TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 285, Number 1, September 1984

FACTORIZING THE POLYNOMIAL OF A CODE

BY

G. HANSEL, D. PERRIN AND C. REUTENAUER

ABSTRACT. We give an extension and a simplified presentation of a theorem of Schützenberger. This theorem describes the factorization of the commutative polynomial associated with a finite maximal code. It is the deepest result known so far in the theory of (variable-length) codes.

1. Introduction. A *code* is, by definition, the basis of a free submonoid of a free monoid. The structure of these objects is far from being completely known by now. The attention has been focused on codes which are both *finite* and *maximal*. Let X be such a code over the alphabet A. It is a remarkable fact that in all known cases one can find two finite subsets Q, Q' of the free monoid A^* such that any word w in A^* has a unique factorization

$$w = q'xq \tag{1}$$

with $q' \in Q'$, $q \in Q$ and $x \in X^*$ the submonoid generated by X.

The identity (1) can be equivalently written in terms of characteristic polynomials as

$$1 - X = Q(1 - A)Q'. \tag{2}$$

The existence of such sets Q and Q' can be proved in some special cases such as the case of prefix codes. They correspond to the case where $Q' = 1$. The conjecture that sets Q' and Q always exist in the general case is probably the main open question concerning codes.

A natural direction is to study what happens with identity (2) by considering the commutative image $1 - \theta(X)$ of the polynomial $1 - X$. It will be shown later on that $1 - \theta(X)$ is divisible by $1 - \theta(A)$. The quotient

$$T = (1 - \theta(X))/(1 - \theta(A))$$

is clearly a polynomial with nonnegative coefficients if (2) holds. Moreover, one can prove that T has nonnegative coefficients if and only if the code X is commutatively equivalent to a prefix code. All this motivates the study of the polynomial T.

It has been proved by Schützenberger in [**4**] that if T is irreducible over $\mathbf{Z}[A]$, then X is either prefix or suffix. This result would clearly be deduced if a factorization of type (2) could be proved to hold.

The purpose of this paper is to develop Schützenberger's theorem in several directions.

In the first place, we prove that for each noncommutative polynomial X with no constant term, the polynomial $1 - \theta(X)$ is equal to the determinant of some linear mapping canonically associated with X (Theorem 4.8).

Received by the editors December 13, 1982 and, in revised form, June 16, 1983.
1980 *Mathematics Subject Classification.* Primary 20M35; Secondary 16A06, 94B45.

0002-9947/84 $1.00 + $.25 per page

Further, we use a sequence of subspaces invariant under this linear mapping to factorize the polynomial $1 - \theta(X)$, in the case where X is a finite maximal code. We show how the factors of $1 - \theta(X)$ are related to the structure of X (Theorem 5.1). The description of these factors is more precise than that given in [**4**]. In particular, one of these factors is related with the degree of the code (condition (iv) in Theorem 5.1). The corresponding formula is already stated in [**4**] but the proof is not complete. Two other factors are related to the so-called sets of left and right contexts (see §3). We prove that each of these two polynomials divides the characteristic polynomial of any maximal set of strict right (resp. left) contexts. This result improves those of [**4**].

2. Preliminaries. Let A be a set called an alphabet. We denote by A^* the free monoid generated by A. Its neutral element is denoted by 1 and $A^+ = A^* \setminus 1$. S denotes the algebra over $\mathbf{Q}$ of noncommutative formal series in A; it is the set of all mappings $A^* \to \mathbf{Q}$. The image of $w \in A^*$ by $\sigma \in S$ is denoted $\sigma(w)$. The product of two elements σ, τ in S is defined by

$$\sigma\tau(w) = \sum_{uv=w} \sigma(u)\tau(v) \qquad (w \in A^*).$$

We denote by $S^{(1)}$ the set of all series without constant term: $S^{(1)} = \{\sigma \in S | \sigma(1) = 0\}$. For $\sigma \in S^{(1)}$, we define $\sigma^* = \sum_{n \geq 0} \sigma^n$ which makes sense because $\sigma(1) = 0$ implies that for any w in A^*, $\sigma^n(w) = 0$ for all but a finite number of integers $n \geq 0$. Classically $\sigma^* = (1 - \sigma)^{-1}$.

Denote by P the subalgebra of polynomials of S, which is the set of $\sigma \in S$ such that $\sigma(w) = 0$ for all but a finite number of $w \in A^*$. Actually, P is the free $\mathbf{Q}$-algebra generated by A. Any series σ in S extends uniquely to a linear form on P, defined by

$$\sigma(p) = \sum_{w \in A^*} \sigma(w)p(w).$$

In this way, S becomes the dual of P.

We denote by $\mathbf{Q}[[A]]$ the ring of series in the commuting variables in A with coefficients in $\mathbf{Q}$. The corresponding ring of polynomials is denoted by $\mathbf{Q}[A]$. The canonical morphism from S onto $\mathbf{Q}[[A]]$ is denoted by θ. Obviously $\theta(P) = \mathbf{Q}[A]$.

For a subset X of A^*, define $\underline{X}$ to be the characteristic series of X, that is

$$\underline{X}(w) = \begin{cases} 1 & \text{if } w \in X, \\ 0 & \text{otherwise.} \end{cases}$$

In the sequel we shall often identify a word $w \in A^*$ with the characteristic series $\{\underline{w}\}$.

A subset X of A^* is a *code* if the submonoid L of A^* it generates is free with basis X. Note that X is a code exactly when $\underline{L} = \{\underline{X}\}^*$.

In general, we denote by X^* the submonoid of A^* generated by X.

A subset X of A^* is said to be *prefix* if no word in X is a proper left factor of another word in X, that is, $XA^+ \cap X = \emptyset$. Note that if $X \subset A^*$ is prefix then either $X = \{1\}$ or $X \subset A^+$. In the latter case, X is a code, as may easily be verified. Recall that a submonoid L is generated by a prefix code if and only if the following

conditions holds:

$$u, uv \in L \Rightarrow v \in L$$

for any words u, v (see [**1**, p. 88]).

A subset X is *suffix* if the symmetric condition $A^+X \cap X = \emptyset$ holds, and *biprefix* if it is both prefix and suffix.

Let L be a subset of A^*. For w in A^* let

$$D_w^L = \{(u, v) \in A^* \times A^* | uwv \in L\}.$$

The relation on A^* defined by $w \sim w' \Leftrightarrow D_w^L = D_{w'}^L$ is a congruence, called the *syntactic congruence* of L. The quotient monoid $M = A^*/\sim$ is the *syntactic monoid* of L. If $\varphi: A^* \to M$ denotes the canonical morphism, one has $\varphi^{-1}\varphi(L) = L$.

A subset L of A^* is *recognizable* if its syntactic monoid is finite. A finite subset is easily shown to be recognizable. Classically, if X is a recognizable subset of A^*, then the submonoid generated by X is also recognizable [**1**, p. 142].

Let X be a code and $L = X^*$. Then X is *complete* if for any $w \in A^+$, $D_w^L \neq \emptyset$. If X is recognizable, it is complete if and only if it is maximal (as a code), see [**1**, p. 94].

Let $X \subset A^*$ be a recognizable code and $\varphi: A^* \to M$ the natural homomorphism from A^* onto the syntactic monoid of X^*. We give here some results on monoids which we need in the sequel (see [**3**]). Since M is finite, it has a unique minimal ideal, say J; J is equal to a disjoint union of the minimal right (resp. left) ideals of M. We denote by Γ (resp. Λ) the set of minimal right (resp. left) ideals of M:

$$J = \bigcup_{R \in \Gamma} R = \bigcup_{L \in \Lambda} L.$$

For any $R \in \Gamma$, $L \in \Lambda$, the intersection $R \cap L$ is a group: all these groups are isomorphic and have in particular the same order.

Let $m \in M$, $R \in \Gamma$ and $L \in \Lambda$. Then $mR \in \Gamma$ and the left translation $x \mapsto mx$ induces a bijection from R on mR. Similarly $Lm \in \Lambda$ and the right translation $x \mapsto xm$ induces a bijection from L on Lm.

When X is complete, the submonoid $\varphi(X^*)$ intersects J, because $\varphi(w) \in J$ and $uwv \in X^*$ implies $\varphi(uwv) \in J \cap \varphi(X^*)$. Let Γ' (resp. Λ') denote the set of minimal right (resp. left) ideals of M which intersect $\varphi(X^*)$. Then, for $R \in \Gamma$ and $L \in \Lambda$, the group $G = R \cap L$ intersects $\varphi(X^*)$ if and only if $R \in \Gamma'$ and $L \in \Lambda'$. The intersection $G \cap \varphi(X^*)$ is a subgroup H which does not depend (up to an isomorphism) on the choice of $(R, L) \in \Gamma' \times \Lambda'$. The index of H in G is by definition the *degree* of the code X, denoted by $d(X)$. The code X is *synchronizing* if $d(X) = 1$.

3. Bernoulli morphisms. A *Bernoulli morphism* is a monoid homomorphism $\pi: A^* \to]0, 1]$ (multiplicative structure), such that

$$\sum_{a \in A} \pi(a) = 1. \tag{3.1}$$

A Bernoulli morphism Π extends in several ways:

(1) First, by linearity, to any polynomial $p \in P$ by

$$\pi(p) = \sum_{w \in A^*} p(w)\pi(w). \tag{3.2}$$

(2) Then π extends to a mapping from the powerset $\mathcal{P}(A^*)$ into $\mathbf{R}_+ \cup \{\infty\}$ by

$$\pi(L) = \sum_{w \in L} \pi(w) \qquad (L \subset A^*). \tag{3.3}$$

In the sequel we shall denote all these extensions by π. Note that for any $n \geq 0$, one has $\pi(A^n) = 1$ and hence π defines a probability on each $\mathcal{P}(A^n)$.

(3) Let $\sigma \in S$. We denote by σ_n the polynomial defined by

$$\sigma_n = \sum_{w \in A^n} \sigma(w) w$$

(σ_n is obtained by keeping only the words of length n). We say that σ *admits a density* (with respect to π) if the sequence $(\pi(\sigma_n))_{n \geq 0}$ has a limit in the average. This limit

$$\delta(\sigma) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \pi(\sigma_i) \tag{3.4}$$

is called the *density* of σ. By definition, a subset L admits a density if the series $\underline{L}$ admits one. This is equivalent to the fact that the sequence $(\pi(L \cap A^n))_{n \geq 0}$ converges in the average. In particular $\delta(A^*) = 1$.

Remark that for $u \in A^*$ and $\sigma \in S$, one has

$$\delta(u\sigma) = \pi(u)\delta(\sigma) \tag{3.5}$$

and, more generally, for $p \in P$,

$$\delta(p\sigma) = \pi(p)\delta(\sigma). \tag{3.6}$$

Note that for (1) and (3), one could take $\mathbf{Q}[A]$ and $\mathbf{Q}[[A]]$ without change, in place of P and S. Furthermore, for two polynomials $p, q \in \mathbf{Q}[A]$, one has $\pi(p) = \pi(q)$ for any Bernoulli morphism π if and only if

$$p \equiv q \mod(1 - \theta(\underline{A})). \tag{3.7}$$

The following result gives some known properties which we shall use in the sequel (see [**2**] e.g.).

PROPOSITION 3.1. *Let $\varphi: A^* \to M$ be a monoid homomorphism and M a finite monoid. Let $\pi: A^* \to]0, 1]$ be a Bernoulli morphism.*

(1) *For any subset N of M, $\varphi^{-1}(N)$ admits a density and the mapping $\nu: \mathcal{P}(M) \to]0, 1]$ defined by $\nu(N) = \delta(\varphi^{-1}(N))$ is a probability.*

(2) *ν is concentrated on the minimal ideal J of M:*

$$\nu(J) = 1. \tag{3.8}$$

(3) *For any right ideal R and any left ideal L, one has $\nu(R \cap L) = \nu(R)\nu(L)$.*

(4) *For any minimal right ideal R and any minimal left ideal L one has for any m in $R \cap L$,*

$$\nu(m) = \frac{\nu(R)\nu(L)}{\mathrm{Card}(R \cap L)} \neq 0. \tag{3.9}$$

Now let $X \subset A^+$ be a recognizable complete code. Define U and V by

$$U = \{u \in A^* | uA^* \cap X^* \neq \emptyset\}, \tag{3.10}$$

$$V = \{v \in A^* | A^* v \cap X^* \neq \emptyset\}. \tag{3.11}$$

U (resp. V) is the set of words *right* (resp. *left*) *completable* in X^*. Note that if $\varphi: A^* \to M$ is the natural morphism on the syntactic monoid of X^*, then $\varphi^{-1}\varphi(U) = U$ and $\varphi^{-1}\varphi(V) = V$ because $\varphi^{-1}\varphi(X^*) = X^*$.

PROPOSITION 3.2. *Let $X \subset A^+$ be a recognizable complete code and d its degree. Let π be a Bernoulli morphism. Then X^* and the sets U, V of words right, left completable in X^* admit a density, and*

$$\delta(X^*) = \frac{1}{d}\delta(U)\delta(V). \tag{3.12}$$

PROOF. Let $\varphi: A^* \to M$ be the natural morphism from A^* onto the syntactic monoid of X^*. Let J be the minimal ideal of M. Let Γ (resp. Λ) be the set of minimal right (resp. left) ideals of M. Let Γ' (resp. Λ') be the set of minimal right (resp. left) ideals which intersect the submonoid $N = \varphi(X^*)$. By (3.8), we have $\delta(X^*) = \nu(N \cap J)$. But

$$N \cap J = \bigcup_{R \in \Gamma'} \bigcup_{L \in \Lambda'} (R \cap L \cap N).$$

By definition of the degree, one has for any $R \in \Gamma'$, $L \in \Lambda'$,

$$\operatorname{Card}(R \cap L \cap N) = d^{-1} \operatorname{Card}(L \cap R).$$

Moreover by (3.9), $\nu(R \cap L \cap N) = \operatorname{Card}(R \cap L \cap N)\nu(R)\nu(L)/\operatorname{Card}(R \cap L)$. Thus we obtain $\nu(R \cap L \cap N) = d^{-1}\nu(R)\nu(L)$. This implies that

$$\delta(X^*) = \sum_{R \in \Gamma'} \sum_{L \in \Gamma'} d^{-1}\nu(R)\nu(L) = d^{-1}\nu\left(\bigcup_{R \in \Gamma'} R\right)\nu\left(\bigcup_{L \in \Lambda'} L\right).$$

But $\varphi(U) \cap J = \bigcup_{R \in \Gamma'} R$ and $\varphi(V) \cap J = \bigcup_{L \in \Lambda'} L$. By (3.8) again, $\delta(U) = \nu(\varphi(U) \cap J)$ and $\delta(V) = \nu(\varphi(V) \cap J)$ and (3.12) follows. □

REMARK 3.1. The proposition above remains still true for any complete code X satisfying the hypothesis (weaker than recognizability) $D_w^X = \emptyset$ for at least one word w. Indeed, this hypothesis ensures that Proposition 3.1 holds for the syntactic monoid M of X^* (see [**2**]). □

Let X be a code. For any word w define $V'_w = \{v \in A^* | wv \in X^*\}$, $U'_w = \{u \in A^* | uw \in X^*\}$ and $V_w = V'_w - V'_w X^+$, $U_w = U'_w - X^+ U'_w$ where $X^+ = X^* - 1$.

By construction $V'_w = V_w \cup V'_w X$. Note that $V_w \cap V'_w X = \emptyset$ by definition of V_w. Moreover, the relation $ux = vy$, $u, v \in V'_w$ and $x, y \in X$ implies $u = v$ and $x = y$: indeed, one has $wux = wvy$, $wu \in X^*$, $wv \in X^*$ which implies (X being a code) $x = y$. Hence,

$$\underline{V'_w} = \underline{V_w} + \underline{V'_w}\underline{X} \quad \text{and} \quad \underline{V_w} = \underline{V'_w}(1 - \underline{X}) \quad \text{or} \quad \underline{V'_w} = \underline{V_w}\underline{X}^*. \tag{3.13}$$

Symmetrically, $\underline{U'_w} = \underline{X}^*\underline{U_w}$.

Note that each word in V_w is a right factor of a word in X. When X is finite, V_w and U_w are thus finite.

The set V_w (resp. U_w) is called the set of strict *right* (resp. *left*) context of w in X^*. We order these sets by inclusion and call a class of strict right contexts V_w *maximal* if for any word w', $V_w \subset V_{w'}$ implies $V_w = V_{w'}$.

PROPOSITION 3.3. *Let X be a finite complete code. Let U, V be the sets of words right, left completable in X^*. Let π be a Bernoulli morphism. Let $M = \varphi(A^*)$ be the syntactic monoid of X^* and J its minimal ideal. For any w in $U \cap \varphi^{-1}(J)$ the set V_w of strict right contexts of w in X^* satisfies*

$$\pi(V_w)\delta(U) = 1. \tag{3.14}$$

For any w in $V \cap \varphi^{-1}(J)$ the set U_w of strict left contexts of w in X^+ satisfies

$$\pi(U_w)\delta(V) = 1. \tag{3.15}$$

PROOF. Since V_w is finite, (3.13) and (3.6) imply

$$\delta(V'_w) = \pi(V_w)\delta(X^*). \tag{3.16}$$

We compute $\delta(V'_w)$: let $m = \varphi(w)$, $N = \varphi(X^*)$ and $T = \{k \in J \mid mk \in N\}$. As $\nu = \delta\varphi^{-1}$ is concentrated on J, one has $\delta(V'_w) = \nu(T)$. If k is in T, the left ideal Mk is minimal and intersects N. Hence T is included in $\bigcup_{L\in\Lambda'} L$. Moreover, for any minimal right ideal $R \in \Gamma$ and any $L \in \Lambda'$, the mapping $k \in R \cap L \to mk$ is a bijection from $R \cap L$ onto $(mM) \cap L$. Since $\operatorname{Card}(mM \cap L \cap N) = d^{-1} \operatorname{Card}(mM \cap L)$, one has $\operatorname{Card}(R \cap L \cap T) = d^{-1} \operatorname{Card}(R \cap L)$.

By (3.9), $\nu(R \cap L \cap T) = d^{-1}\nu(R)\nu(L)$. Hence

$$\nu(T) = \bigcup_{L\in\Lambda'} \bigcup_{R\in\Gamma} d^{-1}\nu(R)\nu(L) = d^{-1}\nu\left(\bigcup_{L\in\Lambda'} L\right).$$

Hence $\nu(T) = d^{-1}\delta(V)$. Furthermore by (3.16),

$$\pi(V_w) = \delta(V'_w)\delta(X^*)^{-1} = \delta(V)d^{-1}\delta(X^*)^{-1}.$$

Using (3.12) we obtain $\pi(V_w) = \delta(U)^{-1}$ and (3.14) follows. (3.15) is proved symmetrically. □

PROPOSITION 3.4 (HYPOTHESIS OF PROPOSITION 3.3). *The following are equivalent.*

(i) *V_w is a maximal set of strict right contexts.*

(ii) *There exists $w' \in U \cap \varphi^{-1}(J)$ such that $V_w = V_{w'}$.*

(iii) $\pi(V_w)\delta(U) = 1$.

PROOF. For any w in A^*, there exists w' in $U \cap \varphi^{-1}(J)$ such that $V_w \subset V_{w'}$: indeed, let $x \in X^* \cap \varphi^{-1}(J)$; then $V_w \subset V_{xw}$. Moreover, since the right ideal $\varphi(xA^*)$ is minimal, there exists v in A^* such that $\varphi(xwv) = \varphi(x)$; hence $xwv \in X^*$. This shows that $w' = xw$ is in $U \cap \varphi^{-1}(J)$.

(i)⇔(ii). If V_w is maximal, let $w' \in U \cap \varphi^{-1}(J)$ such that $V_w \subset V_{w'}$. Then $V_{w'} = V_w$ by maximality.

(ii)⇔(iii). This is (3.14).

(iii)⇔(i). Let $w' \in U \cap \varphi^{-1}(J)$ be such that $V_w \subset V_{w'}$. Then (3.14) implies $\pi(V_w) = \pi(V_{w'})$ and hence $V_w = V_{w'}$ because $\pi > 0$. □

4. Representations. We give below some elements of the linear representation theory of formal power series.

A *representation* of P on a $\mathbf{Q}$-vector space E is an algebra homomorphism $\varphi: P \to \operatorname{End}_{\mathbf{Q}}(E)$ in the algebra of endomorphisms of E. If φ is a representation, then φ_p

denotes the image of $p \in P$ by φ. The *dimension* of the representation is the dimension of E.

An *antirepresentation* of P is a linear mapping $\psi: P \to \mathrm{End}(E)$ such that $\psi_p\psi_q = \psi_{qp}$ for any polynomials p and q. All the results on representations extend easily, by duality, to antirepresentations.

A subspace E' of E is *φ-invariant* if for any $p \in P$, $\varphi_p(E') \subset E'$. In this case the *restriction* of φ to E' is defined as the representation $\varphi': P \to \mathrm{End}(E')$ induced by $\varphi: \varphi'_p = \varphi_p|E'$. Let $E'' = E/E'$. Then φ induces a representation φ'' on E'' by $\varphi''_p(e + E') = \varphi_p(e) + E'$, which makes sense because $\varphi_p(E') \subset E'$; φ'' is the representation on E'' *induced* by φ.

For any $\sigma \in S$ and $p \in P$, define two elements $\lambda_p(\sigma)$ and $\rho_p(\sigma)$ of S by

$$[\lambda_p(\sigma)](w) = \sigma(pw), \tag{4.1}$$

$$[\rho_p(\sigma)](w) = \sigma(wp) \tag{4.2}$$

for $w \in A^*$.

The mappings λ_p and $\rho_p: S \to S$ are linear. For any p, q in P one has $\lambda_p\lambda_q = \lambda_{qp}$ and $\rho_q = \rho_{pq}$. Thus ρ defines a representation of P on S and λ an antirepresentation.

For $\sigma \in S$, denote $E^\sigma = \{\rho_p(\sigma) | p \in P\}$. This subspace of S is clearly ρ-invariant. The restriction of ρ to E^σ, denoted by ρ^σ, is a representation of P called the *representation associated with* σ. Similarly ${}^\sigma E = \{\lambda_p(\sigma) | p \in P\}$. The restriction of λ to ${}^\sigma E$, denoted by ${}^\sigma\lambda$, is the *antirepresentation associated with* σ.

For any p, q in P we have

$$[\lambda_p(\sigma)](q) = [\rho_q(\sigma)](p) = \sigma(pq).$$

This formula allows to define a bilinear mapping ${}^\sigma E \times E^\sigma \to Q$ by

$$\langle \lambda_p(\sigma), \rho_q(\sigma) \rangle = \sigma(pq). \tag{4.3}$$

This mapping is nondegenerate on the right because $\langle \lambda_p(\sigma), \rho_q(\sigma) \rangle = 0$ for any $q \in P$, implies that $\lambda_p(\sigma) = 0$. Hence, through (4.3), ${}^\sigma E$ embeds in the dual of E^σ. Symmetrically E^σ embeds in the dual of ${}^\sigma E$. In particular, E^σ is finite dimensional if and only if ${}^\sigma E$ is, and then their dimensions are equal. In this case, we say that σ is a *recognizable* series. This terminology does not contradict the definitions of §2. Indeed, one shows that a subset X of A^* is recognizable if and only if the series $\underline{X}$ is (see [1]).

Note that for $\alpha \in {}^\sigma E$, $\beta \in E^\sigma$ and $p \in P$, one has

$$\langle \lambda_p(\alpha), \beta \rangle = \langle \alpha, \rho_p(\beta) \rangle. \tag{4.4}$$

Let $\varphi: P \to \mathrm{End}(E)$ be a representation of finite dimension. Let $(e_1, \ldots, e_n)$ be a basis of E; for any $u \in A^*$, let T_u be the matrix of φ_u in this basis. The matrix $T = \sum_{a \in A} \theta(a) T_a$ is an element of $\mathcal{M}_n(\mathbf{Q}[A])$. The *determinant associated* to φ is

$$\det(\varphi) = \det(I_n - T) \tag{4.5}$$

where I_n is the $n \times n$ identity matrix. Evidently, $\det(\varphi)$ does not depend on the choice of the basis.

The following result is an easy consequence of the definitions.

PROPOSITION 4.1. *Let $\varphi: P \to \mathrm{End}(E)$ be a finite dimensional representation of P, E' a φ-invariant subspace of E, $E'' = E/E'$. Let φ' be the restriction of φ to E' and φ'' the representation induced by φ on E''. Then*

$$\det(\varphi) = \det(\varphi')\det(\varphi''). \quad \square \tag{4.6}$$

Recall that $S^{(1)} = \{\sigma \in S \mid \sigma(1) = 0\}$ and $P^{(1)} = S^{(1)} \cap P$.

PROPOSITION 4.2. *Let $\sigma \in 1 + S^{(1)}$ be a recognizable power series. Then*

$$E^\sigma = \mathbf{Q}\sigma \oplus E^{(1)} \tag{4.7}$$

where $E^{(1)} = E^\sigma \cap S^{(1)}$. Let τ be the projection $E^\sigma \to E^{(1)}$ with kernel $\mathbf{Q}\sigma$. Let ψ be the representation of P on $E^{(1)}$ defined by $\psi_a(\alpha) = \tau(\rho_a(\alpha))$ for any $a \in A$ and $\alpha \in E^{(1)}$. Then

$$\theta(\sigma)\det(\rho^\sigma) = \det(\psi). \tag{4.8}$$

PROOF. (4.7) holds because $\sigma(1) = 1$: indeed the sum is direct since $\sigma \notin E^{(1)}$, and for any $\alpha \in E^\sigma$, $\alpha = \alpha(1)\sigma + [\alpha - \alpha(1)\sigma] \in \mathbf{Q}\sigma + E^{(1)}$.

Choose a basis $(e_1, \ldots, e_n)$ of E^σ such that $e_1 = \sigma$ and $e_2, \ldots, e_n \in E^{(1)}$. For w in A^* let T_w be the matrix of ρ_w^σ in this basis and w the matrix of ψ_w in the basis $(e_2, \ldots, e_n)$ of $E^{(1)}$. Then for $a \in A$

$$T_a = \begin{bmatrix} \cdots & \cdots \\ & R_a \end{bmatrix}.$$

Let $T = \sum_{a \in A} \theta(a) T_a$ and $R = \sum_{a \in A} \theta(a) R_a$. By classical formulas

$$[(I_n - T)^{-1}]_{1,1} = \det(I_{n-1} - R)/\det(I_n - T) = \det(\psi)/\det(\rho^\sigma).$$

Now define the $n \times n$ matrix F over S by

$$F = \sum_{a \in A} \underline{a} T_a \quad \text{and} \quad F^* = \sum_{w \in A^*} \underline{w} T_w.$$

Then $F^* = \sum_{n \geq 0} F^n = (I_n - F)^{-1}$. Furthermore, for any word w, $\rho_w(e_1) - \sigma(w)e_1$ is in $E^{(1)}$; hence $[T_w]_{1,1} = \sigma(w)$. This implies $[F^*]_{1,1} = \sigma$. Applying θ, we obtain $T = \theta(F)$ and hence $[(I_n - T)^{-1}]_{1,1} = \theta(\sigma)$, which implies (4.8). $\square$

The following result implies, in particular, that the image under θ of any recognizable series is rational in $\mathbf{Q}[[A]]$.

PROPOSITION 4.3. *Let E be a finite-dimensional ρ-invariant subspace of S. Let φ be the restriction of ρ to E. Let $\sigma \in (1 + S^{(1)}) \cap E$. Then $\theta(\sigma)\det(\varphi) \in \mathbf{Q}[A]$.*

PROOF. Let $E' = E^\sigma$ and $\varphi' = \rho^\sigma$. Then by (4.8) $\theta(\sigma)\det(\varphi') \in \mathbf{Q}[A]$. Let $E'' = E/E'$ and φ'' be the induced representation. Then by (4.6)

$$\theta(\sigma)\det(\varphi) = \theta(\sigma)\det(\varphi')\det(\varphi'') \in \mathbf{Q}[A]. \quad \square$$

Recall that, when $\sigma \in S$ is recognizable, then the spaces ${}^\sigma E$ and E^σ are in duality, by (4.3). For any subspace F of ${}^\sigma E$, we denote its orthogonal space in E^σ by $F^\perp$, that is,

$$F^\perp = \{\beta \in E^\sigma \mid \forall \alpha \in F, \langle \alpha, \beta \rangle = 0\}.$$

PROPOSITION 4.4. *Let $\sigma \in S$ be recognizable. Let F be a λ-invariant subspace of ${}^{\sigma}E$. Then $F^{\perp}$ is a ρ-invariant subspace of E^{σ}. Let μ be the restriction of λ to F and τ the representation induced by ρ on $E^{\sigma}/F^{\perp}$. Then*

$$\det(\mu) = \det(\tau). \tag{4.9}$$

PROOF. $F^{\perp}$ is ρ-invariant because $\alpha \in F$, $\beta \in F^{\perp}$ implies $\langle \alpha, \rho_p(\beta)\rangle = \langle \lambda_p(\alpha), \beta\rangle = 0$ (by (4.4)) for any p in P.

The bilinear form $f: F \times (E^{\sigma}/F^{\perp})$ defined by $f(\alpha, \beta + F^{\perp}) = \langle \alpha, \beta\rangle$ is nondegenerate. Moreover, for any p in P

$$\begin{aligned} f(\alpha, \tau_p(\beta + F^{\perp})) &= f(\alpha, \rho_p(\beta) + F^{\perp}) = \langle \alpha, \rho_p(\beta)\rangle \\ &= \langle \lambda_p(\alpha), \beta\rangle = f(\mu_p(\alpha), \beta + F^{\perp}). \end{aligned}$$

Hence, the linear mappings μ_p and τ_p are the transpose of each other. Thus (4.9) follows. □

In particular, taking $F = {}^{\sigma}E$ with σ recognizable in S, yields

$$\det(\rho^{\sigma}) = \det({}^{\sigma}\lambda). \tag{4.10}$$

We now compute the representations associated to the star σ^* of a series $\sigma \in S^{(1)}$.

PROPOSITION 4.5. *Let σ, σ' in S. Then for each $a \in A$*

$$\rho_a(\sigma\sigma') = \sigma\rho_a(\sigma') + \rho_a(\sigma)\sigma'(1). \tag{4.11}$$

PROOF. It suffices to verify the formula for $\sigma = \underline{w}$, $\sigma' = \underline{w'}$ (w, w' in A^*). This is left to the reader. The formula then extends by linearity to S. □

PROPOSITION 4.6. *Let $\sigma \in S^{(1)}$ and $a \in A$. Then*

$$\rho_a(\sigma^*) = \sigma^*\rho_a(\sigma). \tag{4.12}$$

PROOF. We have $\sigma^* = 1 + \sigma^*\sigma$. Applying (4.11) and using $\sigma(1) = 0$, $\rho_a(1) = 0$ we obtain

$$\rho_a(\sigma^*) = \rho_a(1) + \rho_a(\sigma^*\sigma) = \sigma^*\rho_a(\sigma). \quad \square$$

For $\sigma \in S$, define the following ρ-invariant subspace of E^{σ}:

$$E^{\sigma}_{+} = \{\rho_p(\sigma) | p \in P^{(1)}\}.$$

PROPOSITION 4.7. *Let $\sigma \in S^{(1)}$. Then the mapping $\gamma: \beta \to \sigma^*\beta$ defines an isomorphism from E^{σ}_{+} to $E^{\sigma^*}_{+}$.*

PROOF. We show that $\beta \in E^{\sigma}_{+}$ implies $\sigma^*\beta \in E^{\sigma^*}_{+}$. It is enough to prove it when $\beta = \rho_u(\sigma)$, $u \in A^+$. Let $u = av$, $a \in A$, $v \in A^*$. We use induction on the length of u. If $|u| = 1$, by (4.12), $\sigma^*\beta = \sigma^*\rho_a(\sigma) = \rho_a(\sigma^*) \in E^{\sigma^*}_{+}$. Suppose $|v| \geq 1$, then $\sigma^*\rho_v(\sigma) \in E^{\sigma^*}_{+}$. By (4.11)

$$\rho_a(\sigma^*\rho_v(\sigma)) = \sigma^*\rho_{av}(\sigma) + \rho_a(\sigma^*)\sigma(v). \tag{4.13}$$

This shows that $\sigma^*\rho_u(\sigma) = \sigma^*\rho_{av}(\sigma) \in E^{\sigma^*}_{+}$.

Thus $\gamma(E^{\sigma}_{+}) \subset E^{\sigma^*}_{+}$; γ is clearly injective. Its image is a ρ-invariant subspace of $E^{\sigma^*}_{+}$ because by (4.13)

$$\rho_a(\sigma^*\rho_v(\sigma)) = \sigma^*\rho_{av}(\sigma) + \sigma^*\rho_a(\sigma)\sigma(v).$$

Since $\operatorname{Im}\gamma$ contains all the series $\rho_a(\sigma^*)$ by (4.12), it is all of $E^{\sigma^*}_{+}$. □

As a consequence we prove the following result, which will be used in the next section.

THEOREM 4.8. *Let $p \in P^{(1)}$ be a polynomial without constant term. Then p^* is recognizable and*

$$\det(\rho^{p^*}) = 1 - \theta(p). \tag{4.14}$$

PROOF. Let $E = E^{p^*}$, $E_+ = E_+^{p^*}$ and $E^{(1)} = E \cap S^{(1)}$. We denote by $|q|$ the degree of a polynomial $q \in P$: $|q|$ =maximum of the length of words w such that $q(w) \neq 0$.

Let $m = |p|$; we may suppose that $m \geq 1$ (otherwise $p = 0$ and the result is clear). Let w be of length m such that $p(w) \neq 0$. We have $\rho_w(p) = p(w)1$ and hence $1 \in E_+^p$. By Proposition 4.7 we have $p^* \in E_+$. Hence, E_+ being ρ-invariant, $E_+ \subset E$ and $p^* \in E_+$ imply $E_+ = E$. In particular, E is finite dimensional and p^* is recognizable.

Again by Proposition 4.7, for any $\alpha \in E$ there exists a unique q in E_+^p such that $\alpha = p^*q$ (note that $E_+^p \subset P$). For $i = 0, 1, \ldots, m-1$ denote

$$E_i = \{p^*q | q \in E_+^p,\ |q| \leq i\}. \tag{4.15}$$

We have the inclusions $E_0 \subset E_1 \subset \cdots \subset E_{m-1}$. Moreover, $E_{m-1} = E$ because $E = p^*E_+^p$ and for $q \in E_+^p$, $|q| \leq m-1$. Furthermore, $E_0 = \mathbf{Q}p^*$ because $1 \in E_+^p$.

Let τ be the projection $E \to E^{(1)}$ such that $\tau(p^*) = 0$ and ψ the representation of P on $E^{(1)}$ defined for $a \in A$ by $\psi_a(\alpha) = \tau(\rho_a(\alpha))$.

For $i = 0, 1, 2, \ldots, m-1$ put $F_i = E_i \cap E^{(1)}$. Let $i \geq 1$ and $\alpha \in F_i$. Then $\alpha = p^*q$ with $|q| \leq i$ and $q(1) = 0$ (because $0 = \alpha(1) = p^*(1)q(1)$ and $p^*(1) \neq 0$). Thus by (4.11)

$$\rho_a(\alpha) = p^*\rho_a(q) + \rho_a(p^*)q(1) = p^*\rho_a(q).$$

As $|\rho_a(q)| \leq i-1$ we have $\rho_a(\alpha) \in E_{i-1}$; hence $\psi_a(\alpha) = \tau(\rho_a(\alpha)) \in F_{i-1}$. This shows, by Proposition 4.1, that $\det(\psi) = 1$, because the representation induced by ψ on F_i/F_{i-1} is zero and $0 = F_0 \subset F_1 \subset \cdots \subset F_{m-1} = E^{(1)}$. Now by (4.8), $\theta(p^*)\det(\rho^{p^*}) = 1$; hence, (4.14) holds true because $1 = \theta(1) = \theta(p^*(1-p)) = \theta(p^*)\theta(1-p)$. □

REMARK 4.1. It is a general fact that if $\sigma \in S^{(1)}$ is recognizable, then σ^* is also recognizable (see [**1**, p. 142]). The important and new fact in Theorem 4.8 is (4.14). A similar formula is proved in [**4**] in a different case: let $p \in P^{(1)}$ with *nonnegative* coefficients. It may be verified that there exists a finite-dimensional representation φ of P on a space V such that in some basis of V the matrices T_w of φ_w ($w \in A^*$) have nonnegative coefficients and that $p^*(w) = [T_w]_{1,1}$ (see [**1**, p. 142]). Moreover, one may assume that for each i, j there exists some word w such that $[T_w]_{i,j} > 0$. Then one has

$$\det(\varphi) = 1 - \theta(p). \quad \square \tag{4.16}$$

In the next section, we shall use the results of this section in the case of a series σ of the form $\sigma = \underline{X}^*$ with X a finite complete code.

Let us consider, more generally, a subset Y of A^* and the series $\sigma = \underline{Y}$. Let $\varphi: A^* \to M$ be the natural morphism from A^* onto the syntactic monoid M of Y (see §2). Let $M' = \varphi(Y)$.

Denote $E = E^\sigma$, $\rho = \rho^\sigma$. One has for all $v, v' \in A^*$,

$$\varphi(v) = \varphi(v') \quad \text{iff } \rho_v = \rho_{v'}. \tag{4.17}$$

Indeed, $\rho_v = \rho_{v'}$ implies that, for any u, w in A^*,

$$uvw \in A^* \Leftrightarrow \sigma(uvw) = 1 \Leftrightarrow \rho_v(\rho_w(\sigma))(u) = 1$$
$$\Leftrightarrow \rho_{v'}(\rho_w(\sigma))(u) = 1 \Leftrightarrow uv'w \in A^*.$$

Hence $D_v^{X^*} = D_{v'}^{X^*}$ and, by definition of the syntactic congruence, $\varphi(v) = \varphi(v')$.

Conversely, let $D_v^{X^*} = D_{v'}^{X^*}$; then, in order to show that $\rho_v = \rho_{v'}$, it is enough to prove $\rho_v(\rho_w(\sigma)) = \rho_{v'}(\rho_w(\sigma))$ for any word w. But this is implied by the above relations. This proves (4.17).

The monoid homomorphism defined by restriction of ρ to A^* may thus be factorized through M. For $m \in M$, let ρ_m denote the image by ρ of any element of $\varphi^{-1}(m)$. For a subset N of M denote $\rho_N = \sum_{n \in N} \rho_n$.

Note the formula

$$\langle \sigma, \rho_N(\sigma) \rangle = \mathrm{Card}(N \cap M'). \tag{4.18}$$

(4.17) also holds for $\lambda = {}^\sigma\lambda$ instead of ρ. In the same way, one may use the notation λ_m instead of λ_v for $m = \varphi(v)$.

5. The factorization theorem. The aim of this section is to prove the following result, which is the main theorem of this paper.

THEOREM 5.1. *Let $X \subset A^*$ be a finite complete code. There exist polynomials $p, q, r \in \mathbf{Z}[A]$ such that*

(i)

$$1 - \theta(\underline{X}) = pqr(1 - \theta(\underline{A})). \tag{5.1}$$

(ii *For any maximal set of strict right contexts V_w, the polynomial p divides $\theta(\underline{V_w})$ and $\theta(\underline{V_w}) \equiv p \bmod(1 - \theta(\underline{A}))$.*

(iii) *For any maximal set of strict left contexts U_w, the polynomial r divides $\theta(\underline{U_w})$ and $\theta(\underline{U_w}) \equiv r \bmod(1 - \theta(\underline{A}))$.*

(iv) *The polynomial q is related to the degree $d(X)$ of X by*

$$q \equiv d(X) \mod(1 - \theta(\underline{A})). \tag{5.2}$$

We shall prove this result in several steps. In this section we fix a complete finite code X, and let σ be the characteristic series of X^*; we denote $E = E^\sigma$, $E' = {}^\sigma E$, $\rho = \rho^\sigma$ and $\lambda = {}^\sigma\lambda$. M is the syntactic monoid of X^* and $\varphi: A^* \to M$ is the natural morphism; $M' = \varphi(X^*)$.

By Theorem 4.8 and its dual, we have

$$1 - \theta(\underline{X}) = \det(\rho) = \det(\lambda). \tag{5.3}$$

In order to obtain the desired factorization of $1 - \theta(\underline{X})$ we define a sequence of invariant subspaces of E and E'.

As indicated at the end of §4, one may use the notation ρ_m, λ_m instead of ρ_v, λ_v for $m = \varphi(v)$. Let J be the minimal ideal of M and Γ (resp. Λ) the set of minimal right (resp. left) ideals of M.

Let $E_0 = 0$.

Let E_1 be the subspace of E generated by the elements $\rho_R(\sigma) - \rho_{R'}(\sigma)$ $(R, R' \in \Gamma)$.

Let E_2 be the subspace of E generated by the elements $\rho_R(\sigma)$ $(R \in \Gamma)$.

Let E'_2 be the subspace of E' generated by the elements $\lambda_L(\sigma)$ $(L \in \Lambda)$.
Let E'_3 be the subspace of E' generated by the elemnts $\lambda_L(\sigma) - \lambda_{L'}(\sigma)$ $(L, L' \in \Lambda)$.
Let $E'_4 = E'$.
Finally, let

$$E_4 = E = E'^{\perp}, \quad E_3 = E'^{\perp}_3,$$
$$E'_1 = E^{\perp}_1, \quad E'_0 = E^{\perp}_0 = E'.$$

PROPOSITION 5.2. *The subspaces E_i are ρ-invariant and $E_0 \subset E_1 \subset E_2 \subset E_3 \subset E_4$. The subspaces E'_i are λ-invariant and $E'_0 \supset E'_1 \supset E'_2 \supset E'_3 \supset E'_4$. Moreover, for m in J one has $\rho_m(\sigma) \in E_3$ and $\lambda_m(\sigma) \in E'_1$.*

PROOF. Let $m \in J$: we show that $\rho_m(\sigma) \in E_3$. For this, let $L \in \Lambda$. Then

$$\langle \lambda_L(\sigma), \rho_m(\sigma) \rangle = \langle \sigma, \rho_L \rho_m(\sigma) \rangle = \langle \sigma, \rho_{Mm}(\sigma) \rangle = \mathrm{Card}(Mm \cap M'). \tag{5.4}$$

Hence $\langle \lambda_L(\sigma) - \lambda_{L'}(\sigma), \rho_m(\sigma) \rangle = 0$ and $\rho_m(\sigma) \in E_3$. Symmetrically, $\lambda_m(\sigma) \in E'_1$.

Let us now show that $E_2 \subset E_3$. For $R \in \Gamma$, one has, by definition, $\rho_R = \sum_{r \in R} \rho_r$. Since $R \subset J$, one has $\rho_r(\sigma) \in E_3$ for each $r \in R$. Hence $\rho_R(\sigma) \in E_3$. This shows that $E_2 \subset E_3$. Symmetrically, one has $E'_3 \subset E'_2$. The other inclusions are clear. The fact that E_1 and E_2 are ρ-invariant is a consequence of $\rho_m \rho_R(\sigma) = \rho_{mR}(\sigma)$. Symmetrically, E'_3 and E'_2 are λ-invariant. The other subspaces are orthogonals of invariant subspaces and therefore invariant themselves. □

For $i = 1, 2, 3, 4$ denote by $\rho^{(i)}$ (resp. $\lambda^{(i)}$) the representation induced by ρ (resp. λ) on E_i/E_{i-1} (resp. E'_{i-1}/E'_i) and $p_i = \det \rho^{(i)}$, $q_i = \det \lambda^{(i)}$.

PROPOSITION 5.3. *The polynomials p_i, q_i $(1 \leq i \leq 4)$ have integer coefficients and*

$$1 - \theta(\underline{X}) = p_1 p_2 p_3 p_4 = q_1 q_2 q_3 q_4. \tag{5.5}$$

PROOF. (5.5) results immediately from (5.3) and Proposition 4.1. The polynomials p_i, q_i have rational coefficients. But their constant term is 1 and $1 - \theta(\underline{X}) \in \mathbf{Z}[A]$; hence they have integer coefficients (Gauss' lemma). □

By Proposition 4.4 one has $p_1 = q_1$ and $p_4 = q_4$. We shall see that actually $p_2 = q_2$ and $p_3 = q_3$.

PROPOSITION 5.4. *The polynomials p_2, q_2, p_3, q_3 satisfy*

$$p_2 = q_2 = 1 - \theta(A) \tag{5.6}$$

and $p_3 = q_3$.

PROOF. For $m \in J \cap M'$ and $L \in \Lambda$, one has, by (5.4),

$$\langle \lambda_L(\sigma), \rho_m(\sigma) \rangle = \mathrm{Card}(Mm \cap M') \neq 0.$$

But by Proposition 5.2, one has $\rho_m(\sigma) \in E_3 = E'^{\perp}_3$. Therefore $\lambda_L(\sigma) \notin E'_3$. This shows that $E'_2 \neq E'_3$ and therefore that $\dim(E'_2) = \dim(E'_3) + 1$. For each $m \in M$ and $L \in \Lambda$ one has $\lambda_m(\lambda_L(\sigma)) = \lambda_{Lm}(\sigma) \in \lambda_L(\sigma) + E'_3$. Hence each $a \in A$ induces the identity on E'_2/E'_3 and this implies that $q_2 = 1 - \theta(A)$. Similarly $p_2 = 1 - \theta(A)$. Finally, by (5.5), $p_3 = q_3$. □

REMARK 5.1. We have just shown that for each complete and finite code X, the polynomial $1 - \theta(X)$ is divisible by $1 - \theta(A)$. Clearly, the latter is equivalent

to $\pi(X) = 1$, for each Bernoulli morphism π. This may be established directly (see [**1**, p. 231]).

We study now the polynomials p_1 and p_4. Recall that U (resp. V) denotes the set of words (resp. left) completable in X^* (see §3).

PROPOSITION 5.5. *There exist polynomials $s, t \in \mathbf{Z}[A]$ such that, for any Bernoulli morphism π, one has*

$$\pi(p_1)\delta(U) = \pi(s), \tag{5.7}$$

$$\pi(p_4)\delta(V) = \pi(t). \tag{5.8}$$

PROOF. For $R \in \Gamma'$ define $B_R = \{u \in A^* | \varphi(u)R \in \Gamma'\}$. Let $w \in A^*$ and $m = \varphi(w)$. One has $[\rho_R(\sigma)](w) = [\rho_{mR}(\sigma)](1) = \mathrm{Card}(mR \cap M')$. Hence, denoting by h the cardinality of the groups $R \cap L$ for $R \in \Gamma$, $L \in \Lambda$ and putting $d = d(X)$,

$$[\rho_R(\sigma)](w) = \begin{cases} (h/d)\,\mathrm{Card}\,\Lambda' & \text{if } mR \in \Gamma', \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\underline{B}_R = (h/d)\,\mathrm{Card}\,\Lambda'\rho_R(\sigma)$, which shows that $E^{\underline{B}_R}$ is included in E_2. By Proposition 4.3, $s = \theta(\underline{B}_R)p_1p_2$ is a polynomial.

Let π be a Bernoulli morphism. From $s = \theta(\underline{B}_R)p_1(1-\theta(A))$ we deduce $\theta(\underline{A}^*)s = \theta(\underline{B}_R)p_1$. From this and (3.6) we obtain $\pi(s) = \delta(B_R)\pi(p_1)$. But $\varphi(B_R \cap J) = \varphi(U) \cap J$ because both members are equal to the union of the minimal right ideals which intersect $M' = \varphi(X^*)$. Since $B_R = \varphi^{-1}\varphi(B_R)$, Proposition 3.1 shows that $\delta(B_R) = \nu(\varphi(B_R) \cap J) = \nu(\varphi(U) \cap J) = \delta(U)$. This implies formula (5.7); (5.8) is established dually. □

PROOF OF THEOREM 5.1. Let $p = p_1 = q_1$, $q = p_3 = q_3$ and $r = p_4 = q_4$. Hence (i) is a consequence of Propositions 5.3 and 5.4. We show (ii): by Proposition 3.4 we may suppose $w \in U \cap \varphi^{-1}(J)$. We have $\underline{V'_w} = \lambda_w(\sigma)$ and by Proposition 5.2 we have $\lambda_w(\sigma) \in E'_1$. Hence by Propositions 4.1 and 4.3,

$$u = q_2q_3q_4\theta(\underline{V'_w}) \tag{5.9}$$

is a polynomial. But $\underline{V'_w} = \underline{V_w}\underline{X}^*$ by (3.13), and substituting in (5.9) yields

$$(1 - \theta(\underline{X}))u = q_2q_3q_4\theta(\underline{V_w}). \tag{5.10}$$

Since $1 - \theta(\underline{X}) = q_1q_2q_3q_4$ and $p = q_1$, we obtain

$$pu = \theta(\underline{V_w}). \tag{5.11}$$

This shows that p divides $\theta(\underline{V_w})$. It remains to show $\theta(\underline{V_w}) \equiv p \bmod(1-\theta(\underline{A}))$, or equivalently, $u \equiv 1 \bmod(1-\theta(\underline{A}))$, or that $\pi(u) = 1$ for any Bernoulli morphism Π. By Proposition 5.5 we have $\pi(p)\delta(U) = \pi(s)$ with $s \in \mathbf{Z}[A]$. Since $\delta(U)\pi(\underline{V_w}) = 1$, by Proposition 3.3 we obtain

$$\pi(p) = \pi(s)\pi(\underline{V_w}). \tag{5.12}$$

By (5.11), $\pi(\underline{V_w}) = \pi(p) = \pi(u)$. Comparing with (5.12) gives $\pi(\underline{V_w}) = \pi(s)\pi(\underline{V_w})\pi(u)$. Since, by hypothesis, w is right completable, we have $V'_w \neq \emptyset$, hence $\underline{V_w} \neq \emptyset$ and $\pi(\underline{V_w}) \neq 0$ because $\pi > 0$. Hence

$$\pi(u)\pi(s) = 1. \tag{5.13}$$

This is true for any π, and therefore

$$us \equiv 1 \bmod(1 - \theta(\underline{A})). \tag{5.14}$$

But $\mathbf{Z}[A]/1 - \theta(\underline{A})$ is free, hence $u \equiv s \equiv \pm 1 \bmod(1 - \theta(\underline{A}))$.

We show that, actually, $u \equiv 1$. Let a be a letter and $\gamma\colon \mathbf{Z}[A] \to \mathbf{Z}[a]$ the morphism defined by $\gamma(a) = (a)$ and $\gamma(b) = 0$ for $b \neq a$. Since X is a finite and complete code, there exists a unique n such that $a^n \in X$. Then $1 - a^n = \gamma(1 - \theta(\underline{X}))$. Since $p(1 - \theta(\underline{A}))$ divides $1 - \theta(\underline{X})$, $\gamma(p)$ divides $1 + a + \cdots + a^{n-1}$, hence has no root in $[0, 1]$. The constant term of p is equal to 1, and the same holds for $\gamma(p)$. Hence $\gamma(p)$ is positive on $[0, 1]$. From $pu = \theta(\underline{V_w})$ and the fact that $\underline{V_w}$ has nonnegative coefficients, we have that $\gamma(u)$ is nonnegative on $[0, 1]$. Hence $u \equiv -1 \bmod(1-\theta(A))$ cannot hold since otherwise $\gamma(u)(1) = -1$. This proves (ii).

Condition (iii) holds by duality. We show (iv): by (3.12), $\delta(X^*) = d^{-1}\delta(U)\delta(V)$. The relation $1 - \theta(\underline{X}) = pqr(1 - \theta(\underline{A}))$ implies $\theta(\underline{A^*}) = pqr\theta(\underline{X^*})$; hence $1 = \pi(pqr)\delta(X^*)$. Since $\pi(p)\delta(u) = 1$ and $\pi(r)\delta(u) = 1$ (Proposition 5.5) we obtain $\pi(r) = d$. □

We now study the cases in which the polynomials defined in Theorem 5.1 are trivial.

PROPOSITION 5.6. *Let $p = p_1 = q_1$ and $r = p_4 = q_4$. One has $p = 1$ (resp. $r = 1$) if and only if X is prefix (resp. suffix).*

PROOF. If X is prefix, then $V_x = 1$ for any x in X^*. Since p divides $\theta(\underline{V_x})$, by Theorem 5.1, for any x in $X^* \cap \varphi^{-1}(J)$, we conclude that $p = 1$. Conversely, suppose $p = 1$. Let $y \in X$: we show that $V_y = 1$, which will imply that X is prefix. Let $x \in X^* \cap \varphi^{-1}(J)$; then $V_y \subset V_{xy}$. But $\pi(V_{xy}) = \pi(p) = 1$ (by Theorem 5.1); since $1 \in V_y \subset V_{xy}$, we conclude that $V_{xy} = 1$ and hence $V_y = 1$. □

The other assertions is proved symmetrically.

We obtain the following

THEOREM 5.7. *Let $X \subset A^+$ be a finite complete code. If the polynomial $1-\theta(\underline{X})/1-\theta(\underline{A})$ is irreducible in $\mathbf{Z}[A]$, then one of the following conditions holds:*

(i) *X is prefix and synchronizing.*

(ii) *X is suffix and synchronizing.*

(iii) *X is biprefix.*

PROOF. Let $p = p_1 = q_1$, $q = p_3 = q_3$ and $r = p_4 = q_4$. By Theorem 5.1

$$1 - \theta(X) = (1 - \theta(A))pqr.$$

The hypothesis implies that either $p = q = 1$ or $q = r = 1$ or $p = r = 1$.

But by condition (iv) of Theorem 5.1, $q = 1$ forces $d(X) = 1$, i.e. that X is synchronizing. Therefore, if $p = q = 1$ then X is prefix and synchronizing, if $q = r = 1$ then X is suffix and synchronizing, and if $p = r = 1$ then X is prefix and suffix, i.e. X is biprefix. □

ACKNOWLEDGEMENTS. The authors wish to sincerely thank the referee for suggesting a number of improvements on the first version of this paper.

ADDED IN PROOF. The third author has recently proved a noncommutative version of Theorem 5.1, cf. *Noncommutative factorization of variable-length codes* (to appear).

REFERENCES

1. S. Eilenberg, *Automata, languages and machines*, Vol. A, Academic Press, New York, 1974.
2. G. Hansel and D. Perrin, *Codes and Bernoulli partitions*, Math. Systems Theory **16** (1983), 133–157.
3. G. Lallement, *Semigroups and combinatorial applications*, Wiley, New York, 1979.
4. M. P. Schützenberger, *Sur certains sous-monoïdes libres*, Bull. Soc. Math. France **93** (1965), 209–223.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ROUEN, MONT SAINT AIGNAN, 76130, FRANCE (Current address of G. Hansel)

INSTITUT DE PROGRAMMATION, UNIVERSITÉ PARIS 6, PARIS, FRANCE

Current address (D. Perrin): L.I.T.P., Université Paris 7, 75221, Paris Cedex 05, France

Current address (C. Reutenauer): L.I.T.P., Université Paris 6, 75231 Paris Cedex 05, France