Séminaire d'Informatique Théorique
Année 1976/77
Séance du 8 mars 1977

Institut de Programmation
Laboratoire associé au CNRS 248
4, place Jussieu
75230 Paris Cedex 05

18

Congruences plus que parfaites et langages algébriques

par Jean Berstel

Institut de Programmation

Introduction.

I. Généralités sur les congruences.

1. Définition d'une congruence de Thue.
2. Exemples.
3. Présentations. Problème des mots.
4. Congruence de Thue et congruence syntactique.

II. Confluence.

1. Notations.
2. Définition.
3. Exemples.
4. Un critère de confluence.
5. Quelques conséquences.

III. Congruences algébriques.

1. Congruences algébriques.
2. Une congruence confluente non algébrique.
3. Congruences basiques.
4. Théorème.
5. Un lemme.
6. Construction de la grammaire.
7. Preuve du lemme.
8. Preuve du théorème.
9. Congruences préparfaites.

IV. Langages algébriques congruentiels.

1. Langages congruentiels.
2. Lien avec le monoïde syntactique.
3. Les langages très simples sont congruentiels.

Références et bibliographie.

Introduction

Que le lecteur se rassure : je n'ai pas l'intention de définir une nouvelle classe de congruences ; à ma connaissance, les congruences plus que parfaites n'existent pas et, peut-être, n'existeront jamais.

Le titre donné à cet exposé a pour but de souligner l'impressionnant foisonnement, dans la littérature, de variétés de congruences sur le monoïde libre. Voici quelques qualificatifs que j'ai relevés dans les publications concernées (une bibliographie se trouve à la fin de ces pages): on y parle de congruences, ou plutôt de systèmes préparfaits, quasiparfaits, parfaits, triviaux, spéciaux, strictement spéciaux, précanoniques, canoniques, unitaires, réduits, basiques, simplifiables (à gauche, à droite), directs, minces, voire algébriques.

Pour cet exposé, nous avons choisi d'extraire de la littérature quelques résultats concernant les congruences algébriques ; ce sont les congruences dont toute classe est un langage algébrique. (Il en est ainsi pour la congruence bien connue qui donne le langage de Dyck). Réciproquement, nous présentons quelques résultats connus sur les langages algébriques congruentiels, c'est-à-dire les langages qui peuvent se représenter comme classe (ou union finie de classes) d'une congruence finiment engendrée.

Il y a plusieurs raisons qui justifient que l'on étudie plus précisément les liens entre classes de congruences et langages algébriques :

1. La donnée d'un ensemble (fini) de relations engendrant une congruence sur un monoïde libre X^* fournit ce que l'on appelle une présentation (finie) du monoïde quotient de X^* par cette congruence ; ceci est un procédé répandu en algèbre pour définir des monoïdes ou des groupes. Il est donc naturel de chercher les liens qui peuvent exister entre une notion mathématique bien connue, et une autre notion classique, à savoir les langages algébriques.

2. Les congruences constituent un procédé de définition de langages formels au même titre que les automates, les équations ou les grammaires. Pour certains langages algébriques, à savoir les langages de Dyck ou de Dyck restreint, on trouve un peu partout dans les manuels la définition comme classe du mot vide d'une certaine congruence. Or on s'aperçoit à l'usage, ou mieux encore en lisant le chapitre consacré à ces langages dans le fascicule de Autebert et Cousineau [1] , que le passage de la congruence à la grammaire n'est pas du tout simple, et que ces procédés de définition ne sont donc pas reliés de manière évidente.

3. L'emploi de la définition par congruence est commode pour établir certaines propriétés de certains langages. En voici un exemple : Lorsque l'on veut prouver que le langage E solution de l'équation $\xi = a\xi b\xi c + d$ est générateur du cône des langages algébriques, on a besoin d'un lemme de réduction du type suivant :

Si $w = u f v \in E$, et si $f, f' \in E$, alors $uf'v \in E$.

La preuve, dans ce cas, n'est pas très difficile, mais en voici une qui est particulièrement simple, en admettant que E est congruentiel, plus précisément que $E = [d]_\theta$ pour une certaine congruence θ : On a alors $u f v \equiv d \pmod{\theta}$, et comme $f \equiv f' \pmod{\theta}$, on a $u f v \equiv u f' v \pmod{\theta}$, donc $u f' v \equiv d \pmod{\theta}$, soit $u f' v \in E$. De plus, on peut effectivement prouver que $E = [d]_\theta$, où θ est la congruence engendrée par la relation adbdc = d ; la forme de cette relation, calquée sur la grammaire, montre très clairement l'existence d'un lien entre congruences et langages algébriques.

Notons que le lemme énoncé ci-dessus devient faux si l'on remplace E par le langage $\text{Mir} = \{w \in X^* \mid w = \tilde{w}\}$ des mots miroirs; ceci est à mettre en rapport avec le fait (et en réalité constitue une preuve du fait) que Mir n'est pas un langage congruentiel.

4. Cet exemple montre que l'étude des congruences algébriques et des langages congruentiels peut augmenter nos connaissances sur les langages algébriques. Et en effet, l'étude des congruences et de leurs systèmes de générateurs est un des outils de l'étude du monoïde syntactique des langages algébriques : l'examen des mots irréductibles relativement à un système engendrant la congruence syntactique est utilisé, dans [8] , pour prouver que les langages algébriques ayant des monoïdes syntactiques d'un type particulier sont nécessairement déterministes (pour un exposé systématique de cette méthode, voir [7]). Réciproquement, un résultat comme : "Tout langage algébrique est image homomorphe d'un langage algébrique congruentiel", associé au fait que bon nombre des générateurs des langages algébriques sont congruentiels, doit éclairer la nature de ces générateurs. Une autre question plausible relie les langages congruentiels aux langages élargis ; ces derniers sont-ils toujours congruentiels ?

Esquissons maintenant ce qui va suivre. Une première partie apporte quelques définitions et exemples, et décrit rapidement les liens avec les présentations et la congruence syntactique. Ensuite, nous essaierons d'expliquer les raisons qu'il y a de considérer plus particulièrement les congruences appelées autrefois quasi-parfaites, et que l'on nomme maintenant confluentes. Elles permettent de décider de certaines questions, et surtout de "latériliser" le calcul de la classe d'un mot, en remplaçant l'équivalence par une relation

relation ressemblant à une dérivation et qui est plus maniable.

Ensuite, nous exposons les conditions suffisantes données par M. Nivat [20] pour qu'une congruence soit algébrique. Il nous a paru utile de donner une preuve complète qui n'a pu être faite, par manque de place, dans l'article cité.

Pour terminer, nous considérons inversement les langages congruentiels. Nous exposons en particulier le théorème de Butzbach [13] qui prouve que les langages engendrés par une grammaire "très simple" sont congruentiels.

Dans ces pages, je ne donnerai pas une description des résultats les plus élaborés. La théorie est en effet difficile, et la place (resp. le temps) manque pour de tels développements. Ainsi, les systèmes minces de Y. Cochet [15] ne seront même pas mentionnés. Je voudrais seulement montrer à l'aide de quelques exemples, la difficulté du sujet, son importance, et peut-être son intérêt. Que les spécialistes m'excusent !

I. Généralités sur les congruences.

1. Définition d'une congruence de Thue. Soit X un alphabet fini. Un système de relations sur X est une partie $\mathcal{J}$ de $X^* \times X^*$. Nous supposerons toujours un tel système fini. La congruence engendrée par $\mathcal{J}$, c'est-à-dire la congruence la plus grossière contenant $\mathcal{J}$, est communément appelée la congruence de Thue engendrée par $\mathcal{J}$, et $\mathcal{J}$ est appelé un système de Thue, ou un système thuéien. C'est en effet Axel Thue qui, en 1914, a le premier étudié ces congruences d'un point de vue combinatoire [26].

Les notations varient. Nous écrirons :

$$f \leftrightarrow_{\mathcal{J}} g \qquad \text{ssi} \qquad f = u\alpha v,\ g = u\beta v, \qquad \text{avec } (\alpha,\beta) \in \mathcal{J} \text{ ou } (\beta,\alpha) \in \mathcal{J},$$

et nous notons comme d'habitude $\overset{*}{\leftrightarrow_{\mathcal{J}}}$ ou $\overset{*}{\leftrightarrow}$ sa fermeture réflexive et transitive qui est précisément égale à la congruence engendrée par $\mathcal{J}$. Cette notation est celle de M. Nivat [20] ou de Y. Cochet [15], [17]. On écrit aussi $\sim$ et $\approx$ pour $\leftrightarrow$ et $\overset{*}{\leftrightarrow}$ (Gross, Lentin 2) ou encore $f \equiv g \pmod{\mathcal{J}}$. Deux mots $f,g \in X^*$ sont congrus si $f \overset{*}{\leftrightarrow} g$; la classe de f se note

$$[f]_{\mathcal{J}} = \{g \mid g \overset{*}{\leftrightarrow}_{\mathcal{J}} f\}$$

2. Exemples.

2.1. Considérons, sur $X = \{a,b\}$, le système $\mathcal{J} = \{(a^3,a^2),\ (aba,a^2),\ (bab,b^2),\ (b^3,b^2)\}$.

On a alors

$$abba \longleftrightarrow ababa \longleftrightarrow aaba \longleftrightarrow a^3 \longleftrightarrow a^2.$$

(Cet exemple se trouve dans Gross-Lentin [2] , page 15).

2.2. (Cet exemple m'a été communiqué par Y. Cochet). Sur $X = \{a,b\}$, soient

$$\mathcal{S} = \{(b^2,1),\ (baba,1),\ (abab,1)\},$$
$$\mathcal{S}' = \{(b^2,1),\ (baba,1)\},$$
$$\mathcal{S}'' = \{(b^2,1),\ (aba,b)\}.$$

On a $\overset{*}{\underset{\mathcal{S}}{\longleftrightarrow}} = \overset{*}{\underset{\mathcal{S}'}{\longleftrightarrow}}$, car

$$abab \overset{}{\underset{\mathcal{S}'}{\longleftrightarrow}} bbabab \overset{}{\underset{\mathcal{S}'}{\longleftrightarrow}} bb \overset{}{\underset{\mathcal{S}'}{\longleftrightarrow}} 1,$$

et on a aussi $\overset{*}{\underset{\mathcal{S}'}{\longleftrightarrow}} = \overset{*}{\underset{\mathcal{S}''}{\longleftrightarrow}}$, car

d'une part : $aba \overset{}{\underset{\mathcal{S}'}{\longleftrightarrow}} bbaba \overset{}{\underset{\mathcal{S}'}{\longleftrightarrow}} b$;

d'autre part : $baba \overset{}{\underset{\mathcal{S}''}{\longleftrightarrow}} bb \overset{}{\underset{\mathcal{S}''}{\longleftrightarrow}} 1$.

Une même congruence peut donc être engendrée par plusieurs systèmes.

2.3. La congruence de Dyck engendrée par $\mathcal{S} = \{(x\bar{x},1),\ (\bar{x}x,1) : x \in X\}$

3. Présentations. Problème des mots.

Comme $\overset{*}{\longleftrightarrow}$ est une congruence, le quotient $X^* / \overset{*}{\longleftrightarrow}$ est un monoïde. Réciproquement, si M est un monoïde, la donnée de X et d'un système $\mathcal{S}$ tel que $M \simeq X^* / \overset{*}{\underset{\mathcal{S}}{\longleftrightarrow}}$ est appelé une présentation de M.Ainsi, les trois systèmes $\mathcal{S}, \mathcal{S}', \mathcal{S}''$ de l'exemple 2.2 sont des présentations du groupe diédral infini ; le système de l'exemple 2.3. est une présentation de groupe libre. Comme me l'a fait remarquer J. F. Perrot, un même monoïde ou groupe peut posséder plusieurs présentations distinctes : ces présentations définissent, sur le monoïde libre, des congruences différentes, mais les monoïdes quotients sont isomorphes. Ainsi, $X^* / \overset{*}{\underset{\mathcal{S}''}{\longleftrightarrow}}$ est un groupe qui est produit semi-direct de $\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$; la congruence engendrée par $\mathcal{S}''' = \{(a^2,1),(b^2,1)\}$ donne, comme quotient, le produit libre $(\mathbb{Z} / 2\mathbb{Z}) * (\mathbb{Z} / 2\mathbb{Z})$. C'est un théorème de théorie des groupes qui assure l'isomorphie de ces deux groupes.

Naturellement il se pose la question de savoir si, dans une présentation, deux mots $f, g \in X^*$ représentent le même élément du monoïde présenté, donc si f et g sont congrus. On appelle ceci le problème des mots : déterminer, pour $f, g \in X^*$, si $f \overset{*}{\longleftrightarrow} g$ ou non. En général, ce problème est indécidable (Gross-Lentin [2] , p. 69). Dans des cas particuliers, on cherche, dans chaque classe, un représentant "canonique". Ceci facilite la solution du problème des mots, et fournit une "cross-section" du monoïde quotient, c'est-

à-dire une injection de celui-ci dans X^*. Ainsi, l'ensemble des mots réduits pour la congruence de Dyck permet-il de considérer le groupe libre comme partie de X^*.

On distingue habituellement deux notions qui donnent des représentants canoniques :

f est minimal si $f \overset{*}{\longleftrightarrow} g \Rightarrow |f| \leq |g|$

f est irréductible si $f \longleftrightarrow g \Rightarrow |f| \leq |g|$

Ainsi, dans l'exemple (2.1), abba et a^2 sont irréductibles, mais seul a^2 est minimal. Notons que la notion de minimalité est indépendante du système qui engendre la congruence, alors que l'irréductibilité en dépend directement. Ainsi, dans l'exemple (2.2) le mot aba est irréductible pour $\mathcal{S}$ et $\mathcal{S}'$, mais ne l'est pas pour $\mathcal{S}''$.

Proposition. L'ensemble $\mathrm{Irr}(\mathcal{S})$ des mots irréductibles est un langage rationnel.

Preuve. On a

$$\mathrm{Irr}(\mathcal{S}) = X^* \setminus X^* V X^*,$$

où $V = \{ \alpha \in X^+ \mid \exists \beta \in X^*, |\alpha| > |\beta|, (\alpha,\beta) \in \mathcal{S} \text{ ou } (\beta,\alpha) \in \mathcal{S} \}$. ∎

Je ne sais pas quand le même résultat est vrai pour l'ensemble des mots minimaux (sauf pour les congruences confluentes, voir plus bas).

4. Congruence de Thue et congruence syntactique.

Considérons la classe $[f]_{\mathcal{S}}$ d'un mot f dans une congruence. Alors $[f]_{\mathcal{S}}$ est un langage saturé pour cette congruence. Si $L \subseteq X^*$ est un langage saturé pour $\overset{*}{\longleftrightarrow}_{\mathcal{S}}$, i.e. union (finie ou infinie) de classes, alors la congruence syntactique $\equiv_L$ de L est comparable, et même plus grossière que $\overset{*}{\longleftrightarrow}_{\mathcal{S}}$. Ainsi, une congruence de Thue saturant un langage L est une approximation de la congruence syntactique de L, ou encore le monoïde syntactique $X^* / \equiv_L$ est image homomorphe de $X^* / \overset{*}{\longleftrightarrow}_{\mathcal{S}}$.

Par exemple, considérons la congruence de Dyck restreinte engendrée par $\mathcal{S} = \{ (x\bar{x}, 1) : x \in X \}$. Le langage de Dyck restreint D'^* est égal à $[1]_{\mathcal{S}}$, le quotient $(X \cup \bar{X})^* / \overset{*}{\longleftrightarrow}_{\mathcal{S}}$ est le "free half-group" ou le "monoïde involutif libre" (d'après la terminologie de M. FLiess [3]), alors que le monoïde syntactique $(X \cup \bar{X})^* / \equiv_{D'^*}$ est le "monoïde polycyclique" de M. Nivat, J.F. Perrot [5].

Cette comparaison avec la congruence syntactique permet de montrer qu'un langage n'est pas congruentiel (i.e union finie de classes d'une congruence). Ainsi, le langage

$$\mathrm{Mir} = \{ w \in X^* \mid w = \tilde{w} \}.$$

n'est pas congruentiel. Le serait-il, Mir serait aussi union finie de classes de son monoïde syntactique. Or celui-ci est X^* tout entier !

Pour d'autres exemples, voir IV.2.

II. Confluence.

Les congruences de Thue sans restriction aucune sont trop générales pour que l'on puisse espérer les mettre en relation de manière significative avec les langages algébriques. Il est naturel par exemple de ne considérer que des congruences pour lesquelles le problème des mots est décidable, puisqu'il en est ainsi pour les langages algébriques. Après quelques tâtonnements, une classe spécifique de congruences a été décrite qui possède d'agréables propriétés et qui est assez maniable. La condition de confluence qu'on impose à ces congruences se retrouve dans d'autres circonstances, comme dans les questions relatives à l'unification.

1. Notations.

Nous introduisons un jeu de notations supplémentaires. Soit $\mathcal{S}$ un système de relations sur X. On pose

$f \longleftrightarrow g$ ssi $f = u\alpha v$, $g = u\beta v$, avec $(\alpha,\beta) \in \mathcal{S}$ ou $(\beta,\alpha) \in \mathcal{S}$;
$f \longrightarrow g$ ssi $f \longleftrightarrow g$ et $|f| > |g|$;
$f \longmapsto g$ ssi $f \longleftrightarrow g$ et $|f| = |g|$;
$f \longleftarrow g$ ssi $g \longrightarrow f$.

On a déjà, bien entendu, introduit la première relation. Comme d'habitude, on note $\xrightarrow{*}$, $\overset{*}{\longmapsto}$ les fermetures de $\longrightarrow$ et $\longmapsto$. Il est important de noter que les relations $\xrightarrow{*}$ et $\overset{*}{\longmapsto}$ dépendent du système $\mathcal{S}$ engendrant la congruence Ainsi, dans l'exemple 2.2, on a $aba \xrightarrow[\mathcal{S}']{} b$, mais $aba \xleftarrow[\mathcal{S}']{} bbaba \xrightarrow[\mathcal{S}']{} b$, donc $aba \not\xrightarrow[\mathcal{S}']{*} b$.
Ces notations sont commodes. Ainsi, l'irréductibilité s'exprime par :

$$f \text{ irréductible} \quad \text{ssi} \quad \{g \mid f \longrightarrow g\} = \emptyset.$$

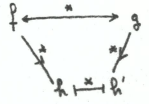
2. Définition.

Un système $\mathcal{S}$ est confluent ssi pour tout $f, g \in X^*$:

$f \overset{*}{\longleftrightarrow} g$ implique : il existe $h, h' \in X^*$ tels que

$$f \xrightarrow{*} h, \quad h \overset{*}{\longmapsto} h', \quad h' \xleftarrow{*} g.$$

Autrement dit, il existe h, h' rendant le diagramme suivant commutatif :



Une autre façon de voir la définition est d'écrire :

$$\overset{*}{\longleftrightarrow} \;=\; \overset{*}{\longrightarrow} \overset{*}{\vdash\!\dashv} \overset{*}{\longleftarrow} \;,$$

ou la juxtaposition des relations correspond au produit de relations binaires.

Note : Un système confluent est appelé quasi-parfait dans la littérature à l'exception de [18] qui utilise le terme "congruence de Church-Rosser", de même que [24] .

Une congruence est confluente s'il existe un système confluent $\mathcal{S}$ qui l'engendre. Ainsi, dans l'exemple 2.2, la congruence est confluente, parce que $\mathcal{S}''$ est confluent (on le verra plus bas), mais ni $\mathcal{S}$ ni $\mathcal{S}'$ ne sont confluents.

Notons une propriété très commode pour vérifier qu'un système n'est pas confluent :

Propriété. Soit $\mathcal{S}$ un système confluent ; si f et f' sont irréductibles et congrus, alors ils ont même longueur.

Preuve : Si $f \overset{*}{\longleftrightarrow} f'$, il existe h, h' tels que

$$f \overset{*}{\longrightarrow} h \overset{*}{\vdash\!\dashv} h' \overset{*}{\longleftarrow} f \;;$$

comme f est irréductible, on a f = h, de même h' = f'. ∎

3. Exemples.

Le système de l'exemple (2.1) n'est pas confluent, car abba et a^2 sont irréductibles, congrus, de longueur différente.

De même, les systèmes $\mathcal{S}$ et $\mathcal{S}'$ de l'exemple (2.2) ne sont pas confluents, car aba et b sont irréductibles et congrus.

3.1. Le système $\{(ab,ba) \;;\; a,b \in X,\ a \neq b\}$ est confluent, car la relation $\longrightarrow$ est vide.

3.2. Les congruences de Dyck et de Dyck restreint sont confluentes.

3.3. Les congruences engendrées par les systèmes

$$\{(adbdc, d)\}\ ,\ \{(abb,b)\}\ ,\ \{(aacacc, ac)\}$$

sont confluentes ; les classes de d, b et ac sont respectivement, on le verra, les langages E, $\mathcal{L}$, M vérifiant

$$E = aEbEc + d \;;\quad \mathcal{L} = a\mathcal{L}\mathcal{L} + b,\quad M = aMMc + ac.$$

3.4. La congruence engendrée par le système

$$\mathcal{S} = \{(abc,ab),\ (bbc,cb)\}$$

est également confluente.

4. Un critère de confluence

Avant de l'énoncer, mettons de l'ordre dans les relations d'un système $\mathcal{S}$. Nous convenons que

(o) $(\alpha,\beta)\in\mathcal{S} \Rightarrow \alpha\neq\beta$;

(1) $(\alpha,\beta)\in\mathcal{S} \Rightarrow |\alpha|\geq|\beta|$;

(2) $(\alpha,\beta)\in\mathcal{S}$ et $|\alpha|=|\beta| \Rightarrow (\beta,\alpha)\in\mathcal{S}$.

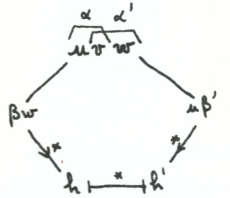
La dernière condition n'est ajoutée que pour faciliter l'écriture du critère.

Critère de confluence.[22] Soit un système de relations sur X ; alors est confluent ssi pour tous (α,β), $(\alpha',\beta')\in\mathcal{S}$, on a :

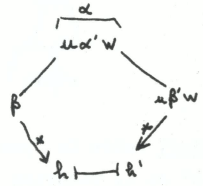
(1) Si $\alpha = uv$, $\alpha' = vw$, pour $u,v,w\in X^+$, alors il existe $h,h'\in X^*$ tel que $\beta w \xrightarrow{*} h$, et $u\beta' \xrightarrow{*} h'$ et $h \overset{*}{\longmapsto} h'$;

(2) Si $\alpha = u\alpha' w$ pour $u,w\in X^*$, il existe h,h' tel que $\beta \xrightarrow{*} h$ et $u\beta' w \xrightarrow{*} h'$, et $h \overset{*}{\longmapsto} h'$.

Ces conditions s'expriment bien par les deux dessins suivants :



et



.

Remarques. 1. Il faut noter que la situation (1) du critère peut se produire de manière non triviale pour $(\alpha,\beta) = (\alpha',\beta')$ lorsque $\alpha = \alpha'$ est une sesquipuissance (voir l'exemple 4.3 ci-dessous).

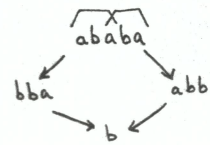
2. Il n'est pas nécessaire d'examiner le cas où $|\alpha| = |\beta|$ et $|\alpha'|=|\beta'|$, mais les trois autres cas ($|\alpha|>|\beta|$ et $|\alpha'|=|\beta'|$, $|\alpha|=|\beta|$ et $|\alpha'|>|\beta'|$, $|\alpha|>|\beta|$ et $|\alpha'|>|\beta'|$) doivent être vérifiés.

Exemples.

4.1. Les systèmes de l'exemple (3.3) sont confluents.

4.2. Le système engendrant la congruence de Dyck (restreinte) est confluent : la situation (1) se produit pour le mot $\bar{x}\,x\,\bar{x}$ (ou $x\,\bar{x}\,x$) et alors on a $\bar{x} \leftarrow \bar{x}\,x\,\bar{x} \longrightarrow \bar{x}$ et $\bar{x} \overset{*}{\longmapsto} \bar{x}$.

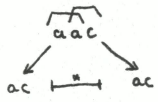
4.3. Considérons le système $\mathcal{S}' = \{(aba,b),(b^2,1)\}$ de l'exemple 2.2. On a le schème



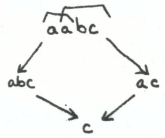
ce qui montre que $\mathcal{S}''$ est confluent.

4.4. (Extrait de Y. Cochet [15], p 55). Considérons, sur $X = \{a,b,c\}$, le système $\{(aa,a), (ac,c), (abc,c)\}$

On a les schémas suivants



et



qui montrent que ce système est confluent.
L'énoncé du critère de confluence se trouve dans de nombreux articles [15, 17, 12, 20]. La preuve de [22] est presque complète : le cas (2) a été oublié, mais cet article est très clair, il contient de nombreuses preuves, et la partie manquante de la preuve du critère peut être facilement comblée.

Remarque. Il est décidable (voir aussi ci-dessous) si un système $\mathcal{S}$ donné est confluent. Mais est-il décidable si une congruence est confluente, i.e. s'il existe un système confluent qui l'engendre ? Y. Cochet (communication personnelle) conjecture que non.

5. Quelques conséquences.

La propriété suivante est valable même si la congruence n'est pas confluente :
Pour tout mot f, les ensembles $\{g \mid f \xrightarrow{*} g\}$ et $\{g \mid f \xmapsto{*} g\}$ sont calculables.
En effet, d'abord ce sont des ensembles finis ; de plus, toute chaîne $f \longrightarrow h_1 \longrightarrow h_2 \longrightarrow \ldots \longrightarrow h_r$ est de longueur $r \leq |f|$ puisque les longueurs des mots décroissent ; enfin, toute chaine $f \longmapsto h_1 \longmapsto \ldots \longmapsto h_r$ telle que $i \neq j \Rightarrow h_i \neq h_j$ est également finie, de longueur $r \leq \mathrm{Card}\, X!$.
De même l'ensemble $\{g \mid f (\rightarrow \cup \longmapsto)^* g\}$ est calculable.

Proposition.- Dans une congruence confluente, le problème des mots est décidable.
En effet, si $f \overset{*}{\longleftrightarrow} g$, il existe h,h' tels que $f \xrightarrow{*} h \xmapsto{*} h' \xleftarrow{*} g$, et l'existence d'un tel couple de mots est décidable d'après les remarques précédentes. ■
Une autre propriété agréable est :
Propriété.- Si $\mathcal{S}$ est confluent, il y a égalité entre mots minimaux et mots irréductibles.

Avec les notations introduites au début de cette section, on a :

f irréductible ssi $\{g \mid f \longrightarrow g\} = \emptyset$;

f minimal ssi $(g \overset{*}{\leftrightarrow} f) \Rightarrow (g \overset{*}{\rightarrow\!\!\!\!\!\!\mapsto} f)$.

On sait déjà que tout mot minimal est irréductible ; réciproquement, si f est irréductible et si $g \overset{*}{\leftrightarrow} f$, alors il existe h,h' tels que

$$f \overset{*}{\longrightarrow} h \overset{*}{\longmapsto} h' \overset{*}{\longleftarrow} g,$$

et alors f = h. ■

III. Congruences algébriques.

1. Congruences algébriques. Une congruence est algébrique si toute classe de cette congruence est un langage algébrique. Notre propos est de donner les conditions suffisantes développées par M. Nivat pour qu'une congruence soit algébrique. Nous ne nous intéressons qu'aux congruences confluentes, car elles ont, de ce point de vue, une propriété remarquable. Soit $\mathcal{S}$ un système confluent, et posons

$$\langle f \rangle_{\mathcal{S}} = \{g \mid g \overset{*}{\longrightarrow} f\}.$$

Propriété.-La congruence engendrée par $\mathcal{S}$ est algébrique si $\langle f \rangle_{\mathcal{S}}$ est un langage algébrique pour tout $f \in X^*$, et ceci est le cas si $\langle f \rangle_{\mathcal{S}}$ est un langage algébrique pour tout mot irréductible $f \in X^*$.

Preuve. Soit $D(f) = \{g \mid f \overset{*}{\longrightarrow\!\!\!\!\!\!\mapsto} g\}$, et $\mathrm{Irr}(f) = D(f) \cap \mathrm{Irr}(\mathcal{S})$. Alors la propriété de confluence se traduit par

$$[f]_{\mathcal{S}} = \bigcup_{g \in D(f)} \langle g \rangle_{\mathcal{S}} = \bigcup_{g \in \mathrm{Irr}(f)} \langle g \rangle_{\mathcal{S}}.$$

Comme D(f) et Irr(f) sont des ensembles finis, l'algébricité de $[f]_{\mathcal{S}}$ découle de l'algébricité des langages $\langle g \rangle$ ■

Je pense que la réciproque de cette propriété est également vraie.

Cette remarque nous procure l'avantage suivant : On peut désormais se restreindre, dans l'examen de l'algébricité, à la relation "latéralisée" $\overset{*}{\longrightarrow}$, c'est-à-dire considérer $\mathcal{S}$ comme un système semi-thueien, au sens de Gross-Lentin [2] p. 34. De plus, ce système semi-thueien a la propriété "extensive" que si $\alpha \longrightarrow \beta$, alors $|\alpha| > |\beta|$. On peut donc éliminer, de $\mathcal{S}$, toutes les "règles" (α,β) avec $|\alpha| = |\beta|$. Néanmoins, l'essentiel reste encore à faire.

2. Une congruence confluente non algébrique.

Considérons le système de l'exemple (3.4), que l'on trouve, sous une forme voisine, dans M. Nivat [20] et Y. Cochet [15] :

$$\mathcal{Y} = \{(abc,\ ab),\ (bbc,\ cb)\}.$$

On a :

$$\begin{array}{lll} cb & \longleftarrow & b^2c\,, \\ cb^2 & \longleftarrow & b^2cb \longleftarrow b^4c\,, \\ \ldots\quad cb^n & \overset{+}{\longleftarrow} & b^{2n}c \qquad (n \geqslant 1), \end{array}$$

d'où l'on déduit :

$$abb^{2^n}c^n \longleftarrow abcb^{2^n}c^n \overset{*}{\longleftarrow} abb^{2^{n+1}}c^{n+1}.$$

On en tire, sans trop de peine :

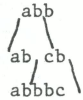
$$\langle ab^2\rangle \cap a^*b^*c^* = \{ab^{2^n+1}c^n \mid n \geqslant 0\}.$$

Le mot ab^2 est irréductible, et la relation $\longmapsto$ est vide, donc

$$D(ab^2) = \{ab^2\}\ ;\ \text{donc}$$
$$[ab^2] = \langle ab^2\rangle,$$

ce qui montre que la congruence n'est pas algébrique.

En examinant la chaîne abb $\longleftarrow$ abcb $\longleftarrow$ abbbc, on voit bien le phénomène qui est intervenu :



Il y a <u>chevauchement</u> entre la "partie longue" de la relation (abc,ab) et la "partie courte" de la relation (bbc,cb). Ce chevauchement permet, comme dans certaines grammaires context-sensitives, un "transfert" qui fait perdre le caractère algébrique. Il est remarquable que l'interdiction de tels chevauchements suffit, pour l'essentiel, à assurer l'algébricité.

3. <u>Congruences basiques</u>.

Soit $\mathcal{Y}$ un système de relations sur X. Nous supposons, comme plus haut les relations de $\mathcal{Y}$ telles que $(\alpha,\beta) \in \mathcal{Y}$ implique $|\alpha| \geqslant |\beta|$. D'après ce qui précède, on peut même supposer $|\alpha| \neq |\beta|$. Posons alors

$$A = \{\alpha \mid \exists \beta :\ (\alpha,\beta) \in \mathcal{Y}\},$$
$$B = \{\beta \mid \exists \alpha :\ (\alpha,\beta) \in \mathcal{Y}\}.$$

Donc A et B sont respectivement l'ensemble des premières resp. deuxièmes coordonnées des relations de $\mathcal{Y}$.

<u>Définition</u>. Le système $\mathcal{Y}$ est <u>basique</u> si, pour tout $\alpha \in A$, $\beta \in B$, on a :

(i) $\alpha = uv$, $\beta = vw \Rightarrow v = 1$ ou $w = 1$;

(ii) $\alpha = vu$, $\beta = wv \Rightarrow v = 1$ ou $w = 1$;

(iii) $\beta = u\alpha w \Rightarrow u = w = 1$.

Les deux premières conditions expriment que les deux mots α et β ne chevauchent pas, la troisième que α n'est pas facteur propre de β .

4. Théorème.

On a le résultat suivant:

Théorème (Nivat [20]).- Si $\mathcal{S}$ est basique, alors $<f>_{\mathcal{S}}$ est un langage algébrique pour tout mot f.

Joint à la proposition du paragraphe 1, on obtient

Corollaire. Si $\mathcal{S}$ est confluent et basique, alors $[f]_{\mathcal{S}}$ est un langage algébrique pour tout f.

Autrement dit : $\mathcal{S}$ confluent et basique $\Rightarrow$ $\mathcal{S}$ algébrique.

Les conditions de confluence et de "basicité" sont indépendantes ; chacune d'elles assure une partie du résultat, et c'est la conjonction des deux qui fournit la conclusion cherchée. Donnons des exemples :

4.1. Si $B \subset \{1\} \cup X$, le système est automatiquement basique. Il en est ainsi pour les congruences de Dyck, ou pour les systèmes

$\{(adbdc, d)\}$, $\{(abb, b)\}$

Un autre cas particulier, à savoir celui d'un système confluent $\mathcal{S}$ avec $B = \{1\}$ (système appelé "trivial" ou "unitaire") a été étudié de manière approfondie : Les classes ont toutes les propriétés des langages de Dyck ; ce sont des langages algébriques non ambigus dont les complémentaires sont aussi des langages algébriques (voir [12], [15]).

4.2. Le système $\{(aacacc, ac)\}$ est basique, donc $[ac]$ est un langage algébrique. (Résultat démontré directement par M. P. Schützenberger [25]

Voici quelques autres systèmes basiques (et confluents) :

4.3. $\mathcal{S} = \{(dabad, ab), (dbabd, ba)\}$.

4.4. $\mathcal{S} = \{(ax, x), (dbxd, bx)\}$.

4.5. $\mathcal{S} = \{(ab, 1), (ac, a)\}$.

5. Un lemme.

La preuve du théorème - que nous donnons plus bas - passe par la construction d'une grammaire et la vérification qu'elle engendre bien le langage cherché. La grammaire exhibée permet de constater, dans les exemples, que les classes correspondent bien aux langages que l'on cherche à décrire par des congruences.

Le lemme que voici est à la base de la construction :

Lemme.- Si $\mathcal{J}$ est basique, alors on a, avec les notations précédentes,

$$\langle f \rangle = \bigcup u_0 \langle \beta_1 \rangle u_1 \langle \beta_2 \rangle \dots \langle \beta_r \rangle u_r,$$

où l'union est sur toutes les factorisations $f = u_0\beta_1 u_1 \beta_2 \dots \beta_r u_r$ avec

$r \geq 0$, $u_i \in X^*$, $\beta_i \in B$, telles que $\beta_i u_i \beta_{i+1} \neq 1$ $(i = 1, .., r-1)$.

Ce lemme est l'analogue du "lemme fondamental" pour les grammaires algébriques (voir [1]), et c'est sa preuve qui utilise le caractère basique de $\mathcal{J}$. Commentons ce lemme :

. La condition $\beta_i u_i \beta_{i+1} \neq 1$ est technique ; elle est imposée pour éviter des factorisations de longueur arbitrairement grande lorsque $1 \in B$.

. Si les langages $\langle \beta \rangle$ pour $\beta \in B$ sont algébriques, il en est de même pour $\langle f \rangle$. Il suffit donc de prouver l'algébricité des langages $\langle \beta \rangle$.

. Si $f \in B$, le lemme ne dit rien, car alors $\langle f \rangle$ figure comme terme de l'union dans le membre droit de l'égalité.

Considérons deux exemples. Pour le système 4.4, on a

$$\langle dbxd \rangle = dbxd \cup d\langle bx \rangle d \cup db\langle x \rangle d$$

Pour la relation (abb, b), on a

$$\langle abb \rangle = abb \cup ab\langle b \rangle \cup a\langle b \rangle b \quad a\langle b \rangle\langle b \rangle$$

Dans ces unions, certains termes sont inutiles, et l'égalité intéressante est : $\langle abb \rangle = a\langle b \rangle\langle b \rangle$. Pour le premier exemple, on peut écrire $\langle dbxd \rangle = d\langle bx \rangle d$ car $db\langle x \rangle d \subseteq d\langle bx \rangle d$, mais l'inclusion inverse est fausse puisque $ddbxdd \in d\langle bx \rangle d \setminus db\langle x \rangle d$.

Ces constatations conduisent au raffinement suivant. Appelons B-factorisation de f une factorisation de f

$$\pi = (u_0, \beta_1, \dots, \beta_r, u_r)$$

vérifiant les conditions du lemme, et appelons π maximale si

. $u_i \notin X^* B X^*$ si $1 \notin B$;

. $u_i \in 1 \cup X \setminus B$ si $1 \in B$.

Notons $\Pi(f)$ l'ensemble des factorisations maximales de f.

Lemme.- On a, pour $f \in X^*$,

$$\langle f \rangle = \bigcup \{ u_0\langle \beta_1 \rangle \dots \langle \beta_r \rangle u_r \mid (u_0, \beta_1, \dots, \beta_r, u_r) \in \Pi(f) \};$$

pour tout $\beta \in B$,

$$\langle \beta \rangle \cdot \beta \cup \bigcup \{ u_0\langle \beta_1 \rangle \dots \langle \beta_r \rangle u_r \mid (u_0, \beta_1, \dots, \beta_r, u_r) \in \Pi(\beta) \setminus (1, \beta, 1) \}$$

$$\cup \bigcup_{(\alpha,\beta) \in \mathcal{J}} \{ u_0\langle \beta_1 \rangle \dots \langle \beta_r \rangle u_r \mid (u_0, \beta_1, \dots, \beta_r, u_r) \in \Pi(\alpha) \}.$$

6. Construction de la grammaire.

Elle est maintenant évidente. On introduit un nonterminal ξ_β pour chaque $\beta \in B$, et on recopie le dernier lemme :

$$\xi_\beta = \beta + \sum \{ u_0 \xi_{\beta_1} \cdots \xi_{\beta_r} u_r \mid (u_0, \beta_1, \ldots, \beta_r, u_r) \in \Pi(\beta) \setminus (1, \beta, 1) \}$$

$$+ \sum_{(\alpha,\beta) \in \mathcal{S}} \sum \{ u_0 \xi_{\beta_1} \cdots \xi_{\beta_r} u_r \mid (u_0, \beta_1, \ldots, \beta_r, u_r) \in \Pi(\alpha) \}.$$

Exemples.

6.1.- Reprenons la relation (abb,b) ; $\Pi(b) = \{(1,b,1)\}$, $\Pi(abb) = \{(a, b, 1, b, 1)\}$, d'où $\xi_b = b + a \xi_b \xi_b$.

6.2.- Pour la congruence engendrée par (adbdc, d) on a $\Pi(adbdc) = \{(a, d, b, d, c)\}$, d'où la grammaire

$$\xi_d = d + a \xi_d b \xi_d c .$$

6.3.- Pour (aacacc, ac), on a $\xi_{ac} = ac + a \xi_{ac} \xi_{ac} c$.

6.4.- Pour le système $\{(ax, x), (dbxd, bx)\}$, on a

$$\xi_x = x + a \xi_x ,$$

et

$$\xi_{bx} = bx + b \xi_x + d \xi_{bx} d + db \xi_x d .$$

6.5.- Pour le système $\{(dabad, ab), (dbabd, ba)\}$, on a

$$\xi_{ab} = ab + d \xi_{ab} ad + da \xi_{ba} d$$

$$\xi_{ba} = ba + d \xi_{ba} bd + db \xi_{ab} d$$

6.6. Pour le système $\{(x\bar{x}, 1)\}$ engendrant la congruence de Dyck restreinte, on a $\Pi(x\bar{x}) = \{(1, 1, x, 1, \bar{x}, 1, 1)\}$, soit

$$\xi_1 = 1 + \xi_1 x \xi_1 \bar{x} \xi_1 .$$

6.7. Considérons enfin le système $\{(ab, 1), (ac, a)\}$. On a

$$\Pi(a) = \{(1, \underline{1}, 1, \underline{a}, 1, \underline{1}, 1)\} , \quad \Pi(ac) = \{(1, \underline{1}, 1, \underline{a}, 1, \underline{1}, c, \underline{1}, 1)\}$$

d'où

$$\xi_1 = 1 + \xi_1 \xi_a \xi_1 b \xi_1$$

$$\xi_a = a + \xi_1 \xi_a \xi_1 + \xi_1 \xi_a \xi_1 c \xi_1 .$$

Un raffinement supplémentaire, au dela des B-factorisations maximales, peut certainement être trouvé qui permet d'éviter l'ambiguïté non nécessaire dans les grammaires des exemples 6.4. et 6.7.

7. Preuve du lemme.

Nous commençons par un lemme préliminaire qui procure la reformulation nécessaire des conditions de la définition des systèmes basiques.

Lemme préliminaire.- Soient $\mathcal{S}$, A, B comme ci-dessus, et soit $f \in X^*$ un mot possédant les deux factorisations

$$f = u_0 \beta_1 u_1 \cdots u_{r-1} \beta_r u_r = u \alpha v,$$

avec $r \geq 0$, $u_0, \ldots, u_r, u, v \in X^*$, $\beta_1, \ldots, \beta_r \in B$, $\alpha \in A$. Alors une et une seule des deux conditions suivantes est réalisée :

(i) il existe deux entiers i, j ($0 \leq i < j \leq r$), et deux factorisations

$$u_i = u'_i u''_i, \quad u_j = u'_j u''_j,$$

telles que

$$u = u_0 \beta_1 \cdots \beta_i u'_i, \quad \alpha = u''_i \beta_{i+1} \cdots \beta_j u'_j, \quad v = u''_j$$

de plus, on peut supposer $\beta_i u'_i \neq 1$ si $i \geq 1$ et $u''_j \beta_{j+1} \neq 1$ si $j < r$;

(ii) il existe un entier i ($0 \leq i \leq r$), et une factorisation

$$u_i = u'_i \alpha u''_i,$$

et alors $u = u_0 \beta_1 \cdots \beta_i u'_i$, $v = u''_i \beta_{i+1} \cdots \beta_r u_r$;

de plus, on peut supposer $\beta_i u'_i \neq 1$ si $i \geq 1$ et $u''_i \beta_{i+1} \neq 1$ si $i < r$.

Preuve.- Les conditions (i) et (ii) s'excluent mutuellement. Si aucune de ces deux situations n'était réalisée, alors ou bien α serait facteur propre d'un des mots $\beta_1, \ldots, \beta_r$, ou bien, il existerait un indice i, et des mots β'_i, β''_i, h tels que

$\beta_i = \beta'_i \beta''_i$ et ($\alpha h = \beta''_i u_i \cdots \beta_r u_r$ ou $h\alpha = u_0 \cdots u_{i-1} \beta'_i$),

ce qui signifierait que α et β_i chevauchent. Si enfin, dans (i) $\beta_i u'_i = 1$ par exemple, on peut trouver une factorisation de u_{i-1} ayant les mêmes propriétés que la factorisation de u_i, alors que $\beta_i u'_i = 1$ dans (ii) permet de trouver une factorisation satisfaisante (i) sur u_{i-1} et u_i. ∎

Le lemme suivant est plus précis que le lemme du paragraphe 5. Son énoncé permet des preuves par récurrence.

LEMME. Soient $\mathcal{S}$ un système basique sur X, et A, B comme ci-dessus. Pour tous mots $f, g \in X^*$, et tout entier $k \geq 0$, on a

$$g \xrightarrow{k} f \tag{7.1}$$

si, et seulement si la condition suivante est satisfaite : il existe un entier

$r \geqslant 0$, une factorisation

$$(7.2) \qquad f = u_o \beta_1 u_1 \beta_2 \cdots \beta_r u_r \quad (u_i \in X^*, \ \beta_i \in B),$$

des mots $h_1, \ldots, h_r$ et une factorisation

$$g = u_o h_1 u_1 h_2 \cdots h_r u_r,$$

et des entiers $k_1, k_2, \ldots, k_r \geqslant 0$ tels que

$$(7.3) \qquad h_i \xrightarrow{k_i} \beta_i \ (1 \leqslant i \leqslant r) \text{ et } k_1 + k_2 + \ldots + k_r = k.$$

De plus, il existe une factorisation de f telle que $\beta_i u_i \beta_{i+1} \neq 1$ pour $i = 1, \ldots, r-1$.

L'intérêt du lemme réside dans le fait que toute réduction (7.1) peut être décomposée en des réductions qui ont pour "base" des mots de B. La précision sur les factorisations (7.2) apportée par la dernière assertion est technique, mais d'importance : il s'agit d'éviter des factorisations arbitrairement longues par répétition d'un facteur $\beta u = 1$.

Preuve. La condition est évidemment suffisante, parce que la relation est régulière.

Nous prouvons qu'elle est nécessaire par récurrence sur l'entier k tel que $g \xrightarrow{k} f$. Si $k = 0$, il n'y a rien à démontrer. Supposons donc $k > 0$. Il existe un mot f' tel que

$$g \xrightarrow{k-1} f' \longrightarrow f.$$

Par conséquent, il existe des factorisations

$$(7.4) \qquad f' = u_o \beta_1 u_1 \beta_2 \cdots \beta_r u_r \quad (u_i \in X^*, \ \beta_i \in B),$$

$$g = u_o \xrightarrow{k_i} h_1 u_1 h_2 \cdots h_r u_r,$$

telles que $h_i \xrightarrow{k_i} \beta_i$, avec $k_1 + k_2 + \ldots + k_r = k - 1$. D'autre part, il existe $(\alpha, \beta) \in \mathcal{S}$, et $u, v \in X^*$ tels que

$$(7.5) \qquad f' = u \alpha v, \quad f = u \beta v.$$

Nous comparons maintenant les deux factorisations (7.4) et (7.5) de f' à l'aide du lemme préliminaire. Ou bien, on a, pour $0 \leqslant i < j \leqslant r$,

$$u = u_o \beta_1 \cdots \beta_i u'_i, \quad \alpha = u''_i \beta_{i+1} \cdots \beta_j u'_j, \quad v = u''_j \beta_{j+1} \cdots \beta_r u_r,$$

et en posant

$$h = u''_i h_{i+1} \cdots h_j u'_j,$$

on a $h \xrightarrow{k'} \beta$, avec $k' = k_{i+1} + \ldots k_j + 1$, ce qui donne

$$g = u_o h_1 \cdots h_i u'_i \, h \, u''_j h_{j+1} \cdots h_r u_r,$$

$$f = u_o\ \beta_1 \cdots\ \beta_i\ u'_i\ \beta\ u''_j\ \beta_{j+1} \cdots\ \beta_r\ u_r,$$

et démontre le lemme dans ce cas ;

ou bien, on a

$$f = u_o\ \beta_1 \cdots \beta_i\ u'_i\ \beta\ u''_i\ \beta_{i+1} \cdots\ \beta_r\ u_r,$$

$$g = u_o\ h_1 \cdots\ h_i\ u'_i\ \alpha\ u''_i\ h_{i+1} \cdots\ h_r\ u_r,$$

ce qui prouve le lemme dans le deuxième cas.

Si enfin il existe un entier i ($1 \leq i \leq r$) tel que $\beta_i u_i\ \beta_{i+1} = 1$, alors on a, avec $h = h_i\ u_i h_{i+1}$, également

$$h \xrightarrow{k_i + k_{i+1}} 1$$

ce qui donne une factorisation (7.2) (7.3) de f et g contenant moins de facteurs que la factorisation initiale. En itérant ce procédé, on obtient une factorisation de la forme annoncée. ∎

8. Preuve du théorème. Nous prouvons le théorème en deux étapes. Pour commencer, nous associons une grammaire analogue à celle du paragraphe 6 à tout système basique ; analogue parce que nous considérons l'ensemble $\Delta(f)$ de toutes les B-factorisations, et non seulement les B-factorisations maximales. Lorsque le théorème est prouvé pour cette grammaire, il est immédiat que l'on peut se borner aux B-factorisations maximales.

Considérons la grammaire $G = \langle V, X, \mathcal{P} \rangle$ dont le vocabulaire nonterminal est $V = \{ \xi_\beta : \beta \in B \}$ et ayant pour règles

$$\xi_\beta = \beta + \sum \{ u_0 \xi_{\beta_1 u_1} \cdots \xi_{\beta_r u_r} \mid (u_0, \beta_1, \ldots, \beta_r, u_r) \in \Delta(\beta) \setminus (1, \beta, 1) \} +$$

$$+ \sum_{\alpha : (\alpha, \beta) \in \mathcal{S}} \sum \{ u_0 \xi_{\beta_1} \cdots \xi_{\beta_r u_r} \mid (u_0, \beta_1, \ldots, \beta_r, u_r) \in \Delta(\alpha) \}.$$

Nous allons prouver que $L_G(\xi_\beta) = \langle \beta \rangle_{\mathcal{S}}$ pour tout $\xi_\beta \in V$.

(i) $L_G(\xi_\beta) \subseteq \langle \beta \rangle_{\mathcal{S}}$. Nous procédons, simultanément sur tous les $\beta \in B$, par récurrence sur l'entier k tel que, pour $f \in L_G(\xi_\beta)$, on ait

$$\xi_\beta \overset{k}{\underset{G}{\vdash}} f.$$

Si $k = 0$, il n'y a rien à prouver ; si $k = 1$, alors $f = \alpha$ ou $f = \beta$, avec $(\alpha, \beta) \in \mathcal{S}$ et on a $\alpha, \beta \in \langle \beta \rangle$. Supposons donc $k > 1$, et soit g tel que

$$\xi_\beta \overset{}{\underset{G}{\vdash}} g \overset{k-1}{\underset{G}{\vdash}} f$$

Il existe des factorisations

$$g = u_o\ \xi_{\beta_1} \quad \cdots \quad \xi_{\beta_r u_r},$$
$$f = u_o\ h_1 \quad \cdots \quad h_r\ u_r,$$

telles que $\xi_{\beta_i} \overset{k_j}{\underset{G}{\vdash}} h_j$, $k_1 + \ldots + k_r = k-1$. Par hypothèse de récurrence, on a $h_j \in \langle\beta_j\rangle$ pour $j = 1, \ldots, r$, et par le lemme

$$f \xrightarrow[\mathcal{S}]{*} u_o \beta_1 \cdots \beta_r u_r.$$

D'autre part, comme $\xi_\beta \to g$ est une règle de la grammaire G, on a $(u_o, \beta_1, \ldots, \beta_r, u_r) \in \Delta(\alpha) \cup \Delta(\beta) \setminus (1, \beta 1)$ d'où

$$u_o \beta_1 \cdots \beta_r u_r \xrightarrow{\mathcal{S}} \beta,$$

donc $f \xrightarrow[\mathcal{S}]{*} \beta$ et $f \in \langle\beta\rangle_{\mathcal{S}}$ Ceci prouve l'inclusion.

(ii) $\langle\beta\rangle_{\mathcal{S}} \subseteq L_G(\xi_\beta)$. Soit $f \in \langle\beta\rangle_{\mathcal{S}}$. Nous raisonnons par récurrence sur l'entier k tel que $f \xrightarrow[\mathcal{S}]{*} \beta$.

Si $k = 0$, alors $f = \beta$. La règle $\xi_\beta \to \beta$ figure dans G, donc $f \in L_G(\xi_\beta)$. Si $k = 1$, alors ou bien $f = \alpha$, avec $(\alpha, \beta) \in \mathcal{S}$, et $(\xi_\beta \to \alpha) \in P$, ou bien il existe une B-factorisation (u_o, β_1, u_1) de β telle que $f = u_o \alpha_1 u_1$, avec $(\alpha_1, \beta_1) \in \mathcal{S}$. Mais alors on a $\xi_\beta \vdash_G u_o \xi_{\beta_1} u_1 \vdash_G u_o \alpha_1 u_1$. Par conséquent, $f \in L_G(\beta)$ dans ces deux cas.

Supposons donc $k > 1$. Il existe un mot f' tel que

$$f \xrightarrow[\mathcal{S}]{k-1} f' \xrightarrow{\mathcal{S}} \beta.$$

Par le lemme, il existe deux factorisations

(8.1) $\quad f' = u_o \beta_1 \ldots \beta_r u_r,$

$$f = u_o h_1 \ldots h_r u_r,$$

telles que $h_i \xrightarrow[\mathcal{S}]{k_i} \beta_i$ pour $i = 1, \ldots, r$, avec $k_1 + \ldots + k_r = k-1$. Par hypothèse de récurrence, on a $\xi_{\beta_i} \vdash_G^* h_i$ pour $i = 1, \ldots, r$, donc, en posant $w = u_o \xi_{\beta_1} \ldots \xi_{\beta_r} u_r$, il vient

(8.2) $\quad w \vdash_G^* f.$

Par ailleurs, on a $f' \xrightarrow{\mathcal{S}} \beta$, et $(u_o, \beta_1, \ldots, \beta_r, u_r)$ est une B-factorisation de f'. Si $f' = \alpha$, avec $(\alpha, \beta) \in \mathcal{S}$, alors la règle

$\xi_\beta \longrightarrow u_o \xi_{\beta_1} \ldots \xi_{\beta_r} u_r$ figure dans G, et on a donc $\xi_\beta \vdash_G^* f$, donc $f \in L_G(\xi_\beta)$. Sinon, il existe une B-factorisation (u, β', v) de β, et $(\alpha', \beta') \in \mathcal{S}$ tels que

(8.3) $\quad f' = u \alpha' v.$

En vertu du lemme préliminaire, les deux factorisations (8.1) et (8.3) de f' impliquent, ou bien l'existence de deux entiers i,j $(0 \leq i < j \leq r)$ et de factorisations $u_i = u'_i u''_i$, $u_j = u'_j u''_j$ telles que

$$\pi_1 = (u_o, \beta_1, \ldots, \beta_i, u'_i, \beta', u''_j, \beta_{j+1}, \ldots, \beta_r, u_r)$$

est une B-factorisation de β, ou bien l'existence d'un entier i et d'une

factorisation $u_i = u'_i \alpha u''_i$ telle que

$$\pi_2 = (u_0, \beta_1, \ldots, \beta_i, u'_i, \beta', u''_i, \beta_{i+1}, \ldots, \beta_r, u_r)$$ est une B-factorisation de β.

Dans le premier cas, on a $\alpha' = u''_i \beta_{i+1} \cdots \beta_j u'_j$, donc

$$\xi_{\beta'} \vdash_G u''_i \xi_{\beta_{i+1}} \cdots \xi_{\beta_j} u'_j$$

$$\xi_\beta \vdash_G u_0 \xi_{\beta_1} \cdots \xi_{\beta_i} u'_i \xi_{\beta'} u''_j \xi_{\beta_{j+1}} \cdots \xi_{\beta_r} u_r$$

et par conséquent

$$\xi_\beta \vdash_G^* w.$$

Dans le deuxième cas, on a

$$\xi_{\beta'} \vdash_G \alpha'$$

$$\xi_\beta \vdash_G u_0 \xi_{\beta_1} \cdots \xi_{\beta_i} u'_i \xi_{\beta'} u''_i \xi_{\beta_{i+1}} \cdots \xi_{\beta_r} u_r$$

et par conséquent également

$$\xi_\beta \vdash w.$$

Joint à (8.2), ceci donne $\xi_\beta \vdash_G^* f$; soit $f \in L_G(\xi_\beta)$.

Considérons enfin la grammaire G' obtenue à partir de G en nous bornons aux B-factorisations maximales. Comme on le voit immédiatement, les langages $L_G(\xi_\beta)$ ($\beta \in B$) sont aussi solutions de cette grammaire G', donc $L_G(\xi_\beta) \subseteq L_{G'}(\xi_\beta)$ pour tout $\beta \in B$. Réciproquement, les langages $L_{G'}(\xi_\beta)$ sont aussi solutions de la grammaire G. D'où l'égalité ■

9. Congruences préparfaites.

Y. Cochet [15] a étudié des congruences vérifiant des conditions moins fortes que la confluence. Soit $\mathcal{S}$ un système de relations, et posons

$$\mapsto = \rightarrow \cup \vdash ; \quad \dashv = \leftarrow \cup \vdash .$$

$\mathcal{S}$ est <u>préparfait</u> si $\overset{*}{\leftrightarrow} = \mapsto^* \dashv^*$. De cette écriture, il résulte immédiatement que la confluence entraîne la préperfection. On s'aperçoit que tous les raisonnement antérieurs restent vrai si l'on se place dans le cadre des congruences préparfaites. Mais l'on ne sait pas, à ce jour, s'il est décidable qu'un système est préparfait. C'est la raison principale par laquelle on a abandonné leur étude au profit des congruences confluentes.

IV. Langages algébriques congruentiels.

1. Langages congruentiels. Un langage $L \subseteq X^*$ est congruentiel s'il existe une congruence engendrée par un système (fini) $\mathcal{S}$ telle que L soit union finie de classes de cette congruence. Nous nous intéressons ici aux langages algébriques qui sont congruentiels. Bien évidemment, tout langage rationnel est congruentiel puisque sa congruence syntactique est finiment engendrée et d'index fini. Il existe un résultat plus précis. Appelons confluent un langage qui est union finie de classes d'une congruence confluente. Alors on a :

Proposition (Y. Cochet [17]). Tout langage rationnel est un langage confluent.

Y. Cochet [17] donne des exemples montrant que les langages confluents ne sont fermés pour aucune des opérations habituelles.

2. Lien avec le monoïde syntactique.

Considérons un langage $L \subseteq X^*$ congruentiel (algébrique ou non). Comme il est union finie de classes, il a nécessairement une image finie dans son monoïde syntactique. Réciproquement, si le monoïde syntactique $\mathcal{M}(L)$ d'un langage $L \subseteq X^*$ possède une présentation finie et si l'image de L dans $\mathcal{M}(L)$ est finie, alors L est congruentiel pour la congruence syntactique. Ainsi, la considération du monoïde syntactique peut apporter des informations sur le caractère congruentiel du langage, et en particulier permettre de prouver qu'il n'est pas congruentiel. En voici deux exemples.

2.1. Un langage (algébrique ou non) L dont le monoïde syntactique est isomorphe à $\mathbb{Z} \times \mathbb{N}$ (ou à $\mathbb{N}^k$, $k \geqslant 1$) n'est pas congruentiel.

En effet, l'image L' de L dans son monoïde syntactique $\mathcal{M}(L)$ rencontre tout idéal non nul (sinon $\mathcal{M}(L)$ ne serait pas syntactique pour L).

Or $\mathbb{Z} \times \mathbb{N}$ (et $\mathbb{N}^k$) contient une chaîne infinie décroissante d'idéaux, donc L' est nécessairement infini ! Le langage algébrique

$L \subset \{x, y, z\}^*$ suivant a pour monoïde syntactique $\mathbb{Z} \times \mathbb{N}$ [9] :

$$L = \{w \mid |w|_z \text{ pair et } |w|_z = |w|_x - |w|_y\} \cup \{w \mid |w|_z \text{ impair et } |w|_z = |w|_y - |w|_x\}$$

2.2. Alors que la propriété précédente est vraie pour tout langage, la preuve de la proposition suivante repose essentiellement sur le caractère algébrique du langage considéré.

Proposition [6, prop. 2]. Soit L un langage algébrique dont le monoïde syntactique est isomorphe au produit direct $G_1 \times G_2$ de deux groupes contenant chacun un élément d'ordre infini ; alors l'image de L dans son monoïde syntactique est infinie.

Il en résulte donc que L n'est pas congruentiel. C'est le cas du langage $L = \{ w \in \{x, y, z, t\}^* \mid |w|_x = |w|_y \text{ et } |w|_z = |w|_t \}$ dont le monoïde syntactique est $\mathbb{Z}^2$.

3. Les langages très simples sont congruentiels.

Donnons d'abord la définition des langages très simples. Une grammaire $G = (V, X, \mathcal{P})$ est très simple si elle vérifie les deux conditions suivantes

(1) pour toute règle $(\xi \longrightarrow \alpha) \in \mathcal{P}$, on a $\alpha \in XV^*$ (elle est sous forme normale de Greibach)

(2) pour tout $x \in X$, il est exactement une règle $(\xi \longrightarrow \alpha) \in \mathcal{P}$ avec $\alpha \in x V^*$. Un langage est très simple s'il est engendré par une grammaire très simple. Dand une telle grammaire, les règles sont indicées par les lettres terminales. Evidemment, on suppose qu'il n'y a pas de règle "inutile", c'est-à-dire que $L_G(\alpha) \neq \emptyset$ pour tout membre droit de règle α.

Exemples 1.- (Butzbach [13]). Soient $V = \{A, B, C\}$, $X = \{a,b,c,d,e,f,g\}$, et

$A \longrightarrow f$

$B \longrightarrow cCA + dC + g$

$C \longrightarrow aCAB + bCBA + e$

2.- Soient $V = \{ A, B, C, D\}$, $X = \{ x,y,z,b,c,c',d,d'\}$, et

$A \longrightarrow xAB + yC + zD$;

$B \longrightarrow bD$;

$C \longrightarrow c + c'$;

$D \longrightarrow d + d'A$.

Théorème (Ph. Butzbach [13]). Un langage très simple est classe d'une congruence engendrée par un système confluent et basique.

Nous ne donnons pas la preuve de ce résultat ; nous nous contentons de décrire la construction du système.

Pour chaque membre droit de règle α, soit $M(\alpha)$ l'ensemble des mots de longueur minimale dérivant de α. Le système $\mathcal{S}$ est alors la réunion des ensembles $M(\alpha) \times M(\alpha')$ pour tous les α, α' membres droits de règles aynt même membre gauche. La preuve du théorème repose sur les propriétés remarquables des langages très simples engendrés par la grammaire (ils sont préfixes, ne chevauchent pas etc...)

Exemples 1. On obtient :

$M(f) = \{f\}$; $M(g) = \{g\}$, $M(dC) = \{de\}$, $M(cCA) = \{cef\}$;

$M(aCAB) = \{aefg\}$, $M(bCBA) = \{begf\}$, $M(e) = \{e\}$;

d'où le système

$$\mathcal{J} = \{ (de,g), (cef,g), (aefg, e), (bcgf,e) \} .$$

2. On obtient :

$M(xAB) = \{ xycbd, xyc'bd, xzdbd \}$, $M(yC) = \{ yc, yc' \}$, $M(zD) = \{ zd \}$;
$M(bD) = \{ bd \}$;
$M(c) = \{ c \}$, $M(c') = \{ c' \}$;
$M(d) = \{ d \}$, $M(d') = \{ d'yc, d'yc', d'zd \}$;

d'où le système

$$\mathcal{J} = \{ (xycbd,yc), (xycbd, yc'), (xycbd,zd),..., (yc', zd) \} \cup \{ (c,c'), (d'yc,d), (d'yc',d), (d'zd,d) \} .$$

Comme corollaire, on obtient

Corollaire.-Tout langage algébrique est image homomorphe d'un langage algébrique congruentiel.

En effet, tout langage algébrique est image homomorphe d'un langage très simple, éventuellement augmenté du mot vide.

Remarque. Comme me l'a fait remarquer L. Boasson, la construction que nous venons d'esquisser pour les grammaires très simple ressemble beaucoup à une construction utilisée par Mc Naughton [4] pour les grammaires parenthétiques. Il est donc vraisemblable que la même conclusion reste valable pour les langages parenthétiques, ce qui mène naturellement à se poser la question de la nature du phénomène commun aux deux familles de langages qui permet d'achever la construction.

Références.

1. J.M. Autebert, G. Cousineau, M. Nivat, Théorie des automates et des langages formels ; I. Les langages algébriques, Institut de Programmation, Paris, 1975-76, polycopié.

2. M. Gross, A. Lentin, Notions sur les grammaires formelles, Gauthier-Villars, Paris, 1967.

3. M. Fliess, Deux applications de la représentation matricielle d'une série rationnelle non commutative, J. of Algebra 13 (1971), p 344-352.

4. R. Naughton, Parenthesis Grammars, J. Assoc. Comp. Machinery 14 (1967), p 490-500.

5. M. Nivat, J.F. Perrot, Une généralisation du monoïde bicyclique, C. R. Acad. Sci. Paris, Série A 271 (1970), p 824-827.

6. J.F. Perrot, Monoïdes syntactiques des langages algébriques, Acta Informatica 7 (1977), p 399-413.

7. J.F. Perrot, Introduction aux monoïdes syntactiques des langages algébriques, in : Actes de l'école de Printemps sur les langages algébriques (Bonascre 1973), Ecole Nat. Sup. des Techniques avancées (à paraitre).

8. J.F. Perrot, J. Sakarovitch, Langages algébriques déterministes et groupes abéliens, in : Automata Theory and Formal Languages, 2nd G.I. Conference , Lecture Notes in Computer Science 33, Springer 1975, p 20-30.

9. J. Sakarovitch, Monoïdes syntactiques et langages algébriques, Thèse 3ème cycle, Univ. Paris VII, 1976.

Bibliographie

10. M. Benois, Simplifiabilité et plongement dans un groupe des monoïdes quotients d'un monoïde libre par une congruence de Thue unitaire, C.R. Acad. Sci Paris, Série A 276 (1973), p 665-668.

11. M. Benois, Monoïdes présentés par certaines congruences, Journées sur les demi-groupes : algèbre et combinatoire, Séminaire Dubreil 1975/76.

12. M. Benois, Y. Cochet, Congruences quasi-parfaites sur le monoïde libre: algèbre et combinatoire, s. 1. 1976, manuscrit, 17 p.

13. Ph. Butzbach, Une famille de congruences de Thue pour lesquelles le problème de l'équivalence est décidable. Application à l'équivalence des grammaires séparées, in M. Nivat (éd.) : Automata, languages and Programming, North-Holland 1973, p 3-12.

14. Ph. Butzbach, Equivalence des grammaires simples, in : Actes de l'école de printemps sur les langages algébriques (Bonascre 1973), Ecole Nat. Sup. des Techniques avancées (à paraître).

15. Y. Cochet, Sur l'algébricité des classes de certaines congruences définies sur le monoïde libre, thèse 3e cycle, Rennes 1971.

16. Y. Cochet, Tous les groupes quotients du monoïde libre par une congruence parfaite unitaire, s. 1. 1975, 4p.

17. Y. Cochet, Langages définis par des congruences, Séminaire Dubreil 19e année, 1975/76, 9 p.

18. Y. Cochet, Church-Rosser congruences on free semi-groups, Proc. Colloquium on algébraic theory of semigroups, Szeged 1976, à paraître.

19. Y. Cochet, M. Nivat, Une généralisation des ensembles de Dyck, Israel J. of Math. 9 (1971), p. 389-395.

20. M. Nivat, On some families of languages related to the Dyck language, Second Annual ACM Symp. on Computing, 1970, p 221-225.

21. M. Nivat, Congruences de Thue et t-langages, Studia Sci. Math. Hungarica 6 (1971), p 243-249.

22. M. Nivat, (avec M. Benois), Congruences parfaites et quasi-parfaites, Séminaire Dubreil, 25e année, 1971/1972, 9 p.

23. M. Nivat, Congruences et théorème de Church-Rosser, Journées sur les demigroupes : algèbre et combinatoire, Séminaire Dubreil 1975/76.

24. R. Sethi, Testing for the Church-Rosser Property, J. Assoc. Computing Mach. 21 (1974), p 671-679.

25. M. P. Schützenberger, Sur un langage équivalent au langage de Dyck, in : P. Suppes et al. (eds), Logic, Methodology and Philosophy of Science IV, North-Holland 1973, p 197-203.

26. A. Thue, Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln, Skr, Vidensk, Selsk. I, 10 (1914), 34 p.