mathbb{Q}$ and S in $\mathbb{Q}\langle A\rangle$. Now, X and Y are in $\mathbb{Z}\langle A\rangle$: put $a=1$ for some letter a and $b=0$ for the other letters; it shows that $\beta,\gamma\in\mathbb{Z}$. Furthermore, $X-\beta=(A-1)T\in\mathbb{Z}\langle A\rangle$, so that $T\in\mathbb{Z}\langle A\rangle$ by Gauss' lemma. Similarly $S\in\mathbb{Z}\langle A\rangle$. The relation $\alpha=\beta\gamma$ is clear. □

We come now to the proof of the results about continuant polynomials. Recall that

$$p(x_1,\ldots,x_n)=p(x_1,\ldots,x_{n-1})x_n+p(x_1,\ldots,x_{n-2}). \tag{5.4}$$

In fact, as noted in [7], $p(x_1,\ldots,x_n)$ may be obtained by the 'leapfrog construction': consider the monomial $x_1\cdots x_n$ and all monomials obtained by erasing some x_ix_{i+1} in it and by iterating this process. Then $p(x_1,\ldots,x_n)$ is just the sum of these monomials (without multiplicities). This shows that we also have

$$p(x_1,\ldots,x_n)=x_1p(x_2,\ldots,x_n)+p(x_3,\ldots,x_n).$$

But we shall use the symmetric relation:

$$p(x_n,\ldots,x_1)=x_np(x_{n-1},\ldots,x_1)+p(x_{n-2},\ldots,x_1). \tag{5.5}$$

Proof of Lemma 4.6. Induction on n.

For $n=0$ or 1, the result is clear.

Let $n \geq 2$. If $p(x_1, \ldots, x_{n-1})$ and $p(x_{n-1}, \ldots, x_1)$ are nonzero, then we conclude by induction, Gauss' lemma and the relation (4.7). Otherwise, $p(x_1, \ldots, x_{n-1}) = p(x_{n-1}, \ldots, x_1) = 0$ by induction. Then, by (5.4) and (5.5) we obtain $p(x_1, \ldots, x_n) = p(x_1, \ldots, x_{n-2})$ and $p(x_n, \ldots, x_1) = p(x_{n-2}, \ldots, x_1)$. Again, we conclude by induction. □

Proof of Lemma 4.7. (1) We have $\deg(x_1), \ldots, \deg(x_{n-1}) \geq 1$. We show that this implies that the degrees of $1, p(x_1), p(x_2, x_1), \ldots, p(x_{n-1}, \ldots, x_1)$ are strictly increasing. This is surely true for the two first polynomials. Let $i, 2 \leq i \leq n-1$. Then by (5.5)

$$p(x_i, \ldots, x_1) = x_i p(x_{i-1}, \ldots, x_1) + p(x_{i-2}, \ldots, x_1).$$

By induction, $\deg(p(x_{i-1}, \ldots, x_1)) > \deg(p(x_{i-2}, \ldots, x_1))$. This implies that

$$\deg(p(x_i, \ldots, x_1)) = \deg(x_i p(x_{i-1}, \ldots, x_1)) > \deg(p(x_{i-1}, \ldots, x_1)).$$

This proves the claim.

(2) We show the lemma by induction on n. Note that if the condition on the degrees is fullfilled for $x_1, \ldots, x_n$, then a fortiori for $x_1, \ldots, x_{n-1}$.

By assumption, $p(x_n, \ldots, x_1)$ is congruent to some scalar α and $p(x_{n-1}, \ldots, x_1)$ to some scalar $\beta \bmod(A-1)$. Now by Lemma 5.1, eq. (5.5) and the degree inequality of 1., we obtain that x_n is congruent to some scalar $\gamma \bmod(A-1)$. By (5.5) again, we have

$$p(x_{n-2}, \ldots, x_1) = p(x_n, \ldots, x_1) - x_n p(x_{n-1}, \ldots, x_1)$$

which shows that $p(x_{n-2}, \ldots, x_1)$ is congruent to $\alpha - \gamma\beta$. By induction we conclude that $p(x_1, \ldots, x_{n-1}) \equiv \beta$ and $p(x_1, \ldots, x_{n-2}) \equiv \alpha - \beta\gamma$. Hence by (5.4) $p(x_1, \ldots, x_n) \equiv \beta\gamma + \alpha - \beta\gamma = \alpha$, as desired. □

6. Comments

Theorem 1 gives the following formula, for each maximal and finite code C:

$$C - 1 = X(d(A-1) + (A-1)Z(A-1))Y.$$

In all known cases, especially in the Perrin's family of nonsynchronizing, indecomposable, prefix and nonsuffix codes [18], or in the Vincent's family of nonsynchronizing, indecomposable, nonprefix and nonsuffix codes [27], the polynomials X, Y, Z have nonnegative coefficients, and have even a combinatorial interpretation. This raises the question (related to the factorization conjecture) whether this is always true or not. In the case where C is biprefix (i.e. prefix and suffix), one has

$$C - 1 = d(A-1) + (A-1)Z(A-1).$$

This was already known, moreover the polynomial Z has a special combinatorial interpretation, see [1], [5], [18].

Schützenberger's factorization theorem may be easily deduced from the equations of Section 3. Indeed, from (3.2), (3.3) and (4.1), one has

$$dA^* - Q = SC^*P,$$

$$A^* - G_1 = SC^*P_1,$$

$$A^* - D_1 = S_1C^*P.$$

These three formulas easily imply

$$C - 1 = P_1(1-(1-A)G_1)^{-1}(d(A-1)+(A-1)Q(A-1))(1-D_1(1-A))^{-1}S_1. \tag{6.1}$$

Taking the commutative image, we thus obtain

$$\varrho(C) - 1 = \frac{\varrho(P_1)\varrho(S_1)(\varrho(A)-1)(d+(\varrho(A)-1)\varrho(Q))}{1+(\varrho(A)-1)T}$$

for some polynomial T in $\mathbb{Z}[A]$. As $\mathbb{Z}[A]$ is factorial and as $\mathbb{Z}[A]/(\varrho(A)-1)$ is a free commutative $\mathbb{Z}$-algebra, the polynomial $1+(\varrho(A)-1)T$ splits in 3 factors, which divide respectively $\varrho(P_1)$, $\varrho(S_1)$ and $d+(\varrho(A)-1)\varrho(Q)$ and which are equal to $\pm 1 \bmod \varrho(A)-1$. To force $+1$, one uses the operator λ (as at the end of Section 4) and to obtain conditions (i) and (ii) of Schützenberger's theorem as stated in the introduction, one uses the conditions (3.4) and (3.5) (ibid.).

7. Applications

As a first application of Theorem 1, we give a noncommutative version of a theorem of Schützenberger [25].

Corollary 1. *Let C be a maximal and finite code. If the polynomial $C-1$ has no more than two irreducible factors in $\mathbb{Z}\langle A\rangle$, then C has two of the three following properties:*

(i) *C is prefix.*
(ii) *C is suffix.*
(iii) *C is synchronizing.*

Note that if $C-1$ has only one irreducible factor, then $C=A$ and C has (trivially) the three properties.

The second application gives some information on the cardinality of a code.

Corollary 2. *Let C be a maximal and finite code. Then*

$$|C| \equiv 1 \bmod(|A|-1).$$

Proof. By Theorem 1, $C-1=P(A-1)S$ for some polynomials P, S in $\mathbb{Z}\langle A\rangle$. It suffices to apply to this equation the algebra homomorphism defined by $a\mapsto 1$ for any letter a to obtain the corollary. □

Remark. There is some connection with the Schreier formula: if H is any subgroup of finite index of the free group G generated by A and C any basis of H, then

$$|C|=1+(|A|-1)[G:H].$$

In fact, if t is any $|A|$-ary complete tree with c external nodes and d internal nodes, then

$$c=1+(|A|-1)d.$$

The Schreier formula may be obtained using this relation (see [16, Propositions I.3.7 and I.3.9]).

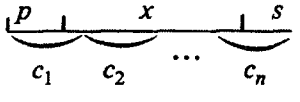
The analogy now becomes apparent if one notes that a maximal and finite prefix code on A may be viewed as a complete $|A|$-ary tree (see [1, Chapter 2]).

Let C be any code and x a word. A *context* of x in C is a couple of words (p, s) such that

$$pxs=c_1\cdots c_n \qquad (n\geq 0,\ c_i \text{ in } C)$$

where p is a proper left factor of c_1 and s is a proper right factor of c_n (if $x=1$, one admits $(1, 1)$ as a context).

This definition is illustrated by the following diagramm



The *context series* of x is then the sum

$$\sum_{(p,s)} p\otimes s$$

extended to all contexts (p, s) of x in C; it is an element of the complete tensor product

$$\mathbb{Z}\langle\langle A\rangle\rangle\otimes\mathbb{Z}\langle\langle A\rangle\rangle.$$

If C is finite, it is an element of $\mathbb{Z}\langle A\rangle\otimes\mathbb{Z}\langle A\rangle$ (such an element will be called a *polynomial*).

Example. If x is the empty word, its context polynomial is

$$1\otimes 1+\sum_{\substack{ps\in C\\ p,s\neq 1}} p\otimes s.$$

Corollary 3. *Let C be a maximal and finite code, with $C-1=P(A-1)S$, $P, S\in\mathbb{Z}\langle A\rangle$*

(cf. Theorem 1). *Let* $\mathcal{I}$ *be the ideal of* $\mathbb{Z}\langle A\rangle\otimes\mathbb{Z}\langle A\rangle$ *generated by* $(A-1)\otimes 1$ *and* $1\otimes(A-1)$. *Then any context polynomial is equal to* $P\otimes S \bmod \mathcal{I}$.

Proof. Let x be any word. Define a linear mapping

$$\lambda : \mathbb{Z}\langle\langle A\rangle\rangle \to \mathbb{Z}\langle\langle A\rangle\rangle\otimes\mathbb{Z}\langle\langle A\rangle\rangle$$

by

$$\lambda(w) = \sum_{uxv=w} u\otimes v, \quad \text{for any word } w.$$

We have $\lambda(A^*)=A^*\otimes A^*$, as is easily seen. Furthermore, by definition of the context polynomial $X=\sum p\otimes s$ of x, we have $\lambda(C^*)=\sum C^*p\otimes sC^*$, hence $\lambda(C^*)=(C^*\otimes 1)X(1\otimes C^*)$.

Define for any formal power series S and any word w the series

$$Sw^{-1}=\sum_{u\in A^*}(S,uw)\,u \quad \text{and} \quad w^{-1}S=\sum_{u\in A^*}(S,wu)\,u.$$

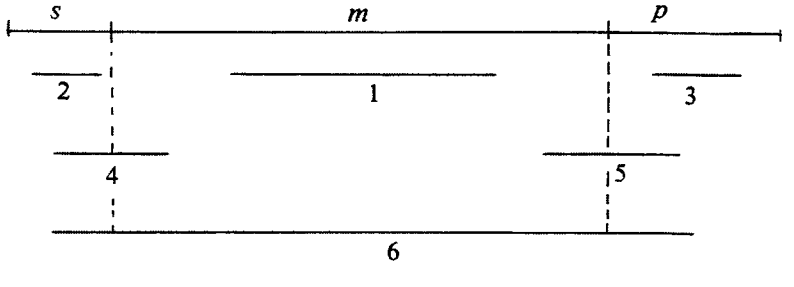
The mappings $S\mapsto Sw^{-1}$ and $S\mapsto w^{-1}S$ are linear (and where already used in the proof of Lemma 5.1). Moreover, if $S=u$ is a word, then uw^{-1} is 0 unless u ends with the suffix w, $u=u'w$ say, in which case $uw^{-1}=u'$. A symmetric remark may be done for $w^{-1}u$. Note that if S is a polynomial, then so are Sw^{-1} and $w^{-1}S$.

Let s, m, p be words. Then

$$\lambda(smp)=(s\otimes 1)\lambda(m)(1\otimes p)+\lambda(s)(1\otimes mp)+(sm\otimes 1)\lambda(p)$$
$$+\sum_{\substack{x=uv\\ u,v\neq 1}}(su^{-1}\otimes v^{-1}m\cdot p)+(s\cdot mu^{-1}\otimes v^{-1}p)$$
$$+\sum_{u,v\neq 1}(umv,x)(su^{-1}\otimes v^{-1}p)$$

(where (umv,x) is the coefficient of x in the series umv: it replaces the subscript $x=umv$ under the last $\sum$, so that the formula becomes linear in m).

The shortest proof of this formula is the following diagramm, representing the six possibilities for x to be a factor of the word smp:



The above formula being linear in each of s, m, p, it is still true for any series S, M, P instead of s, m, p.

We have $A^* = SC^*P$, hence

$$A^* \otimes A^* = \lambda(A^*) = \lambda(SC^*P)$$
$$= (S \otimes 1)\lambda(C^*)(1 \otimes P) + \lambda(S)(1 \otimes C^*P) + (SC^* \otimes 1)\lambda(P)$$
$$+ \sum_{\substack{x=uv \\ u,v \neq 1}} (Su^{-1} \otimes v^{-1}C^* \cdot P) + (S \cdot C^*u^{-1} \otimes v^{-1}P)$$
$$+ \sum_{u,v \neq 1} (uC^*v, x)(Su^{-1} \otimes v^{-1}P).$$

Note that the last summand is a polynomial, because (uC^*v, x) vanishes if u, v are long words. Furthermore, $\lambda(C^*) = (C^* \otimes 1)X(1 \otimes C^*)$ where X is the context polynomial of x. Let $d = |x|$. Then for $|v| < d$

$$v^{-1}C^* = v^{-1}(1 + C + \cdots + C^{d-1} + C^dC^*)$$

is the sum of a polynomial and of $v^{-1}C^d \cdot C^*$. Similarly, for $|u| < d$, C^*u^{-1} is the sum of a polynomial and of $C^* \cdot C^du^{-1}$. All this implies that

$$A^* \otimes A^* = (SC^* \otimes 1)X(1 \otimes C^*P) + \lambda(S)(1 \otimes C^*P) + (SC^* \otimes 1)\lambda(P)$$
$$+ \sum_{\substack{x=uv \\ u,v \neq 1}} (Su^{-1} \otimes v^{-1}C^d \cdot C^*P) + (SC^* \cdot C^du^{-1} \otimes v^{-1}P) + R$$

where R is some polynomial. Now, we multiply by $P(1-A) \otimes 1$ on the left and $1 \otimes (1-A)S$ on the right, and note that $P(1-A)SC^* = 1 = C^*P(1-A)S$; we obtain

$$P \otimes S = X + (P(1-A) \otimes 1)\lambda(S) + \lambda(P)(1 \otimes (1-A)S)$$
$$+ \sum_{\substack{x=uv \\ u,v \neq 1}} (P(1-A) \cdot Su^{-1} \otimes v^{-1}C^d) + (C^du^{-1} \otimes v^{-1}P \cdot (1-A)S)$$
$$+ (P(1-A) \otimes 1)R(1 \otimes (1-A)S).$$

This implies the corollary. □

As a consequence of the previous result, we obtain an invariance property, due to Hansel and Perrin [13]. They proved it in a more general case, for codes that are *nondense* (instead of finite; however, see the remark).

Let $\pi : A^* \to \mathbb{R}_+$ be a *Bernoulli morphism*, that is, a multiplicative monoid homomorphism such that $\pi | A$ is a probability on A.

The *average length* of C is the number

$$\sum_{w \in C} |w| \, \pi(w).$$

Corollary 4 (Hansel, Perrin [13]). *Let C be a maximal and finite code and x any word. Then the sum $\sum \pi(p)\pi(s)$ extended to all contexts (p, s) of x in C is equal to the average length of C.*

Proof. We extend π to an algebra homomorphism $\mathbb{Z}\langle A\rangle \otimes \mathbb{Z}\langle A\rangle \to \mathbb{R}_+$ by $\pi(a\otimes 1)=\pi(1\otimes a)=\pi(a)$ for any letter a. Then the above sum is just the image of the context polynomial of x. By Corollary 3, this number does not depend on x, because $\pi(A)=1$. Hence it is equal to

$$\pi(1\otimes 1)+\sum_{\substack{ps\in C\\ p,s\neq 1}} \pi(p\otimes s)$$

(take $x=1$). As $\pi(C)=1=\pi(1\otimes 1)$, this is equal to

$$\sum_{\substack{ps\in C\\ s\neq 1}} \pi(p)\pi(s)$$

which is the average length of C. □

Remark. A *nondense* code is a code C which does not intersect all ideals of A^*. This condition extends finiteness and is itself a finiteness condition, see [1], [13]. Corollary 4 is still true for such codes, as shown in [13]. The techniques used here allow to obtain this result if one uses the following fact: if L is a nondense subset of A^*, then $\sum_{w\in L}\pi(w)$ converges, see [15, proof of Lemma 6.4.10]. Then use the formula (3.2): $A^*=SC^*P_1+G_1$. As S, P_1 and G_1 are subsets of the set of all factors of C, they are nondense. Now, the proof of Corollary 3 may be adapted to obtain Corollary 4 in this more general case.

The previous remark raises the following question: if C is a nondense and maximal code, is it possible to write

$$C-1=P(A-1)S$$

for some polynomials P, S with bounded coefficients and nondense support? and if C is moreover rational, is it possible to take P, S rational?

A positive answer would be of interest, because one had then a complete characterization of nondense (resp. rational) and maximal codes: indeed, Theorem 2 may be extended, with a similar proof.

Acknowledgements

Thanks are due to Pr. D. Perrin and Pr. P.M. Cohn for helpful discussions and correspondence during the preparation of this paper.

References

[1] J. Berstel and D. Perrin, The Theory of Codes (Academic Press, New York, to appear).

[2] F. Blanchard and D. Perrin, Relèvement d'une mesure ergodique par un codage, Z. Wahrscheinlichkeit. 54 (1980) 303–311.

[3] J.-M. Boë, Sur les codes synchronisants coupants, Proc. Colloquium Arco Felice, Naples (C.N.R., Roma, 1981) 7-10.
[4] J.-M. Boë, A. de Luca and A. Restivo, Minimal complete sets of words, Theoret. Comput. Sci. 12 (1980) 325-332.
[5] Y. Césari, Propriétés combinatoires des codes bipréfixes complets finis, in: D. Perrin, ed., Actes de la 7ème école de printemps d'informatique théorique (Jougne, 1979) 29-46.
[6] A.H. Clifford and G.B. Preston, The Algebraic Theorey of Semigroups, Vol. 1 (Amer. Math. Soc., Providence, RI, 1961).
[7] P.M. Cohn, Free associative algebras, Bull. London Math. Soc. (1969) 1-39.
[8] P.M. Cohn, Free Rings and Their Relations (Academic Press, New York, 1971).
[9] P.M. Cohn, The universal field of fractions of a semifir, I: Numerators and denominators, Proc. London Math. Soc. (3) 44 (1982) 1-32.
[10] C. De Felice, On the triangle conjecture, Inform. Process. Lett. 14 (1982) 197-200.
[11] S. Eilenberg, Automata, Languages and Machines, Vol. A (Academic Press, New York, 1974).
[12] G. Hansel, Baionnettes et cardinaux, Discrete Math. 39 (1982) 331-335.
[13] G. Hansel and D. Perrin, Codes and Bernoulli partitions, Math. System Theory 16 (1983) 133-157.
[14] G. Hansel, D. Perrin and C. Reutenauer, Factorizing the polynomial of a code, Trans. Amer. Math. Soc. 285 (1984) 91-105.
[15] G. Lallement, Semigroups and Combinatorial Applications (Wiley, New York, 1979).
[16] R.C. Lyndon and P. Schupp, Combinatorial Group Theory (Springer, Berlin, 1977).
[17] S. Mauceri and A. Restivo, A family of codes commutatively equivalent to prefix codes, Inform. Process. Lett. 12 (1981) 1-4.
[18] D. Perrin, Codes asynchrones, Bull. Soc. Math. France 105 (1977) 385-404.
[19] D. Perrin and M.P. Schützenberger, un problème élémentaire de la théorie de l'information, Colloques Internationaux du CNRS, No. 276 (Cachan, 1977).
[20] D. Perrin and M.P. Schützenberger, A conjecture on sets of difference of integer pairs, J. Combin. Theory (B) 30 (1981) 91-93.
[21] J.-E. Pin and I. Simon, A note on the triangle conjecture, J. Combin. Theory (A) 32 106-109.
[22] A. Restivo, On codes having no finite completions, Discrete Math. 17 (1977) 309-31.
[23] C. Reutenauer, Sur un théorème de Schützenberger, Notes Comptes Rendus Acad. Sci. Paris 296 (1983) 619-621.
[24] C. Reutenauer, Sulla fattorizzazione dei codici, Ricerche di Matematica 32 (1983) 115-130.
[25] M.P. Schützenberger, Sur certains sous-monoïdes libres, Bull. Soc. Math. France 93 (1965) 209-223.
[26] P. Shor, J. Combin. Theory (A) 38 (1985) 110-112.
[27] M. Vincent, Une famille de codes indécomposables, Thèse 3ème cycle, Univ. Sci. Techniques Languedoc, Montpellier (1982).