Theoretical Computer Science 38 (1985) 123-132
North-Holland

NOTE

ENSEMBLES CODE-COMPATIBLES ET UNE GÉNÉRALISATION DU THÉORÈME DE SARDINAS–PATTERSON

Do Long VAN

Institute of Mathematics, P/O Box 631 Bo Ho, Hanoi, Vietnam, et L.I.T.P., Université Paris 7, 2 Place Jussieu, 75221 Paris Cedex 05, France

Communicated by M. Nivat
Received June 1984
Revised November 1984

Résumé. On note A^∞ le monoïde de tous les mots finis et infinis sur un alphabet A. La code-compatibilité d'une paire (X, Y) de parties de A^∞ est définie. Une condition nécessaire et suffisante, qui est une généralisation du théorème de Sardinas et Patterson, pour que (X, Y) soit code-compatible est établie. Il est démontré que la classe des sous-monoïdes de A^∞ engendrés par un code infinitaire est formée par l'intersection, et aussi que, pour tous codes infinitaires X et Y, $X^* \cap Y^* = (X \cap Y)^*$ ssi (X, Y) est code-compatible.

Abstract. One denotes by A^∞ the monoid of all finite and infinite words over an alphabet A. The code-compatibility of a pair (X, Y) of subsets of A^∞ is here defined. A necessary and sufficient condition, which is a generalization of the Sardinas–Patterson theorem, for (X, Y) to be code-compatible is established. It is shown that the class of the submonoids of A^∞ generated by an infinitary code is closed by intersection, and also that, for any two infinitary codes X and Y, $X^* \cap Y^* = (X \cap Y)^*$ iff (X, Y) is code-compatible.

Introduction

Etant donné un alphabet non-vide A on note A^* le monoïde libre engendré par A, i.e., l'ensemble de tous les mots finis sur A, y compris le mot vide noté 1, muni de l'opération de concaténation. La longeur d'un mot f de A^* est notée $|f|$, et, pour tout n, $1 \leq n \leq |f|$, $f(n)$ désigne la n-ième lettre du mot f. L'ensemble des mots infinis sur A est noté A^ω. Chaque mot u de A^ω est une application $u: \mathbb{N}^+ \to A$ qu'on écrit souvent sous la forme $u = u(1)u(2)\ldots$. On pose $A^\infty = A^* \cup A^\omega$, $A^{+\infty} = A^\infty - \{1\}$ et on appelle *infinitaire* (respectivement *finitaire, purement infinitaire*) toute partie X de A^∞ (respectivement A^*, A^ω).

On munit A^∞ d'un produit prolongeant celui de A^* de la manière suivante:

$$\forall u \in A^\omega \; \forall \alpha \in A^\infty \; : \; u\alpha = u,$$

$$\forall f \in A^* \; \forall u \in A^\omega \; : \; (fu)(n) = \begin{cases} f(n) & \text{pour } 1 \leq n \leq |f|, \\ u(n-|f|) & \text{pour } n > |f|. \end{cases}$$

Il n'est pas difficile de vérifier que A^∞ est alors un monoïde.

Pour chaque partie X de A^∞ on note $X_{\text{fin}} = X \cap A^*$ et $X_{\text{inf}} = X \cap A^\omega$ et définit

$$X^{(0)} = \{1\},$$

$$X^{(1)} = X,$$

$$X^{(i)} = X_{\text{fin}} X^{(i-1)}, \quad i \geq 2.$$

On appelle *code infinitaire* toute partie X de A^∞ telle que, pour tous $n, m \geq 1$ et pour tous $x_1 \ldots x_n \in X^{(n)}$, $x'_1 \ldots x'_m \in X^{(m)}$, l'égalité

$$x_1 \ldots x_n = x'_1 \ldots x'_m$$

implique $n = m$ et $x_i = x'_i$ $(i = 1, \ldots, n)$. Les codes infinitaires ont été considerés en [6, 7]. Dans cette note, la code-compatibilité d'une paire (X, Y) de parties de A^∞ est introduite. Une condition nécessaire et suffisante, qui est une généralisation du théorème de Sardinas-Patterson (cf. [4, 3, 1, 6]), pour qu'une paire (X, Y) de parties de A^∞ soit code-compatible est établie. Il est démontré que la classe des sous-monoïdes quasi-libres i.e., des sous-monoïdes engendrés par un code infinitaire, est fermée par intersection, et que, pour tous codes infinitaires X et Y, $X^* \cap Y^* = (X \cap Y)^*$ ssi (X, Y) est code-compatible.

Dans la suite, sauf spécification contraire, le mot 'code' désignera un code infinitaire. Rappelons que pour toutes parties X et Y de A^∞ les parties $Y^{-1}X$ et XY^{-1} sont définis comme suit:

$$Y^{-1}X = \{\alpha \in A^\infty \mid \exists \beta \in Y : (\beta\alpha \in X) \;\&\; (|\beta| = \infty \rightarrow \alpha = 1)\},$$

$$XY^{-1} = \{\alpha \in A^\infty \mid \exists \beta \in Y : \alpha\beta \in X\}.$$

1. Ensembles code-compatibles

Soient X et Y deux parties de A^∞. On dit que la paire (X, Y) est *code-compatible* si, pour tous $n, m \geq 1$ et pour tous $x_1 \ldots x_n \in X^{(n)}$, $y_1 \ldots y_m \in Y^{(m)}$, l'égalité

$$x_1 \ldots x_n = y_1 \ldots y_m$$

implique $n = m$ et $x_i = y_i$ $(i = 1, \ldots, n)$.

Evidemment, une partie X de A^∞ est alors un code ssi (X, X) est code-compatible.

Exemple 1.1. Soient $A = \{a, b\}$, $X = \{a, ab, ba\}$, $Y = \{b, ab, ba\}$. Il n'est pas difficile de verifier que (X, Y) est code-compatible quoique ni X ni Y ne soient des codes.

Exemple 1.2. Soient $A=\{a, b\}$, $X=\{a, ba\}$, $Y=\{a, ba\}$. Evidemment, X et Y sont des codes. Mais (X, Y) n'est pas code-compatible car $a.ba=ab.a$.

Une paire (X, Y) de parties de A^{∞} est dit *préfixe-compatible* (*suffixe-compatible*) si aucun élément de X n'est facteur gauche (droite) propre d'un élément de Y et réciproquement. Une paire (X, Y) est *bipréfixe-compatible* si elle est à la fois préfixe-compatible et suffixe-compatible. On a évidemment la proposition suivante.

Proposition 1.3. *Toute paire préfixe-compatible (suffixe-compatible, bipréfixe-compatible) $(X, Y)\neq(\{1\},\{1\})$ est code-compatible. En particulier, toute partie préfixe (suffixe, bipréfixe) $X\neq\{1\}$ est un code.*

Proposition 1.4. *Si (X, Y) est code-compatible, alors (X^k, Y^k) est aussi code compatible pour tout $k\geqslant 1$. En particulier, si X est un code, alors X^k est aussi un code pour tout $k\geqslant 1$.*

Preuve. Poson $X'=X^k$, $Y'=Y^k$. Soient $x_1'\ldots x_n'\in X'^{(n)}$, $y_1'\ldots y_m'\in Y'^{(m)}$ $(n, m\geqslant 1)$ tels que

$$x_1'\ldots x_n'=y_1'\ldots y_m'.$$

Soient ensuite

$$x_i'=x_{i1}\ldots x_{ir_i}\quad (i=1,\ldots,n),$$

$$y_j'=y_{j1}\ldots y_{js_j}\quad (j=1,\ldots,m),$$

où $x_{il}\in X$, $y_{jt}\in Y$ $(1\leqslant l\leqslant r_i;\ 1\leqslant t\leqslant s_j;\ 1\leqslant r_i, s_j\leqslant k)$. Comme $x_1',\ldots,x_{n-1}'\in X_{\text{fin}}'$, $y_1',\ldots,y_{m-1}'\in Y_{\text{fin}}'$, on doit avoir $r_1=\cdots=r_{n-1}=s_1=\cdots=s_{m-1}=k$. On a donc

$$x_{11}\ldots x_{1k}\ldots x_{n-1,1}\ldots x_{n-1,k}x_{n1}\ldots x_{nr_n}$$
$$=y_{11}\ldots y_{1k}\ldots y_{m-1,1}\ldots y_{m-1,k}y_{m1}\ldots y_{ms_m},$$

où la partie gauche et la partie droite sont dans $X^{((n-1)k+r_n)}$ et $Y^{((m-1)k+s_m)}$ respectivement. Comme (X, Y) est code-compatible, on en déduit $(n-1)k+r_n=(m-1)k+s_m$, donc $r_n=s_m$, et par conséquent $n=m$ et $x_{it}=y_{it}$ pour $i=1,\ldots,n$; $t=1,\ldots,r_i$, d'où $x_i'=y_i'$ pour $i=1,\ldots,n$. Ainsi, (X^k, Y^k) est code-compatible. $\square$

Disons que (X, Y) est *contenu* dans (X', Y') et notons $(X, Y)\subseteq(X', Y')$ si $X\subseteq X'$ et $Y\subseteq Y'$. Soit maintenant $\mathcal{F}$ l'ensemble ordonné par $\subseteq$ des parties code-compatibles contenant une paire code-compatible (X, Y), et soit $\mathcal{C}$ une chaîne (i.e., partie totalement ordonnée) de $\mathcal{F}$. Il est facile de vérifier que $(\bigcup_{(X',Y')\in\mathcal{C}} X', \bigcup_{(X',Y')\in\mathcal{C}} Y')$ est le plus petit majorant de $\mathcal{C}$. D'après le lemme de Zorn, $\mathcal{F}$ contient un élément maximal. On a donc la proposition suivante.

Proposition 1.5. *Toute paire code-compatible (X, Y) sur un alphabet A est contenue* *dans une paire code-compatible maximale sur A. En particulier, tout code X sur A est contenu dans un code maximal sur A.*

2. Généralisation du théorème de Sardinas–Patterson

Pour chaque paire (X, Y) de parties de A^{∞} on définit de la manière suivante les ensembles $U_i(X, Y)$, $V_i(X, Y)$, $W_i(X, Y)$, abrégés par U_i, V_i, W_i $(i=1,2,\ldots)$:

$$U_1 = Y^{-1}X - \{1\}, \qquad V_1 = X^{-1}Y - \{1\},$$
$$U_{i+1} = Y^{-1}U_i \cup V_i^{-1}X, \qquad V_{i+1} = X^{-1}V_i \cup U_i^{-1}Y,$$
$$W_i = U_i \cup V_i, \quad i \geqslant 1.$$

Lemme 2.1. *Pour tous $X, Y \subseteq A^{+\infty}$:*

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

$$\forall k \in \{1,\ldots,n\}\ \exists i, j \geqslant 0:$$
$$(\exists u \in U_k: uX^{(i)} \cap Y^{(j)} \neq \emptyset,\ i+j+k=n,\ |u|=\infty \rightarrow i=0) \vee$$
$$(\exists v \in V_k = X^{(i)} \cap vY^{(j)} \neq \emptyset,\ i+j+k=n,\ |v|=\infty \rightarrow j=0). \tag{2.1}$$

(ii) $$\forall n\ \forall k \in \{1,\ldots,n\}:$$
$$[\exists i, j \geqslant 0\ (\exists u \in U_k: uX^{(i)} \cap Y^{(j)} \neq \emptyset,\ i+j+k=n,\ |u|=\infty \rightarrow i=0) \vee$$
$$(\exists v \in V_k: X^{(i)} \cap vY^{(j)} \neq \emptyset,\ i+j+k=n,\ |v|=\infty \rightarrow j=0)] \rightarrow 1 \in W_n.$$

Preuve. Les énoncés se prouvent par récurrence descendente sur k. Dans la suite, pour simplifier des notations on notera respectivement par (a) et (b) les expressions:

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

et

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

(i) Supposons que $n \geqslant 2$ soit le nombre naturel le plus petit tel que $1 \in W_n$.

Si $k=n$, alors selon que $1 \in U_n$ ou $1 \in V_n$ on a bien (a) avec $u=1$, $i=j=0$ ou (b) avec $v=1$, $i=j=0$ respectivement.

Supposons maintenant que $n > k \geqslant 1$ et que l'énconcé vrai pour $n, n-1, \ldots, k+1$. Comme $1 \in W_n$, il existe, d'après l'hypothèse de récurrence deux entiers i', j' et il existe ou bien $u' \in U_{k+1}$ tel que

(a′) $\quad u'X^{(i')} \cap Y^{(j')} \neq \emptyset,\ i'+j'+k+1=n,\ |u'|=\infty \rightarrow i'=0,$

ou bien $v' \in V_{k+1}$ tel que

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

Supposons, par exemple, (a) vrai (dans le cas où (b) est vrai, le raisonnement se fait d'une façon similaire). On a donc $x \in X^{(i')}$, $y \in Y^{(j')}$ tels que

$$u'x = y.$$

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

Cas 1. $u' \in Y^{-1}U_i$, i.e., il existe $z \in Y$, $u \in U_k$ tels que

$$u = eu', \qquad |z| = \infty \to u' = 1.$$

On a donc

$$ux = zu'x = zy.$$

Si $|u'| = \infty$, alors $i' = 0$, $x = 1$, $j' + k + 1 = n$, $|u| = \infty$, $z \in Y_{\text{fin}}$ et $u = zy$. D'où $uX^{(0)} \cap Y^{(j'+1)} \neq \emptyset$. Ainsi on a (a), et par conséquent (2.1), avec $i = 0$, $j = j' + 1$.

Si $|u'| < \infty$ et $|u| < \infty$, alors $z \in Y_{\text{fin}}$. Donc $uX^{(i')} \cap Y^{(j'+1)} \neq \emptyset$. On a alors (a), et par conséquent (2.1), avec $i = i'$, $j = j' + 1$.

Si $|u'| < \infty$ et $|u| = \infty$, alors $u' = 1$ 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 $uX^{(0)} \cap Y^{(1)} \neq \emptyset$. On a donc (a), et par conséquent (2.1), avec $i = 0$, $j = 1$.

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

Cas 2. $U' \in V_k^{-1}X$, i.e., il existe $v \in V_k$, $z \in X$ tels que

$$z = vu', \qquad |v| = \infty \to u' = 1.$$

On a alors

$$zx = vu'x = vy.$$

Si $|u'| = \infty$, alors $i' = 0$, $j' + k + 1 = n$, $z \in X_{\text{inf}}$, $|v| < \infty$ et $z = vy$. D'où $X^{(1)} \cap vY^{(j')} \neq \emptyset$, i.e., on a (b), et par conséquent (2.1), avec $i = 1$, $j = j'$.

Si $|u'| < \infty$ et $z \in X_{\text{fin}}$, alors $|v| < \infty$. L'égalité $zx = vy$ implique $X^{(i'+1)} \cap vY^{(j')} \neq \emptyset$. Ainsi on a (b), et par conséquent (2.1), avec $i = 1' + 1$, $j = j'$.

Si $|u'| < \infty$ et $z \in X_{\text{inf}}$, alors $u' = 1$ et $z = v$. Si $i' = j' = 0$, alors $k + 1 = n$. Comme $z = v$, on a $X^{(1)} \cap vY^{(0)} \neq \emptyset$, i.e., on a (b), et par conséquent (2.1), avec $i = 1$, $j = 0$. Si $i', j' \neq 0$, alors $k + 1 < n$ ce qui n'est pas possible parce que $1 = u' \in U_{k+1} \subseteq W_{k+1}$.

(ii) Soit $k \in \{1, \ldots, n\}$ et supposons

$$\forall i, j \geq 0:$$

$$(\exists u \in U_k \colon uX^{(i)} \cap Y^{(j)} \neq \emptyset,\ i + j + k = n,\ |u| = \infty \to i = 0) \lor$$

$$(\exists v \in V_k \colon X^{(i)} \cap vY^{(j)} \neq \emptyset,\ i + j + k = n,\ |v| = \infty \to j = 0).$$

On doit montrer que $1 \in W_n$. Supposons qu'il existe $u \in U_k$ tel que (a) soit satisfait (dans le cas où il existe $v \in V_k$ tel que (b) soit satisfait le raisonnement se fait d'une façon similaire).

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

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

$$ux_1 \ldots x_i = y_1 \ldots y_j$$

avec $x_1, \ldots, x_i \in X^{(i)}$, $y_1, \ldots, y_j \in Y^{(j)}$. Deux cas sont possibles:

Cas 1. $|u| = \infty$. Alors $i = 0, j + k = n, j \geq 1$ et $u = y_1 \ldots y_j$. D'où $u' = y_2 \ldots y_j \in U_{k+1}$. On a alors $u'X^{(0)} \cap Y^{(j-1)} \neq \emptyset$, $0 + (j-1) + (k+1) = n$. D'après l'hypothèse de récurrence, $1 \in W_n$.

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

Supposons $j \geq 1$. Si $|u| \geq |y|$, disons $u = y_1 u'$, alors $u' \in U_{k+1}$ et $u'x_1 \ldots x_i = y_2 \ldots y_j$. Donc $u'X^{(i)} \cap Y^{(j-1)} \neq \emptyset$, $i + (j-1) + (k+1) = n$, $|u'| = \infty \to i = 0$. D'aprés l'hypothèse de récurrence on doit avoir $1 \in W_n$. Si $|u| < |y_1|$, disons $y_1 = uv$, alors $v \in V_{k+1}$ et $x_1 \ldots x_i = vy_2 \ldots y_j$. D'où $X^{(i)} \cap vY^{(j-1)} \neq \emptyset$, $i + (j-1) + (k+1) = n, |v| = \infty \to (j-1) = 0$.

D'après l'hypothèse de récurrence on a $1 \in W_n$. $\square$

Théorème 2.2. *Soient X et Y deux parties de $A^{+\infty}$. Alors (X, Y) est code-compatible ssi aucun des ensembles $W_i(X, Y)$ ne contient le mot vide* 1.

Preuve. Si (X, Y) n'est pas code-compatible, il existe $i, j \geq 1$, $x_1 \ldots x_i \in X^{(i)}$, $y_1 \ldots y_j \in Y^{(j)}$ tels que

$$x_1 \ldots x_i = y_1 \ldots y_j \quad \text{avec } x_1 \neq y_1.$$

Deux cas sont possibles:

Cas 1. $|x_1| > |y_1|$. Alors $x_1 = y_1 u$ avec $1 \neq u \in U_1$.

Si $|x_1| = \infty$, alors $i = 1$, $|y_1| < \infty$, $|u| = \infty$. On a donc $u = y_2 \ldots y_j, j \geq 2$. D'où $uX^{(0)} \cap Y^{(j-1)} \neq \emptyset$. En vertu du Lemme 2.1(ii) on doit avoir $1 \in W_{0+(j-1)+1} = W_j$.

Si $|x_1| < \infty$, alors $|u| < \infty$. On a donc $ux_2 \ldots x_i = y_2 \ldots y_j$, $j \geq 2$. D'où $uX^{(i-1)} \cap Y^{(j-1)} \neq \emptyset$. En vertu du Lemme 2.1(ii), $1 \in W_{(i-1)+(j-1)+1} = W_{i+j-1}$.

Cas 2. $|x_1| < |y_1|$. Alors $x_1 v = y_1$ avec $1 \neq v \in V_1$. Le raisonnement se fait d'une façon similaire.

Supposons maintenant qu'il existe des ensembles W_i qui contiennent le mot vide 1. Soit $n \geq 2$ le nombre naturel le plus petit tel que $1 \in W_n$. En vertu du Lemme 2.1(i) il existe deux entiers $i, j \geq 0$ tels que ou bien il existe $u \in U_1$ tel que (a), ou bien il existe $v \in V_1$ tel que (b). Il suffit de traiter le premier cas. Soit

$$ux_1 \ldots x_i = y_1 \ldots y_j$$

avec $x_1 \ldots x_i \in X^{(i)}$, $y_1 \ldots y_j \in Y^{(j)}$.

Comme $u \in U_1$, il existe $x \in X$, $y \in Y$ tels que

$$x = yu,$$

où $x \neq y$ car $u \neq 1$.

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

$$xx_1\ldots x_i = yux_1\ldots x_i = yy_1\ldots y_j$$

avec $x\neq y$, ce qui montre que (X, Y) n'est pas code-compatible.

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

$$u=y_1\ldots y_j.$$

D'où

$$x=yu=yy_1\ldots y_j$$

avec $x\neq y$, ce qui montre également que (X, Y) n'est pas code-compatible. □

Exemple 1.1 (*suite*). On a $U_i(X, Y)=\{a\}$, $V_i(X, Y)=\{b\}$, et par conséquent $W_i(X, Y)=\{a, b\}$, pour tout $i\geq 1$. En vertu du Théorème 2.2, (X, Y) est code-compatible.

Exemple 1.2 (*suite*). On a

$$\begin{array}{lll} U_1(X, Y)=\emptyset, & V_1(X, Y)=\{b\}, & W_1(X, Y)=\{b\}, \\ U_2(X, Y)=\{a\}, & V_2(X, Y)=\emptyset, & W_2(X, Y)=\{a\}, \\ U_3(X, Y)=\{1\}, & V_3(X, Y)=\{1\}, & W_3(X, Y)=\{1\}. \end{array}$$

En vertu du Théorème 2.2, (X, Y) n'est pas code-compatible.

Evidemment pour tout $X\subseteq A^\infty$, $U_i(X, X)=V_i(X, X)=W_i(X, X)$, $i=1, 2, \ldots.$ Donc $U_i(X, X)$ noté aussi par $U_i(X)$ peut se récrire comme suit

$$U_1(X)=X^{-1}X-\{1\},$$

$$U_{i+1}(X)=X^{-1}U_i(X)\cup U_i(X)^{-1}X, \quad i\geq 1.$$

En vertu du Théorème 2.2 on a donc le corollaire suivant.

Corollaire 2.3 (cf. [6]). *Pour toute partie X de A^∞, X est un code ssi aucun des ensembles $U_i(X)$ ne contient le mot vide* 1.

3. Intersection des sous-monoides de A^∞

Proposition 3.1. *La classe des sous-monoides de A^∞, $A=\{a, b\}$, qui ont un ensemble générateur minimum n'est pas fermée par l'intersection.*

Preuve. Soient

$$X=\{a^iba^{i+1}b \mid i=1 \pmod 2\}\cup\{a^ib \mid i=1 \pmod 6\}$$
$$\cup\{a^iba^{i+1}b\ldots \mid i=2 \pmod 6\},$$

$$Y=\{a^iba^{i+1}ba^{i+2}b \mid i=1 \pmod 3\} \cup \{a^iba^{i+1}b \ldots a^{i+4}b \mid i=1 \pmod 6\}$$
$$\cup \{a^iba^{i+1}b \ldots \mid i=6 \pmod 6\}.$$

Il n'est pas difficile de vérifier que X et Y sont des ensembles générateurs minimums des sous-monoides X^* et Y^* respectivement.

Maintenant, si Z est un ensemble générateur arbitraire de $X^* \cap Y^*$, alors Z doit contenir $\{a^iba^{i+1}b \ldots a^{i+5}b \mid i=1 \pmod 6\}$ et aussi un nombre infini des éléments $a^iba^{i+1}b \ldots$, $i=1 \pmod 6$. Mais alors, en supprimant de Z un nombre fini de ces derniers éléments on a quand même un ensemble générateur de $X^* \cap Y^*$. Donc $X^* \cap Y^*$ n'a pas d'ensemble générateur minimum. $\square$

Pour tout sous-monoide M de A^∞ on pose

$$F_M=(M_{\text{fin}}-1)-(M_{\text{fin}}-1)^2, \quad I_M=M_{\text{inf}}-F_M M_{\text{inf}},$$
$$R_M=M_{\text{inf}} \cap F_M^\omega \quad \text{et} \quad G_M=F_M \cup I_M \cup R_M.$$

Il est montré dans [7] que G_M est un ensemble générateur de M.

Maintenant soit X une partie de A^∞. Soient z_1 et z_2 deux éléments de $(X^*)_{\text{inf}}$. Disons que z_1 est *contenu* dans z_2, $z_1 > z_2$, s'il existe $u \in F^+_{X^*}=(X^+_{\text{fin}}-X^+_{\text{fin}}X^+_{\text{fin}})^+$ tel que $z_1=uz_2$.

Lemme 3.2. *Si $X \subseteq A^\infty$ est un code, alors toute chaîne ascendante d'éléments de $(X^*)_{\text{inf}}$,*

$$z_1 < z_2 < \cdots < z_n < \cdots$$

est finie.

Preuve. Supposons qu'il existe une chaîne ascendante infinie d'éléments de $(X^*)_{\text{inf}}$,

$$z_1 < z_2 < \cdots < z_n < \cdots.$$

Pour chaque $n \geq 2$ il existe, par la définition de la relation "$<$", des éléments $u_1, \ldots, u_{n-1}$ de $F^+_{X^*}$ tels que

$$z_1=u_1 \ldots u_{n-1}z_n.$$

Soient $z_1=x_1 \ldots x_r \in X^{(r)}$, $z_n=x'_1 \ldots x'_s \in X^{(s)}$ avec x_r, $x'_s \in X_{\text{inf}}$. Soient $u_i=x_{i1} \ldots x_{it_i}$, $x_{ik} \in X_{\text{fin}}$ $(i \leq k \leq t_i,\ i=1, \ldots, n)$. Alors

$$z_1=x_1 \ldots x_r=x_{11} \ldots x_{1t_1} \ldots x_{n-1,1} \ldots x_{n-1,t_{n-1}}x'_1 \ldots x'_s.$$

Avec n assez grand on a évidemment

$$|x_1 \ldots x_{r-1}| < |x_{11} \ldots x_{1t_1} \ldots x_{n-1,1} \ldots x_{n-1,t_{n-1}}x'_1 \ldots x'_{s-1}|,$$

et, par conséquent, z_1 a deux factorisations différentes en éléments de X, contrairement à ce que X est un code. $\square$

Théorème 3.3. *L'intersection d'une famille quelconque de sous-monoïdes quasi-libres de A^∞ est aussi un sous-monoïde quasi-libre.*

Preuve. Soit $(M_i)_{i\in I}$ une famille de sous-monoïdes quasi-libres de A^∞ et soit $M = \bigcap_{i\in I} M_i$. Notons par X_i la base de M_i $(i\in I)$ et par $\mathcal{M}(I_M \cup R_M)$ l'ensemble des éléments *maximaux* de $I_M \cup R_M$ ainsi défini:

$$\mathcal{M}(I_M \cup R_M) = \{z\in I_M\cup R_M \mid \neg\exists z'\in I_M\cup R_M : z<z'\}.$$

Posons

$$Z = F_M \cup \mathcal{M}(I_M\cup R_M).$$

Démontrons que M est quasi-libre avec la base Z. Tout d'abord comme G_M est un ensemble générateur de M, en vertu du Lemme 3.2, Z est aussi un ensemble générateur de M, $Z^* = M$. Il suffit de démontrer que Z est un code. En effet, si Z n'est pas un code, il existe $z_1 \ldots z_n \in Z^{(n)}$, $z'_1 \ldots z'_m \in Z^{(m)}$ $(n, m \geq 1)$ tels que

$$z_1 \ldots z_n = z'_1 \ldots z'_m$$

avec $z_1 \neq z'_1$, disons $|z_1|>|z'_1|$. Alors $z_1 = z'_1 u$ pour un mot $u\neq 1$. Deux cas sont possibles:

Cas 1. $z_1\in F_M$. Alors $z'_1 \in F_M$.

Soient $z_j = x_{j1}\ldots x_{jr_j}$, $z'_k = x'_{k1}\ldots x'_{ks_k}$, où x_{jl}, $x'_{kt}\in X_i$ pour i quelconque de I $(1\leq l\leq r_j,\ 1\leq t\leq s_k,\ j=1,\ldots,n,\ k=1,\ldots,m)$. Alors

$$x_{11}\ldots x_{1r_1}\ldots x_{n1}\ldots x_{nr_n} = x'_{11}\ldots x'_{1s_1}\ldots x'_{m1}\ldots x'_{ms_m}.$$

Comme X_i est un code, il en résulte

$$\sum_{j=1}^{n} r_j = \sum_{k=1}^{m} s_k \quad \text{et} \quad x_{11} = x'_{11}, \ldots, x_{nr_n} = x'_{ms_m}.$$

L'égalité $z_1 = z'_1 u$ implique $r_1 > s_1$ et $u = x_{1,s_1+1}\ldots x_{1r_1}$. Ça signifie que $u\in M_i$ pour tout $i\in I$, i.e., $u\in M$, contrairement à ce que $z_1 \in F_M$.

Cas 2. $z_1 \in \mathcal{M}(I_M\cup R_M)$. Alors $n=1$, $m\geq 2$, donc

$$z_1 = z'_1 \ldots z'_m,$$

où $z'_1,\ldots,z'_{m-1}\in F_M$, $z'_m \in \mathcal{M}(I_M\cup R_M)$. Mais alors on a $z_1 < z'_1$ ce qui est en contradiction avec la maximalité de z_1. Ainsi, Z doit être un code. □

Théorème 3.4. *Soient X et Y deux codes sur un alphabet A. Alors $X^*\cap Y^* = (X\cap Y)^*$ ssi (X, Y) est code-compatible.*

Preuve. Supposons que (X, Y) soit code-compatible. Soit $z\in X^*\cap Y^*$. Alors il existe $x_1\ldots x_n \in X^{(n)}$, $y_1 \ldots y_m \in Y^{(m)}$ $(n, m\geq 1)$ tels que

$$z = x_1 \ldots x_n = y_1 \ldots y_m.$$

De la code-compatibilité de (X, Y) on en déduit $n = m$ et $x_i = y_i$ pour $i = 1, \ldots, n$. Donc $z \in (X \cap Y)^*$. Ceci montre que $X^* \cap Y^* \subseteq (X \cap Y)^*$. L'inclusion inverse $X^* \cap Y^* \supseteq (X \cap Y)^*$ est triviale. Ainsi $X^* \cap Y^* = (X \cap Y)^*$.

Réciproquement, supposons que $X^* \cap Y^* = (X \cap Y)^*$. Soit ensuite

$$x_1 \ldots x_n = y_1 \ldots y_m$$

avec $x_1 \ldots x_n \in X^{(n)}$, $y_1 \ldots y_m \in Y^{(m)}$ $(n, m \geqslant 1)$. Alors il existe $z_1 \ldots z_l \in (X \cap Y)^{(l)}$ tel que

$$z_1 \ldots z_l = x_1 \ldots x_n = y_1 \ldots y_m.$$

Comme X est un code, on a $l = n$ et $z_i = x_i$ $(i = 1, \ldots, l)$. D'autre part, comme Y est un code, on doit avoir $l = m$ et $z_i = y_i$ $(i = 1, \ldots, l)$. Donc $n = m$ et $x_i = y_i$ $(i = 1, \ldots, n)$, ceci montre que (X, Y) est code-compatible. □

Remerciements

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

Bibliographie

[1] J. Berstel, D. Perrin et M.P. Schützenberger, *Théorie des Codes* (LITP, Paris, 1981) Chapitres I–IV.
[2] S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1974).
[3] J.A. Riley, The Sardinas/Patterson and Levenstein theorems, *Inform. Control* **10** (1967) 120–136.
[4] A.A. Sardinas and G.W. Patterson, A necessary and sufficient condition for unique decomposition of coded message, *IER Conv. Record* **8** (1953) 104–108.
[5] B. Tilson, The intersection of free submonoids of a free monoid is free, *Semigroup Forum* **4** (1972) 345–350.
[6] D.L. Van, Codes avec des mots infinis, *RAIRO Informatique Théorique* **16** (1982) 371–386.
[7] D.L. Van, Sous-monoïdes et codes avec des mots infinis, *Semigroup Forum* **26** (1983) 75–87.