

---

## *Factorization of Codes*

### 10.0. Introduction

There is a noncommutative polynomial canonically associated with a finite code: it is the sum of the codewords, minus 1. When the code is maximal, this polynomial has some striking factorization properties, which reflect probabilistic and combinatorial properties of the code, such as the property of being prefix, suffix or synchronizing. When the code is prefix, the factorization is directly related to the tree representation of the code. When the code is biprefix, one has even more combinatorial data explaining the factorization, as explained in Chapter ???? on finite maximal biprefix codes. In the general case, the factorization of the polynomial has no direct combinatorial interpretation, but is related via the factorization conjecture to a kind of coset decomposition of the free monoid with respect to the submonoid generated by the code. The factorization conjecture is the main open problem in the theory of codes.

### 10.1. The results

Recall that for a subset  $C$  of  $A^*$ ,  $\underline{C}$  denotes its *characteristic series*:  $\underline{C} \in \mathbf{N}\langle\langle A \rangle\rangle$ . If  $C$  is finite, then  $\underline{C} \in \mathbf{N}\langle A \rangle$ . The *degree* of a finite maximal code has been defined in ????

**THEOREM 10.1.1.** *Let  $C \subset A^*$  be a finite maximal code and  $d$  its degree. Then for some polynomials  $P, Q, S$  in  $\mathbf{Z}\langle A \rangle$ , one has*

$$\underline{C} - 1 = P(d(\underline{A} - 1) + (\underline{A} - 1)Q(\underline{A} - 1))S. \quad (10.1.1)$$

Moreover, if  $C$  is prefix (resp. suffix), then  $S = 1$  (resp.  $P = 1$ ).

Note that when  $C$  is biprefix, then a stronger assertion is ????, since it is shown in this case that  $\underline{C} - 1$  has a factorization (1.1) with  $P = S = 1$  and  $Q \in \mathbf{N}\langle A \rangle$ . Note also that, for general  $C$ , in all known cases,  $Q$  has nonnegative coefficients, and moreover  $P, S$  have coefficients 0,1. However, it is not known if it is true in every case.

COROLLARY 10.1.2. *Let  $C$  be a finite maximal code in  $A^*$ . Then for some polynomials  $P, S$  in  $\mathbf{Z}\langle A \rangle$ , one has*

$$\underline{C} - 1 = P(\underline{A} - 1)S. \quad (10.1.2)$$

■

Note that, again, in all known cases, a factorization (1.2) exists with  $P, S$  being characteristic polynomials of some finite sets:

$$P = \underline{U}, S = \underline{V}. \quad (10.1.3)$$

Whether this is always true is not known and constitutes the *factorization conjecture*. Note that Eq.(1.2), together with (1.3), may be rewritten as

$$A^* = \underline{V}\underline{C}^*\underline{U}. \quad (10.1.4)$$

Indeed, by Eq.(1.2)  $P, S$  are invertible in  $\mathbf{Z}\langle\langle A \rangle\rangle$ , and so Eq.(1.2) implies:  $(1 - \underline{C})^{-1} = \underline{V}^{-1}(1 - \underline{A})^{-1}\underline{U}^{-1}$ . Then by ????, we obtain Eq.(1.4). Observe that Eq.(1.4) means that each word  $w$  in  $A^*$  has exactly one factorization  $w = vmu$ , with  $v \in V, m \in C^*, u \in U$ . Note the analogy with the coset decomposition of a group with respect to a subgroup.

The previous result has the following converse. Thus finite maximal codes are completely characterized.

THEOREM 10.1.3. *Let  $W$  be in  $\mathbf{N}\langle A \rangle$  without constant term, and  $P, S$  in  $\mathbf{C}\langle A \rangle$  such that  $W - 1 = P(\underline{A} - 1)S$ . Then  $W$  is the characteristic polynomial of a finite maximal code  $C$ . If moreover  $S$  (resp.  $P$ ) is constant, then  $C$  is a prefix (resp. suffix) code.*

*Proof*

Denote by  $\text{supp}(T)$  the *support* of the series  $T \in \mathbf{C}\langle\langle A \rangle\rangle$ , that is, the set of words having a nonzero coefficient in  $T$ . Note that

$$\text{supp}(T_1T_2) \subset \text{supp}(T_1)\text{supp}(T_2), \text{supp}(T^*) \subset \text{supp}(T)^*.$$

Define  $C = \text{supp}(W)$ . Then  $C$  is finite by assumption. Since  $W - 1 = P(\underline{A} - 1)S$  and since  $W$  has no constant term,  $P$  and  $S$  are invertible in  $\mathbf{C}\langle\langle A \rangle\rangle$ , and we obtain

$$\underline{A}^* = SW^*P. \quad (10.1.5)$$

We show that  $C$  is complete (see ???? for the definition of a complete set). Indeed, let  $w$  be any word, and choose  $u$  of length  $\geq \text{deg}(S), \text{deg}(P)$ . Then  $uwu$  appears in the left-hand side of Eq.(1.5), so that by the remarks at the beginning of the proof, we obtain  $uwu = smp$ , for some  $s \in \text{supp}(S), m \in C^*, p \in \text{supp}(P)$ . By the choice of  $u$ , we obtain that  $w$  is a factor of  $m$ ; hence  $C^* \cap A^*wA^*$  is not empty, and  $C$  is complete.

Now, applying Th.????, we deduce that  $C$  is a maximal code, provided that we have shown that  $\pi(C) = 1$ , where  $\pi$  is some Bernoulli morphism. Since  $C$  is complete and finite, we have  $\pi(C) \geq 1$ , by ????. On the other hand,

if we extend  $\pi$  naturally to an algebra homomorphism  $\mathbf{C}\langle A \rangle \rightarrow \mathbf{C}$ , we obtain  $\pi(W)-1 = \pi(P)\pi(\underline{A}-1)\pi(S) = 0$  and  $\pi(W) = 1$ . Thus, since  $W$  has coefficients in  $\mathbf{N}$ ,  $\pi(C) \leq \pi(W) = 1$ , and we deduce that  $\pi(C) = 1$ .

Now, if  $S$  is a constant, we may suppose that  $S = 1$  and Eq.(1.5) becomes  $A^* = W^*P$ . A similar argument as before shows that  $C$  is right complete. Thus by ?????,  $C$  is a prefix code. ■

## 10.2. Division and factorization of noncommutative polynomials

Let  $K$  be a (commutative) field. We begin with a result on Euclidean division. Given two polynomials  $X, Y$  in  $K\langle A \rangle$ , we say that the *left Euclidean division* of  $X$  by  $Y$  is possible if for some polynomials  $Q, R$ , one has  $X = YQ + R$  and  $\deg(R) < \deg(Y)$ . It is not always possible if  $|A| \geq 2$ , but the next result gives a sufficient condition for it (this condition is easily seen to be also necessary).

**THEOREM 10.2.1.** *Let  $X, Y, P, Q_1, Q_2, R_1$  in  $K\langle A \rangle$  be such that*

$$XP + P_1 = YQ_1 + R_1, \quad (10.2.1)$$

*with  $P \neq 0$ ,  $\deg(P_1) \leq \deg(P)$  and  $\deg(R_1) < \deg(Y)$ . Then for some polynomials  $Q, R$ , one has*

$$X = YQ + R, \quad \deg(R) < \deg(Y).$$

The following consequence is immediate.

**COROLLARY 10.2.2.** *If  $X, Y, X', Y'$  are nonzero polynomials such that  $XY' = YX'$ , then for some polynomials  $Q, R$ , one has  $X = YQ + R$  and  $\deg(R) < \deg(Y)$ .* ■

In order to prove Th.2.1, we use the *lexicographic order* in the free monoid  $A^*$ :  $A$  is totally ordered and  $u \leq v$  if either  $|u| < |v|$ , or if  $|u| = |v| = n$  and  $u$  is smaller or equal to  $v$  in the lexicographic order from left to right in  $A^n$ .

Denote, for each nonzero polynomial  $P$ , by  $gw(P)$  the *greatest word* appearing in  $P$ . Then we have

$$gw(P + Q) = gw(P),$$

if  $\deg(Q) < \deg(P)$ , and

$$gw(PQ) = gw(P)gw(Q).$$

*Proof* of Theorem 1.2. By assumption, we have  $Y \neq 0$  (otherwise  $\deg(R_1) < \deg(0) = -\infty$ , which is impossible) and we may assume  $\deg(Y) \geq 1$ , since the case  $\deg(Y) = 0$  is immediate. The case  $\deg(X) < \deg(Y)$  is also easy. So we may assume  $\deg(X) \geq \deg(Y) \geq 1$ . Observe that  $\deg(P_1) \leq \deg(P) < \deg(XP)$

and  $\deg(R_1) < \deg(Y) \leq \deg(X) \leq \deg(XP)$ . This shows that  $Q_1$  is nonzero. By the two displayed equations above, we have  $gw(XP) = gw(XP + P_1 - R_1) = gw(YQ_1)$ , and  $gw(X)gw(P) = gw(Y)gw(Q_1)$ . Hence the word  $gw(Y)$  is a left factor of  $gw(X)$  and we may write  $gw(X) = gw(Y)u$ ,  $u \in A^*$ . Hence for some  $\alpha \in K$ , we have  $X = X' + \alpha Y u$ , with  $gw(X') < gw(X)$ . By Eq.(2.1), we then obtain

$$X'P + P_1 = Y(Q_1 - \alpha uP) + R_1.$$

Thus we conclude by induction on  $gw(X')$  that the left division of  $X'$  by  $Y$  is possible, hence that of  $X$  too.  $\blacksquare$

Let  $x_1, x_2, \dots$  be a sequence of elements of a ring, of length at least  $n$ . We define the  $n$ -th *continuant polynomial* relative to this sequence by  $p(x_1, \dots, x_n)$ , where  $p(x_1, \dots, x_n)$  is the 1,1 coefficient of the matrix

$$\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_n & 1 \\ 1 & 0 \end{pmatrix}.$$

It is a simple exercise to show that this matrix is actually equal to

$$\begin{pmatrix} p(x_1, \dots, x_n) & p(x_1, \dots, x_{n-1}) \\ p(x_2, \dots, x_n) & p(x_2, \dots, x_{n-1}) \end{pmatrix}. \quad (10.2.2)$$

Indeed, for the entry in position 2,1 for example, one sees that it is  $p(x_2, \dots, x_n)$  by computing the product of the first matrix by the product of the remaining ones and using induction.

For sake of coherence, the 0-th continuant polynomial is  $p() = 1$ , and the  $(-1)$ -th is equal to 0. From Eq.(2.2), one deduces that

$$p(x_1, \dots, x_n) = p(x_1, \dots, x_{n-1})x_n + p(x_1, \dots, x_{n-2}), \quad (10.2.3)$$

and

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

We often use the latter equation in the form

$$p(x_n, \dots, x_1) = x_n p(x_{n-1}, \dots, x_1) + p(x_{n-2}, \dots, x_1). \quad (10.2.4)$$

By induction, one deduces a relation due to Wedderburn:

$$p(x_1, \dots, x_n) p(x_{n-1}, \dots, x_1) = p(x_1, \dots, x_{n-1}) p(x_n, \dots, x_1). \quad (10.2.5)$$

To prove it, use Eq.(2.3) for the left-hand side, and Eq.(2.4) for the right-hand side.

The next result shows that, in essence, each relation  $XY' = YX'$  in  $K \langle A \rangle$  comes from a relation of the form (2.5).

**THEOREM 10.2.3.** *Let  $X, Y, X', Y'$  be nonzero polynomials in  $K \langle A \rangle$  such that  $XY' = YX'$ . Then there exist  $n \geq 1$  and polynomials  $U, V, x_1, \dots, x_n$  such that*

$$X = U p(x_1, \dots, x_n), Y' = p(x_{n-1}, \dots, x_1) V,$$

$$Y = Up(x_1, \dots, x_{n-1}), X' = p(x_n, \dots, x_1)V.$$

Furthermore,  $x_1, \dots, x_{n-1}$  have positive degree, and if  $\deg(X) > \deg(Y)$ , then  $x_n$  also has positive degree.

The proof is a simple noncommutative version of the Euclidean algorithm, obtained by iteration of the Euclidean division of Cor.2.2.

*Proof*

The hypothesis and Cor.2.2 imply that  $X = YQ_1 + R_1$ , for some polynomials  $Q_1$  and  $R_1$  with  $\deg(R_1) < \deg(Y)$ ; note that if  $\deg(X) > \deg(Y)$ , then  $\deg(Q_1) > 0$ . We have  $XY' = YX'$ , hence  $(YQ_1 + R_1)Y' = YX'$ , which implies  $R_1Y' = Y(X' - Q_1Y')$ ; since  $\deg(R_1) < \deg(Y)$ , we deduce that  $\deg(X' - Q_1Y') < \deg(Y')$  and we have  $X' = Q_1Y' + R'_1$ ,  $\deg(R'_1) < \deg(Y')$  (thus the left Euclidean division of  $X'$  by  $Y'$  is possible). Note that  $R_1 = 0 \Leftrightarrow R'_1 = 0$ . We may write  $(X, Y) = (Y, R_1) \begin{pmatrix} Q_1 & 1 \\ 1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} Q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Y' \\ R'_1 \end{pmatrix}$ . Now we have  $YR'_1 = R_1Y'$ , and we continue with  $Y, R'_1, R_1, R_1$  in place of  $X, Y', Y, X'$ . We then have  $Y = R_1Q_2 + R_2$ ,  $\deg(R_2) < \deg(R_1)$ ,  $Y' = Q_2R'_1 + R'_2$ , and this time  $\deg(Q_2) > 0$ . Then we have  $(Y, R_1) = (R_1, R_2) \begin{pmatrix} Q_2 & 1 \\ 1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} Y' \\ R'_1 \end{pmatrix} = \begin{pmatrix} Q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R'_1 \\ R'_2 \end{pmatrix}$ . Now we have  $R_2R'_1 = R_1R'_2$ . We iterate and find a sequence of remainders  $R_1, R_2, \dots$ , (resp.  $R'_1, R'_2, \dots$ ), with strictly decreasing degrees, such that for each  $i$ ,  $R_i = 0 \Leftrightarrow R'_i = 0$ . Hence for some  $n \geq 1$ ,  $R_{n-1}, R'_{n-1} \neq 0$  and  $R_n, R'_n = 0$ . Thus

$$(X, Y) = (R_{n-1}, 0) \begin{pmatrix} Q_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Q_1 & 1 \\ 1 & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} Q_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R'_{n-1} \\ 0 \end{pmatrix},$$

with  $\deg(Q_n), \dots, \deg(Q_2) \geq 1$ . This implies the theorem, in view of Eq.(2.2).  $\blacksquare$

We shall also need the next result in the proof of Th.1.1 (with  $\underline{A} - 1$  playing the role of the polynomial of degree 1).

**THEOREM 10.2.4.** *Let  $B$  be a polynomial of degree 1, and  $x_1, \dots, x_n$  be polynomials such that  $x_1, \dots, x_{n-1}$  have positive degree. If*

$$p(x_{n-1}, \dots, x_1), p(x_n, \dots, x_1)$$

*are congruent to a scalar, modulo the right ideal  $BK \langle A \rangle$ , then for each  $i = 1, \dots, n$ ,  $p(x_1, \dots, x_i)$  and  $p(x_i, \dots, x_1)$  are congruent to the same scalar modulo this ideal.*

To prove this, we need a lemma.

LEMMA 10.2.5. *Let  $x_1, \dots, x_n$  be polynomials.*

- (i)  $p(x_1, \dots, x_n) = 0 \Leftrightarrow p(x_n, \dots, x_1) = 0$ .
- (ii) *If the degrees of  $x_1, \dots, x_{n-1}$  are strictly positive, then*

$$1, p(x_1), \dots, p(x_{n-1}, \dots, x_1)$$

*have strictly increasing degrees.*

*Proof* Now (i) is proved using Eq.(2.5) if  $p(x_{n-1}, \dots, x_1)$  and  $p(x_1, \dots, x_{n-1})$  are both nonzero, and Eqs.(2.3) and (2.4) if they are both zero (by induction, if one is zero, so is the other). Similarly (ii) is proved by induction, using Eq.(2.4). ■

*Proof* of Th.2.4 Note that the condition on the degrees for  $n$  implies that for  $n - 1$ ; hence we may use induction. The case  $n = 1$  is evident, so let us prove the result for  $n > 1$ .

If  $p(x_{n-1}, \dots, x_1)$  vanishes, then  $p(x_1, \dots, x_{n-1})$  also vanishes by Lemma 2.5 (i). Then by Eq.(2.3) and (2.4), we have  $p(x_1, \dots, x_n) = p(x_1, \dots, x_{n-2})$  and  $p(x_n, \dots, x_1) = p(x_{n-2}, \dots, x_1)$ . Thus we conclude the proof by induction in this case.

Suppose that  $p(x_{n-1}, \dots, x_1) \neq 0$ . Then by Eq.(2.4),

$$p(x_n, \dots, x_1) = x_n p(x_{n-1}, \dots, x_1) + p(x_{n-2}, \dots, x_1) = BQ + \alpha$$

for some  $Q \in K \langle A \rangle$  and  $\alpha \in K$ . By Lemma 2.5 (ii), the hypothesis of Th.2.1 is fulfilled, so that one may perform the left Euclidean division of  $x_n$  by  $B$ ; hence  $x_n$  is congruent to a scalar  $\gamma$  mod.  $BK \langle A \rangle$ . Then the equality above shows that  $p(x_{n-2}, \dots, x_1)$  is congruent to a scalar mod.  $BK \langle A \rangle$ : indeed, if  $U, V$  are congruent to scalars  $u, v$ , then  $UV$  is congruent to  $uv$ . Hence we conclude by induction, the same equality and Eq.(2.3). ■

We consider now polynomials over  $\mathbf{Z}$  and  $\mathbf{Q}$ . A nonzero polynomial  $P \in \mathbf{Z} \langle A \rangle$  is called *primitive* if the greatest common divisor of its coefficients is 1. The *content* of a nonzero  $P \in \mathbf{Q} \langle A \rangle$  is the unique nonzero  $c(P) \in \mathbf{Q}_+$  such that  $P/c(P)$  is primitive; the latter polynomial is then denoted by  $\bar{P}$ . Hence  $P = c(P)\bar{P}$ . Actually,  $\bar{P}$  is the unique primitive polynomial such that  $P = q\bar{P}$  for some nonzero  $q \in \mathbf{Q}_+$ .

The next result is the analogue for noncommutative polynomials of *Gauss' lemma*.

- LEMMA 10.2.6. (i) *If  $P, Q$  in  $\mathbf{Z} \langle A \rangle$  are primitive, then so is  $PQ$ .*  
(ii) *If  $P, Q$  are in  $\mathbf{Q} \langle A \rangle$ , then  $c(PQ) = c(P)c(Q)$  and  $\overline{PQ} = \bar{P}\bar{Q}$ .*

*Proof*

For (i), if  $PQ$  is not primitive, some prime number  $p$  divides all its coefficients. One obtains a contradiction by reducing coefficients in  $\mathbf{Z}/p\mathbf{Z}$ , since polynomials over a field do not have zero divisors. Now (ii) follows easily from (i). ■

**THEOREM 10.2.7.** *Let  $P_1, P_2, P_3, P_4$  be nonzero polynomials in  $\mathbf{Z}\langle A \rangle$ , with  $P_2$  invertible in  $\mathbf{Q}\langle\langle A \rangle\rangle$ , and such that  $P_1P_2^{-1}P_3 = P_4$ . Then there exist  $R_1, R_2, R_3, R_4$  in  $\mathbf{Z}\langle A \rangle$  such that  $P_1 = R_1R_2, P_2 = R_3R_2, P_3 = R_3R_4, P_4 = R_1R_4$ .*

Note that the last four equalities imply the first one.

*Proof*

We begin by proving the corresponding statement with  $\mathbf{Q}$  and  $\mathbf{Z}$  replaced by  $K$ , a (commutative) field. Then we use Gauss' lemma to draw our conclusion in  $\mathbf{Z}\langle A \rangle$ .

1. Consider the subset  $E$  of  $K\langle A \rangle^{2 \times 1}$  of vectors  $V$  such that  $(1, -P_1P_2^{-1})V = 0$ . Clearly  $E$  is a right  $K\langle A \rangle$ -module. Note that  $V$  contains the transpose of  $(P_1, P_2)$  and that of  $(P_4, P_3)$ . Choose  $V$  to be nonzero in  $E$  and of smallest possible degree, where  $\deg(V)$  is the maximum degree of its two components. If the constant term of  $V$  is zero, then we may write  $V = \sum_{a \in A} V_a a$ , with  $V_a \in K\langle A \rangle^{2 \times 1}$ . Then each  $V_a$  must be in  $E$ : indeed,  $U = (1, -P_1P_2^{-1})$  is by assumption in  $\mathbf{Z}\langle\langle A \rangle\rangle^{2 \times 1}$ , so that  $UV = \sum_{a \in A} UV_a a = 0$ , and we deduce that for any  $a \in A$ ,  $UV_a = 0$ . This contradicts the minimality of  $V$ . Hence the constant term of  $V$  is nonzero.

We show that  $W \in VK\langle A \rangle$  for any  $W \in E$  (which will imply that  $E = VK\langle A \rangle$ ), by induction on  $\deg(W)$ . This is clear if  $\deg(W) < \deg(V)$ . Now suppose that  $\deg(W) \geq \deg(V)$ . If  $W$  has constant term zero, then as above  $W = \sum_{a \in A} W_a a$ ,  $W_a \in E$ ,  $\deg(W_a) < \deg(W)$ : thus  $W_a$  is in  $VK\langle A \rangle$  by induction, and so is  $W$ . If  $W$  has nonzero constant term, we may find  $\alpha \in K$  such that  $W' = W - \alpha V$  has constant term 0 and we conclude as before that  $W' \in VK\langle A \rangle$ , hence  $W \in VK\langle A \rangle$ : indeed, each constant term,  $W_1$ , of an element of  $E$  satisfies  $(1, \beta)W_1 = 0$ , where  $\beta$  is the constant term of  $-P_1P_2^{-1}$ ; hence the  $K$ -space of these  $W_1$  is of dimension 1, necessarily spanned by the constant term of  $W$ .

Now  $E = VK\langle A \rangle$ . Let  $V = \begin{pmatrix} Q_1 \\ Q_3 \end{pmatrix}$ . Then for some  $Q_2, Q_4$ , one has:

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} Q_1 \\ Q_3 \end{pmatrix} Q_2, \quad \begin{pmatrix} P_4 \\ P_3 \end{pmatrix} = \begin{pmatrix} Q_1 \\ Q_3 \end{pmatrix} Q_4, \text{ which concludes this part.}$$

2. By Part 1., we have  $P_1 = Q_1Q_2, P_2 = Q_3Q_2, P_3 = Q_3Q_4, P_4 = Q_1Q_4$  with  $Q_i \in \mathbf{Q}\langle A \rangle$ . Let  $c_i = c(Q_i)$ . Then by Lemma 2.6, we have  $c(P_1) = c_1c_2, c(P_2) = c_3c_2, c(P_3) = c_3c_4, c(P_4) = c_1c_4$ . Thus  $c(P_4) = c(P_1)c(P_2)^{-1}c(P_3)$ . Since the  $P_i$  are in  $\mathbf{Z}\langle A \rangle$ , each  $c(P_i)$  is in  $\mathbf{N}$ , so that  $c(P_1) = d_1d_2, c(P_2) = d_3d_2, c(P_3) = d_3d_4, c(P_4) = d_1d_4$  for some  $d_i$  in  $\mathbf{N}$ . Furthermore, by Gauss' lemma,  $\bar{P}_1 = \bar{Q}_1\bar{Q}_2, \bar{P}_2 = \bar{Q}_3\bar{Q}_2, \bar{P}_3 = \bar{Q}_3\bar{Q}_4, \bar{P}_4 = \bar{Q}_1\bar{Q}_4$ . Let  $R_i = d_i\bar{Q}_i$ . Then  $R_i \in \mathbf{Z}\langle A \rangle$ . We have  $P_1 = c(P_1)\bar{P}_1 = d_1d_2\bar{Q}_1\bar{Q}_2 = R_1R_2$ . Similarly,  $P_2 = R_3R_2, P_3 = R_3R_4, P_4 = R_1R_4$ , which concludes the proof. ■

We shall also need the following result.

**LEMMA 10.2.8.** *Let  $B$  be a primitive polynomial of degree 1 which vanishes for some integer values of the variables. Let  $P, Q \in \mathbf{Z}\langle A \rangle$  and  $\alpha \in \mathbf{Z} \setminus 0$  be such that  $PQ \equiv \alpha \pmod{B\mathbf{Z}\langle A \rangle}$ . Then  $P \equiv \beta, Q \equiv \gamma \pmod{B\mathbf{Z}\langle A \rangle}$  for some  $\beta, \gamma$  in  $\mathbf{Z}$  with  $\alpha = \beta\gamma$ .*

*Proof*

Now  $PQ = BQ' + \alpha$  for some  $Q' \in \mathbf{Z}\langle A \rangle$ . Since  $Q \neq 0$  (because  $\alpha \neq 0$ ), we may apply Th. 2.1:  $P = BT + \beta$ ,  $T \in \mathbf{Q}\langle A \rangle$ ,  $\beta \in \mathbf{Q}$ . Thus  $BQ' + \alpha = \beta Q + BTQ$ . We have  $\beta \neq 0$  (since  $\alpha \neq 0$ , and  $\deg(B) = 1$ ). Hence  $Q = \gamma + BS$  for some  $S \in \mathbf{Q}\langle A \rangle$ , and  $\gamma \in \mathbf{Q}$ , with  $\alpha = \beta\gamma$ . Now, the assumption on  $B$  and the fact that  $P, Q \in \mathbf{Z}\langle A \rangle$  implies that  $\beta, \gamma \in \mathbf{Z}$ . Since  $BT = P - \beta$ , we obtain by Gauss' lemma  $c(B)c(T) = c(P - \beta) \in \mathbf{N}$ , hence  $c(T) \in \mathbf{N}$ , for  $B$  being primitive. Thus  $T \in \mathbf{Z}\langle A \rangle$ . Similarly we obtain  $S \in \mathbf{Z}\langle A \rangle$ .  $\blacksquare$

Finally we mention without proof the following lemma, which is an easy consequence of Gauss' lemma, Eq.(2.5), Lemma 2.5 (i) and an induction using Eq.(2.3) and Eq.(2.4).

LEMMA 10.2.9. *If  $a_1, \dots, a_n \in \mathbf{Q}\langle A \rangle$ , then  $p(a_1, \dots, a_n)$  and  $p(a_n, \dots, a_1)$  are both zero or have the same content.*

### 10.3. Proof of Theorem 1.1

For a word  $u$  and a series  $S \in \mathbf{Z}\langle\langle A \rangle\rangle$ , recall the notation

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

Observe that  $(uv)^{-1}S = v^{-1}(u^{-1}S)$ . The notation  $Sv^{-1}$  is defined symmetrically. Note that  $u^{-1}(Sv^{-1}) = (u^{-1}S)v^{-1}$ ; henceforth, we may denote this series  $u^{-1}Sv^{-1}$ . If  $u = a$  is a letter, then

$$a^{-1}(S_1S_2) = (a^{-1}S_1)S_2 + (S_1, 1)(a^{-1}S_2). \quad (10.3.1)$$

This relation is easily verified when  $S_1, S_2$  are words, and extended by linearity to series.

LEMMA 10.3.1. *Let  $C$  be a finite code. For each pair of words  $u, v$ , there exist polynomials  $S(u), P(u), F(u, v)$  with coefficients 0,1 such that*

$$u^{-1}\underline{C}^*v^{-1} = S(u)\underline{C}^*P(v) + F(u, v).$$

The proof of this lemma is somewhat technical, but straightforward, once Eq.(3.1) is noted.

*Proof*

Define the polynomial  $S(u)$  inductively by  $S(1) = 1$  and

$$S(va) = a^{-1}(S(v)) + (S(v), 1)(a^{-1}\underline{C}), \quad (10.3.2)$$

if  $u = va$ ,  $a \in A$ ,  $v \in A^*$ . We show first that  $u^{-1}\underline{C}^* = S(u)\underline{C}^*$ . This is clear if  $u = 1$ . Now we have, for  $u = va$ ,

$$u^{-1}\underline{C}^* = (va)^{-1}\underline{C}^* = a^{-1}(v^{-1}\underline{C}^*) = a^{-1}(S(v)\underline{C}^*),$$

by induction. Hence by Eq.(3.1),

$$u^{-1}\underline{C}^* = (a^{-1}S(v))\underline{C}^* + (S(v), 1)(a^{-1}\underline{C}^*).$$

Using Eq.(3.1) again, we have

$$a^{-1}\underline{C}^* = a^{-1}(1 + \underline{C}\underline{C}^*) = (a^{-1}\underline{C})\underline{C}^*,$$

since  $(\underline{C}, 1) = 0$ , for  $C$  being a code. Thus,

$$u^{-1}\underline{C}^* = (a^{-1}S(v))\underline{C}^* + (S(v), 1)(a^{-1}\underline{C})\underline{C}^*,$$

which implies that  $u^{-1}\underline{C}^* = S(u)\underline{C}^*$ . This relation also shows that  $S(u)$  has coefficients 0,1, since so have  $\underline{C}^*$  and  $u^{-1}\underline{C}^*$ .

The polynomial  $P(v)$ , with coefficients 0,1 is defined symmetrically, and one has  $\underline{C}^*v^{-1} = \underline{C}^*P(v)$ .

We now define  $F(u, v)$  by induction on  $|v|$ . Let  $F(u, 1) = 0$ , and for  $v = aw$ , let  $F(u, v) = F(u, aw) = (P(w), 1)(S(u)a^{-1}) + F(u, w)a^{-1}$ . Then  $F(u, v)$  is a polynomial. We now verify the formula in the lemma. For  $v = 1$ , it follows from what we have seen above. For  $v = aw$ , we have by induction and the symmetric of Eq.(3.1),

$$\begin{aligned} u^{-1}\underline{C}^*v^{-1} &= (u^{-1}\underline{C}^*w^{-1})a^{-1} = (S(u)\underline{C}^*P(w) + F(u, w))a^{-1} \\ &= S(u)\underline{C}^*(P(w)a^{-1}) + S(u)(\underline{C}^*a^{-1})(P(w), 1) \\ &\quad + (S(u)a^{-1})(\underline{C}^*, 1)(P(w), 1) + F(u, w)a^{-1}. \end{aligned}$$

Now as above, we have  $\underline{C}^*a^{-1} = \underline{C}^*(\underline{C}a^{-1})$ , and  $(\underline{C}^*, 1) = 1$ . Thus

$$\begin{aligned} u^{-1}\underline{C}^*v^{-1} &= S(u)\underline{C}^*(P(w)a^{-1} + (\underline{C}a^{-1})(P(w), 1)) \\ &\quad + (S(u)a^{-1})(P(w), 1) + F(u, w)a^{-1} = S(u)\underline{C}^*P(aw) + F(u, aw), \end{aligned}$$

by definition of  $F(u, aw)$  and that of  $P(aw)$ , symmetric of Eq.(3.2). To conclude note that the relation in the lemma implies that  $F(u, v)$  has coefficients 0,1, since  $u^{-1}\underline{C}^*v^{-1}$  has coefficients 0,1 and  $S(u)\underline{C}^*P(v)$  has nonnegative coefficients. ■

**LEMMA 10.3.2.** *Let  $C$  be a finite maximal code of degree  $d$ . Then there exist words  $u_1, \dots, u_d, v_1, \dots, v_d$  with  $u_1, v_1 \in C^*$ , such that for any  $1 \leq i \leq d$ :*

$$\underline{A}^* = \sum_{1 \leq j \leq d} u_i^{-1}\underline{C}^*v_j^{-1} = \sum_{1 \leq i \leq d} u_i^{-1}\underline{C}^*v_j^{-1},$$

and for any  $1 \leq j \leq d$ :

$$\underline{A}^* = \sum_{1 \leq i \leq d} u_i^{-1}\underline{C}^*v_j^{-1} = \sum_{1 \leq i \leq d} u_i^{-1}\underline{C}^*v_j^{-1}.$$

*Proof*

By ????, there exists a finite monoid  $M$ , and a surjective monoid homomorphism  $\phi : A^* \rightarrow M$  such that  $C^* = \phi^{-1}\phi(C^*)$ ; moreover, there exists an idempotent  $e$  in  $J \cap \phi(C^*)$ , where  $J$  is the minimal ideal of  $M$ ,  $G = eMe$  is a finite group with neutral element  $e$  and  $H = G \cap \phi(C^*)$  is a subgroup of index  $d$ . In particular,  $e \in \phi(C^*)$  and  $\phi^{-1}(e) \subset C^*$ .

Let  $u_1, \dots, u_d, v_1, \dots, v_d$  be words in  $\phi^{-1}(G)$  such that  $G = \cup_{1 \leq i \leq d} \phi(v_i)H = \cup_{1 \leq j \leq d} H\phi(u_j)$ . We may assume that  $\phi(u_1) = \phi(v_1) = e$ , and that  $\phi(u_i)$  is the inverse of  $\phi(v_i)$  in  $G$ ; from that, we deduce that  $u_1, v_1 \in \phi^{-1}(e) \subset \phi^{-1}\phi(C^*) = C^*$ .

Fix  $j$ ,  $1 \leq j \leq d$ . Let  $w \in A^*$ . Observe that  $\phi(v_j) \in G$ , hence that  $e\phi(wv_j) = e\phi(w)\phi(v_j) = e\phi(w)\phi(v_j)e$  is in  $eMe = G$ ; thus  $e\phi(wv_j)$  is in some  $\phi(v_i)H$ , for some uniquely determined  $i$ , depending on  $w$ . We show that:

$$e\phi(wv_j) \in \phi(v_i)H \Leftrightarrow u_i w v_j \in C^*.$$

Indeed,  $e\phi(wv_j) \in \phi(v_i)H \Leftrightarrow \phi(u_i)e\phi(wv_j) \in \phi(u_i)\phi(v_i)H \Leftrightarrow \phi(u_i w v_j) \in H \Leftrightarrow u_i w v_j \in C^*$  (since  $\phi(u_i w v_j) = e\phi(u_i w v_j)e \in G$ ).

Thus we obtain: for any  $w$  in  $A^*$ , there is a unique  $i$  such that  $w \in u_i^{-1}C^*v_j^{-1}$ , which implies the second equality in the lemma and the first by symmetry.  $\blacksquare$

The following lemma is easily derived.

**LEMMA 10.3.3.** *Let  $C$  be a finite maximal code of degree  $d$ . There exist polynomials  $P, P_1, S, S_1, L_1, R_1$  with coefficients 0,1 and a polynomial  $Q$  with coefficients in  $\mathbf{N}$  such that*

- (i)  $dA^* - Q = SC^*P$ ;
- (ii)  $\underline{A}^* = L_1 + SC^*P_1$ ;
- (iii)  $\underline{A}^* = R_1 + S_1C^*P$ ;
- (iv)  $P_1, S_1$  have constant term 1;
- (v)  $L_1, R_1$  have constant term 0;
- (vi)  $C$  is prefix (resp. suffix) if and only if  $S_1 = 1$  (resp.  $P_1 = 1$ ).

Note that (ii) and (iii) are each a weaker form of the factorization conjecture, see Eq.(1.4).

*Proof*

By Lemma 3.1,  $u_i^{-1}C^*v_j^{-1} = S(u_i)C^*P(v_j) + F(u_i, v_j)$ , where  $S(u_i), P(v_j), F(u_i, v_j)$  are polynomials with coefficients 0,1. Thus, Lemma 3.2 implies that for any  $i$ ,

$$\underline{A}^* = \sum_{1 \leq j \leq d} S(u_i)C^*P(v_j) + \sum_{1 \leq j \leq d} F(u_i, v_j),$$

and for any  $j$ ,

$$\underline{A}^* = \sum_{1 \leq i \leq d} S(u_i)C^*P(v_j) + \sum_{1 \leq i \leq d} F(u_i, v_j).$$

Let  $P = \sum_{1 \leq j \leq d} P(v_j)$ ,  $S = \sum_{1 \leq i \leq d} S(u_i)$ ,  $P_1 = P(v_1)$ ,  $S_1 = S(u_1)$ ,  $L_1 = \sum_{1 \leq i \leq d} F(u_i, v_1)$ ,  $R_1 = \sum_{1 \leq j \leq d} F(u_1, v_j)$ ,  $Q = \sum_{1 \leq i, j \leq d} F(u_i, v_j)$ .

Then we deduce (i), (ii) and (iii); the assertion on the coefficients follows from (ii) and (iii):  $\underline{A}^* = L_1 + S\underline{C}^*P_1$  has 1 as only coefficient, so  $L_1, S, P_1$  must have coefficients 0,1, since they have coefficients in  $\mathbf{N}$ .

The fact that  $u_1 \in C^*$  (Lemma 3.2) and the equation  $u_1^{-1}\underline{C}^* = S(u_1)\underline{C}^*$  (proof of Lemma 3.1) implies that  $S_1 = S(u_1)$  has constant term 1, since so has  $u_1^{-1}\underline{C}^*$ . This implies (iv).

Now  $S$  has a positive integer as constant term, and  $\underline{A}^*, \underline{C}^*, P_1$  have constant term 1; hence (ii) implies that  $L_1$  has constant term 0. This proves (v).

If  $C$  is prefix, then  $u_1^{-1}\underline{C}^* = \underline{C}^*$ , by ??????. Since  $u_1^{-1}\underline{C}^* = S(u_1)\underline{C}^*$ , we must have  $S_1 = S(u_1) = 1$ . Conversely, if  $S_1 = 1$ , we have  $\underline{A}^* = R_1 + \underline{C}^*P_1$ , which shows, as at the end of the proof of Th.1.3, that  $C$  is right complete (the presence of polynomial  $R_1$  does not change the general idea of the argument), and hence that  $C$  is a prefix code. ■

We now prove Th.1.1. In the calculations below, we shall invert several elements of  $\mathbf{Z}\langle\langle A \rangle\rangle$ , whose invertibility is a consequence of Lemma 3.3.(iv) and (v). By part (ii) of this lemma, we have  $\underline{A}^* - L_1 = S\underline{C}^*P_1$ . Thus  $S\underline{C}^*P_1 = (1 - \underline{A})^{-1}(1 - (1 - \underline{A})L_1)$ . Hence

$$(1 - \underline{A})SC^* = (1 - (1 - \underline{A})L_1)P_1^{-1}.$$

By Lemma 3.3.(i), we have  $d - (1 - \underline{A})Q = (1 - \underline{A})SC^*P$ ; thus, with the help of the previous equation, we obtain  $d - (1 - \underline{A})Q = (1 - (1 - \underline{A})L_1)P_1^{-1}P$ . This implies  $P = P_1(1 - (1 - \underline{A})L_1)^{-1}(d - (1 - \underline{A})Q)$ . We apply Th.2.7 to the last equality and we obtain the existence of  $E, F, G, H$  in  $\mathbf{Z}\langle A \rangle$  such that  $P_1 = EF$ ,  $1 - (1 - \underline{A})L_1 = GF$ ,  $d - (1 - \underline{A})Q = GH$ ,  $P = EH$ . Thus Lemma 2.8 implies that  $G = \pm 1 \pmod{(1 - \underline{A})\mathbf{Z}\langle A \rangle}$ . Replacing if necessary  $E, F, G, H$  by their negatives, we may suppose that  $G \equiv 1$  (in the remainder of the proof,  $\equiv$  will mean modulo  $(1 - \underline{A})\mathbf{Z}\langle A \rangle$ ). Then Lemma 2.8 again implies that  $H \equiv d$ . Thus

$$P = E(d + (\underline{A} - 1)I), \quad I \in \mathbf{Z}\langle A \rangle.$$

By Lemma 3.3.(iii), we have  $(1 - \underline{A})^{-1}(1 - (1 - \underline{A})R_1) = \underline{A}^* - R_1 = S_1\underline{C}^*P$ . Hence

$$(1 - \underline{C})S_1^{-1} = P(1 - (1 - \underline{A})R_1)^{-1}(1 - \underline{A}),$$

which implies by the previous displayed equation

$$\underline{C} - 1 = E(d + (\underline{A} - 1)I)(1 - (1 - \underline{A})R_1)^{-1}(\underline{A} - 1)S_1.$$

This is very close to Eq.(1.1), but with a central inverted polynomial, which we must eliminate. For this we use Th.2.7 again: there exists  $J, K, L, M$  in  $\mathbf{Z}\langle A \rangle$  such that  $E(d + (\underline{A} - 1)I) = JK$ ,  $1 - (1 - \underline{A})R_1 = LK$ ,  $(\underline{A} - 1)S_1 = LM$ ,  $\underline{C} - 1 = JM$ . Let  $\pi$  be a positive Bernoulli morphism, that is, a multiplicative monoid homomorphism  $A^* \rightarrow \mathbf{R}_+ \setminus 0$ , such that  $\sum_{a \in A} \pi(a) = 1$ . We extend it linearly to an algebra homomorphism  $\mathbf{Q}\langle A \rangle \rightarrow \mathbf{R}$ .

We may assume that  $\pi(K) \geq 0$ . Then we deduce from Lemma 2.8 that  $K = 1 + (\underline{A} - 1)K'$  and  $L = 1 + (\underline{A} - 1)L'$  for some  $K', L'$  in  $\mathbf{Z}\langle A \rangle$ . Thus  $(\underline{A} - 1)S_1 = (1 + (\underline{A} - 1)L')M = M + (\underline{A} - 1)L'M$ , which implies that  $M = (\underline{A} - 1)M'$  for some  $M'$  in  $\mathbf{Z}\langle A \rangle$ . Thus

$$\underline{C} - 1 = J(\underline{A} - 1)M', \quad (10.3.3)$$

and

$$E(d + (\underline{A} - 1)I) = J(1 + (\underline{A} - 1)K'). \quad (10.3.4)$$

Eq.(3.3) will imply Eq.(1.1), if we show that  $J$  is of the form  $J_1(d + (\underline{A} - 1)J_2)$ . This is the most technical part of the proof. It follows from Eq.(3.4) and the divisibility property of Th.2.3. The difficulty is that in this theorem, the polynomials involved have coefficients in  $\mathbf{Q}$ ; therefore a lot of work is required to draw the conclusion in  $\mathbf{Z}$ .

So, Th.2.3 applied to Eq.(3.4) guarantees the existence of polynomials  $x_1, \dots, x_n, U, V$  in  $\mathbf{Q}\langle A \rangle$  such that

$$\begin{aligned} E &= Up(x_1, \dots, x_n), d + (\underline{A} - 1)I = p(x_{n-1}, \dots, x_1)V, \\ J &= Up(x_1, \dots, x_{n-1}), 1 + (\underline{A} - 1)K' = p(x_n, \dots, x_1)V. \end{aligned}$$

We write  $p_i, q_i$  for  $p(x_1, \dots, x_i)$  and  $p(x_i, \dots, x_1)$ . We apply Th.2.1 to the two equalities at the right, and obtain that  $q_{n-1}$  and  $q_n$  are both congruent to a scalar  $\text{mod.}(\underline{A} - 1)\mathbf{Q}\langle A \rangle$ . Thus Th.2.4 implies that  $p_{n-1}$  and  $q_{n-1}$  (resp.  $p_n$  and  $q_n$ ) are congruent to the same scalar  $\text{mod.}(\underline{A} - 1)\mathbf{Q}\langle A \rangle$ . Furthermore, by Lemma 2.9,  $c(p_{n-1}) = c(q_{n-1})$  and  $c(p_n) = c(q_n)$ .

Observe that  $1 - (\underline{A} - 1)R_1$  is primitive, since  $R_1$  has coefficients 0,1. Thus the equation  $1 - (1 - \underline{A})R_1 = LK$  implies that  $L, K$  are primitive, since they are in  $\mathbf{Z}\langle A \rangle$ . We have  $K = 1 + (\underline{A} - 1)K' = q_n V$ , hence by Gauss' lemma  $c(q_n)C(V) = c(K) = 1$ , and  $\bar{q}_n \bar{V} = \bar{K} = K$ . This equality together with Lemma 2.8 implies that  $\bar{V} = \epsilon + (\underline{A} - 1)V', V' \in \mathbf{Z}\langle A \rangle, \epsilon \pm 1$ . Now  $\underline{C} - 1 = JM$  and  $\underline{C} - 1$  is primitive, hence  $J$  is primitive. Since  $JK = E(d + (\underline{A} - 1)I)$ , Gauss' lemma again implies that  $d + (\underline{A} - 1)I$  is primitive. Since  $d + (\underline{A} - 1)I = q_{n-1}V$ , the same lemma implies that  $d + (\underline{A} - 1)I = \bar{q}_{n-1}\bar{V}$ . Lemma 2.8 now implies that  $\bar{q}_{n-1} = \epsilon d + (\underline{A} - 1)N, N \in \mathbf{Z}\langle A \rangle$ .

We have seen that  $p_{n-1}$  and  $q_{n-1}$  are congruent to the same scalar  $\text{mod.}(\underline{A} - 1)\mathbf{Q}\langle A \rangle$  and that  $c(p_{n-1}) = c(q_{n-1})$ . Hence  $\bar{p}_{n-1}$  and  $\bar{q}_{n-1}$  are congruent to the same scalar  $\text{mod.}(\underline{A} - 1)\mathbf{Q}\langle A \rangle$ , and we have  $\bar{p}_{n-1} = \epsilon d + (\underline{A} - 1)P, P \in \mathbf{Q}\langle A \rangle$ . But  $\bar{p}_{n-1} - \epsilon d = (\underline{A} - 1)P$  and  $(\underline{A} - 1)$  is primitive, so that by Gauss' lemma,  $c(P) = c(\bar{p}_{n-1} - \epsilon d) \in \mathbf{Z}$  and  $P$  is in  $\mathbf{Z}\langle A \rangle$ .

Now,  $J$  is primitive and  $J = Up_{n-1}$ , hence  $J = \bar{J} = \bar{U}\bar{p}_{n-1}$ , which implies  $J = \bar{U}(\epsilon d + (\underline{A} - 1)P)$ . Thus Eq.(3.3) implies

$$\underline{C} - 1 = \bar{U}(\epsilon d + (\underline{A} - 1)P)(\underline{A} - 1)M'.$$

This implies that for some polynomials  $X, Y, Z$  in  $\mathbf{Z}\langle A \rangle$  (defined by  $X = \pm \bar{U}$ ,  $Y = \pm P$ ,  $Z = \pm M'$ ) and  $\epsilon_1 = \pm 1$ , one has

$$\underline{C} - 1 = X(\epsilon_1 d(\underline{A} - 1) + (\underline{A} - 1)Y(\underline{A} - 1))Z,$$

with  $\pi(X), \pi(Z) \geq 0$ .

Now define the linear mapping  $\lambda : \mathbf{Q}\langle A \rangle \rightarrow \mathbf{R}$  by  $\lambda(w) = |w|\pi(w)$  for each word  $w$  in  $A^*$ . It is easily shown that  $\lambda$  is a  $\pi$ -derivation, that is,  $\lambda(P_1P_2) = \lambda(P_1)\pi(P_2) + \pi(P_1)\lambda(P_2)$ , for  $P_1, P_2$  in  $\mathbf{Q}\langle A \rangle$ . Applying  $\lambda$  to the previous relation: we obtain  $\lambda(\underline{C}) = \pi(X)\epsilon_1 d\pi(Z)$ . Since  $\lambda(\underline{C}) > 0$ , this shows that  $\epsilon_1 = 1$ .

To conclude the proof of Th.1.1, observe that if  $C$  is prefix, then  $S_1 = 1$  by Lemma 3.3.(vi); since  $(\underline{A} - 1)S_1 = LM$  and  $M = (\underline{A} - 1)M'$ , we obtain that  $\underline{A} - 1 = L(\underline{A} - 1)M'$ . Thus  $M' = \pm 1$  and  $Z = \pm M' = \pm 1$ . Since  $\pi(Z) \geq 0$ , we deduce  $Z = 1$ .

On the other hand, if  $C$  is suffix,  $P_1 = 1$  by Lemma 3.3.(vi) again. Since  $P_1 = EF$ , we obtain  $E = \pm 1$ . Since  $E = Up_n$ , we obtain by Gauss' lemma,  $\pm 1 = \bar{U}\bar{p}_n$ , hence  $X = \pm \bar{U} = \pm 1$ ; since  $\pi(X) \geq 0$ ,  $X = 1$ .  $\blacksquare$

REMARK 10.3.4. A closer look at the previous proof proves the following claim: under the hypothesis of Th.1.1, one has

$$\underline{C} - 1 = X(d(\underline{A} - 1) + (\underline{A} - 1)Y(\underline{A} - 1))Z,$$

and moreover

$$P_1 = X(1 + (\underline{A} - 1)X'), S_1 = (1 + Z'(\underline{A} - 1))Z,$$

for some polynomials  $X, Y, Z, X', Z'$  in  $\mathbf{Z}\langle A \rangle$ , and in particular

$$\pi(X) = \pi(P_1), \pi(Z) = \pi(S_1).$$

Recall that  $P_1, S_1$  are as defined in Lemma 3.3 and its proof, and therefore satisfy:

$$u_1^{-1}\underline{C}^* = S_1\underline{C}^*, \underline{C}^*v_1^{-1} = \underline{C}^*P_1$$

for some words  $u_1, v_1$  in  $C^*$ . Note that the *average length*  $\sum_{w \in C} \pi(w)|w|$  of  $C$  is equal to  $\lambda(\underline{C}) = \pi(X)d\pi(Z)$ .

We prove the claim, by going through the proof of Th.1.1: we have  $P_1 = EF$ ,  $F \equiv 1$  (by Lemma 2.8 since  $G \equiv 1$  and  $GF \equiv 1$ ),  $E = \bar{U}\bar{p}_n$  (by Gauss' lemma, since  $E = Up_n$ , and  $E$  being primitive since  $P_1$  is and  $P_1 = EF$ ); furthermore  $\bar{q}_n \equiv \pm 1$  (by Lemma 2.8, since  $\bar{q}_n\bar{V} = K \equiv 1$ ), which implies, by an argument similar to that for  $p_{n-1}$  and  $q_{n-1}$  in the proof of Th.1.1, that  $\bar{p}_n \equiv \pm 1$ ; thus we obtain that  $\bar{p}_nF \equiv \pm 1$ , and  $P_1 = \bar{P}_1 = \bar{U}\bar{p}_nF$ , which is the product of  $\pm X$  with a polynomial which is  $\equiv \pm 1$ . Since  $\pi(P_1) > 0$  and  $\pi(X) \geq 0$ , we obtain finally that  $P_1$  is of the desired form  $X(1 + (\underline{A} - 1)X')$ .

On the other hand,  $Z = \pm M'$ ;  $M = (\underline{A} - 1)M'$ ;  $(\underline{A} - 1)S_1 = (1 + (\underline{A} - 1)L')M$ . Thus  $(\underline{A} - 1)S_1 = (1 + (\underline{A} - 1)L')(\underline{A} - 1)M'$ , which implies that  $S_1 = (1 + L'(\underline{A} - 1))M'$ , and  $\pi(S_1) = \pi(M')$ . Since  $\pi(S_1) > 0$  and  $\pi(Z) \geq 0$ , we have in fact  $S_1 = (1 + L'(\underline{A} - 1))Z$ , which proves the claim.

## 10.4. Applications

Let  $\pi$  be a Bernoulli morphism. Recall that the *average length* (with respect to  $\pi$ ) of a finite code  $C$  is the number  $\sum_{w \in C} \pi(w)|w|$ . Moreover, the measure  $\pi$  is said to be positive if  $\pi(w) > 0$  for any word  $w$ .

**COROLLARY 10.4.1.** *Let  $C$  be a finite maximal code and  $\pi$  be some positive Bernoulli measure. The average length of  $C$  is greater or equal to the degree of  $C$ , with equality if and only if  $C$  is biprefix.*

*Proof*

By Remark 3.4, we have  $\pi(X) = \pi(P_1)$  and  $\pi(Z) = \pi(S_1)$ . By Lemma 3.3,  $\pi(S_1) \geq 1$  (resp.  $\pi(P_1) \geq 1$ ), with equality if and only if  $P_1 = 1$  (resp.  $S_1 = 1$ ). Thus, since the average length of  $C$  is equal to  $\lambda(\underline{C}) = \pi(X)d\pi(Z)$ , we obtain that it is  $\geq d$ .

If equality holds, then we must have  $P_1 = S_1 = 1$ . Then  $C$  is biprefix by Lemma 3.3 (vi).  $\blacksquare$

Let  $x$  be any word and  $C$  a finite code. Consider the set  $E(x)$  of pairs of words  $(u, v)$  such that  $uxv$  is in the submonoid  $C^*$  generated by  $C$ ; this set has a natural partial order defined by  $(u, v) \leq (u', v')$  if for some  $m_1, m_2 \in C^*$ , one has  $u' = m_1u, v' = vm_2$  (so that  $u'mv' = m_1umvm_2$ ). A *context* of  $x$  with respect to  $C$  is an element in  $E(x)$  which is minimal for this order. In other words, a context of  $x$  is a pair  $(p, s)$  such that: either  $pxs = c_1 \dots c_n, c_i \in C, n \geq 1$ , with  $p$  a proper left factor of  $c_1$  and  $s$  a proper right factor of  $c_n$ , or  $pxs = 1$ : for  $x = 1$  (and also for  $x \in C^*$ )  $(1, 1)$  is a context). Observe that the set of contexts of a word is finite. Its *measure* is by definition  $\sum \pi(p)\pi(s)$ , where the sum is over all contexts  $(p, s)$  of  $x$ .

**COROLLARY 10.4.2.** *The measure of the set of contexts of a word with respect to a finite maximal code is equal to the average length of this code.*

We prove in fact a noncommutative version of this result.

*Proof*

Fix a finite maximal code  $C$  and a word  $x$ . Define a mapping  $e$  from  $\mathbf{Z}\langle\langle A \rangle\rangle$  into the complete tensor product  $\mathbf{Z}\langle\langle A \rangle\rangle \otimes_{\mathbf{Z}} \mathbf{Z}\langle\langle A \rangle\rangle$ , by  $e(w) = \sum_{uxv=w} u \otimes v$ . It is easily seen that  $e(\underline{A}^*) = \underline{A}^* \otimes \underline{A}^*$ . Furthermore, the very definition of a context implies that  $e(\underline{C}^*) = \sum_{p,s} \underline{C}^* p \otimes s \underline{C}^*$ , where the sum is extended to all contexts  $(p, s)$  of  $x$  with respect to  $C$ . Thus  $e(\underline{C}^*) = (\underline{C}^* \otimes 1)X(1 \otimes \underline{C}^*)$ , where  $X = \sum p \otimes s$ , summed over all contexts of  $x$ .

Suppose that  $x$  is nonempty; then we have for any words  $s, m, p$ :

$$\begin{aligned} e(smp) &= (s \otimes 1)e(m)(1 \otimes p) + e(s)(1 \otimes mp) + (sm \otimes 1)e(p) \\ &+ \sum_{u,v \neq 1, x=uv} (su^{-1} \otimes (v^{-1}m)p + s(mu^{-1}) \otimes v^{-1}p) + \sum_{u,v \neq 1} (umv, x)su^{-1} \otimes v^{-1}p, \end{aligned}$$

where we use  $u^{-1}$  in the same way as the notation recalled at the beginning of Section 3, and where  $(,)$  is the scalar product on  $\mathbf{Z}\langle A \rangle$  that has  $A^*$  as an orthonormal basis.

The proof of this formula follows by inspection, once the 6 possibilities for the word  $x$  to be a factor of the word  $sm p$  have been observed: either  $x$  appears as a factor of  $m$ , or of  $s$  or  $p$ , or  $x$  is an overlapping factor of the product  $sm$  or  $mp$ , or finally  $x$  is factor of  $sm p$  which starts properly in  $s$  and ends properly in  $p$ .

Note that the previous formula is linear in each of  $s, m, p$ , so it extends to series  $S, M, P$ . Now we have by Cor.1.2,  $\underline{A}^* = S\underline{C}^*P$ , where  $P, S$  are polynomials. Hence we obtain

$$\begin{aligned} \underline{A}^* \otimes \underline{A}^* &= e(\underline{A}^*) = e(S\underline{C}^*P) \\ &= (S \otimes 1)e(\underline{C}^*)(1 \otimes P) + e(S)(1 \otimes \underline{C}^*P) + (S\underline{C}^* \otimes 1)e(P) \\ &\quad + \sum_{u,v \neq 1, x=uv} (Su^{-1} \otimes (v^{-1}\underline{C}^*)P + S(\underline{C}^*u^{-1}) \otimes v^{-1}P) \\ &\quad + \sum_{u,v \neq 1} (u\underline{C}^*v, x)Su^{-1} \otimes v^{-1}P. \end{aligned}$$

Note that the last summand is a finite sum,  $R$ , and that  $e(\underline{C}^*) = (\underline{C}^* \otimes 1)X(1 \otimes \underline{C}^*)$ . By the proof of Lemma 3.1, where  $S(v)$  and  $P(u)$  are defined, we thus have

$$\begin{aligned} \underline{A}^* \otimes \underline{A}^* &= (S\underline{C}^* \otimes 1)X(1 \otimes \underline{C}^*P) + e(S)(1 \otimes \underline{C}^*P) + (S\underline{C}^* \otimes 1)e(P) \\ &\quad + \sum_{u,v \neq 1, x=uv} (Su^{-1} \otimes S(v)\underline{C}^*P + S\underline{C}^*P(u) \otimes v^{-1}P) + R. \end{aligned}$$

Let us multiply by  $P(1 - \underline{A}) \otimes 1$  on the left and by  $1 \otimes (1 - \underline{A})S$  on the right. Since  $P(1 - \underline{A})S$  is the inverse of  $\underline{C}^*$ , we obtain

$$\begin{aligned} P \otimes S &= X + (P(1 - \underline{A}) \otimes 1)e(S) + e(P)(1 \otimes (1 - \underline{A})S) \\ &\quad + \sum_{u,v \neq 1, x=uv} (P(1 - \underline{A})(Su^{-1}) \otimes S(v) + P(u) \otimes (v^{-1}P)(1 - \underline{A})S) \\ &\quad + (P(1 - \underline{A}) \otimes 1)R(1 \otimes (1 - \underline{A})S). \end{aligned}$$

Note that when  $x$  is the empty word, then formula for  $e(smp)$  has to be slightly modified: the  $\Sigma$ 's are replaced by  $-s \otimes mp - sm \otimes p$ , and from here on the argument is similar and hence we omit it.

This shows that the sum of the contexts of the word  $x$  is equal to  $P \otimes S$  modulo the two sided ideal of  $\mathbf{Z}\langle A \rangle \otimes \mathbf{Z}\langle A \rangle$  generated by  $\underline{A} - 1 \otimes 1$  and  $1 \otimes (\underline{A} - 1)$ .

The homomorphism  $\pi \otimes \pi : \mathbf{Z}\langle A \rangle \otimes \mathbf{Z}\langle A \rangle \rightarrow \mathbf{R}$  vanishes on this ideal. Thus the measure of the set of contexts is equal to  $\pi(P)\pi(S)$ . Now, using  $\underline{C} - 1 = P(\underline{A} - 1)S$ , we find that the average length of  $C$  is equal to  $\lambda(\underline{C}) = \pi(P)\pi(S)$ .  $\blacksquare$

For later use in symbolic dynamics ????, we quote the following consequence of Th.1.1.

COROLLARY 10.4.3. *Let  $C$  be a finite maximal prefix code of degree  $> 1$ . Then one has a factorization  $\underline{C} - 1 = L(\underline{A} - 1)R$ , with  $L, R \in \mathbf{Z}\langle A \rangle$  and  $R$  nonconstant.*

*Proof*

By Th.1.1, we have a factorization  $\underline{C} - 1 = P(\underline{A} - 1)(d + Q(\underline{A} - 1))$ . If  $Q = 0$ ,  $d$  divides  $-1$ , a contradiction. Hence  $Q$  is nonzero and  $d + Q(\underline{A} - 1)$  is nonconstant. ■

A code of degree 1 is called *synchronizing*. If  $C$  is a finite set of words in  $A^*$ , denote by  $\underline{C}$  the sum in  $\mathbf{Z}[A]$  of the commutative images of the words in  $C$ .

COROLLARY 10.4.4. *Let  $C$  be a finite maximal code on the alphabet  $A$ . Then  $\underline{C} - 1$  is a multiple of  $\underline{A} - 1$ . If the quotient of these two polynomials is irreducible in  $\mathbf{Z}[A]$ , then  $C$  has at least two of the following properties: prefix, suffix, synchronizing.*

REMARK 10.4.5. Note that the first assertion is already a consequence of ????. It implies the following nice result on the cardinality of the code:  $|C| \equiv 1 \pmod{(|A| - 1)}$ . In fact, with the notation of Cor.1.2, one has  $|C| = 1 + ps \pmod{(|A| - 1)}$ , where  $p, s$  denote the image of  $P, S$  under the homomorphism sending each letter onto 1 (and thus  $\underline{C}$  onto  $|C|$ ). Note that in the particular case where  $C$  is a finite prefix code, this equality on the cardinality has the following interpretation:  $ps$  is the number of internal nodes of the  $|A|$ -ary tree representing  $C$ , and the previous equality comes from the corresponding equality relating the number of external and internal nodes of a rooted tree, see ????. The previous equality also has some analogy with the Schreier formula asserting that if  $H$  is a subgroup of the free  $G$  group generated by  $A$ , then  $H$  is free of rank  $h$ , with  $h = 1 + |G/H|(|A| - 1)$ .

*Proof* of the Corollary.

Let  $\rho$  the canonical homomorphism  $\mathbf{Z}\langle A \rangle \rightarrow \mathbf{Z}[A]$ . Then by Remark 3.4, we have  $\underline{C} - 1 = \rho(X)\rho(Z)(d + \rho(Y)(\underline{A} - 1))(\underline{A} - 1)$ , which proves the first assertion. If the quotient is irreducible, then we must have two of the three following equalities:  $\rho(X) = \pm 1$ ,  $\rho(Z) = \pm 1$ ,  $d + \rho(Y)(\underline{A} - 1) = \pm 1$ .

The equality  $\rho(X) = \pm 1$  implies, by Remark 3.4, that  $\pi(S_1) = 1$ , hence  $S_1 = 1$ , and then that  $C$  is prefix (Lemma 3.3.(vi)). We deal with the second equality similarly.

If the third equality holds, then we must have  $\rho(Y) = 0$ , and  $d = \pm 1$ , which implies  $d = 1$ , hence  $C$  is synchronizing. ■

## 10.5. Notes

The results in Section 1 and the proof in Section 3 are from [12]. Th.1.1 extends a commutative factorization result by Schützenberger [14]. Th.2.1 and Cor.2.2 are a particular case of Paul Cohn's weak algorithm, see [4]; for their proofs, we

have followed a lexicographic argument from [9]. Th.2.3 and Th.2.7 are from [4]. Th.2.4, Lemma 2.8 and 2.9 are from [12]. Cor.4.1 is due to Schützenberger [13]. Cor.4.2 is due to Hansel and Perrin [8]. Cor.4.4 is from [14].

Note that the relations (ii) and (iii) in Lemma 3.3 are each a weak form of the factorization conjecture, since  $L_1$  is a finite sum of words (for the conjecture, one would need to have  $L_1 = 0$ ); this form was also found by [17]. For partial results on the factorization conjecture, see [11], [2], [7], [5], [6]. For results involving constructions of factorizing codes and multiple factorizations, see [10], [16], [3].

It is conjectured that each finite maximal code is commutatively equivalent to a prefix code, meaning that there exists a prefix code having the same commutative image as the initial code. This would be a consequence of the factorization conjecture; indeed, it was shown by Schützenberger that if the quotient mentioned in Cor.4.4 has nonnegative coefficients, then the code is commutatively equivalent to a prefix code; see [1] Th.VIII.6.1 ????. Note that not every finite code is commutatively equivalent to a prefix code (according to an example from [15]).

## Bibliography

- [1] J. Berstel and D. Perrin. *The theory of codes*. Academic Press, 1985.
- [2] J.-M. Boë. Sur les codes synchronisants coupants. In A. de Luca, editor, *Non-commutative structures in algebra and geometric combinatorics*. Consiglio Nazionale delle Ricerche, Roma, 1981.
- [3] V. Bruyère and C. De Felice. Synchronization and decomposability for a family of codes. *International Journal of Algebra and Computation*, 2, 1992.
- [4] P. Cohn. *Free rings and their relations*. First Edition 1971. London Mathematical Monographs No.19. Academic Press, 1985.
- [5] C. De Felice. On the factorization conjecture. In *STACS'92*. Lecture Notes in Computer Science 577, 1992.
- [6] C. De Felice. A partial result about the factorization conjecture for finite variable-length codes. *Discrete Mathematics*, 122, 1993.
- [7] C. De Felice and C. Reutenauer. Solution partielle de la conjecture de factorisation des codes. *Notes aux Comptes Rendus de l'Académie des Sciences, Paris*, 302, 1986.
- [8] G. Hansel and D. Perrin. Codes and bernoulli partitions. *Mathematical Systems Theory*, 16, 1983.
- [9] G. Melançon. Constructions des bases standards des  $K\langle A \rangle$ -modules à droite. *Theoretical Computer Science*, 117, 1993.
- [10] D. Perrin. Codes asynchrones. *Bulletin de la Société mathématique de France*, 105, 1977.
- [11] A. Restivo. On codes having no finite completion. *Discrete Mathematics*, 17, 1977.
- [12] C. Reutenauer. Noncommutative factorization of variable-length codes. *Journal of Pure and Applied Algebra*, 36, 1985.
- [13] M.-P. Schützenberger. On a special class of recurrent events. *Annals of Mathematical Statistics*, 32, 1961.

- [14] M.-P. Schützenberger. Sur certains sous-monoïdes libres. *Bulletin de la Société mathématique de France*, 93, 1965.
- [15] P. Shor. A counterexample to the triangle conjecture. *Journal of Combinatorial Theory Ser.A*, 38, 1983.
- [16] M. Vincent. Construction de codes indécomposables. *RAIRO Informatique Théorique*, 19, 1985.
- [17] L. Zhang and C. Gu. On factorization of finite maximal codes. In M. Ito, editor, *Words, languages and combinatorics*. World Scientific, 1992.