

RAIRO

INFORMATIQUE THÉORIQUE

DO LONG VAN

Codes avec des mots infinis

RAIRO – Informatique théorique, tome 16, n° 4 (1982), p. 371-386.

http://www.numdam.org/item?id=ITA_1982__16_4_371_0

© AFCET, 1982, tous droits réservés.

L'accès aux archives de la revue « RAIRO – Informatique théorique » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques*

<http://www.numdam.org/>

CODES AVEC DES MOTS INFINIS (*)

par DO LONG VAN ⁽¹⁾

Communiqué par J. BERSTEL

Résumé. — On considère les codes dans le cadre des mots infinis. Une condition nécessaire et suffisante pour qu'un ensemble de mots soit un code est établie. Il est démontré que tout code maximal sur un alphabet composé au moins de deux lettres est complet, et aussi que, pour tout ensemble préfixe $X \neq \{1\}$, X est un code préfixe-maximal ssi X est un code faiblement complet à droite. Quelques opérations sur les codes préfixes sont examinées.

Abstract. — Codes with infinite words are considered. A necessary and sufficient condition for a set of words to be a code is established. It is shown that any maximal code over an alphabet consisting of at least two letters is complete, and also that, for any prefix set $X \neq \{1\}$, X is a prefix-maximal code iff X is a righthand weakly complete code. Some operations over the prefix codes are examined.

1. DÉFINITION

Soit A un alphabet non-vide. On note A^* le monoïde libre engendré par A , A^ω l'ensemble des mots infinis sur A , i.e. l'ensemble des applications $u : \mathbb{N}^+ \rightarrow A$, et on pose $A^\infty = A^* \cup A^\omega$, $A^{+\infty} = A^\infty - \{1\}$. Pour tout $u \in A^\omega$, $u(n)$ est la n -ième lettre du mot u . On munit A^∞ d'un produit prolongeant celui de A^* de la manière suivante :

$$\forall u \in A^\omega \forall v \in A^\infty = uv = u,$$

$$\forall u \in A^* \forall v \in A^\omega uv(n) = \begin{cases} u(n) & \text{si } 1 \leq n \leq |u|, \\ v(n - |u|) & \text{si } n > |u|. \end{cases}$$

L'ensemble A^∞ est alors un monoïde.

Pour toute partie $X \subset A^\infty$ on note :

$$X_{\text{fin}} = X \cap A^*,$$

$$X_{\text{inf}} = X \cap A^\omega,$$

et on définit :

$$\begin{cases} X^{(0)} = \{1\}, \\ X^{(i)} = X_{\text{fin}}^i \cup X_{\text{fin}}^{i-1} X_{\text{inf}}, & i \geq 1. \end{cases}$$

(*) Reçu en novembre 1981, et révisé en février 1982.

(1) Institut de Mathématiques, 208 D Doi Can, Hanoi, Vietnam; L.I.T.P., Université Paris-VII.

On note X^* le sous-monoïde de A^ω engendré par X et pose $X^+ = X^* - \{1\}$. Evidemment chaque mot w de X^+ peut se présenter sous l'une des deux formes suivantes :

- (i) $w = x_1 x_2 \dots x_n, n \geq 1, x_i \in X_{fin} (i = 1, \dots, n)$;
- (ii) $w = x_1 x_2 \dots x_n, n \geq 1, x_i \in X_{fin} (i = 1, \dots, n-1), x_n \in X_{inf}$.

DÉFINITION 1.1 : Une partie X de A^ω est un *code* sur A si chaque élément w de X^+ peut se présenter uniquement sous l'une des deux formes (i) et (ii); ou, d'une façon équivalente X est un code sur A si pour tous $n, m \geq 1$ et pour tous $x_1 \dots x_n \in X^{(n)}, x'_1 \dots x'_m \in X^{(m)}$, l'égalité :

$$x_1 \dots x_n = x'_1 \dots x'_m,$$

implique $n = m$ et $x_i = x'_i$ pour $i = 1, \dots, n$.

EXEMPLE 1.1 : Pour tout alphabet A , toute partie X de A^ω est un code sur A .

EXEMPLE 1.2 : L'ensemble $X = a^* b \cup a^\omega$ est un code sur $A = \{a, b\}$.

EXEMPLE 1.3 : L'ensemble $X = \{b, ba, a^\omega\}$ n'est pas un code car $b \cdot a^\omega = ba \cdot a^\omega$.

PROPOSITION 1.1 : Si $X \subset A^\omega$ est un code, alors X^k est aussi un code pour tout $k > 0$.

Preuve : Posons $Y = X^k$. Soient $y_1 \dots y_n \in Y^{(n)}, y'_1 \dots y'_m \in Y^{(m)} (n, m \geq 1)$ tels que :

$$y_1 \dots y_n = y'_1 \dots y'_m.$$

Soient ensuite :

$$y_i = x_{i1} \dots x_{ir_i} \quad (i = 1, \dots, n),$$

$$y'_j = x'_{j1} \dots x'_{js_j} \quad (j = 1, \dots, m),$$

où $x_{il}, x'_{jt} \in X (1 \leq l \leq r_i, 1 \leq t \leq s_j, 1 \leq r_i, s_j \leq k)$.

Comme $y_1, \dots, y_{n-1}, y'_1, \dots, y'_{m-1}$ sont des éléments de Y_{fin} , on doit avoir $r_1 = \dots = r_{n-1} = s_1 = \dots = s_{m-1} = k$. On a donc :

$$\begin{aligned} &x_{11} \dots x_{1k} \dots x_{n-1,1} \dots x_{n-1,k} x_{n1} \dots x_{nr_n} \\ &= x'_{11} \dots x'_{1k} \dots x'_{m-1,1} \dots x'_{m-1,k} x_{m1} \dots x_{ms_m}, \end{aligned}$$

où la partie gauche et la partie droite sont dans $X^{(n-1)k+r_n}$ et $X^{(m-1)k+s_m}$

respectivement. Comme X est un code, il en résulte que :

$$(n-1)k + r_n = (m-1)k + s_m,$$

donc $r_n = s_m$, et par conséquent $n = m$, et $x_{it} = x'_{it}$ pour $i = 1, \dots, n; t = 1, \dots, r_i$, d'où $y_i = y'_i$ pour $i = 1, \dots, n$. Ainsi X^k est un code.

Une partie X de A^∞ est *préfixe (suffixe)* si aucun élément de X n'est facteur gauche (droit) propre d'un élément de X . Une partie X est *bipréfixe* si elle est à la fois préfixe et suffixe.

Comme dans le cas des codes ordinaires, on a les propositions suivantes dont les preuves sont ici adoptées.

PROPOSITION 1.2 : *Toute partie préfixe (suffixe, bipréfixe) $X \subset A^{+\infty}$ est un code sur A .*

PROPOSITION 1.3 : *Tout code X sur A est contenu dans un code maximal sur A .*

Soient X et Y deux parties de A^∞ . On note :

$$\begin{aligned} Y^{-1}X &= \{z \mid \exists y \in Y : yz \in X, |y| = \infty \rightarrow z = 1\}, \\ XY^{-1} &= \{z \mid \exists y \in Y : zy \in X, |z| = \infty \rightarrow y = 1\}. \end{aligned}$$

Ensuite pour toute partie X de A^∞ on définit :

$$\begin{cases} U_1 = X^{-1}X - \{1\}; \\ U_{i+1} = X^{-1}U_i \cup U_i^{-1}X, & i \geq 1. \end{cases}$$

Pour établir une condition nécessaire et suffisante pour qu'une partie $X \subset A^\infty$ soit un code on a besoin du :

LEMME 1.4 : *Pour toute partie $X \subset A^{+\infty}$:*

(i) *Si $n \geq 2$ est le nombre naturel le plus petit tel que $1 \in U_n$, alors :*

$\forall k \in \{1, \dots, n\} \exists u \in U_k \exists i, j \geq 0 :$

$$uX^{(i)} \cap X^{(j)} \neq \emptyset, \quad i+j+k=n, \quad |u| = \infty \rightarrow i=0; \quad (1.1)$$

(ii) $\forall n \forall k \in \{1, \dots, n\} :$

$$(\exists u \in U_k \exists i, j \geq 0 = uX^{(i)} \cap X^{(j)} \neq \emptyset, \quad i+j+k=n, |u| = \infty \rightarrow i=0) \rightarrow 1 \in U_n.$$

Preuve : Les énoncés se prouvent par récurrence descendante sur k .

(i) Soit $n \geq 2$ le nombre naturel le plus petit tel que $1 \in U_n$. Si $k = n$, on a bien, pour $u = 1, i = j = 0$, l'expression (1.1).

Soit maintenant $n > k \geq 1$, et supposons l'énoncé vrai pour $n, n-1, \dots, k+1$. Comme $1 \in U_n$, il existe, d'après l'hypothèse de récurrence, $v \in U_{k+1}$ et deux entiers $i', j' \geq 0$ tels que :

$$vX^{(i')} \cap X^{(j')} \neq \emptyset, \quad i' + j' + k + 1 = n, \quad |v| = \infty \rightarrow i' = 0.$$

On a donc $x \in X^{(i')}, y \in X^{(j')}$ tels que :

$$vx = y.$$

Comme $v \in U_{k+1}$, deux cas sont possibles :

Cas 1 : $v \in X^{-1}U_k$, i. e. il existe $z \in X, u \in U_k$ tels que :

$$u = zv.$$

On a alors :

$$ux = zvx = zy.$$

Si $|v| = \infty$, alors $i' = 0, x = 1, j' + k + 1 = n, |u| = \infty, z \in X_{\text{fin}}$ et $u = zy$. D'où $uX^{(0)} \cap X^{(j'+1)} \neq \emptyset$ Ainsi on a (1.1) avec $i = 0, j = j' + 1$.

Si $|v| < \infty$ et $|u| < \infty$, alors $z \in X_{\text{fin}}$. Donc $uX^{(i')} \cap X^{(j'+1)} \neq \emptyset$ On a alors (1.1) avec $i = i', j = j' + 1$.

Si $|v| < \infty$ et $|u| = \infty$, alors $v = 1$ et $u = z$. Les entiers i' et j' doivent alors en même temps être égaux à 0 ou non.

Si $i' = j' = 0$, alors $k + 1 = n$, l'égalité $u = z$ implique $uX^{(0)} \cap X^{(1)} \neq \emptyset$. On a donc (1.1) avec $i = 0, j = 1$.

Si $i', j' \neq 0$, alors $k + 1 < n$, ce qui n'est pas possible, car on a $1 = v \in U_{k+1}$.

Cas 2 : $v \in U_k^{-1}X$, i. e. il existe $u \in U_k, z \in X$ tels que :

$$uv = z.$$

On a alors :

$$uy = uvx = zx.$$

Si $|v| = \infty$, alors $i' = 0, x = 1, j' + k + 1 = n, z \in X_{\text{inf}}, |u| < \infty$ et $uy = z$. D'où $uX^{(j')} \cap X^{(1)} \neq \emptyset$, i. e. on a (1.1) avec $i = j', j = 1$.

Si $|v| < \infty$ et $z \in X_{\text{fin}}$, alors $|u| < \infty$. L'égalité $uy = zx$ implique $uX^{(j')} \cap X^{(i'+1)} \neq \emptyset$. Ainsi on a (1.1) avec $i = j', j = i' + 1$.

Si $|v| < \infty$ et $z \in X_{\text{inf}}$, alors $v = 1$ et $u = z$.

Si $i' = j' = 0$, alors $k + 1 = n$. Comme $u = z$, on a $uX^{(0)} \cap X^{(1)} \neq \emptyset$, i.e. on a (1.1) avec $i = 0, j = 1$.

Si $i', j' \neq 0$, alors $k + 1 < n$, ce qui n'est pas possible parce que $1 = v \in U_{k+1}$.

(ii) Soit $\exists u \in U_k \exists i, j \geq 0$:

$$uX^{(i)} \cap X^{(j)} \neq \emptyset, \quad i + j + k = n, \quad |u| = \infty \rightarrow i = 0.$$

On doit montrer que $1 \in U_n$.

Si $k = n$ alors $i = j = 0$. D'où $u = 1 \in U_k = U_n$.

Soit maintenant $n > k \geq 1$, et supposons l'énoncé vrai pour $n, n - 1, \dots, k + 1$.

Soit :

$$ux_1 \dots x_i = x'_1 \dots x'_j$$

avec $x_1 \dots x_i \in X^{(i)}, x'_1 \dots x'_j \in X^{(j)}$. Deux cas sont possibles :

Cas 1 : $|u| = \infty$. Alors $i = 0, j + k = n, j \geq 1$ et $u = x'_1 \dots x'_j$. D'où $u' = x'_2 \dots x'_j \in U_{k+1}$. On a alors $u'X^{(0)} \cap X^{(j-1)} \neq \emptyset, 0 + (j-1) + (k+1) = n$. D'après l'hypothèse de récurrence, $1 \in U_n$.

Cas 2 : $|u| < \infty$. Si $j = 0$ alors $i = 0, u = 1, k = n$. D'où $1 \in U_n$. Soit $j \geq 1$.

Si $u = x'_1 u'$, alors $u' \in U_{k+1}$ et $u'x_1 \dots x_i = x'_2 \dots x'_j$. Donc $u'X^{(i)} \cap X^{(j-1)} \neq \emptyset, i + (j-1) + (k+1) = n$. D'après l'hypothèse de récurrence on doit avoir $1 \in U_n$.

Si $x'_1 = uu'$, alors $u' \in U_{k+1}$ et $u'x'_2 \dots x'_j = x_1 \dots x_i$. D'où $u'X^{(j-1)} \cap X^{(i)} \neq \emptyset, (j-1) + i + (k+1) = n$. D'après l'hypothèse de récurrence on a $1 \in U_n$.

THÉORÈME 1.5 : *La partie $X \subset A^{+\infty}$ est un code ssi aucun des ensembles U_n définis ci-dessus ne contient le mot vide 1.*

Preuve : Si X n'est pas un code, il existe $i, j \geq 1, x_1 \dots x_i \in X^{(i)}, x'_1 \dots x'_j \in X^{(j)}$ tels que :

$$x_1 \dots x_i = x'_1 \dots x'_j, \quad x_1 \neq x'_1.$$

Deux cas sont donc possibles :

Cas 1 : $x'_1 \in x_1(A^{+\infty})^{-1}$. Alors $x_1 = x'_1 u, 1 \neq u \in U_1$.

Si $|x_1| = \infty$, alors $i = 1, |x'_1| < \infty, |u| = \infty$. On a $u = x'_2 \dots x'_j, j \geq 2$. D'où $uX^{(0)} \cap X^{(j-1)} \neq \emptyset$. En vertu du lemme 1.4 (ii) on doit avoir $1 \in U_{0+(j-1)+1} = U_j$.

Si $|x_1| < \infty$, alors $|u| < \infty$. On a donc $ux_2 \dots x_i = x'_2 \dots x'_j, j \geq 2$. D'où $uX^{(i-1)} \cap X^{(j-1)} \neq \emptyset$. En vertu du lemme 1.4 (ii), $1 \in U_{(i-1)+(j-1)+1} = U_{i+j-1}$.

Cas 2 : $x_1 \in x'_1 (A^{+\infty})^{-1}$. Le raisonnement se fait d'une façon similaire.

Supposons maintenant qu'il existe des ensembles U_i qui contiennent le mot vide 1. Soit n le nombre le plus petit tel que $1 \in U_n$. En vertu du lemme 1.4 (i) il existe $u \in U_1$ et deux entiers $i, j \geq 0$ tels que :

$$uX^{(i)} \cap X^{(j)} \neq \emptyset, \quad i+j+1=n, \quad |u|=\infty \rightarrow i=0.$$

Soit :

$$ux_1 \dots x_i = x'_1 \dots x'_j$$

avec $x_1 \dots x_i \in X^{(i)}$, $x'_1 \dots x'_j \in X^{(j)}$.

Comme $u \in U_1$, il existe $x, x' \in X$ tels que :

$$x = x' u,$$

où $x \neq x'$ car $u \neq 1$.

Si $|u| < \infty$, alors $x, x' \in X_{\text{fin}}$. On a donc :

$$xx_1 \dots x_i = x' ux_1 \dots x_i = x' x'_1 \dots x'_j, \quad x \neq x',$$

ce qui montre que X n'est pas un code.

Si $|u| = \infty$, alors $i=0$, $x \in X_{\text{inf}}$, $x' \in X_{\text{fin}}$. Donc :

$$u = x'_1 \dots x'_j.$$

D'où :

$$x = x' u = x' x'_1 \dots x'_j, \quad x \neq x',$$

ce qui montre également que X n'est pas un code.

Si $X \subset A^{+\infty}$ est une partie préfixe, on a $U_1 = X^{-1}X - \{1\} \neq \emptyset$. Ainsi on obtient :

COROLLAIRE 1.6 : *Toute partie préfixe $X \subset A^{+\infty}$ est un code.*

EXEMPLE 1.3 (suite) : Soit $X = \{b, ba, a^\omega\}$. On a $U_1 = \{a\}$, $U_2 = \{a^\omega\}$, $U_3 = \{1\}$. Donc X n'est pas un code.

2. CODES COMPLETS

DÉFINITION 2.1 : Soit X une partie de A^∞ .

(i) X est dense si :

$$\forall w \in A^\omega \quad A^* w A^\omega \cap X \neq \emptyset;$$

(ii) X est complet si X^* est dense, i. e. :

$$\forall w \in A^\omega \quad A^* w A^\omega \cap X^* \neq \emptyset.$$

PROPOSITION 2.1 : Pour toute partie X de A^ω :

(i) X est dense ssi :

$$\forall w \in A^\omega \quad A^* w \cap X_{\text{inf}} \neq \emptyset \tag{2.1}$$

(ii) X est complet ssi :

$$\forall w \in A^\omega \quad A^* w \cap X_{\text{fin}}^* X_{\text{inf}} \neq \emptyset \tag{2.2}$$

Preuve : Comme chaque mot de A^* est facteur gauche d'un mot quelconque de A^ω , les conditions (i) et (ii) de la définition 2.1 équivalent aux conditions (2.1) et (2.2) respectivement.

EXEMPLE 2.1 : Soit $A = \{a, b\}$. L'ensemble $X = b A^\omega$ est évidemment un code dense sur A .

EXEMPLE 2.2 : Soient $A = \{a, b\}$, $u_1 = ab^2 ab^3 ab^4 \dots$, $u = bu_1$. Alors $-A^* u\}$ est un ensemble (pas un code) complet qui n'est pas dense. En effet, comme $A^* u \cap X_{\text{inf}} = A^* u \cap (a A^\omega - A^* u) = \emptyset$, X n'est pas dense. Montrons que X est complet. Il est facile de vérifier que $A^* \subset (A^*)^{-1} X_{\text{fin}}^*$ et que $u_1 \in X_{\text{inf}}$, donc $u = bu_1 \in X_{\text{fin}} X_{\text{inf}}$. Si $w \in X_{\text{inf}}$ alors évidemment $A^* w \cap X_{\text{fin}}^* X_{\text{inf}} \neq \emptyset$. Supposons $w \in A^\omega - X_{\text{inf}}$. Si $w \in A^* u$, soit $w = vu$ pour $v \in A^*$, alors il existe $v' \in A^*$ tel que $v'v \in X_{\text{fin}}^*$, donc :

$$v' w = v' (vu) = (v'v)u \in X_{\text{fin}}^* X_{\text{fin}} X_{\text{inf}} \subset X_{\text{fin}}^* X_{\text{inf}},$$

d'où $A^* w \cap X_{\text{fin}}^* X_{\text{inf}} \neq \emptyset$. Supposons maintenant $w \in A^\omega$ et w commence par b . Posons $v = aw$. Si $v \in X_{\text{inf}}$ alors évidemment $A^* w \cap X_{\text{fin}}^* X_{\text{inf}} \neq \emptyset$; si $v \in X_{\text{inf}}$ alors $v \in A^* u$, donc $A^* v \cap X_{\text{fin}}^* X_{\text{inf}} \neq \emptyset$, d'où $A^* w \cap X_{\text{fin}}^* X_{\text{inf}} \neq \emptyset$. Nous avons donc (2.2), i. e. X est complet.

PROPOSITION 2.2 : Sur un alphabet composé d'une seule lettre, il existe des codes maximaux qui ne sont pas complets.

Preuve : Si A est un alphabet arbitraire, alors aucune partie X de A^* n'est complète, car $X_{\text{fin}}^* X_{\text{inf}} = \emptyset$.

Soit A est l'alphabet composé d'une seule lettre a . Soit X un singleton de A^* . Alors X est évidemment un code maximal. Mais d'après la remarque ci-dessus, il n'est pas complet.

THÉORÈME 2.3 : *Tout code maximal sur un alphabet A composé au moins de deux lettres est complet.*

Preuve : Soient A un alphabet composé au moins de deux lettres et X un code maximal sur A . Il suffit, pour prouver que X est complet, de démontrer que :

$$\forall w \in A^{\circ} \quad A^* w \cap X^* \neq \emptyset.$$

Supposons qu'il existe un mot $w \in A^{\circ}$ tel que :

$$A^* w \cap X^* = \emptyset \tag{2.3}$$

Deux cas sont possibles :

Cas 1 : Il n'existe aucun mot $u \neq 1$ tel que $w = uw$. Posons :

$$Y = X \cup \{w\}.$$

En vertu de (2.3), $w \in X$.

Si Y n'est pas un code, il existe $x_1 \dots x_n \in Y^{(n)}$, $x'_1 \dots x'_m \in Y^{(m)}$, $n, m \geq 1$ tels que :

$$x_1 \dots x_n = x'_1 \dots x'_m, \quad x_1 \neq x'_1. \tag{2.4}$$

Il n'est pas possible que tous les x_i, x'_j soient dans X , car X est un code. Le mot w doit donc être présent, par exemple, dans la partie gauche de (2.4), d'où $x_n = w$. En vertu de (2.3), w doit également être présent dans la partie droite de (2.4), d'où $x'_m = w$. Alors on obtient de (2.4) :

$$x_1 \dots x_{n-1} = x'_1 \dots x'_{m-1},$$

avec $n, m \geq 2$; $x_i, x'_j \in X$ ($i = 1, \dots, n-1$; $j = 1, \dots, m-1$), $x_1 \neq x'_1$, ce qui n'est pas possible, car X est un code. Ainsi Y est un code, ce qui est en contradiction avec la maximalité du code X .

Cas 2 : Il existe un mot $u \neq 1$ tel que $w = uw$. Alors $w = u^{\circ}$. Soit $w = aw'$ avec $a \in A$. Choisissons $b \in A - \{a\}$ et posons $y = b^{|u|} w$. Comme chaque facteur de la longueur $|u|$ du mot w contient au moins une lettre a , il n'existe aucun mot $v \neq 1$ tel que $y = vy$. De (2.3) il découle que :

$$A^* y \cap X^* = \emptyset.$$

Posons :

$$Y = X \cup \{y\}.$$

En raisonnant d'une manière similaire on arrive à la conclusion que Y est un code, ce qui est en contradiction avec la maximalité du code X .

La réciproque du théorème 2.3 n'est pas vraie, comme il sera montré dans l'exemple suivant :

EXEMPLE 3.1 : Soit $A = \{a, b\}$. Le code $X = bA^\omega$ est dense et par conséquent complet. Mais il n'est pas maximal car A^ω est aussi un code.

3. CODES PRÉFIXE-MAXIMAUX

Soit X une partie de A^ω . On pose :

$$X^\omega = X^* \cup X_{fin}^\omega = X_{fin}^* \cup X_{fin}^* X_{inf} \cup X_{fin}^\omega.$$

DÉFINITION 3.1 : Pour tout $X \subset A^\omega$:

(i) X est dense à droite si :

$$\forall w \in A^\omega = wA^\omega \cap X \neq \emptyset.$$

(ii) X est complet à droite si X^* est dense à droite;

(iii) X est faiblement complet à droite si X^ω est dense à droite.

PROPOSITION 3.1 : Pour tout $X \subset A^\omega$:

(i) X est dense à droite ssi :

$$A^\omega = X_{inf}; \tag{3.1}$$

(ii) X est complet à droite ssi :

$$A^\omega = X_{fin}^* X_{inf}; \tag{3.2}$$

(iii) X est faiblement complet à droite ssi :

$$A^\omega = X_{fin}^* X_{inf} \cup X_{fin}^\omega. \tag{3.3}$$

Preuve : (i) Comme chaque mot de A^* est facteur gauche d'un mot quelconque de A^ω , on a :

$$\begin{aligned} \forall w \in A^\omega \ wA^\omega \cap X \neq \emptyset &\Leftrightarrow \forall w \in A^\omega, \quad w \in X; \\ &\Leftrightarrow A^\omega = X; \\ &\Leftrightarrow A^\omega = X_{inf}. \end{aligned}$$

(ii) X est complet à droite ssi X^* est dense à droite. En vertu de (i) ceci équivaut à :

$$A^\omega = (X^*)_{\text{inf}} = X_{\text{fin}}^* X_{\text{inf}}.$$

(iii) Le raisonnement est similaire à celui de (ii).

EXEMPLE 3.1 : Pour tout alphabet A , l'ensemble $X = A^\omega$ est le seul code dense à droite.

EXEMPLE 3.2 : Soit $A = \{a, b\}$. L'ensemble $X = a \cup b A^\omega \cup a^\omega$ est complet à droite mais pas dense à droite. En effet, on a :

$$A^\omega = a^* (b A^\omega \cup a^\omega) = X_{\text{fin}}^* X_{\text{inf}},$$

mais le mot ab^ω , par exemple, n'appartient pas à l'ensemble $b A^\omega \cup a^\omega = X_{\text{inf}}$, i. e. $A^\omega \neq X_{\text{inf}}$.

EXEMPLE 3.3 : Soit $A = \{a, b\}$. L'ensemble $X = a \cup b A^\omega$ est un code faiblement complet à droite qui n'est pas complet à droite. En effet, on a :

$$A^\omega = a^* b A^\omega \cup a^\omega = X_{\text{fin}}^* X_{\text{inf}} \cup X_{\text{fin}}^\omega,$$

mais $a^\omega \notin a^* b A^\omega = X_{\text{fin}}^* X_{\text{inf}}$, i. e. $A^\omega \neq X_{\text{fin}}^* X_{\text{inf}}$.

PROPOSITION 3.2 : Soit X un ensemble préfixe de A^ω . Alors les conditions suivantes sont équivalentes :

- (i) X est complet à droite;
- (ii) X est dense à droite;
- (iii) $X = A^\omega$.

Preuve : Les implications (iii) \Rightarrow (ii) \Rightarrow (i) sont évidentes.

(i) \Rightarrow (ii) : si X est complet à droite, alors, en vertu de la proposition 3.1 (ii), $A^\omega = X_{\text{fin}}^* X_{\text{inf}}$. Il suffit de démontrer que $X_{\text{fin}} = \emptyset$. Supposons que $X_{\text{fin}} \neq \emptyset$ et $x \in X_{\text{fin}}$. Comme X est préfixe, $x A^\omega \cap X_{\text{inf}} = \emptyset$. En particulier $x^\omega \in X_{\text{inf}}$. Alors il existe $x_1 \dots x_n \in X_{\text{fin}}^* X_{\text{inf}}$, $n > 1$, $x_i \in X_{\text{fin}}$ ($i = 1, \dots, n-1$), $x_n \in X_{\text{inf}}$ tels que :

$$x^\omega = x_1 \dots x_n.$$

Comme X est préfixe, on doit avoir $x = x_1$. D'où :

$$x^\omega = x_2 \dots x_n.$$

D'une façon similaire on obtient $x = x_2 = \dots = x_{n-1}$. Donc :

$$x^\omega = x_n \in X_{\text{inf}},$$

contradiction. Ainsi $X_{\text{fin}} = \emptyset$ et $A^\omega = X_{\text{inf}}$, i. e. X est dense à droite.

(ii) \Rightarrow (iii) : si X est dense à droite, alors $A^\omega = X_{\text{inf}}$. Comme X est préfixe, on a alors $X_{\text{fin}} = \emptyset$. D'où $A^\omega = X$.

PROPOSITION 3.3 : Pour tout $X \subset A^\omega$, les conditions suivantes sont équivalentes :

- (i) XA^ω est dense à droite;
- (ii) $A^\omega = X(A^{+\omega})^{-1} \cup X \cup X_{\text{fin}} A^{+\omega}$;
- (iii) $\forall f \in A^\omega \exists u, v \in A^\omega \exists x \in X = fu = xv, |f| = \infty \rightarrow u = 1, |x| = \infty \rightarrow v = 1$.

Preuve : (i) \Rightarrow (iii) : si XA^ω est dense à droite, alors :

$$\forall f \in A^\omega = fA^\omega \cap XA^\omega \neq \emptyset.$$

Si $|f| = \infty$, on a $f \in XA^\omega = X_{\text{fin}} A^\omega \cup X_{\text{inf}}$.

Si $f \in X_{\text{fin}} A^\omega$, il existe $v \in A^\omega, x \in X_{\text{fin}}$ tels que $f = xv$. Si $f \in X_{\text{inf}}$, on a $f = x, x \in X_{\text{inf}}$.

Si $|f| < \infty$, il existe $u \in A^\omega$ tel que $fu \in XA^\omega$. Si $fu \in X_{\text{fin}} A^\omega$, il existe $x \in X_{\text{fin}}, v \in A^\omega$ tels que $fu = xv$. Si $fu \in X_{\text{inf}}$, il existe $x \in X_{\text{inf}}$ tel que $fu = x$.

(iii) \Rightarrow (ii) : si $fu = xv$ avec $|f| = \infty \rightarrow u = 1, |x| = \infty \rightarrow v = 1$, alors $f \in X(A^{+\omega})^{-1}, f \in X, f \in X_{\text{fin}} A^{+\omega}$ selon que $|f| < |x|, |f| = |x|$ ou $|f| > |x|$.

(ii) \Rightarrow (i) : si $A^\omega = X(A^{+\omega})^{-1} \cup X \cup X_{\text{fin}} A^{+\omega}$, alors :

$$A^\omega = X_{\text{fin}} A^\omega \cup X_{\text{inf}} = (XA^\omega)_{\text{inf}}.$$

En vertu de la proposition 3.1, XA^ω est dense à droite.

PROPOSITION 3.4 : Pour tout $X \subset A^{+\omega}$, XA^ω est dense à droite ssi X est faiblement complet à droite.

Preuve : En vertu de la proposition 3.1 (i), XA^ω est dense à droite ssi :

$$A^\omega = (XA^\omega)_{\text{inf}} = X_{\text{fin}} A^\omega \cup X_{\text{inf}}.$$

D'après la proposition 3.1 (iii), X est faiblement complet à droite ssi :

$$A^\omega = X_{\text{fin}}^* X_{\text{inf}} \cup X_{\text{fin}}^\omega.$$

Comme $X_{\text{fin}}^* X_{\text{inf}} \cup X_{\text{fin}}^\omega \subset X_{\text{fin}} A^\omega \cup X_{\text{inf}}$, la complétude faible de X implique la densité de XA^ω . Pour prouver l'implication inverse on doit montrer que si XA^ω est dense à droite, alors $X_{\text{fin}} A^\omega \cup X_{\text{inf}} \subset X_{\text{fin}}^* X_{\text{inf}} \cup X_{\text{fin}}^\omega$, et pour ça, il suffit de démontrer que :

$$X_{\text{fin}} A^\omega = X_{\text{fin}}^* X_{\text{inf}} \cup X_{\text{fin}}^\omega.$$

Soit u un élément de $X_{\text{fin}} A^\infty$, alors il existe $x_1 \in X_{\text{fin}}$, $u_1 \in A^\infty$ tels que $u = x_1 u_1$. Si $u_1 \in X_{\text{inf}}$, on a $u = x_1 u_1 \in X_{\text{fin}} X_{\text{inf}} \subset X_{\text{fin}}^* X_{\text{inf}}$. Si non, on doit avoir $u_1 \in X_{\text{fin}} A^\infty$, i. e. il existe $x_2 \in X_{\text{fin}}$, $u_2 \in A^\infty$ tels que $u_1 = x_2 u_2$. Si $u_2 \in X_{\text{inf}}$, on a $u = x_1 u_1 = x_1 x_2 u_2 \in X_{\text{fin}}^2 X_{\text{inf}} \subset X_{\text{fin}}^* X_{\text{inf}}$. Si non, on doit avoir $u_2 \in X_{\text{fin}} A^\infty$, ... Ainsi soit il existe $n \geq 1$, $x_i \in X_{\text{fin}}$ ($i=1, \dots, n$), $U_n \in X_{\text{inf}}$ tels que $u = x_1 \dots x_n u \in X_{\text{fin}}^n X_{\text{inf}} \subset X_{\text{fin}}^* X_{\text{inf}}$, soit $u \in X_{\text{fin}}^\infty$.

THÉORÈME 3.5 : *Pour tout ensemble préfixe $X \subset A^\infty$, les conditions suivantes sont équivalentes :*

(i) X est préfixe-maximal;

(ii) XA^∞ est dense à droite.

De plus, si $X \neq \{1\}$, ceci équivaut à :

(iii) X est faiblement complet à droite.

Preuve : En vertu de la proposition 3.4, (ii) et (iii) sont équivalentes quand $X \neq \{1\}$. Montrons l'équivalence de (i) et (ii). Comme X est préfixe, pour tout $y \in A^\infty$ l'ensemble $X \cup \{y\}$ est préfixe ssi y n'appartient pas à $X_{\text{fin}} A^{+\infty} \cup X(A^{+\infty})^{-1}$, i. e. ssi $y \in A^\infty - (X_{\text{fin}} A^{+\infty} \cup X(A^{+\infty})^{-1})$.

D'où X est préfixe-maximal ssi $X = A^\infty - (X_{\text{fin}} A^{+\infty} \cup X(A^{+\infty})^{-1})$, i. e. ssi

$$A^\infty = X(A^{+\infty})^{-1} \cup X \cup X_{\text{fin}} A^{+\infty}.$$

En vertu de la proposition 3.3, ceci équivaut à ce que XA^∞ est dense à droite.

Remarque : Pour $X = \{1\}$, $XA^\infty = A^\infty$ est dense à droite, mais $X^\infty = \{1\}$ ne l'est pas, i. e. X n'est pas faiblement complet à droite.

COROLLAIRE 3.6 : *Soit $X \subset A^{+\infty}$ et $Y = X - X_{\text{fin}} A^{+\infty}$. Alors X est faiblement complet à droite ssi Y est préfixe-maximal.*

Preuve : En vertu de la proposition 3.4, X est faiblement complet à droite ssi XA^∞ est dense à droite. Comme $XA^\infty = YA^\infty$ et Y est préfixe, le résultat découle du théorème 3.5.

4. OPÉRATIONS SUR LES CODES PRÉFIXES

THÉORÈME 4.1 : *Soient X, Y_1, \dots, Y_n des parties non-vides de A^∞ , et soit $X = X_1 \cup \dots \cup X_n$ une partition de X . Posons :*

$$Z = X_1 Y_1 \cup \dots \cup X_n Y_n \quad (4.1)$$

et $J = \{j | j \in \{1, \dots, n\}, (X_j)_{\text{fin}} \neq \emptyset\}$.

(i) Si $X, Y_j (j \in J)$ sont des parties préfixes (resp. préfixe-maximales), alors Z est préfixe (resp. préfixe-maximale).

(ii) Si Z est préfixe, alors $Y_j (j \in J)$ sont préfixes;

(iii) Si X est préfixe et Z est préfixe-maximale, alors $X, Y_j (j \in J)$ sont préfixe-maximales.

Preuve : De (4. 1) on a :

$$Z = \bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{fin}} \cup \bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{inf}} \cup \bigcup_{i=1}^n (X_i)_{\text{inf}}. \quad (4.2)$$

(i) Soient $X, Y_j (j \in J)$ des parties préfixes. Montrons que Z est préfixe. Soient z et z' deux éléments de Z tels que $z \in z' (A^\infty)^{-1}$. Il existe alors $u \in A^\infty$ tel que :

$$z' = zu, \quad |z| = \infty \rightarrow u = 1.$$

Si $|z| = \infty$ alors $u = 1$ et par conséquent $z' = z$.

Soit $|z| < \infty$. Par (4. 2), il existe $j \in \{1, \dots, n\}$, $x \in (X_j)_{\text{fin}}$, $y \in (Y_j)_{\text{fin}}$ tels que :

$$z = xy.$$

Deux cas sont possibles :

Si $z' \in \bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{fin}} \cup \bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{inf}}$, il existe $k \in \{1, \dots, n\}$, $x' \in (X_k)_{\text{fin}}$, $y' \in Y_k$ tels que :

$$z' = x' y'.$$

Alors :

$$x' y' = xyu.$$

Comme X est préfixe, $x = x', j = k$, et par conséquent :

$$y' = yu; \quad y, y' \in Y_k.$$

Comme Y_k est préfixe, on a alors $y' = y$, d'où $u = 1$, et par conséquent $z' = z$.

Si $x' \in \bigcup_{i=1}^n (X_i)_{\text{inf}}$, il existe $j \in \{1, \dots, n\}$, $x' \in (X_j)_{\text{inf}}$ tels que $z' = x'$. Alors, comme $|z| < \infty$, et $|z'| = \infty$, on a $|u| = \infty$. Donc :

$$x' = xyu \quad \text{avec } yu \neq 1,$$

ce qui n'est pas possible car X est préfixe.

Soient maintenant $X, Y_j (j \in J)$ des parties préfixe-maximales. Alors, par théorème 3.5, $XA^\infty, Y_j A^\infty (j \in J)$ sont denses à droite. En vertu de la proposition 3.1 on a :

$$A^\omega = (XA^\infty)_{\text{inf}} = X_{\text{fin}} A^\omega \cup X_{\text{inf}}$$

et :

$$A^\omega = (Y_j A^\infty)_{\text{inf}} = (Y_j)_{\text{fin}} A^\omega \cup (Y_j)_{\text{inf}}.$$

Alors :

$$\begin{aligned} (ZA^\infty)_{\text{inf}} &= \left(\bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{fin}} \right) A^\omega \cup \bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{inf}} \cup \bigcup_{i=1}^n (X_i)_{\text{inf}} \\ &= \bigcup_{j \in J} (X_j)_{\text{fin}} (Y_j)_{\text{fin}} A^\omega \cup \bigcup_{j \in J} (X_j)_{\text{fin}} (Y_j)_{\text{inf}} \cup \bigcup_{i=1}^n (X_i)_{\text{inf}} \\ &= \bigcup_{j \in J} (X_j)_{\text{fin}} ((Y_j)_{\text{fin}} A^\omega \cup (Y_j)_{\text{inf}}) \cup \bigcup_{i=1}^n (X_i)_{\text{inf}} \\ &= \bigcup_{j \in J} (X_j)_{\text{fin}} A^\omega \cup \bigcup_{i=1}^n (X_i)_{\text{inf}} \\ &= \left(\bigcup_{j \in J} (X_j)_{\text{fin}} \right) A^\omega \cup \bigcup_{i=1}^n (X_i)_{\text{inf}} \\ &= \left(\bigcup_{i=1}^n (X_i)_{\text{fin}} \right) A^\omega \cup \bigcup_{i=1}^n (X_i)_{\text{inf}} = X_{\text{fin}} A^\omega \cup X_{\text{inf}} = A^\omega. \end{aligned}$$

Donc, par proposition 3.1, ZA^∞ est dense à droite. En vertu du théorème 3.5, Z est préfixe-maximale.

(ii) Supposons que Z soit une partie préfixe. Soit $j \in J$ et soient y, y' deux éléments de Y_j tels que $y \in y' (A^\infty)^{-1}$. Alors il existe $u \in A^\infty$ tel que $y' = yu$ et $|y| = \infty \rightarrow u = 1$. Pour tout $x \in (X_j)_{\text{fin}}$, on a $xy' = xyu$ et $|xy| = \infty \rightarrow u = 1$ i. e. $xy \in (xy') (A^\infty)^{-1}$. Comme Z est préfixe, on doit avoir $xy = xy'$, d'où $y = y'$. Ainsi Y_j est préfixe.

(iii) Supposons que X soit une partie préfixe et Z une partie préfixe-maximale.

Evidemment $ZA^\infty \subset XA^\infty$. Comme Z est préfixe-maximale, ZA^∞ doit être dense à droite. On a alors :

$$A^\omega = (ZA^\infty)_{\text{inf}} \subset (XA^\infty)_{\text{inf}},$$

i. e. $A^\omega = (XA^\infty)_{\text{inf}}$.

D'où XA^∞ est dense à droite, et par conséquent X est préfixe-maximale.

Soit $j \in J$. Montrons que Y_j est préfixe-maximale. Il suffit pour ça de démontrer que $A^\omega \subset (Y_j A^\infty)_{\text{inf}}$.

Comme Z est préfixe-maximale, on a :

$$A^\omega = (ZA^\infty)_{\text{inf}} = \left(\bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{fin}} \right) A^\omega \bigcup_{i=1}^n (X_i)_{\text{fin}} (Y_i)_{\text{inf}} \cup \bigcup_{i=1}^n (X_i)_{\text{inf}}. \quad (4.3)$$

Soit maintenant $w \in A^\omega$. Pour tout $x \in (X_j)_{\text{fin}}$ on a $xw \in A^\omega$. Par (4.3) et comme X est préfixe, deux cas sont possibles :

Cas 1 : Il existe $k \in \{1, \dots, n\}$, $x' \in (X_k)_{\text{fin}}$, $y' \in (Y_k)_{\text{fin}}$, $u \in A^\omega$ tels que $xw = x' y' u$. Or X est préfixe, $x = x'$ et $k = j$. Alors $w = y' u \in (Y_j)_{\text{fin}} A^\omega$.

Cas 2 : Il existe $k \in \{1, \dots, n\}$, $x' \in (X_k)_{\text{fin}}$, $y' \in (Y_k)_{\text{inf}}$ tels que $xw = x' y'$. Alors $x = x'$ et $k = j$. D'où $w = y' \in (Y_j)_{\text{inf}}$.

Ainsi $A^\omega \subset (Y_j)_{\text{fin}} A^\omega \cup (Y_j)_{\text{inf}} = (Y_j A^\infty)_{\text{inf}}$.

Pour $n=1$ on obtient par théorème 4.1 (i).

COROLLAIRE 4.2 : *Si X et Y sont deux parties préfixes (resp. préfixe-maximales), alors XY est préfixe (resp. préfixe-maximale).*

COROLLAIRE 4.3 : *Soit X une partie de A^∞ telle que $X_{\text{fin}} \neq \emptyset$, et soit $n \geq 1$. Alors X est préfixe (resp. préfixe-maximale) ssi X^n est préfixe (resp. préfixe-maximale).*

Preuve : Si X est préfixe, alors, en vertu du corollaire 4.2 et par récurrence, X^n est préfixe.

Réciproquement, si $Z = X^n$ est préfixe, alors, car $Z = X^{n-1} X$, par théorème 4.1 (ii), X est préfixe. Ensuite, notant que $Z = X X^{n-1}$ on déduit du théorème 4.1 (iii) que si Z est de plus préfixe-maximale, alors X est préfixe-maximale.

COROLLAIRE 4.4 : *Soient X et Y deux parties préfixes, $X = X_1 \cup X_2$ une partition de X . Alors $Z = X_1 \cup X_2 Y$ est préfixe. De plus, si $(X_2)_{\text{fin}} \neq \emptyset$, alors Z est préfixe-maximale ssi X et Y le sont.*

Preuve : On a $Z = X_1 Y^1 \cup X_2 Y$ avec $Y' = \{1\}$. Comme Y' est préfixe-maximale, le résultat découle du théorème 4.1.

Comme un cas particulier de ce corollaire on a :

COROLLAIRE 4.5 : Soient X et Y deux parties préfixes, $x \in X_{\text{fin}}$. Alors $Z = (X - \{x\}) \cup xY$ est préfixe, et Z est préfixe-maximale ssi X et Y le sont.

COROLLAIRE 4.6 : Soit Z une partie préfixe, $P = Z(A^{+\infty})^{-1}$. Alors pour tout $p \in P$, $Y_p = p^{-1}Z$ est une partie préfixe. Pour toute partie préfixe Q de P , $(Z - \bigcup_{p \in Q} pY_p) \cup Q$ est une partie préfixe. De plus, si Z est préfixe-maximale, alors les Y_p ($p \in Q$) et X sont préfixe-maximales.

Preuve : Nous avons $Z = (X - Q) \cup \bigcup_{p \in Q} pY_p = X_0 Y_0 \cup \bigcup_{p \in Q} X_1 Y_p$ avec $X_0 = X - Q$, $Y_0 = \{1\}$, $X_p = \{p\}$ ($p \in Q$). En vertu du théorème 4.1 il suffit, pour prouver l'assertion, de démontrer que X est préfixe.

Comme $pY_p = Z \cap pA^{+\infty}$, on a :

$$X = (Z - QA^{+\infty}) \cup Q = T \cup Q,$$

où Q est préfixe par hypothèse, et $T = Z - QA^{+\infty}$ est préfixe car c'est une partie de Z .

Aucun élément de Q n'est facteur gauche des éléments de T car $QA^{+\infty} \cap T = QA^{+\infty} \cap (Z - QA^{+\infty}) = \emptyset$.

Réciproquement, comme Z est préfixe, aucun élément de T n'est facteur gauche des éléments de Q . Ainsi X est préfixe.

Comme un cas particulier de ce corollaire on obtient :

COROLLAIRE 4.7 : Soit Z une partie préfixe et soit $p \in Z(A^{+\infty})^{-1}$. Alors $Y_p = p^{-1}Z$ et $X = (Z - pY_p) \cup \{p\}$ sont des parties préfixes. De plus, si Z est préfixe-maximale, il en est de même de Y_p et de X .

L'auteur remercie Monsieur le Professeur D. Perrin dont la direction et les encouragements constants ont créés d'excellentes conditions de cette étude.

BIBLIOGRAPHIE

1. D. PERRIN, éd., *Théorie des codes*, Actes de la septième Ecole de Printemps d'informatique théorique, Jougue, 1979.
2. J. BERSTEL, D. PERRIN et M. P. SCHÜTZENBERGER, *Théorie des codes* (à paraître).
3. S. EILENBERG, *Automata Languages and Machines*, vol. A, Academic Press, New York, 1974.