SÉMINAIRE SCHÜTZENBERGER

DOMINIQUE PERRIN

Sous-monoïdes et automates

Séminaire Schützenberger, tome 1 (1969-1970), exp. n° 10, p. 1-23
<http://www.numdam.org/item?id=SMS_1969-1970__1__A8_0>

Séminaire SCHÜTZENBERGER-LENTIN-NIVAT
(Problèmes mathématiques
de la Théorie des automates)
Année 1969/70, n° 10, 23 p.

27 janvier 1970

SOUS-MONOÏDES ET AUTOMATES

par Dominique PERRIN

I. Rappel de quelques définitions et propriétés préliminaires.

1. Monoïdes.

Un monoïde M est un ensemble muni d'une loi de composition associative et d'un élément neutre. Un sous-monoïde est un sous-ensemble stable contenant l'élément neutre.

Nous nous intéressons ici à une classe particulière de sous-monoïdes, qui sont les sous-monoïdes préfixes complets [5].

Définition. - Soit P un sous-monoïde du monoïde M. On dit que P est préfixe, s'il vérifie la condition :

$(\mathcal{U}_r)$ $\forall\, u, v \in M$, $uv \in P$ et $u \in P \Longrightarrow v \in P$.

On dit que P est complet, s'il vérifie :

$(\mathcal{R}_r)$ $\forall\, u \in M$, $uM \cap P \neq \emptyset$.

Si P et Q sont deux sous-monoïdes de M, $P \subset Q \subset M$, P peut être un sous-monoïde préfixe complet de Q, sans être un sous-monoïde préfixe complet de M. Ainsi, l'ensemble des puissances d'ordre pair de l'entier 2 est un sous-monoïde préfixe complet du monoïde multiplicatif des puissances de 2, mais n'est pas un sous-monoïde préfixe complet du monoïde multiplicatif des entiers naturels.

On vérifie facilement la proposition suivante :

PROPOSITION. - Soient P et Q deux sous-monoïdes de M ; $P \subset Q \subset M$.

(i) Si P est un sous-monoïde préfixe complet de Q, et Q un sous-monoïde préfixe complet de M, alors P est un sous-monoïde préfixe complet de M ;

(ii) Si P et Q sont des sous-monoïdes préfixes complets de M, alors P est un sous-monoïde préfixe complet de Q.

De plus :

PROPOSITION. - Soit M un groupe. Un sous-monoïde P de M est un sous-groupe, si, et seulement s'il est préfixe complet.

Tout sous-monoïde d'un groupe est d'ailleurs complet.

Exemples : Soit $\mathbb{Z}$ l'ensemble des entiers relatifs qui forment un groupe additif. Le sous-monoïde $\mathbb{N}$ des entiers naturels n'est pas préfixe. Par ailleurs $2\mathbb{N}$ est, par exemple, un sous-monoïde préfixe complet de $\mathbb{N}$.

2. Automates ([1] et [4]).

(a) DÉFINITION. - Soient M un monoïde, et S un ensemble. On appelle automate admettant M comme monoïde d'entrée et S comme ensemble d'états, tout homomorphisme de M dans S^S .

On note $\mathcal{A} = \langle M , S , \varphi \rangle$, où φ est un homomorphisme de M dans S^S .

Quand aucune confusion ne sera possible, nous noterons sm $(s \in S , m \in M)$ pour $s\varphi(m)$, qui est un élément de S .

(b) Structure algébrique d'un automate. - Un automate peut être considéré comme une algèbre universelle, possédant S comme ensemble de base et φM comme ensemble de lois de compositions unaires.

Une congruence d'automates sera donc une relation d'équivalence ρ sur S , telle que

$$\forall\, s , s' \in S , \quad s \equiv s' \mod (\rho) \implies \forall\, m \in M , \quad sm \equiv s'm \mod (\rho) .$$

On définit de même un homomorphisme d'automates et un automate quotient.

(c) L'équivalence modulo (K) .

DÉFINITION. - Soit K une partie du monoïde M . On dit que deux éléments m et m' de M sont équivalents modulo (K) , si, pour tout élément q de M , mq appartient à K si, et seulement si, $m'q$ appartient à K :

$$\forall\, m , m' \in M , \quad m \equiv m' \mod(K) \iff \{\forall\, q \in M , \quad mq \in K \iff m'q \in K\} .$$

(1) L'équivalence modulo (K) est régulière à droite.

(2) K est union de classes modulo (K) .

(3) L'équivalence modulo (K) est la plus grossière des équivalences régulières à droite qui saturent K (c'est-à-dire telles que K soit union de classes).

En effet, si l'équivalence ρ possède les propriétés ci-dessus,

$\forall\, m, m' \in M,\ m \equiv m' \mod(\rho) \Longrightarrow \{\forall\, q \in M,\ mq \in K \Longrightarrow m'q \in K\}$,

car $mq \equiv m'q \mod(\rho)$, et K est saturé modulo (ρ) .

(d) Automate reconnaissant une partie K de M . - Soient $\mathfrak{A} = \langle M, S, \varphi\rangle$ un automate, et s_0 un élément de S . On dit que $\mathfrak{A}$ reconnaît une partie K de M , si K est l'image réciproque par φ du stabilisateur de s_0 . K est alors nécessairement un sous-monoïde préfixe de M :

$$K = \{k \in M \mid s_0 k = s_0\} .$$

(e) L'automate $\mathfrak{A}(P)$. - Soit P un sous-monoïde préfixe complet de M . Soit S l'ensemble des classes de l'équivalence modulo (P) .

L'équivalence modulo (P) étant régulière à droite, M opère naturellement sur S : $\forall\, m \in M$, $\forall\, s \in S$, $sm = s' \in S$, si, pour des représentants q et q' des classes s et s' ,

$$qm = q' .$$

Soit φ l'homomorphisme ainsi défini de M dans S^S . Alors l'automate associé à φ , qu'on note $\mathfrak{A}(P)$, est, par définition, l'automate de P :

$$\mathfrak{A}(P) = \langle M, S, \varphi\rangle .$$

(i) $\mathfrak{A}(P)$ reconnaît P : P est la classe de l'élément neutre de M modulo (P) , et si on note s_0 cette classe, on a donc $P = \{p \in M \mid s_0 p = s_0\}$.

(ii) $\mathfrak{A}(P)$ est image homomorphe de tout automate reconnaissant P .

En effet, ceci revient à dire que l'équivalence modulo (P) est la plus grossière des équivalences régulières à droite qui saturent P .

(f) Exemple. - Soit M le monoïde bicyclique, c'est-à-dire le monoïde à deux générateurs x et y avec la relation $xy = e$.

Le sous-monoïde P engendré par y est préfixe et complet : tout élément de M s'écrit $y^n x^m$ $(n, m \in \underset{\sim}{N})$ et $y^n x^m y^m = y^n \in P$.

Les classes d'équivalence modulo (P) sont les ensembles $\{y^n x^m\}_{n \in \underset{\sim}{N}}$, et nous noterons une telle classe m . De plus, $m.x = m + 1$ et $m.y = m - 1$, si $m \neq 0$ et $0.y = 0$.

L'automate $\mathfrak{A}(P)$ a donc un ensemble d'états en bijection avec $\underset{\sim}{N}$; de plus, l'homomorphisme φ qui correspond à cet automate est une représentation isomorphe de M .

P est inclus dans le sous-monoïde Q engendré par y et x^2 qui est préfixe

et complet. $\mathcal{A}(Q)$ a deux états :

$$\alpha = \{y^n x^{2k}\}_{n\in\underset{\sim}{N},k\in\underset{\sim}{N}} ; \qquad \beta = \{y^n x^{2k+1}\}_{n\in\underset{\sim}{N},k\in\underset{\sim}{N}} ,$$

$$\alpha x = \beta ; \quad \beta x = \alpha \qquad \text{et} \qquad \alpha y = \beta ; \quad \beta y = \alpha .$$

On voit que $\mathcal{A}(Q)$ est isomorphe au quotient de $\mathcal{A}(P)$ par la congruence d'automate suivante : $m , m' \in \underset{\sim}{N}$, $m \equiv m'$, ssi $m - m'$ est pair.

3. Cas du monoïde libre [2].

Le cas où M est un monoïde libre nous intéresse plus particulièrement, car les objets définis ci-dessus peuvent alors être déterminés plus aisément.

Soient X un ensemble, X^* le monoïde libre sur X. Les éléments de X^* sont souvent appelés des mots, et X un alphabet.

Nous noterons $\ell_X(f)$ la longueur sur l'alphabet X du mot f de X^*.

(a) Codes. - Soit P un sous-monoïde préfixe complet de X^*. Il est isomorphe à un monoïde libre ; si A est le sous-ensemble de X^* qui engendre librement P, on dit que A est un code préfixe complet (sur X).

On vérifie qu'un code préfixe complet est une partie A de X^*, telle que, pour tout mot f de X^*, l'une exactement des deux éventualités suivantes se réalise : soit f est facteur gauche propre d'un mot de A, soit f a un facteur gauche dans A.

Nous dirons toujours ici, par abus de langage, code pour code préfixe complet.

Si A est un code, nous ne distinguerons pas le monoïde libre sur l'ensemble A et le sous-monoïde de X^* engendré par A.

La propriété suivante est fondamentale :

Si A et B sont deux codes sur X, $A \subset B \Longrightarrow A = B$ (ce qui se vérifie aisément).

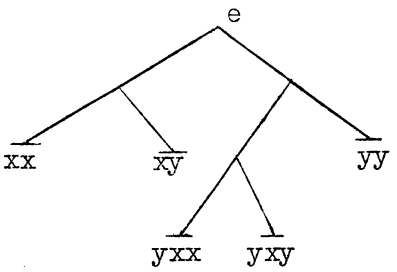
Nous avons vu au paragraphe 1 que, si $A^* \subset B^* \subset X^*$, où A et B sont deux sous-ensembles de X^* :

- Si A est un code sur B (c'est-à-dire si A^* est un sous-monoïde préfixe complet de B^*), et B un code sur X, alors A est un code sur X ;
- Si A et B sont des codes sur X, alors A est un code sur B.

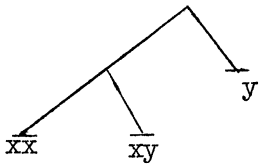
Remarque. - Les codes peuvent être représentés graphiquement par des "arbres", comme le montre l'exemple suivant :

$$X = \{x , y\} , \qquad A = \{xx , xy , yxx , yxy , yy\} .$$

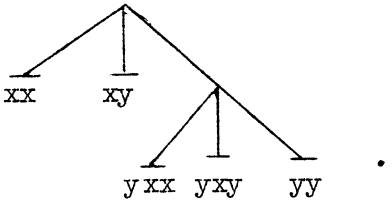
Le schéma correspondant est :



Si B est le code : $B = \{xx , xy , y\}$, alors A est inclus dans B^* . B est représenté par



L'ensemble B a trois éléments, et le code A sur l'ensemble B peut être schématisé ainsi :



(b) Préfixes d'un code. - Soit A un code sur X . Pour tout élément f de X^*, on peut écrire $f = at$, $a \in A^*$, $t \in X^* \setminus AX^*$.

L'ensemble $(X^* \setminus AX^*)$ des mots qui n'ont pas de facteur gauche dans A est, par définition, l'ensemble des préfixes de A .

A^* étant complet, l'ensemble de ses préfixes s'identifie à l'ensemble des facteurs gauches propres des mots de A .

Nous utiliserons souvent, dans la suite, les remarques suivantes, qui sont très simples :

(i) La relation suivante se vérifie facilement : Soit A un code sur X ;

$$\{e\} \cup (X^* \setminus AX^*)X = (X^* \setminus AX^*) \cup A .$$

(ii) Soit $t \in X^* \setminus AX^*$ un préfixe du code A . L'ensemble H des mots h de X^* tels que th soit dans A est un code,

$$H = \{h \in X^* \mid th \in A\} \quad \text{est un code sur } X .$$

Dans l'exemple précédent, l'ensemble des mots h de X^* tels que $yh \in A$ est le code

$$B = \{xx , xy , y\} .$$

(c) Calcul de l'automate $\mathcal{A}(A^*)$.

(i) Soient f et f' deux mots de X^* ; on pose

$$f = at , \quad f' = a't' ; \qquad a , a' \in A^* ; \qquad t , t' \in X^* \setminus AX^* .$$

Pour que f et f' soient équivalents modulo (A^*) , il faut et il suffit que t et t' le soient :

$$f \equiv f' \mod (A^*) \iff t \equiv t' \mod (A^*) .$$

(ii) Soient t et t' deux préfixes de A différents de l'élément neutre. t et t' sont équivalents modulo (A^*) , si, et seulement s'ils sont équivalents modulo (A) :

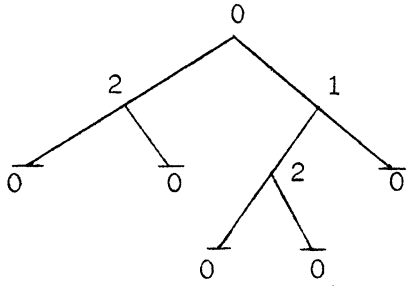
$$\forall\ t , t' \in XX^* \setminus AX^* , \qquad t \equiv t' \mod (A^*) \iff t \equiv t' \mod (A) .$$

En effet, si t est équivalent à t' modulo (A^*) , et si th est dans A , alors $t'h$ est dans A^* , et on peut poser $h = uv$ avec $t'u \in A$; mais alors $tu \in A^*$, et donc $h = u$, $t'h \in A$. Ainsi $t \equiv t' \mod (A)$.

Si t est équivalent à t' modulo (A) , et si th est dans A^* , t étant différent du mot vide, on peut poser $h = uv$ avec $tu \in A$, $v \in A^*$. Alors $t'u \in A$, et donc $t'h \in A^*$, ce qui montre que $t \equiv t' \mod (A^*)$.

(iii) En vertu des remarques précédentes, l'automate $\mathcal{A}(A^*)$ se calcule aisément à l'aide du schéma présenté ci-dessus : il suffit de connaître la classe modulo (A^*) de chacun des préfixes de A , et pour cela de connaître leur classe modulo (A) , excepté pour l'élément neutre, qui est équivalent aux éléments de A .

Ainsi, dans l'exemple précédent, $A = \{xx , xy , yxx , yxy , yy\}$,



,

$\mathcal{A}(A^*) = \langle X , S , \varphi \rangle$, $S = \{0 , 1 , 2\}$.

Nous noterons alors ainsi les applications φx et φy :

$$\varphi x = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix} ; \qquad \varphi y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} ,$$

ce qui signifie : $0x = 2$, $1x = 2$, $2x = 0$.

(d) Codes bornés. - La définition suivante sera fréquemment utilisée dans la suite

DÉFINITION. - Soit $A \subset X^*$ un code. On dit que A est borné sur X , si les longueurs des mots de A sur l'alphabet X sont bornées :

$$\exists\, k \in \underset{\sim}{N} : \qquad \forall\, a \in A , \quad \ell_X(a) \leqslant k .$$

Soient A et B deux codes sur X ; $A^* \subset B^* \subset X^*$. Alors A est borné sur X , si, et seulement si, A est borné sur B , et B est borné sur X .

En effet,

$$\sup_{a \in A} \ell_X(a) = \left[\sup_{a \in A} \ell_B(a)\right] \left[\sup_{b \in B} \ell_X(b)\right] .$$

II. Introduction.

1° Notre propos est d'étudier la correspondance qui peut exister entre les congruences de l'automate $\mathcal{A}(P)$ d'un sous-monoïde préfixe complet P et les sous-monoïdes préfixes complets Q contenant P . Ce problème avait été évoqué par M. P. SCHÜTZENBERGER [6]. Le travail qui est présenté ici est le fruit d'une collaboration avec J.-F. PERROT [3]. Notre but sera plus clair si nous présentons d'abord le cas où M est un groupe.

2° Soit G un groupe. Soit H un sous-groupe de G . Les classes d'équivalence modulo (H) , qui sont les états de l'automate $\mathcal{A}(H)$, s'identifient aux classes à droite relativement à H .

L'homomorphisme φ correspondant à l'automate $\mathcal{A}(H)$ s'identifie à la représentation de G sur les classes à droite relativement à H :

$$\varphi : \quad g \in G \longmapsto \begin{pmatrix} Hx \\ \\ Hxg \end{pmatrix} .$$

Les congruences de $\mathcal{A}(H)$ sont les systèmes d'imprimitivité du groupe de permutations φG . Soit ρ une congruence de $\mathcal{A}(H)$; soit K l'image réciproque par φ du stabilisateur de la classe de H modulo ρ . Alors l'automate de K , $\mathcal{A}(K)$,

est isomorphe au quotient $\mathcal{A}(H)/\rho$. De plus, l'application ainsi définie est une bijection de l'ensemble des congruences de $\mathcal{A}(H)$ sur l'ensemble des sous-groupes de G contenant H .

3° Nous montrons d'abord par des exemples que, dans le cas des monoïdes, cette correspondance n'est pas simple (ce n'est pas, en général, une bijection). Nous verrons ensuite qu'on peut définir entre les deux ensembles évoqués une correspondance de Galois et que, sous certaines conditions, elle se réduit à une bijection, si M est un monoïde libre.

III. Exemples.

1° Soit M le monoïde d'applications d'un ensemble S dans lui-même, engendré par les deux éléments :

$$x = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} ; \qquad y = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} ; \qquad S = \{0 , 1 , 2\}$$

(la notation ci-dessus a été introduite au chapitre I, § 2 (c)),

$$M = \{e , y , y^2 , x , xy , xy^2\} .$$

Le stabilisateur de l'élément 0 de S est un sous-monoïde préfixe complet, noté P :

$$P = \{e , x\} .$$

Nous allons voir que l'automate $\mathcal{A}(P)$ n'a pas d'image homomorphe non triviale, mais que P n'est pas un sous-monoïde préfixe complet maximal de M .

L'automate $\mathcal{A}(P)$ a deux états s et t correspondant à la partition de M en classes modulo (P) :

$$s = \{y , y^2 , xy , xy^2\} ; \qquad t = \{e , x\} .$$

$\mathcal{A}(P)$ n'a donc pas d'image homomorphe non triviale. P est inclus dans le sous-monoïde préfixe complet de M suivant :

$$Q = \{e , y^2 , x , xy^2\} .$$

2° Soit M le monoïde libre sur $X = \{x , y\}$. Soit P le sous-monoïde préfixe complet de X^* engendré par l'ensemble $A \subset X^*$;

$$A = (x^2)^* \{X^2 \setminus x^2\} .$$

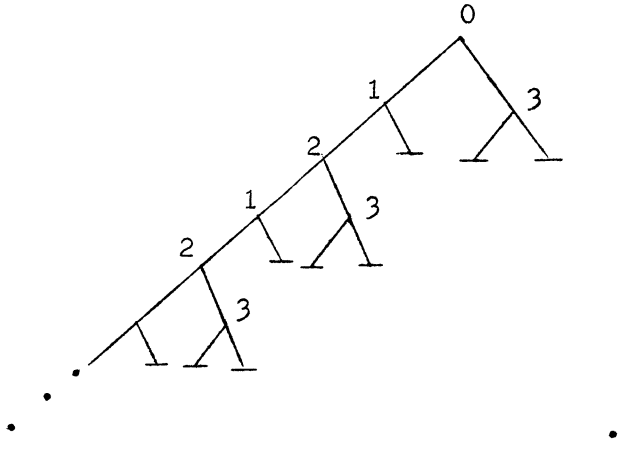
Son automate a quatre états : $S = \{0 , 1 , 2 , 3\}$,

$$x = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}; \qquad y = \begin{pmatrix} 3 & 0 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix} .$$

$\mathcal{A}(P)$ admet deux congruences : $\theta = /02/13/$ et $\theta' = /02/1/3/$. Or le seul sous-monoïde préfixe complet contenant P est $Q = (X^2)^*$. On voit aisément que

$$\mathcal{A}(Q) \simeq \mathcal{A}(P)/\theta \ .$$

A peut être schématisé ainsi :



IV. Définition d'une correspondance de Galois.

1. Définition.

Soit $P \subset M$ un sous-monoïde préfixe complet de M .

Soit L_P l'ensemble des sous-monoïdes préfixes complets de M contenant P .
Soit K_P l'ensemble des congruences de l'automate de P ; $\mathcal{A}(P) = \langle M , S , \varphi \rangle$.

L_P et K_P sont naturellement ordonnés. On définit alors deux applications $\lambda : K_P \to L_P$ et $\mu : L_P \to K_P$.

(a) Soit $\theta \in K_P$ une congruence de $\mathcal{A}(P)$.
Le quotient $\mathcal{A}(P)/\theta$ reconnaît un sous-monoïde préfixe complet Q contenant P :

$$Q = \{q \in M \mid s_0 \, q \equiv s_0 \mod (\theta)\} \ ,$$

où $s_0 \in S$ est la classe de e . Posons

$$\lambda(\theta) = Q \in L_P \ .$$

(b) Soit $Q \in L_P$; posons $S_Q = \zeta(Q)$, où ζ est la surjection canonique de M sur S , c'est-à-dire

$$S_Q = \{s \in S \mid \exists \, q \in Q , \ s_0 \, q = s\}$$

(où s_0 est l'élément de S qui est la classe de l'élément neutre modulo (P)).

L'ensemble des congruences de $\mathfrak{A}(P)$ telles que la classe de s_0 contienne S_Q est non vide (il contient la congruence à une seule classe), et est stable par intersection (conjonction des équivalences). Il contient donc un plus petit élément, soit donc $\mu(Q) \in K_P$ ce plus petit élément.

PROPOSITION. - λ et μ définissent une anti-correspondance de Galois entre K_P et L_P .

Démonstration.

1° Si θ , $\theta' \in K_P$, $\theta \leqslant \theta'$ $\Longrightarrow$ $\lambda(\theta) \supseteq \lambda(\theta')$.

2° Si Q et R sont deux éléments de L_P , $Q \subseteq R$ $\Longrightarrow$ $\mu(Q) \leqslant \mu(R)$. En effet, $S_Q \subseteq S_R$, de façon évidente.

Si $\mu(Q)$ n'est pas plus fine que $\mu(R)$, leur conjonction $\mu(Q) \cap \mu(R)$ est strictement plus fine que $\mu(Q)$, et la classe de s_0 relativement à cette conjonction contient S_Q .

3° Si $\theta \in K_P$, alors $\mu_0 \lambda(\theta) \leqslant \theta$. Si $Q \in L_P$, alors $\lambda_0 \mu(Q) \supseteq Q$. Ce qui achève la démonstration.

λ et μ sont donc des bijections inverses de l'ensemble des fermés de K_P sur l'ensemble des fermés de L_P , c'est-à-dire, par définition, les éléments de la forme $\mu_0 \lambda(\theta)$ où $\theta \in K_P$, et $\lambda_0 \mu(Q)$ où $Q \in L_P$.

Cette correspondance possède la propriété supplémentaire :

PROPOSITION. - Pour tous Q dans L_P , et θ dans K_P , $\mu(Q)$ et $\lambda(\theta)$ sont des fermés de K_P et L_P respectivement, c'est-à-dire

$$\mu_0 \lambda_0 \mu(Q) = \mu(Q) \; ; \qquad \lambda_0 \mu_0 \lambda(\theta) = \lambda(\theta) \; .$$

On le vérifie facilement.

2. Les fermés de L_P .

La définition de μ sera plus claire si l'on remarque que :

PROPOSITION. - Q est un fermé dans L_P , si, et seulement si, l'équivalence modulo (P) est plus fine que l'équivalence modulo (Q) .

Démonstration. - Si $(P) \leqslant (Q)$, alors l'équivalence modulo (Q) induit sur S (qui est le quotient de M par l'équivalence modulo (Q)) une équivalence qui est une congruence d'automate. La classe de s_0 est précisément S_Q , et ainsi

$$\lambda_0\,\mu(Q) = Q \qquad \text{et} \qquad Q \text{ est fermé dans } L_P \ .$$

Si $(P) \not\leq (Q)$, cela revient à dire que Q n'est pas saturé modulo (P), ou encore

$$\exists\, m, m' \in M, \qquad m \equiv m' \ (P), \quad m \in Q, \quad m' \notin Q \ .$$

Ce qui signifie que $m' \in \lambda_0\,\mu(Q)$, et donc que $\lambda_0\,\mu(Q) \not\supseteq (Q)$. Et ceci exprime que Q n'est pas fermé dans L_P.

3. Les fermés de K_P.

Si θ est fermé dans K_P, $\mathfrak{A}(\lambda(\theta))$ est image homomorphe de $\mathfrak{A}(P)/\theta$; il ne lui est pas, en général, isomorphe.

Cependant, $\lambda(\theta)$ étant alors fermé dans L_P, d'après la proposition précédente, l'équivalence modulo $(\lambda(\theta))$ est plus grossière que l'équivalence modulo (P), et elle induit donc sur S une congruence θ' telle que

$$\mathfrak{A}(\lambda(\theta)) \simeq \mathfrak{A}(P)/\theta' \ .$$

Cette remarque motive la modification apportée à la correspondance, et que nous exposons ci-dessous.

Soit λ' l'application de K_P dans lui-même, définie ainsi : Soit θ une congruence de $\mathfrak{A}(P)$. L'ensemble des congruences θ' de $\mathfrak{A}(P)$ telles que $\lambda(\theta) = \lambda(\theta')$ est stable par union (disjonction des équivalences), et est non vide. Il admet donc un élément maximal, que nous définissons comme $\lambda'(\theta)$.

Posons $\mu' = \lambda'_0\,\mu$, notons L'_P et K'_P les ensembles de fermés de L_P et K_P, et K''_P l'image par λ de K'_P. On peut alors énoncer :

PROPOSITION. - μ' est une bijection de L'_P sur K''_P. Si θ est une congruence de $\mathfrak{A}(P)$, et Q un élément de L_P, $\theta = \mu'(Q)$ si, et seulement si,

$$\mathfrak{A}(Q) \simeq \mathfrak{A}(P)/\theta \ .$$

4. Remarque.

La définition de l'application μ' n'est pas simple (elle nécessite une sorte de "minimax"). On pourrait être tenté de définir une application analogue de L_P dans K_P, au moins des deux façons suivantes :

(a) Avec les mêmes notations que ci-dessus, on peut chercher si l'ensemble des congruences, dont la classe de s_0 est contenue dans S_Q, possède un élément maximal (qui serait alors tout désigné pour être $\mu'(Q)$). L'exemple suivant montre qu'il n'en est rien.

Soient $X = \{x , y\}$, $M = X^*$, $P = A^*$, où A est la partie de X^* suivante : Posons

$$B = (\{x\} \cup \{y\})y^* x \ ,$$

$$A = (B \setminus \{\{xyx\} \cup \{yx\}\}) \cup (\{xyx\}B) \cup (\{yx\}B) \qquad \text{(voir le schéma)} \ .$$

$\mathfrak{A}(P)$ a cinq états : $S = \{0 , 1 , 2 , 3 , 4\}$ (où 0 est la classe de l'élément neutre),

$$x = \begin{pmatrix} 3 & 2 & 4 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix} ; \qquad y = \begin{pmatrix} 1 & 4 & 4 & 1 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix} \ .$$

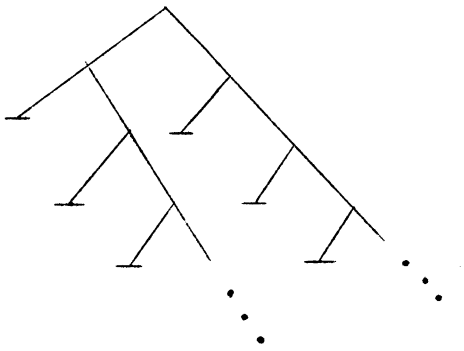
Les congruences non triviales de $\mathfrak{A}(Q)$ sont les suivantes :

$$\theta = /02/134/ \ ; \qquad \theta' = /03/1/24/ \ .$$

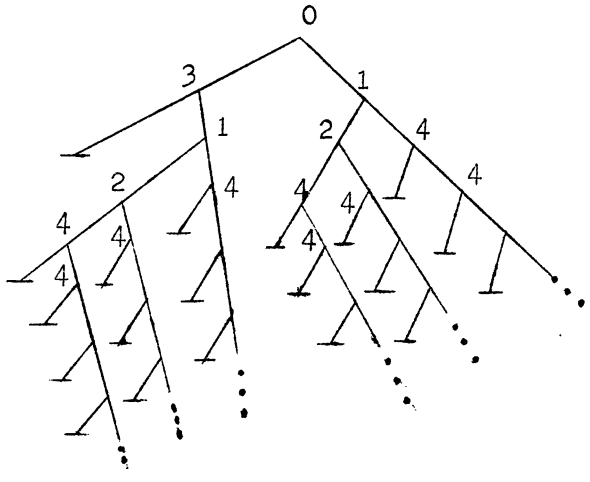
Or P est inclus dans le monoïde préfixe complet Q engendré par l'ensemble $y^* x$. L'ensemble S_Q a quatre éléments :

$$S_Q = \{0 , 2 , 3 , 4\} \ .$$

Les congruences θ et θ' sont telles que la classe de 0 est contenue dans S_Q. L'ensemble des congruences telles que la classe de s_0 est contenue dans S_Q n'a pas d'élément maximal. B peut être représenté par



A est alors représenté ainsi :



(b) La disjonction des équivalences modulo (P) et modulo (Q) est une équivalence régulière à droite plus grossière que l'équivalence modulo (P) ; elle définit donc une congruence d'automate, soit, par définition, $\beta(Q) \in K_P$.

$\beta(Q)$ coïncide avec $\mu(Q)$, si Q est un fermé de L_P . Mais l'exemple suivant montre que, si $Q \subset R$, où Q et R sont deux éléments de L_P , on n'a pas nécessairement $\beta(Q) \leqslant \beta(R)$. $M = X^*$, $X = \{x , y\}$. $P = A^*$, où A est défini par

$$A = X^* yx \setminus X^* yxXX^* \ .$$

Soit $Q = B^*$, où $B = (\{x\} \cup \{y\})y^* x$. Soit $R = C^*$, où $C = y^* x$. Alors $P \subset Q \subset R \subset X^*$. L'automate $\mathcal{A}(P)$ a pour ensemble d'états $S = \{0 , 1 , 2\}$,

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix} ; \qquad y = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix} \ .$$

$\beta(Q)$ est la congruence triviale (tous les états sont congrus). $\beta(R)$ est la congruence $/01/2/$.

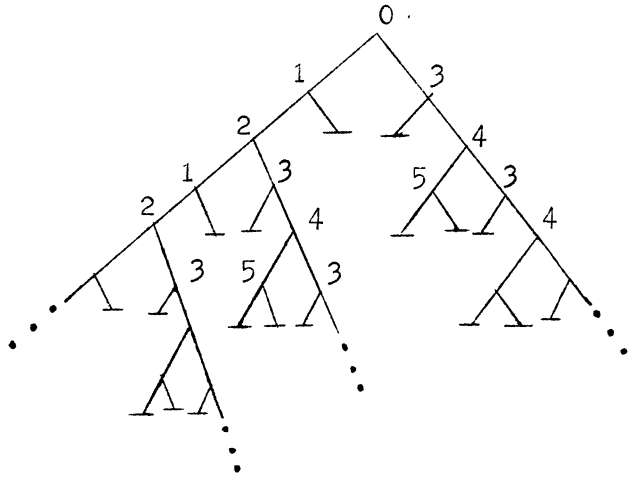
Nous terminons ce paragraphe en donnant un exemple de calcul de K_P et L_P .

V. Exemple.

Soit $X = \{x , y\}$. Nous prenons pour P le sous-monoïde engendré par le code :

$$A = (x^2)^* \{[(y^2)^* (X^2 \setminus y^2)] \setminus x^2\} \ .$$

A se schématise ainsi :



$$x = \begin{pmatrix} 1 & 2 & 1 & 0 & 5 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \ ,$$

$$y = \begin{pmatrix} 3 & 0 & 3 & 4 & 3 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \ .$$

(a) L'ensemble K_P a quatre éléments (en dehors des deux congruences triviales):

$$\theta_1 = /0,2,4/1,3,5/ \ ; \qquad \theta_2 = /0,2,4/1,5/3/ \ ;$$
$$\theta_3 = /0,2/1,5/3/4/ \ ; \qquad \theta_4 = /0,2/1/3/4/5/ \ .$$

(b) L'ensemble L_P est infini ; il contient les éléments suivants :

$$\{Q_n\}_{n\in\mathbb{N}} \; ; \quad Q_n = B_n^* \, , \qquad \text{où} \quad B_n = \bigcup_{i=0}^{n-1} (x^2)^i \, \{[(y^2)^* \, \{X^2 \setminus y^2\}] \setminus x^2\} \cup x^{2n} \, ,$$

on peut encore écrire directement :

$$B_n = \{A \setminus \{x^{2n} \, X^* \cap A\}\} \cup x^{2n} \; ;$$

$$\{R_n\}_{n\in\mathbb{N}} \; ; \quad R = C_n^* \, , \qquad \text{où} \quad C_n = \bigcup_{i=0}^{n-1} (y^2)^i \, \{X^2 \setminus y^2\} \cup y^{2n} \, ,$$

ou encore

$$C_n = \{B_1 \setminus \{y^{2n} \, X^* \cap B_1\}\} \cup y^{2n} \, .$$

Alors

$$A^* \subset Q_n \subset Q_1 \subset R_m \subset R_1 \subset X^* \, ,$$

pour tout couple n et m d'entiers (on remarque que $R_1 = (X^2)^*$).

(c) Les applications λ et μ sont :

$$\lambda(\theta_1) = R_1 \; ; \qquad \lambda(\theta_2) = R_1 \; ; \qquad \lambda(\theta_3) = \lambda(\theta_4) = Q_1 \; ;$$

$$\forall \, n \in \mathbb{N} \, , \qquad \mu(Q_n) = \mu(Q_1) = \theta_4 \; ; \qquad \mu(R_n) = \mu(R_1) = \theta_2 \, .$$

L'ensemble K_P' des éléments de K_P qui sont des fermés est :

$$K_P' = \{\theta_2 \, , \, \theta_4\} \, .$$

De même,

$$L_P' = \{R_1 \, , \, Q_1\} \, .$$

L'application λ' est :

$$\lambda'(\theta_2) = \theta_1 \; ; \qquad \lambda'(\theta_4) = \theta_3 \; ; \qquad K_P'' = \{\theta_1 \, , \, \theta_3\} \, .$$

L'application μ' est alors :

$$\mu'(Q_1) = \theta_3 \; ; \qquad \mu'(R_1) = \theta_1 \, .$$

On peut vérifier que $\mathcal{A}(A^*)/\theta_1 \simeq \mathcal{A}[(X^2)^*]$, $\mathcal{A}(A^*)/\theta_3 \simeq \mathcal{A}(Q_1)$.

VI. Etude des fermés.

1.

Nous savons peu de choses des fermés de cette correspondance, dans le cas où M est un monoïde quelconque. La proposition suivante, qui donne une condition suffisante, permet cependant de régler le cas des monoïdes commutatifs.

Les notations sont celles du chapitre V.

PROPOSITION. - Si $Q \in L_P$ vérifie la condition :

$(\mathcal{U}_1)$ $\forall\, u, v \in M$, $uv \in Q$, $v \in Q \Longrightarrow u \in Q$;

alors Q est un fermé dans L_P.

(La condition ci-dessus définit les sous-monoïdes bipréfixes (préfixes à droite et à gauche) [2].)

Démonstration. - Si Q n'est pas un fermé, l'équivalence modulo (P) n'est pas plus fine que l'équivalence modulo (Q), comme nous l'avons vu ; ce qui signifie encore que Q n'est pas saturé par l'équivalence modulo (P) :

$$\exists\, m, m' \in M, \quad m \equiv m' \ (P), \quad m \in Q, \quad m' \notin Q .$$

P satisfait $(\mathcal{U}_r)$, et donc il existe n dans M tel que mn soit dans P. $m'n$ est alors dans P, donc dans Q. Or, Q étant préfixe,

$$m \in Q, \quad mn \in Q \Longrightarrow n \in Q ,$$

d'où la contradiction avec l'hypothèse :

$$\exists\, m', n \in M, \quad m'n \in Q, \quad m' \notin Q, \quad n \in Q .$$

On peut alors énoncer :

PROPOSITION. - Soit M un monoïde commutatif. Soit P un sous-monoïde préfixe complet de M. Il y a bijection entre les congruences θ de l'automate $\mathcal{A}(P)$ et les sous-monoïdes préfixes complets Q de M contenant P. θ et Q se correspondent, si, et seulement si,

$$\mathcal{A}(P)/\theta \simeq \mathcal{A}(Q) .$$

Démonstration.

(i) Dans un monoïde commutatif, les sous-monoïdes qui vérifient la condition $(\mathcal{U}_r)$ vérifient aussi la condition $(\mathcal{U}_1)$, et les éléments de L_P sont donc des fermés.

(ii) Nous montrons maintenant que toute congruence $\theta \in K_P$ est fermée dans K_P. Soit $\theta \in K_P$; posons $Q = \lambda(\theta)$; notons encore θ l'équivalence sur M induite par l'équivalence θ sur S.

Il nous suffit de montrer :

$$\forall\, m, m' \in M, \qquad m \equiv m' \mod (Q) \implies m \equiv m' \mod (\theta) .$$

Or, P étant complet, il existe n dans M, tel que mn soit dans P.

Alors $m'n \in Q$; posons $m'n = q \in Q$,

$$m'nm = qm , \qquad \text{et donc} \qquad mnm' = qm .$$

Ainsi $mnm' \equiv m' \mod (P)$, car $mn \in P$, et $qm \equiv m \mod (\theta)$, car $q \equiv e \ (\theta)$, par définition de Q. Enfin $m \equiv m' \mod (\theta)$, ce qui achève la démonstration.

Remarque. - Si φ est l'homomorphisme de M dans S^S correspondant à l'automate $\mathcal{A}(P)$, on peut observer que φM est un groupe (sa représentation de permutation sur S étant régulière, puisque c'est un groupe abélien et transitif), quand M est abélien.

2. Cas du monoïde libre.

Nous avons indiqué, au chapitre I, que les notions étudiées ici se laissent mieux appréhender dans le cas où M est un monoïde libre, et nous avons introduit une terminologie particulière. Nous allons voir que, dans ce cas, on peut donner un certain nombre de propriétés des fermés pour la correspondance définie au chapitre IV, quoique de nombreux problèmes restent ouverts.

(a) Les fermés de K_{A^*}. - Soient $A \subset X^*$ un code, $\mathcal{A}(A^*)$ son automate. Et soit θ une congruence de $\mathcal{A}(A^*)$.

La fermeture de θ dans K_P, c'est-à-dire $\mu_0 \lambda(\theta)$, est la congruence θ' de $\mathcal{A}(A^*)$ la plus fine, telle que les classes de s_0 modulo (θ) et modulo (θ') soient égales :

$$\forall\, \theta \in K_P, \quad \mu_0 \lambda(\theta) = \inf\{\theta' \in K_P \mid \forall\, s \in S, \ s \equiv s_0 \mod (\theta) \iff s \equiv s_0 \mod (\theta')\} .$$

Ainsi :

PROPOSITION. - Un élément θ de K_P est un fermé, si, et seulement s'il est minimal parmi tous les éléments θ' de K_P qui définissent la même classe de s_0, où s_0 désigne l'état de $\mathcal{A}(A^*)$ qui est la classe de l'élément neutre modulo (A^*) ;

$$\forall\, \theta \in K_P, \quad \theta = \mu_0 \lambda(\theta)$$
$$\iff \theta = \inf\{\theta' \in K_P \mid \forall\, s \in S, \ s \equiv s_0 \mod (\theta) \iff s \equiv s_0 \mod (\theta')\} .$$

Un cas particulièrement simple est celui qui se produit s'il n'existe qu'une congruence d'image donnée par λ , ou, ce qui revient au même, une seule congruence telle que la classe de s_0 soit un sous-ensemble donné de S . Cette congruence est alors évidemment un fermé.

Une condition suffisante pour qu'il en soit ainsi est évidemment la suivante : Soient θ une congruence de $\mathcal{A}(A^*)$, et B^* l'image de θ par λ :

$$B^* = \{b \in X^* \mid s_0 b \equiv s_0 \mod (\theta)\} .$$

Si chaque classe modulo (B^*) a un représentant, et un seul, dans $X^* \setminus BX^*$, θ est la seule congruence de $\mathcal{A}(A^*)$ d'image B^* par λ . En effet, sous cette hypothèse, il existe un seul automate reconnaissant B^* .

Un cas plus intéressant est le suivant :

PROPOSITION 1. - Soit θ un élément de K_P ; $B^* = \lambda(\theta)$. S'il existe un élément b de B^* tel que $bB \subset A$ (ce qui est évidemment le cas si A est borné sur B), θ est la seule congruence de $\mathcal{A}(A^*)$ d'image B^* par λ . Et donc $\mathcal{A}(A^*)/\theta \simeq \mathcal{A}(B^*)$.

Démonstration. - Nous noterons encore θ l'équivalence régulière à droite induite sur X^* par la congruence θ de $\mathcal{A}(A^*)$.

Il faut montrer que, $\forall\, f , f' \in X^*$, $f \equiv f' \ (B^*) \implies f \equiv f' \ (\theta)$. Soient donc f et f' deux éléments de X^* , $f \equiv f' \mod (B^*)$. On pose $f = hp$, $f' = h'p'$, où $h , h' \in B^*$, $p , p' \in X^* \setminus BX^*$ (p et p' sont des préfixes de B). Alors $p \equiv p' \mod (B^*)$, $f \equiv p \mod (\theta)$ et $f' \equiv p' \mod (\theta)$, puisque, par définition de B^* , $h , h' \equiv e \mod (\theta)$.

Soit alors b l'élément de B^* tel que $bB \subset A$, dont nous avons supposé l'existence. De la même façon, $f \equiv bp \mod (\theta)$ et $f' \equiv bp' \ (\theta)$. De plus, bp et bp' sont équivalents modulo (A^*) , car

$$p \equiv p' \mod (B^*) \implies \{\forall\, k \in X^* , \ pk \in B \iff p'k \in B\} .$$

Ainsi,

$$\forall\, k \in X^* , \qquad bpk \in A \iff pk \in B \iff p'k \in B \iff bp'k \in A .$$

Ceci montre, par transitivité, que $f \equiv f' \mod (\theta)$, ce qui achève la démonstration.

(b) Etude des fermés de L_{A^*} . - Nous avons vu, au chapitre IV, qu'un élément B^* de L_{A^*} était un fermé, si, et seulement si, l'équivalence modulo (A^*) était plus fine que l'équivalence modulo (B^*) , ce qui s'exprime encore en disant que B^* est une partie de X^* saturée modulo (A^*) .

Dans l'étude des fermés de L_{A^*} , certains codes jouent un rôle important. Nous les nommons chaînes.

(b1) Chaînes.

DÉFINITION. - Un code B sur X est une chaîne, s'il existe un code C et une partition de C en deux sous-ensembles non vides C_0 et C_1 tels que $B = C_0^* C_1$.

Exemple : $X = \{x , y\}$, $C = X$, $C_0 = \{x\}$, $C_1 = \{y\}$. $B = x^* y$ est une chaîne.

La caractérisation suivante est utile :

PROPOSITION. - Soit B un code. Les trois énoncés suivants sont équivalents :

(i) B est une chaîne ;

(ii) Il existe un élément c de XX^* tel que

$$cB \subset B \ ;$$

(iii) Il existe un élément c de XX^* tel que

$$\forall\, h \in X^* , \qquad ch \in B \implies h \in B \ .$$

Démonstration. - Si B est une chaîne, $B = C_0^* C_1$, alors, $\forall\, c \in C_0$, $c_0 B \subset B$, et (i) implique (ii).

(ii) est équivalent à (iii), car $\{h \mid ch \in B\}$ est un code pour tout préfixe c de B .

(ii) implique (i), car, de $cB \subset B$, on déduit que, pour tout entier n , $c^n B \subset B$, et donc $c^*\{B \setminus (cX^* \cap B)\} \subset B$. Mais le premier membre est un code, et donc $c^*\{B \setminus (cX^* \cap B)\} = B$. Ainsi B est une chaîne.

La proposition suivante précise la remarque (ii) du chapitre I, § 2 (c).

PROPOSITION. - Les restrictions aux préfixes d'un code B des équivalences modulo (B) et modulo (B^*) sont égales, si, et seulement si, B n'est pas une chaîne.

Démonstration. - Si B est une chaîne, il existe c dans XX^* tel que $cB \subset B$. Alors c est équivalent modulo (B) à l'élément neutre, et c n'est pas dans B^* .

Si les équivalences en question sont distinctes, il existe un préfixe c de A qui est équivalent modulo (B) à l'élément neutre (I, § 2 (c)). Ainsi, $cB \subset B$, et B est une chaîne.

Remarque. - La restriction à $X^* \setminus BX^*$ de l'équivalence modulo (B) est égale à la restriction à cet ensemble de l'équivalence :

$$\forall\, h \in XX^* , \qquad fh \in A^* \iff f'h \in A^* \ .$$

Nous aurons à faire usage de la proposition suivante :

PROPOSITION 2. - Soient B un code sur X , et c un élément de $X^* \setminus B^*$ tel que $cB \subset B^*$.

Si l'ensemble des entiers n tels que $cb \in B^n$, pour b dans B , est borné,

$$\exists\, k \in \mathbb{N} , \qquad \forall\, b \in B , \quad cb \in B^n \implies n \leqslant k \ .$$

Alors B est une chaîne.

Démonstration. - Soit k le plus grand entier tel que $cb \in B^k$ pour b dans B . Si $k = 1$, B est une chaîne. Supposons donc $k \geqslant 2$.

Soit b un élément de B tel que $cb \in B^k$, et posons $b = uv$, avec $cu \in B^{k-1}$, $v \in B$. Alors, pour tout h dans X^* , si $uh \in B$, de $cuh \in B^*$, on déduit que, $h \in B$, $\forall\, h \in X^*$, $uh \in B \implies h \in B$. Ainsi B est une chaîne.

Exemples :

1° $X = \{x , y\}$, $B = x^* yy^* x$. Alors $yB \subset B \cup B^2$; en effet,

$$yB = y^2 y^* x + (yx)x^* yy^* x \ .$$

Le code B est effectivement une chaîne : $xB \subset B$.

2° Nous montrons qu'il existe des codes B qui ne sont pas des chaînes, tels qu'il existe c dans $X^* \setminus B^*$, avec $cB \subset B^*$.

Soient $X = \{x , y\}$, $B_0 = xx^* y$, $B_1 = yy^* x$, et posons $B = B_1 + B_0(B_1 + xB_0^* B_1)$. B n'est pas une chaîne, mais $yB \subset B^*$, car

$$yB_1 \subset B_1 , \qquad yB_0 = yxB_0 + yxy \ ,$$

$$yB_0 B_1 = yxB_0 B_1 + yxyB_1 \subset B_1 B_0 B_1 + B_1^2 \subset B^2 \ ,$$

$$yB_0 xB_0^* B_1 = yxB_0 xB_0^* B_1 + yxyx B_0^* B_1 \subset B^2 + B^2(B_0^* B_1) \ .$$

Il reste à montrer que $B_0^* B_1 \subset B^*$. Or

$$B_0^* B_1 = (B \setminus B_0 xyx) + B_0 xyx(B_0 + y)B_0^* B_1 \ ,$$

et

$$yB_0^* B_1 \subset (yx)^* B_0^* B_1 \ .$$

Une récurrence sur la longueur des mots de $B_0^* B_1$ montre alors la propriété cherchée.

(b2) Après avoir introduit la notion de chaîne, nous commençons l'étude des fermés de L_{A^*} . Deux lemmes sont nécessaires.

LEMME 1. - Soient A et B deux codes sur l'alphabet X ; $A \subset B^* \subset X^*$, et A est borné sur B .

S'il existe un préfixe f de A , qui n'est pas dans B^* , tel que l'ensemble $\{h \in X^* \mid fh \in A\}$ est un code sur B qui est borné sur B , alors :

Il existe un préfixe ℓ de A , qui n'est pas dans B^* , tel que :

(i) $\{h \in X^* \mid \ell h \in A\}$ est un code sur B ;
(ii) $\ell B \subset B^*$.

Démonstration. - Pour tout préfixe t de A vérifiant les mêmes hypothèses que f , on pose $\psi(t) = i$, si la longueur maximale des mots de $\{h \in X^* \mid th \in A\}$ sur l'alphabet B est i .

Supposons, par récurrence sur $\psi(k)$, qu'il existe un préfixe k de A possédant les mêmes propriétés que f , avec $\psi(k) \leqslant \psi(f)$. Soit $kB \subset B^*$, et la démonstration est achevée ; soit il existe un mot b de B tel que $kb \notin B^*$, alors, de $k \in X^* \setminus AX^*$, on déduit $kb \in X^* \setminus AX^* \cup A$, car $\{h \in X^* \mid kh \in A\} \subset B^*$. Mais kb n'est pas dans A , car $kb \notin B^*$. Ainsi, $kb \in X^* \setminus AX^*$, $kb \notin B^*$; $\{h \in X^* \mid kbh \in A\}$ est un code sur B , borné sur B . De plus $\psi(kb) = \psi(k) - 1$, et ceci achève la démonstration, car, pour $\psi(k) = 1$, $kB \subset A \subset B^*$.

LEMME 2. - Soient A et B deux codes sur X ; $A \subset B^*$, et A est borné sur B .

Si l'ensemble $(X^* \setminus AX^*) \cap B^*$ des préfixes de A qui sont dans B^* n'est pas saturé modulo (A) , B est une chaîne.

Démonstration. - Soient t et t' deux préfixes de A , tels que

$$t \equiv t' \mod (A) \; ; \qquad t \in B^* \; ; \quad t' \notin B^* \; ,$$

Le mot t' vérifie les hypothèses du lemme 1, car

$$\{h \in X^* \mid t'h \in A\} = \{h \in X^* \mid th \in A\} \; ,$$

et le deuxième membre est un code sur B qui est borné sur B . Il existe donc un préfixe ℓ de A , tel que $\ell \notin B^*$, $\ell B \subset B^*$; $\{h \in X^* \mid \ell h \in A\}$ est un code sur B . Alors, pour tout b dans B , l'entier n tel que $\ell b \in B^n$ est borné par la longueur maximale des mots de A sur B . En vertu de la proposition 2,

B est alors une chaîne.

Ces deux lemmes ont pour conséquence deux théorèmes :

THÉORÈME 1. - Soient A et B deux codes sur X ; $A \not\subseteq B^* \subseteq X^*$, et A est borné sur B . Alors B^* est une partie saturée modulo (A^*), si, et seulement si, B n'est pas une chaîne.

Démonstration. - Si B est une chaîne, soit β un élément de XX^* tel que $\beta B \subset B$, et soit a un mot de A de longueur maximale sur B ; on pose

$$a = bb' \; ; \qquad b \in B^* \; ; \quad b' \in B \; .$$

Alors $bB \subset A$, et donc $b \equiv b\beta \mod (A)$, car

$$\forall\, k \in X^* , \qquad bk \in A \iff k \in B \iff \beta k \in B \iff b\beta k \in A \; .$$

Mais, du fait que A est strictement inclus dans B^*, il s'ensuit que b est différent du mot vide, et donc que $b \equiv b\beta \mod (A^*)$. Or $b\beta$ n'est pas dans B^*, et B^* n'est donc pas saturé modulo (A^*) .

Réciproquement, si B^* n'est pas saturé modulo (A^*), il existe b et b' tels que $b \in B^*$, $b' \notin B^*$, $b \equiv b' \mod (A^*)$. Si on pose alors $b = at$, $b' = a't'$, avec $a , a' \in A^*$, $t , t' \in X^* \setminus AX^*$, $t \in B^*$, $t' \notin B^*$, $t \equiv t' \mod (A)$. L'ensemble $(X^* \setminus AX^*) \cap B^*$ n'est donc pas saturé modulo (A), et, d'après le lemme 2, B est une chaîne.

THÉORÈME 2. - Soient C et D deux codes sur X ; $C \subset D^*$, et C est borné sur D . Alors, si C est une chaîne, D en est une.

Démonstration. - On suppose que C est une chaîne, et que D n'en est pas une. Soit f dans XX^*, tel que $fC \subset C$, et posons $f = uv$, $u \in D^*$, $v \in X^* \setminus DX^*$. Alors $fu \equiv u \mod (C)$, car, $\forall\, h \in X^*$, $fuh \in C \iff uh \in C$. Or, d'après le lemme 2, l'ensemble $(X^* \setminus CX^*) \cap D^*$ est saturé modulo (C), et fu est donc dans D^*, ce qui implique $vu \in D^*$. Alors $f^n = u(vu)^{n-1} v$ est un préfixe de C qui a plus de n facteurs gauches dans D, et C n'est donc pas borné sur D, ce qui achève la démonstration.

Remarque. - Sous les hypothèses du théorème, il est faux que

$$\forall\, d \in XX^* , \qquad dC \subset C \implies dD \subset D \; .$$

(c) Résumé des résultats. - Soit A un code sur X . Le théorème 2 montre que, si A n'est pas une chaîne, il existe un code I tel que $A \subset I^*$, A est borné sur I, I n'est pas une chaîne, et

$$A \subset B^* \subset I^* \implies B \text{ n'est pas une chaîne ,}$$

$$A \subset I^* \subset B^* \text{ et } A \text{ borné sur } B \implies B \text{ est une chaîne .}$$

Ainsi, d'après les théorèmes 1 et 2 et la proposition 1 :

THÉORÈME 3. - Soit A un code sur X qui n'est pas une chaîne. Pour tout sous-ensemble $\mathfrak{I}$ totalement ordonné par inclusion de L_{A^*}, il existe un code I : $I^* \in \mathfrak{I}$, I n'est pas une chaîne, A est borné sur I, tel que :

Si θ est la congruence de $\mathcal{A}(A^*)$ telle que $\mathcal{A}(A^*)/\theta \simeq \mathcal{A}(I^*)$:

(i) Il y a bijection entre les codes B tels que $A \subset B^* \subset I^*$ et les congruences β de $\mathcal{A}(A^*)$ plus fines que θ, β et B se correspondant si, et seulement si,

$$\mathcal{A}(A^*)/\beta \simeq \mathcal{A}(B^*) \ ;$$

(ii) Pour tout élément B^* de $\mathfrak{I}$, avec $I^* \subsetneq B^*$, et A est borné sur B, B^* n'est pas saturé modulo (A^*) ;

(iii) Pour toute congruence β de $\mathcal{A}(A^*)$ plus grossière que θ, $\mathcal{A}(A^*)/\theta$ reconnaît un code B tel que A n'est pas borné sur B .

Ainsi, si on schématise la partie $\mathfrak{I}_b$ de $\mathfrak{I}$ constituée des B^* tels que A est borné sur B ,

$$A^* \subset \text{.....} \subset I^* \subset \text{.....} \subset A_0^* \subset \text{.....} \ .$$

$\mathfrak{I}_b$; ? ; fermés ; non fermés

Remarque. - Si A est une chaîne, alors aucun des éléments B^* de L_{A^*} tels que A est borné sur B n'est fermé dans L_{A^*} .

Enfin, un code borné n'étant évidemment pas une chaîne, le résultat principal de ce chapitre est :

THÉORÈME 4 [3]. - Soit A un code borné sur l'alphabet X . Il y a bijection entre les congruences β de $\mathcal{A}(A^*)$ et les codes B tels que $A^* \subset B^* \subset X^*$, β et B se correspondant dans cette bijection si, et seulement si,

$$\mathcal{A}(B^*) \simeq \mathcal{A}(A^*)/\beta \ .$$

BIBLIOGRAPHIE

[1] GINZBURG (A.). - Algebraic theory of automata. - New York, Academic Press, 1968.

[2] NIVAT (Maurice). - Eléments de la théorie générale des codes, Automata theory, p. 278-294. - New York, Academic Press, 1966.

[3] PERRIN (D.) et PERROT (J.-F.). - Sur les codes préfixes complets finis, C. R. Acad. Sc. Paris, t. 269, 1969, Série A, p. 1116-1118.

[4] PERROT (J.-F.). - On the relationship between finite automata, finite monoïds, and prefix codes, Proceedings of the ACM Symposium on theory of computing [1970. Northampton (Mass.)] (à paraître).

[5] SCHÜTZENBERGER (Marcel Paul). - On a family of submonoïds, Publ. math. Inst. Hung. Acad. Sc., t. 6, 1961, p. 381-391.

[6] SCHÜTZENBERGER (Marcel Paul). - On an application of semigroup methods to some problems of coding, IRE Transactions on Information Theory, IT-2, 1956, p. 47-60.

(Texte reçu le 3 juillet 1970)

Dominique PERRIN
5 rue de Quatrefages
75 - PARIS 05