Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par
Jean Berstel, Alain Lascoux et Dominique Perrin

*

Tome 6 : 1964–1968

Institut Gaspard-Monge, Université Paris-Est
2009

Introduction
Tome VI : 1964–1969

Le plus connu et le plus cité des articles de cette période est *On finite monoids having only trivial subgroups* [1965-4], où il caractérise les langages rationnels dont le monoïde syntactique est apériodique, c'est-à-dire n'a pas de groupe non trivial. C'est le résultat pionnier dans ce qui deviendra la théorie des variétés des langages reconnaissables, et c'est l'un des résultats les plus marquants dans la recherche des groupes dans les monoïdes ou, autrement dit, dans la recherche de ce qui se retrouve, de la théorie des groupes, dans la théorie des monoïdes. C'est aussi un élément décisif d'un autre point de vue. Les langages rationnels dont le monoïde syntaxique n'a pas de groupe non trivial sont aussi ceux qui sont définissables dans la théorie du premier ordre de l'ordre linéaire. Ils forment donc une famille de langages rationnels d'un intérêt particulier. Le théorème de M.-P. Schützenberger montre que l'appartenance à cette classe est décidable, un fait d'une importance considérable. S. Eilenberg, dans le volume B de son traité ([4],page 253) écrit : « Next to Kleenes's Theorem, Schützenberger's Theorem is probably the most important result dealing with recognizable sets. ».

Le lien avec la théorie des variétés est fait dans l'article *Sur certaines variétés de monoïdes finis* [1966-2] qui paraît dans les actes du colloque *Automata Theory* qui réunit en 1964, à Ravello, à l'invitation de Caianiello la plupart des grands noms de la théorie des automates comme McNaughton ou Rabin ou de la calculabilité comme Martin Davis. Il étudie dans cet article la variété des monoïdes dont tous les sous-groupes sont dans une variété donnée de groupes finis (ce qui constitue une généralisation du cas des monoïdes apériodiques) et montre que la variété correspondante de langages rationnels est fermée par produit. La preuve utilise ce qui est maintenant appelé le *produit de Schützenberger* de deux monoïdes, qui permet de construire un monoïde reconnaissant le produit de deux langages à partir de monoïdes reconnaissant les facteurs du produit.

Plusieurs articles de cette période ont trait à la décomposition des monoïdes. C'est, en effet, en 1965 que Krohn et Rhodes publient leur résultat : tout semigroupe est un produit en couronne de semigroupes élémentaires et de groupes [9]. La portée de ce résultat est discutée dans sa présentation au congès de l'IFIP en 1965 *On the algebraic theory of automata* [1965-9]. De même, sa Note aux Comptes Rendus [1966-5] *Sur les produits semi-directs droits de monoïdes* avec Maurice Nivat (avec un errata en [1967-1]) poursuit dans cette direction, suivie par d'autres articles dont il sera question dans les tomes suivants, comme

[1970-2].

L'article [1965-6] *On a factorization of free monoids* contient son théorème sur les factorisations de monoïdes libres. Il donne comme exemple (Example 2) la factorisation en mots de Lyndon qui pourtant, au sens strict, ne figure pas dans l'article de Chen, Fox et Lyndon de 1958 qui est cité en référence [2]. Ce dernier contient cependant la preuve que les crochets formés sur les mots de Lyndon sur un alphabet A forment une base de l'algèbre de Lie libre $L(A)$, d'où le résultat via le fait que l'algèbre enveloppante de $L(A)$ est l'algèbre associative libre sur A.

Cette période est aussi celle d'autres articles importants en théorie des codes. Décrivons brièvement leur contenu.

Codes à longueur variables [1965-8], un texte qui a été d'une importance fondamentale pour ses élèves et disciples, est resté non publié. Ce sont les notes de cours sur la théorie des codes, écrites pour un colloque à Royan. On y trouve, outre un résumé de résultats, nombre de conjectures qui ont nourri les recherches de ses élèves, même si la plupart se sont avérées fausses. Dominique Perrin a rédigé une version raisonnée de ces notes. La fameuse école de Royan, organisée par Dominique Foata, s'est tenue du 26 août au 8 septembre 1965. L'intitulé officiel était « Nato Summer School on Combinatorial Methods in Coding and Information Theory ». Parmi les participants, il y avait notamment Barlotti, Berlekamp, Bose, Hocquenghem, Kasami, Nivat, Peterson, Schützenberger, Wolfowitz.

L'article *On the synchronizing properties of certain prefix codes* [1964-1] contient la théorie des codes sémaphores. L'article est centré sur le théorème concernant les codes sémaphores synchronisés : tout code sémaphore est une puissance d'un code sémaphore synchronisé. L'article contient nombre d'autres résultats dont le calcul de la série génératrice d'un code sémaphore, la preuve d'un énoncé concernant les ensembles coupants minimaux (annoncé en [1962-2]). L'article donne deux preuves du résultat principal. L'une est entièrement combinatoire et assez difficile à suivre. L'autre est algébrique. Elle utilise un résultat intermédiaire lui-même remarquable : si le groupe d'un code préfixe X est un groupe de permutations régulier, alors le code X se décompose en $X = Y \circ Z \circ T$ où Y, T sont synchronisés et Z est un code à groupe. Parmi les très nombreux résultats que contient cet article figure la borne supérieure à la taille minimale des ensembles coupants annoncée en [1962-8]. Il contient à ce sujet une inexactitude de détail qui a eu une suite intéressante. Il est en effet affirmé qu'en longueur 5 sur 2 lettres, la taille minimale est 9. Cette affirmation a été consciencieusement reprise par ses élèves dans le livre de Lothaire *Combinatorics on Words* (Exercice 5.1.4) paru en 1983 [10]. Plus tard, en 2001, Christopher Saker, alors étudiant à l'université d'Essex, a remarqué que cette borne est fausse et qu'il existe un ensemble coupant de 8 éléments, ce qui est clairement le minimum puisque c'est le nombre de mots de classes de conjugués de mots de longueur 5 sur 2 lettres. En 2004, Champarnaud, Hansel et Perrin parviennent à prouver qu'il est toujours vrai que le cardinal minimum d'un ensemble coupant de mots de longueur n sur un alphabet donné est le nombre de classes de conjugués de mots de longueur n sur cet alphabet [1]. Finalement, David Penman et Christopher Saker ont trouvé la référence d'un article de J. Mykkeltveit datant de 1972 et dans lequel il prouve le même résultat par une méthode totalement différente en réponse à une conjecture de Golomb [11].

L'article [1965-1] *Sur certains sous-monoïdes libres*, paru dans le Bulletin de la Société Mathématique de France est dédié à A. D. Wallace, le père des

semigroupes topologiques. Il contient un résultat majeur de la théorie : si X est un code maximal fini sur l'alphabet A, l'image commutative du polynôme $1-X$ est divisible par $1-A$ et le quotient n'est irréductible que si le code est préfixe. Ce résultat sera amélioré plus tard par Reutenauer qui a montré en 1985 qu'il était encore vrai en variables non commutatives. La preuve donnée dans l'article n'est pas tout à fait complète, et une version complète a été publiée en 1984 par Hansel, Perrin et Reutenauer [8].

La note aux Comptes rendus *Sur une question concernant certains sous-monoïdes libres* [1965-3] répond à une question posée dans l'article de Golomb et Gordon paru la même année [7]. Elle caractérise les distributions de longueur des codes circulaires par une inégalité faisant intervenir le nombre de colliers primitifs de longueur donnée.

L'article *On a question concerning certain free submonoids* [1966-7] contient la solution d'une conjecture proposée par Gilbert et Moore en 1959 [5]. Il s'agit du théorème suivant lequel un code maximal fini qui n'est pas préfixe a un délai de déchiffrage infini.

Dans *On synchronizing prefix codes* [1967-5], un résultat très peu connu est établi. Il donne une caractérisation des distributions de longueurs des codes préfixes synchronisés. Il s'agit donc d'un cas particulier du théorème de coloriage des routes récemment établi par Trakhtman.

L'article *On a question of Eggan* [1966-6], avec Françoise Dejean, est une contribution au problème de la hauteur d'étoile des langages rationnels. Il donne, en réponse à une question posée par Eggan en 1963, une construction simple montrant qu'il existe des langages de hauteur arbitrairement grande.

L'article *A remark on acceptable sets of numbers* [1968-1] est le seul que M.-P. Schützenberger ait écrit sur les ensembles reconnaissables d'entiers en base donnée. Il paraît donc un an avant que Cobham publie son théorème montrant qu'un ensemble reconnaissable dans deux bases multiplicativement indépendantes est reconnaissable dans toute base [3]. L'article contient deux résultats qui donnent des familles d'entiers dont l'ensemble des représentations n'est pas algébrique (context-free).

Dans le bref article intitulé *Classification of Chomsky Languages* [1966-9], M.- P. Schützenberger propose une présentation particulière des langages algébriques : ceux-ci sont vus essentiellement comme des images, par des transductions rationnelles de langages de Dyck. La classification repose sur les caractéristiques des morphismes et des langages rationnels utilisés dans la transduction. Cette approche de la théorie des langages algébriques conduira aux travaux de Maurice Nivat sur les transductions [12] et les langages dits « T-compilables » [13]. Elle donnera sa pleine mesure dans le développement ultérieur de la théorie des familles de langages, cônes rationnels et full AFL où l'école française rivalise avec les chercheurs américains [6]. La courte discussion qui suit la présentation est instructive. A première vue, le sujet du débat avec Dijkstra semble un peu surréaliste ; pourtant, une lecture attentive y révèle à quel point M.-P. Schützenberger envisageait le traitement des questions autour des mots et des langages comme des questions mathématiques au sens propre : il refuse de s'aventurer sur un terrain où les objets manipulés font l'objet de quelque interprétation que ce soit.

[1] Jean-Marc Champarnaud, Georges Hansel, and Dominique Perrin. Unavoidable sets of constant length. *Internat. J. Algebra Comput.*, 14(2) :241–251, 2004.

[2] K.-T. Chen, R. H. Fox, and Roger C. Lyndon. Free differential calculus. IV. The quotient groups of the lower central series. *Ann. of Math. (2)*, 68 :81–95, 1958.

[3] Alan Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory*, 3 :186–192, 1969.

[4] Samuel Eilenberg. *Automata, Languages, and Machines. Vol. B.* Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. With two chapters ("Depth decomposition theorem" and "Complexity of semigroups and morphisms") by Bret Tilson, Pure and Applied Mathematics, Vol. 59.

[5] Edgar N. Gilbert and Edward F. Moore. Variable-length binary encodings. *Bell System Tech. J.*, 38 :933–967, 1959.

[6] Seymour Ginsburg and Sheila Greibach. Abstract families of languages. In *Studies in abstract families of languages*, pages 1–32. Mem. Amer. Math. Soc., No. 87. Amer. Math. Soc., Providence, R.I., 1969.

[7] Solomon W. Golomb and Basil Gordon. Codes with bounded synchronization delay. *Information and Control*, 8 :355–372, 1965.

[8] Georges Hansel, Dominique Perrin, and Christophe Reutenauer. Factorizing the polynomial of a code. *Trans. Amer. Math. Soc.*, 285(1) :91–105, 1984.

[9] Kenneth Krohn and John Rhodes. Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines. *Trans. Amer. Math. Soc.*, 116 :450–464, 1965.

[10] M. Lothaire. *Combinatorics on words.* Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1997. Corrected reprint of the 1983 original.

[11] Johannes Mykkeltveit. A proof of Golomb's conjecture for the de Bruijn graph. *J. Combinatorial Theory Ser. B*, 13 :40–45, 1972.

[12] Maurice Nivat. Transductions des langages de Chomsky. *Ann. Inst. Fourier (Grenoble)*, 18(fasc. 1) :339–455, 1968.

[13] Maurice Nivat. Une propriété des langages compilables. *C. R. Acad. Sci. Paris Sér. A-B*, 267 :A244–A246, 1968.

Année 1964

Bibliographie

[1] Marcel-Paul Schützenberger. On the synchronizing properties of certain prefix codes. *Information and Control*, 7 :23–36, 1964.

[2] Jean Larisse and Marcel-Paul Schützenberger. Sur certaines chaînes de Markov non homogènes. *Publ. Inst. Statist. Univ. Paris*, 13 :57–66, 1964.

Reprinted from Information and Control, Volume 7, No. 1, March 1964

INFORMATION AND CONTROL **7**, 23–36 (1964)

On the Synchronizing Properties of Certain Prefix Codes

M. P. Schützenberger

Faculté des Sciences, Poitiers, France

A special family J of prefix codes is considered. It is verified that if $A \in \mathbf{J}$ has not a certain synchronizing property, then $A = C^p$ $(p > 1)$, where C is another code from the same family.

I. INTRODUCTION

Let F be the free monoid generated by the set ("alphabet") X; F consists of its neutral element 1 (the so-called "empty word") and of the set $X^* = X \cup X^2 \cup \cdots \cup X^n \cdots$ of all words of positive degree (or "length"). We denote by $\mathbf{X}^*$ the collection of all nonempty subsets of X^* and we consider the family J of all prefix codes A that can be defined by taking an arbitrary $H \in \mathbf{X}^*$ and by letting a word f belong to A iff f has some right factor (or "final segment") in H, i.e. $f \in FH$, and no proper (i.e., $\neq f$) left factor (or "initial segment") of f has the same property, i.e., $f \notin FHX^*$.

This theory is due to B. Mandelbrot, who studied in details the especially important case where H is a particular letter (the so-called "space") of the alphabet (cf. bibliography in Mandelbrot (1957) and Mandelbrot (1961)). A special case obtains by selecting an arbitrary subset of states of a definite automaton, and by defining A as the set (provided it belongs to $\mathbf{X}^*$) of all words at the last letter of which the distinguished set is reached for the first time. This construction is part of a more general theory, due to P. G. Neuman (Neuman (1962)).

Both of the authors quoted have emphasized the synchronizing properties of the codes of the family J. Indeed, let us say that the prefix code A is *almost surely synchronizing* if there exists at least one word $a \in F$ such that $fa \in A^*$ $(= A \cup A^2 \cup \cdots \cup A^n \cdots)$ for all $f \in F$. In Winograd's theory (Winograd (1963), cf. also Winograd (1962)) a would be called a *universal synchronizing word*. If $\mathbf{J}_1$ denotes the subset of all almost surely synchronizing codes of J, we intend to verify $\mathbf{J} =$

$\{A^p : p>0,\ A \in \mathbf{J}_1\}$. In other terms, if $A \in \mathbf{J}$ is *not* a.s. synchronizing then there exists a unique $C \in \mathbf{J}_1$ and natural number $p > 1$ which are such that A consists of all products of p words from C. These notions may be clarified by the following examples in which $X = \{x, y\}$.

(i) $H = \{x\}$; then $A = FH\backslash FHX^*$ $(= \{f \in FH : f \notin FHX^*\})$ consists of all words x, yx, y^2x, $\cdots$, y^nx, $\cdots$. Since obviously $FA \subset A^*$, A belongs to $\mathbf{J}_1$.

(ii) $H = \{xx, xyx, xyy, yyx, yyyy\}$. The corresponding prefix code A consists of H and the words yxx, $yxyx$, $yxyy$, $yyyx$. In fact, $A = C^2$ where $C = FH'\backslash FH'X^*$ with $H' = \{x, yy\}$. Since $CA^* \subset A^*C$ and $A^* \cap A^*C = \phi$, A does not belong to $\mathbf{J}_1$ but it is the square of the code $C \in \mathbf{J}_1$.

(iii) As a related counter example one might consider the prefix code A consisting of x and of all the words of the form y^dxf where $d = 1, 2, \cdots, n, \cdots$ and where f is an arbitrary word of degree ("length") d. Thus $A \notin \mathbf{J}$ because for instance, x, $yxx \in A$ and $yxx \in FAX^*$. Since for every $f' \in F$ of degree d' one has $f'x^d \in A^*$ when $d > d'$, every word of F can be "resynchronized." However, under the same hypothesis $y^df' \in F\backslash A^*F$, and one sees that there exists no universal synchronizing word, i.e., no word which resynchronizes all the words of F.

II. DEFINITIONS AND NOTATIONS

For the sake of completeness we recall first some well-known facts concerning prefix codes and we summarize some general properties of the family $\mathbf{J}$.

By definition, a prefix code is a set $A \in \mathbf{X}^*$ which satisfies the condition

$$\mathfrak{u}_r' : AX^* \cap A = \phi.$$

Indeed $\mathfrak{u}_r'$ simply expresses that every word of F has at most one left factor in A. Thus, letting $T = F\backslash AF$, we have $F = T \cup A^*T$ and we can define inductively a mapping $\tau : F \to T$ by setting for any word f, $\tau f = f$ if $f \in T$; $\tau f = \tau f'$ if $f = af'$ where $a \in A$. Thus $\tau f = 1$, iff $f \in \{1\} \cup A^*$. The identity $\tau ff' = \tau((\tau f)f')$ is easily checked by examining the two cases of $f \in T$ and $f \notin T$. By construction, for all $f \in F$, τFf $(= \{\tau f'f : f' \in F\})$ is the same as τTf $(= \{\tau tf : t \in T\})$. It follows that for any f, f', $f'' \in F$ one has Card $\tau Tff'f'' \leqq$ Card $\tau Tf'$. Indeed, on the one hand, $\tau Tff'f'' = \tau((\tau Tf)f'f'') \subset \tau' Tf'f''$ and, on the other hand, Card $\tau Tf'f'' =$ Card $\tau((\tau Tf')f'') \leqq$ Card $\tau Tf'$.

Let p denote the minimum value (possibly infinite) of Card τTa over all $a \in A^*$. Since $1 \in \tau Ta$ for $a \in A^*$, p is positive and since

$\tau Ta = \{1\}$ is equivalent to $Fa \in A^*$, one sees that $p = 1$ iff A is a.s. synchronizing.

We now return to the family $\mathbf{J}$.

Property 1. For each $H \in \mathbf{X}^*$ the set $A = FH\backslash FHX^*$ belongs to $\mathbf{X}^*$ and it satisfies the conditions:

$$\mathfrak{U}'_{r_j}: FAX^* \cap A = \phi;$$

$$\mathfrak{N}_{rj}: FA \subset AF.$$

Reciprocally, if the prefix code A satisfies $\mathfrak{N}_{rj}$, then $A = FH\backslash FHX^*$ where $H = A\backslash X^*A$; further, $H \cap (X^*H \cup HX^* \cup X^*HX^*) = \phi$ and $AF = FHF$.

Proof: Let $H \in \mathbf{X}^*$. The set $A = FH\backslash FHX^*$ is a subset of X^*; A is not empty since it contains every word of H of minimal degree. Consider a word of the form faf' where $f \in F$, $a \in A$, $f' \in X^*$. By hypothesis, $a = f''h$ for some $f'' \in F$ and $h \in H$; thus $faf' = ff''hf' \in FHX^*$ and, as a result, $faf' \notin A$. This proves that A satisfies $\mathfrak{U}'_{r_j}$; hence $\mathfrak{U}'_r$, since $AX^* \subset FAX^*$.

Consider now $f \in F$ and $a \in A$. Again $a = f''h$ for some $f'' \in F$ and $h \in H$. Hence $fa \in FH$ and fa has a left factor, say $f'''h'$, of minimal degree that belongs to FH and, by construction, that does not belong to FHX^*. Thus $F'''h' \in A$ and this proves $\mathfrak{N}_{r_j}$.

Reciprocally consider any set $A \in \mathbf{X}^*$ and define $H = A\backslash X^*A$. By construction $H \cap X^*H = \phi$ and the right factor in A of minimal degree of every word of A belongs to H. Thus, $H \in \mathbf{X}^*$, and $H \subset A \subset X^*H \cup H = FH$. In fact, H is the least set H' such that $A \subset FH'$.

Assume now that A satisfies $\mathfrak{N}_{r_j}$; if $f \in F$ and $h \in F$ are such that fh has no proper left factor in FH, fh has no proper left factor in A since $A \subset FH$. However, since $H \subset A$, we have $fh \in FA$, hence $fh \in AF$ and thus, $fh \in A$. This proves $FH\backslash FHX^* \subset A$.

Assuming finally that A is a prefix code, we see that $A \cap FHX^* = \phi$, i.e., $A = FH\backslash FHX^*$ because every word of FHX^* has a proper left factor in $FH\backslash FHX^*$, hence in A. Thus A satisfies $\mathfrak{U}'_{r_j}$. Since $H \cap X^*H = \phi$ and since $HX^* \cup X^*HX^* = FHX^* \subset FAX^*$, it follows that $H \cap (HX^* \cup X^*H \cup X^*HX^*) = \phi$, showing that in fact H is the least set H' such that $FH'F = FAF$. Since $\mathfrak{N}_{r_j}$ implies $FAF = AF$, it follows that $AF = FHF$, or, in equivalent fashion, that $T\,(= F\backslash AF)$ is equal to $F\backslash FHF$.

Remark 1. If A is a prefix code, one has $A^pX^* \cap A^p = \phi$ for any

positive p. Thus if $A \in \mathbf{J}$ one has also $A^p \in \mathbf{J}$ for any positive p because of the relations $FA^p = (FA)A^{p-1} \subset AFA^{p-1} = A(FA)A^{p-2} \subset A^2FA^{p-2} \cdots \subset A^{p-1}FA \subset A^{p-1}AF = A^pF$ which show that A^p satisfies $\mathfrak{N}_{r_j}$. Observing that for $p > p' > 0$, $FA^pX^* \subset FA^{p'}X^*$, one concludes that $FA^pX^* \cap A^{p'} = \phi$. Clearly $A^p \notin \mathbf{J}_1$ for $p > 1$.

As an application let us consider two words $a, a' \in A$, a word $\bar{a} \in A^m$ (where $\bar{a} \in A^\circ$ is understood to mean $\bar{a} = 1$) and two right factors t_i' and t_j' of a' such that $0 \leqq \deg t_i' \leqq \deg t_j' < \deg a'$. We verify that, provided $t_j'\bar{a}a \notin A^*$, one has $\deg \tau t_i\bar{a}a \leqq \deg \tau t_j'\bar{a}a$. Indeed, by the definition of τ, there exist two elements u_i and u_j of X^* such that $t_i'\bar{a}u_i$, $t_j'\bar{a}u_j \in A^*$ and $u_i\tau t_i'\bar{a}a = u_j\tau t_j'\bar{a}a = a$. If $t_i' = 1$, the result is proved. Thus we can assume that none of u_i and u_j is equal to a and, as a result, both of the words $a_i = t_i'\bar{a}u_i$ and $a_j = t_j'\bar{a}u_j$ have $\bar{a}$ as a proper factor and are proper factors of $a'\bar{a}a$. However, $\bar{a} \in A^m$; $a'\bar{a}$, $\bar{a}a \in A^{m+1}$; $a'\bar{a}a \in A^{m+2}$. Hence $a_i, a_j \in A^{m+1}$. By hypothesis t_i' is a right factor of t_j' and, thus, $a_j \in Fa_iX^*$ is excluded. It follows that either $u_i = u_j$ (and then $\tau t_i'\bar{a}a = \tau t_j'\bar{a}a$) or u_j is a proper left factor of u_i (and then $\deg t_i'\bar{a}a < \deg t_j'\bar{a}a$). The verification is concluded.

Remark 2. Let B be a prefix code and ξ an epimorphism (homomorphism onto) of $B^\dagger = \{1\} \cup B^*$ onto an abelian group G of order $p > 1$. We suppose that $A \in \mathbf{J}$ is contained in the kernel $B^\dagger \cap \xi^{-1}1$ of ξ and we prove that under these hypotheses

(i) There exists a prefix code C such that $A = CP$;

(ii) $C \in \mathbf{J}$ and, moreover, $C \in \mathbf{J}_1$ if B is a.s. synchronizing.

VERIFICATION OF (i)

Let $B_0 = B \cap \xi^{-1}1$; $B_1 = B \backslash B_0$; $C = B_0^\dagger B_1$ where $B_0^\dagger = \{1\} \cup B_0^*$. Since ξ is an epimorphism, B_1 is not empty and, clearly, C is a prefix code. We call C-degree of a word $f \in B^*$, the number of its factor from B_1 and we note that no $a \in A$ has C-degree zero. Indeed, otherwise, we could take some $b \in B_1$, and, since ba has no left factor in $A \subset \xi^{-1}1$, A would not satisfy $\mathfrak{N}_{r_j}$.

Let $a \in A$ of minimal C-degree q and $g = c_1c_2 \cdots c_q \in C^q$. Applying $\mathfrak{N}_{r_j}$ to c_qa shows that $c_qa = a'f'$ where $a' \in A$ and where $\xi f' = \xi c_q \neq \xi 1$. Thus $f' \in C^*B_0^\dagger$. Since a has minimal C-degree we must have in fact $f' \in CB_0^\dagger$ and a' has also C-degree q. By reiterating the argument we see that $gb \in A$ for some word $b \in B_0^\dagger$ which is necessarily a left factor of a. Thus $g \in A$ would have been proved if we had taken an element $a \in A \cap B_1C^*$ of C-degree q. However, choosing $c_1 \in B_1$, the relation

$gb \in A$ shows that such an element a does exist and we can conclude that $C^q \subset A$.

It follows that $C_1 \subset \xi^{-1}u$ for some element $u \in G$ of order q. Thus, since ξ is an epimorphism, G is a cyclic group and $p = q$. Finally since A satisfies $\mathfrak{U}_r$, the relations $A \cap B_0^\dagger = \phi$, $C^p \subset A$ and $A \subset (\{1\} \cup (C^p)^*)B_0^\dagger$ show that $A = C^p$ and (i) is proved.

VERIFICATION OF (ii)

It suffices to show that C satisfies $\mathfrak{N}_{r_j}$. Assume $Fc' \subset CF$ already proved for all words $c' \in C$ of degree less than m and consider a word $c \in C$ of degree m and any $f \in F$. If c admits another word $c' \in C$ as a proper right factor we have $fc \in Fc'$ and $fc \in CF$ results from the induction hypothesis. Thus we may assume $c \notin X^*C$, and we consider fc^p. By $A = C^p$ and $\mathfrak{N}_{r_j}$ we have $fc^p = c_1c_2 \cdots c_pf'$ where $c_1, c_2, \cdots, c_p \in C$ and $f' \in F$. Because of the induction hypothesis, c_pf' cannot be a factor of c, thus deg $c <$ deg c_pf', and cancelling gives $fc^{p-1} = c_1c_2 \cdots c_{p-1}f''$ for some $f'' \in X^*$. In the same manner, deg $c <$ deg $c_{p-1}f''$; hence $fc^{p-2} = c_1c_2 \cdots c_{p-2}f'''$, and so on. Finally we obtain $fc = c_1f''''$ and $Fc \in CF$ is proved. This ends the verification.

We shall need later the following formulation of this remark: If $A \in \mathbf{J}$ and if $B = B_0 \cup B_1 (B_1 \neq \phi)$ is a partition of a prefix code B such that $A \subset C^pB_0^\dagger$ where $C = B_0^\dagger B_1$, then $A = C^p$ and $C \in \mathbf{J}$. That $C \in \mathbf{J}_1$ when B is a.s. synchronizing is trivial.

The next remarks are not needed for the verification of the main result.

Remark 3. For $h, h' \in H (= A\backslash X^*A)$, let $R_{h',h} = \{f \in X^*\backslash Fh : h'f \in Fh\}$. Thus $h'R_{h',h} = (h'F \cap Fh)\backslash Fh'hF$ is a finite set and $Fh'R_{h',h} \subset Fh$. Because of $\mathfrak{N}_{r_j}$ and $\mathfrak{U}_{r_j}$, any word $f \in Fh$ has a unique maximal left factor $a \in A^*$ (since $A^* = \cup \{A^* \cap Fh : h \in H\}$), and, by definition, either $f = a \in A^* \cap Fh$ or $f \in aR_{h',h}$ where h' is determined by $a \in A^* \cap Fh'$. Reciprocally if $a \in A^* \cap Fh'$, one has $aR_{h',h} \subset Fh$. Thus, for each $h \in H$, one has the equation $Fh = (A^* \cap Fh) \cup \{(A^* \cap Fh')R_{h',h} : h' \in H\}$ where, as it is easily checked, every word of F appears at most once in each member. Assuming that the finite sets $R_{h',h}$ $(h, h' \in H)$ are given, this provides a system of equations from which the sets $A^* \cap Fh$ (hence A^* itself) can be computed by standard substitution methods. Another system having the same properties consists of the equation $\{1\} \cup TX = T \cup A$ and the equations

$$Th = (A \cap Fh) \cup \{(A \cap Fh')\, R_{h',h} : h' \in H\} \quad (h \in H).$$

These systems are due essentially to Von Mises and to W. Feller; the relevant bibliography can be found in (Feller, 1958) and in (David and Barton, 1962).

Remark 4. Let us verify that for $A \in \mathbf{J}$ the set $H_p = A^p \backslash X^* A^p$ is equal to $A^p \cap \tilde{A}^p$, where $\tilde{A} = HF \backslash X^* HF$. Observing that the condition $H \cap (X^*H \cup HX^* \cup X^*HX^*) = \phi$ on $H = A \backslash X^* A$ is symmetric and recalling that $F \backslash AF = T = F \backslash FHF$, we immediately deduce that $T = F \backslash F\tilde{A}$ and that $\tilde{A}$ itself satisfies the relations $\tilde{A} \cap X^*\tilde{A}F = \phi$ and $\tilde{A}F \subset F\tilde{A}$. Thus, using $A^pT \subset (FHF)^p \subset A^pF$ and $A^pT \cap A^{p+1}F = \phi$, we obtain the equations

$$(FHF)^p \backslash (FHF)^{p+1} = A^pT = T\tilde{A}^p; \ (FHF)^p = FA^pF = F\tilde{A}^pF.$$

Since H_p is the least subset H' such that $FH'F = FA^pF$, this shows that $H_p \subset A^p \cap \tilde{A}^p$. Further, for any $h \in A^p \cap \tilde{A}^p$, if $h = f'f''$ ($f' \in X^*$, $f'' \in F$), the word f'' belongs to $F \backslash FA^p$, hence it does not belong to $(FHF)^p$. This proves that $A^p \cap \tilde{A}^p \subset H_p$, and it concludes the verification.

Remark 4bis. In view of the symmetric relation $F \backslash AF = F \backslash F\tilde{A}$, a close connection between A and $\tilde{A}$ is to be expected. We verify that there exists a bijection ("1 to 1 mapping onto") $\rho : A \to \tilde{A}$ sending each $a \in A$ on one of its *conjugates* (i.e., on a word of the form $f''f'$, where $f', f'' \in F$ satisfy $a = f'f''$). Indeed, let $a = fh \in A$; $f \in F$, $h \in H$. If $h = f'f''$ where $f' \in F$ and $f'' \in X^*$, ff' belong to T, hence $ff' \notin HF$. However, for $f'' = h$, (and $f' = 1$), $f''f \in HF$. Thus h has a right factor $f'' \in X^*$ of minimal degree which is such that $f''ff' \in HF$, and, because of its minimality, $f''ff' \notin X^*HF$, i.e., $f''ff' \in \tilde{A}$. We define $\rho a = f''ff'$.

Since another mapping $\tilde{\rho} : \tilde{A} \to A$ can be defined in a perfectly symmetric fashion and since, then, both of the mappings $\tilde{\rho}\rho : A \to A$ and $\rho\tilde{\rho} : \tilde{A} \to \tilde{A}$ are identity mappings, the remark is verified.

Remark 5. We assume here that Card $X = k < \infty$ and we define $\alpha(k, n)$ as the minimum number of words in the sets $H \in X^n$ that satisfy the condition Card $(FH \backslash FHX^*) < \infty$. For instance, $\alpha(1, n) = 1$; $\alpha(k, 1) = k$; $\alpha(k, 2) = 2^{-1}k(k + 1)$; $\alpha(2, 5) = 9$. The exact value of $\alpha(k, n)$ is not known in the general case, but we can verify that $\alpha(k, n) \geqq n^{-1}k^n$ and that, assuming $k, n > 1$, $\lim nk^{-n}\alpha(k, n) = 1$ for $\mathrm{Max}(k, n) \to \infty$.

Let us recall that a word f is said to be *primitive* iff $f = f'^p$ ($f' \in F$, $p > 0$) implies $p = 1$. The number of conjugate classes of

primitive words of degree n is

$$\psi_k(n) = n^{-1} \sum \{k^{n|d}\mu(d) : d \mid n\}$$

where $\mu(\ )$ denotes Möbius function (Moreau quoted in (Lucas, 1891)).

VERIFICATION OF $\alpha(k, n) \geqq n^{-1} k^n$

Observe that for $f \in X^n$ and $m > 0$, any factor of degree n of f^m has the form f'^d where f' is a primitive word of degree d' and $dd' = n$. Thus the condition that $FH \backslash FHX^*$ is finite implies that H contains a d-th power of at least one word from each conjugate class of primitive words of degree d' ($dd' = n$). It follows that

$$\alpha(k, n) \geqq \sum \{\psi_k(d') : d' \mid n\} = n^{-1} \sum \{k^{n|d}\varphi(d) : d \mid n\} \geqq n^{-1}k^n$$

(where $\varphi(\ )$ is Euler's function) and the inequality is verified. It follows that, more generally, if $H' \in X \cup X^2 \cdots \cup X^n$ is such that $FH' \backslash FH'X^*$ is finite, one has $\sum \{k^{n-\deg h'} : h' \in H'\} \geqq n^{-1}k^n$ since we can derive from H' a subset $H \subset X^n$ (satisfying also $FH \backslash FHX^*$ finite) by replacing each $h' \in H'$ by the set of all words $h \in X^n$ which admit h' as a left factor.

VERIFICATION OF $\lim nk^{-n}\alpha(k, n) = 1$

Let $\leqq$ denote a lexicographic order on F. We use the results given in (Chen, Fox, and Lyndon, 1956) and, following these authors, we define $K \subset X^*$ by the condition that $f \in K$ iff $f = f'f''$ for $f', f'' \in X^*$ implies $f < f''$. It is known that K consists of the first word (in lexicographic order) from each conjugate class of primitive conjugate words of positive degree. Together with K we define $\bar{K} = \{(f'f'')^p f' : f'f'' \in K; p > 0\}$ and we verify the following statement:

If $f \in X^*$ is such that $f = f_1f_2 = f_3f_4$ for $0 < \deg f_1 = \deg f_4$ implies $f_1 \leqq f_n$, then $f \in \bar{K}$.

PROOF: If there exists no word $g \neq 1, f$ which is at the same time a left and a right factor of f, each relation $f_1 \leqq f_4$ can be replaced by $f_1 < f_4$. Then, identically, $f = f_1f_2 < f_4$, i.e., $f \in K$. Thus we have only to discuss the case where f admits some nontrivial word as a proper left and right factor. Then it is known that f has the form $(g_1g_2)^{1+p}g_1$ where $p \geqq 0$ and where g_1g_2 is primitive. Let g_1' and g_2' be defined by the conditions $g_1g_2 = g_1'g_2'$ and $g_2'g_1' \in K$.

If $\deg g_1' < \deg g_1$ or if $p > 0$, $g_2'g_1'$ is itself a factor of f. Because of

our hypothesis on f, it cannot satisfy $g_2'g_1' < g_1g_2$ (because the right factor f_4 of f beginning with $g_2'g_1'$ would be in the relation $<$ with the corresponding left factor f_1 of the same degree). However $g_2'g_1' \in K$ implies $g_2'g_1' \leqq g_1'g_2'$ $(= g_1g_2)$. Thus $g_2'g_1' = g_1g_2$ and we have verified $f \in \bar{K}$ for this case.

Finally let us assume $p = 0$ and deg $g_1' \geqq$ deg g_1. Without loss of generality we can further assume that g_1 has maximum degree among the words which are at the same time a proper left and a right factor of f. There exists g_3 such that $g_1' = g_1g_3$ and $g_2 = g_3g_2'$. Since $f = g_1g_2g_1 = g_1g_3g_2'g_1$, one has $g_1g_4 \leqq g_2'g_1$ where g_4 is the left factor of degree deg g_2' of g_3g_2'. However $g_2'g_1'$ $(= g_2'g_1g_3) \leqq g_1'g_2'$ $(= g_1g_3g_2')$ from which we conclude that $g_2'g_1 \leqq g_1g_4$ and finally that $g_2'g_1 = g_4g_4$. By construction g_1g_4 is a left factor of f. Since we have assumed g_1 to be the common left and right factor of maximal length of f, we must have $g_2' = g_4 = 1$, hence $g_1g_2 = g_1'g_2' = g_2'g_1' \in K$ and the verification is concluded. In fact, $\bar{K}$ is the set of all left factors of the elements of K.

Consider now $H = \bar{K} \cap X^n$. Each long enough word $s = x_{i_1}\, x_{i_2} \cdots x_{i_m}$ contains at least one factor $f = x_{i_j}\, x_{i_{j+1}} \cdots x_{j+n-1} \in X^n$ $(j \leqq m - 2n + 2)$ which is such that $f \leqq x_{i_{j'}}\, x_{i_{j'+1}} \cdots X_{i_{j'+n-1}}$ for $j \leqq j' \leqq j + n - 1$. What we have just proved shows that $f \in \bar{K}$. Thus $FH \backslash FHX^*$ is finite.

In a similar manner, let H' consist of all words of the form x^n $(x \in X)$ and of the form xh where $x \in X$, $h \in R \cap X^{n-1}$ and $h < x$. We also have Card $(FH' \backslash FH'X^*) < \infty$. Indeed as it is easily verified, when $x_{i_{j+1}}\, x_{i_{j+2}} \cdots x_{j+n-1} \in \bar{K} \cap X^{n-1}$, one has $x_{i_j}\, x_{i_{j+1}} \cdots x_{j+n-1} \in H'$ or $x_{i_j}\, x_{i_{j+1}} \cdots x_{i_{j+n-2}} \in K \cap X^{n-1}$ depending upon $x_{i_{j+1}} < x_{i_j}$ or not. Thus $\alpha(k, n) \leqq$ Min (Card H, Card H') identically.

Now, since Card $K \cap X^m = \psi_k(m) \leqq m^{-1}k^m$ we have Card $H = \sum_{0<m\leqq n} \psi_k(m) \leqq n^{-1}k^n(1 + \sum_{0<m<n} n\, m^{-1}\, k^{m-n})$ from which it follows that for each $\epsilon > 0$ there exists $k_\epsilon < \infty$ such that $n\, k^{-n}\, \alpha(k, n) < 1 + \epsilon$ for all n and $k > k_\epsilon$.

On the other hand,

$$\text{Card } H' \leqq k + (k - 1) \text{ Card } (\bar{K} \cap X^{n-1})$$
$$\leqq k + (k - 1) \sum_{0<m<n} m^{-1}k^m = n^{-1}k^n\, (n(n - 1)^{-1} + u_n)$$

where u_n is determined inductively by $u_3 = (2k)^{-1}$ and $u_{n+1} = k^{-1}$ $(u_n + (n - 1)^{-1}\, (n - 2)^{-1})$. Since $\lim_{n\to\infty} u_n = 0$, there exists, for each $\epsilon > 0$ and $k > 1$ some $n_{k,\epsilon} < \infty$ such that $n\, k^{-n}\, \alpha(k, n) < 1 + \epsilon$ for all $n > n_{k,\epsilon}$. The verification of Remark 5 is concluded.

III. VERIFICATION OF THE MAIN PROPERTY

We intend to show that if $A \in \mathbf{J}\backslash\mathbf{J}_1$ there exists another prefix code $C \in \mathbf{J}_1$ and a natural number $p > 1$ such that $A = C^p$. For this, let $A \in \mathbf{J}$ and observe that condition $\mathfrak{N}_{r_j}$ expresses that for each $a \in A$ and $f \in F$, $\tau\bar{f}a$ is a right factor of a. Thus Card $\tau Ta \leqq \deg a$. Recalling the notations introduced at the beginning of Section II, this proves that p is finite and, since $p = 1$ is equivalent to $A \in \mathbf{J}_1$, we assume now $p > 1$. Letting $Q = \{a \in A^* : \text{Card } \tau Ta = p\}$, we know that $FQF \cap A^* \subset Q$ and, for each $f \in F$ and $q \in Q$, $\tau Tfq = \tau Tq$. The p elements of τTq indexed by increasing degree will be denoted by $\tau_0 q$ ($=1$ since $Q \subset A^*$), $\tau_1 q, \cdots, \tau_{p-1} q$. We shall use repeatedly the fact that an equation like $\tau fq = \tau_i q$ is equivalent to the existence of an element $\bar{a} \in A^*$ such that $fq = \bar{a}\tau_i fq$.

We verify first a few easy consequences of the definitions.

3.1 *For all* $q, q' \in Q$ *and* $i \in [0, p-1]$, $\tau((\tau_i q)q') = \tau_i q'$.

Proof: Because of the relation $\tau Tq' = \tau Tqq' = \tau((\tau Tq)q')$ and the fact that τTq and $\tau Tq'$ have the same finite cardinality, there corresponds to each $\tau_i q' \in \tau Tq'$ one and only one element, say $\tau_{i'} q$, of τTq that satisfies $\tau((\tau_{i'} q)q') = \tau_i q'$. However, we have $q' = \bar{a}'a'$ where $\bar{a}' \in \{1\} \cup A^*$, $a' \in A$ and the elements $\tau_i q'$ are right factors of a'. A similar observation can be made for q. Thus by Remark 1, we know that $i \leqq j$ implies $i' \leqq j'$. Thus $i = i'$ identically and 3.1 is proved. In fact, if f is any right factor of $\tau_j q$, Remark 1 shows that $\tau fq' = \tau_{j'} q'$ where $j' \leqq j$. Thus, denoting by $\bar{B}_j$ the set of all words $\bar{f}$ that satisfies the conditions

(*) for each $q' \in Q$, $\tau\bar{f}q' = \tau_j q'$;

(**) for each $q' \in Q$ and right factor f of $\bar{f}$, $\deg \tau fq' \leqq \deg \tau\bar{f}$ we have proved that $\{\tau_j q : q \in Q\} \subset \bar{B}_j$, identically. As a consequence we have

3.2 $A \subset \bar{B}_1^p$.

Proof: Let $a \in A$ and, taking a fixed $q \in Q$, let the p words $u_1, u_2, \cdots, u_p$ be defined by the relations $u_1 = \tau_1 qa$; $u_2 u_1 = \tau_2 qa$; $u_3 u_2 u_1 = \tau_3 qa$; $\cdots$; $u_{p-1} u_{p-2} \cdots u_2 u_1 = \tau_{p-1} qa$; $u_p u_{p-1} \cdots u_2 u_1 = a$. By *1* we know that, for each $i \in [0, p-1]$, $\tau((\tau_i qa)qa) = \tau_i qa$, or, in other terms, that the word $q_i = u_i u_{i-1} \cdots u_1 qa u_p u_{p-1} \cdots u_{i+1}$ belongs to A^*. In fact since it admits q as a factor, it belongs to Q. Since for $i \in [1, p-1]$ we have $\tau((\tau_{i+1} qa)qa) = \tau_{i+1} qa$, that is, $\tau(u_{i+1} q_i u_i u_{i-1} \cdots u_2 u_1) = u_{i+1} u_i \cdots u_2 u_1$, it follows that $\tau_1 q_i = u_{i+1}$ for $i = 1, 2, \cdots, p-1$ and 3.2 is proved.

Using the same notations it is readily seen that if $b, b' \in \bar{B}_1$ then, $bb' \notin$

$\bar{B}_1$. Indeed we have $b'qa = q_1' u_1$ with $q_1' \in Q$ and $bb'qa = bq_1' u_1 = q_2' u_2 u_1$ with $q_2' \in Q$ showing that $\tau bb'qa = \tau_2 qa$. In similar fashion if $b \in \bar{B}_0$ and $b' \in \bar{B}_1$ it is easily seen that $bb', b'b \notin \bar{B}_0$.

3.3 *If $f \in F$ and $q, q' \in Q$ are such that $\tau fq = \tau_1 q$ and $\tau fq' = \tau_0 q$, then $bf \notin \bar{B}_0 \cup \bar{B}_1$ for any $b \in \bar{B}_0 \cup \bar{B}_1$.*

PROOF: As said before $\tau fq' = \tau_0 q$ is equivalent to the hypothesis that fg' is a certain element, say q_0, of Q. In similar manner, using 3.1, $fq = \tau_1 q$ implies that $\tau fqq = \tau_1 q$ i.e. that $fqq = q_1 \tau_1 q$ where $q_1 \in Q$.

Let $b \in \bar{B}_0$. This implies $bq_0, bq, \in A^*$. Thus $\tau bq_0 = \tau bf^* q' = \tau_0 q'$ and $\tau bfqq = \tau(q_1 \tau_1 q) = \tau_1 q$ showing that $bf \notin \bar{B}_0 \cup \bar{B}_1$.

Let $b \in \bar{B}_1$. This implies $bfq' = bq_0 = q_0' \tau_1 q_0 = q_0' \tau_1 q'$ and $bq_1 = q_1' \tau q_1$ where $q_0', q_1' \in Q$. Thus $\tau bfq' = \tau_1 q'$ and $\tau bfqq = \tau((q_1' \tau q_1)\tau_1 q) = \tau((\tau_1 q_1)\ (\tau_1 q) \neq \tau_1 q$ showing again that $bf \notin \bar{B}_0 \cup \bar{B}_1$ and concluding the proof of 3.3.

This practically ends the verification of our main property. Let $B = (\bar{B}_0 \cup \bar{B}_1) \setminus (\bar{B}_0 \cup \bar{B}_1) X^*$. By construction B is a prefix code. Further, if b and bf are two elements of $\bar{B}_0 \cup \bar{B}_1$, the same must be true of f because of 3 and the fact that if condition (**) is satisfied by bf it is also satisfied by f. Thus $\bar{B}_0 \cup \bar{B}_1 \subset B^*$. Let now $B_0 = \bar{B}_0 \cap B$ and $B_1 = \bar{B}_1 \cap B$. Using the remarks made at the end of 2 we obtain $\bar{B}_0 \subset B_0^*$ and $\bar{B}_1 \subset B_1 \cup B_0^* B_1 \cup B_1 B_0^*$. Thus, by Remark 2 and 3.2, $A = C^p$ where the prefix code $C = B_1 \cup B_0^* B_1$ belongs to J. Finally, taking a word $a \in A$ of the form $a = b^p$ where $b \in B_1$, we have $\tau_i fa = b^i \in C^*$ for all $f \in F$. Thus the parameter p associated with C has value 1, that is, $C \in \mathbf{J}_1$ and the proof is concluded.

IV. AN ALTERNATIVE VERIFICATION OF THE MAIN PROPERTY

A more systematic verification of the main property can be given if one uses the theory of monoids instead of insisting on a self-contained argument as it was done above. It will appear that the main property follows instantly from Remark 1 and Remark 2 once proved the simple Property 2 below.

We recall first without proof some classical results on the minimal ideals of a monoid and some of their more or less obvious consequences. The reader is referred for more details to the existing literature and especially to (Clifford and Preston, 1961).

Let us recall that a homomorphism φ of F onto a quotient monoid is said to be *compatible* with a subset F' of F iff $\varphi^{-1}\varphi F' = F'$. To each $F' \subset F$ one can associate a *maximal compatible homomorphism* $\varphi = \varphi_{F'}$

by the condition that φF is a homomorphic image of $\varphi' F$ for any homomorphism φ' compatible with F' (Teissier, 1951).

Consider now a set $A \subset X^*$ and, letting $A^\dagger = \{1\} \cup A^*$ and $\varphi = \varphi_{A^\dagger}$, assume that the following conditions are satisfied:

$(\mathfrak{U}_d)$. For all $f \in F \backslash A^\dagger$, $fA^\dagger \cap A^\dagger f \cap A^\dagger = \phi$.

$(\mathfrak{R}_d)$. For all $f \in F$, $A^\dagger \cap FfF \neq \phi$.

$(\mathfrak{M}_k)$. φF admits minimal right ideals R_i $(i \in I)$ and minimal left ideals L_j $(j \in J)$.

Let $I' = \{i \in I : R_i \cap \varphi A^\dagger \neq \phi\}$, $J' = \{j \in J : L_j \cap \varphi A \neq \phi\}$ and select arbitrarily a pair of indices—(say $(1, 1)$) in $I' \times J'$. It is classical (Suschkewitsch, 1928) that there exists an isomorphism γ of $R_1 \cap L_1$ onto a group G (which will be identified with a basis of its ring over the integers). Letting $e_{i,j}$ denote the idempotent contained in $R_i \cap L_j$ we define the $J \times I$ matrix Γ by $\Gamma_{j,i} = \gamma(e_{1,j} \cdot e_{i,1})$.

It follows instantly from the hypothesis that there exists an isomorphic representation of φF by pairs of matrices $(\mu f, \nu f)$ where μf (resp. νf) is a $J \times J$ (resp. $I \times I$) matrix with entries in $\{0\} \cup G$, and that one has:

4.1.1. *For all* $f \in F$, $\mu f \cdot \Gamma = \Gamma \cdot \nu f$.

Consider the restriction Γ' of Γ to $J' \times I'$ (i.e., let Γ' be a $J' \times I'$ matrix such that $\Gamma'_{j,i} = \Gamma_{j,i}$ for $j \in J'$, $i \in I'$); let μ' and ν' be the restrictions of μ and ν to $J' \times J'$ and to $I' \times I'$ respectively. There exists a minimal sub-group G' of G that has the following properties:

4.2. *For each* $a \in A^\dagger$, $\mu' a \cdot \Gamma' = \Gamma' \cdot \nu' a$ *and all the entries of* Γ', $\mu' a$ *and* $\nu' a$ $(a \in A^\dagger)$ *belong to* $\{0\} \cup G'$.

4.3. *The only invariant subgroup of* G *contained in* G' *is the trivial subgroup* $\{e\}$ *consisting of the neutral element* e *of* G.

4.4. $A^\dagger$ *consists of all the words* $f \in F$ *such that both* $\mu' f$ *and* $\nu' f$ *have at least one entry in* G'.

It is useful to note that since Γ and Γ' have all their entries in G, 4.1 and 4.2 imply that μf and $\mu' a (a \in A\dagger)$ (resp. νf and $\nu' a$) have one and only one nonzero entry in each row (resp. column).

One can also observe that for $f \in R_i \cap L_j$ the matrix μf (resp. νf) has its jth column (resp. ith row) equal to the ith column (resp. jth row) of Γ multiplied on the right (resp. left) by $\gamma(e_{1,1} \cdot \varphi f \cdot e_{1,1})$. Finally, because of 4.3, one has $G = G'$ iff $G = \{e\}$, that is iff there exists at least one word $a \in A^\dagger$ such that $aFa \subset A^\dagger$.

We assume henceforth that A is a prefix code, i.e., that $A^\dagger$ satisfies the condition

$(\mathfrak{U}_r)$ For all $f \in F \backslash A^\dagger$, $A^\dagger f \cap A^\dagger = \phi$ which is obviously more restric-

tive than $(\mathfrak{U}_d)$. Because of $(\mathfrak{N}_d)$ and $(\mathfrak{M}_k)$, $(\mathfrak{U}_r)$ is equivalent to

$(\mathfrak{N}_r)$ For each $f \in F, fF \cap A^\dagger \neq \phi$ (that is, $I = I'$).

It is known that a consequence of $I' = I$ is that μ gives an isomorphic representation of φF. Thus $\mu^{-1}\mu\, A^\dagger = A^\dagger$ and, for any $b \in \varphi F$, we can write μb instead of the more cumbersome $\mu\varphi^{-1}b$.

On the other hand, we shall see that $\nu^{-1}\nu A^\dagger \subset A'^\dagger$ where A' is a prefix code such that $A \subset A'^*$ and that the following is true.

4.5. $\gamma(R_1 \cap L_1 \cap \varphi A'^\dagger) = G'$ and $J'' = \{j \in J : L_j \cap \varphi A'^\dagger \neq \phi\}$ is the set of all $j \in J$ such that $\Gamma_{j,i} \in G'$ for each $i \in I$.

Proof: By construction $A^\dagger \subset \nu^{-1}\nu A^\dagger$. Since $I' = I$ implies $\nu = \nu'$, the properties 4.1 and 4.2 show directly that $f \in \nu^{-1}\nu A^\dagger$ if all the entries of νf belong to $\{0\} \cup G'$. This proves that the set of all $f \in F$ satisfying this last condition is a submonoid, say $A'^\dagger$, of F having the property 4.5 since then, $L_j \cap \varphi A'^\dagger \neq \phi$ iff $e_{i,j} \in \varphi A'^\dagger$ for each $i \in I$.

For the sake of completeness we verify that $A'^\dagger$ satisfies $(\mathfrak{U}_r)$. Let $f' \in F \backslash A'^\dagger$, i.e. let f be such that, e.g., $(\nu f')_{i,i'} \in G \backslash G'$. Since every matrix νf $(f \in F)$ has one and only one zero entry in each column, it follows that for each $f \in \nu^{-1}\nu A'^\dagger$ one has $(\nu\, \mathrm{ff}')_{i'',i'} \in G \backslash G'$ for at least one $i'' \in I$. Thus $A'^\dagger(F \backslash A'^\dagger) \subset F \backslash A'^\dagger$ and the verification is concluded.

It follows from the properties of φ that $A' = A$ iff ν is an isomorphic representation and that under the present hypothesis $A'^\dagger$ can be defined directly as the set of all $f \in F$ such that $fA^\dagger a \subset A^\dagger$ for at least one $a \in A^\dagger$. Clearly $A'^\dagger = F$ iff A is a.s. synchronizing.

Property 2. If G is an abelian group there exists an a.s. synchronizing code B and an epimorphism $\xi : B^\dagger \to G$ such that $A \subset B^* \cap \xi^{-1}e$.

Proof: Let $L'' = \bigcup \{L_j : j \in J''\}$ and consider an element $b \in \varphi\bar{B}$ where $B = \{f \in F : L''\varphi f \cap L'' \neq \phi\}$. In equivalent manner, consider an element $b \in \varphi\Gamma$ such that $(\mu b)_{j,j'} = u \in G$ for at least one pair $j, j' \in J''$.

For any other $j'' \in J''$ let $j''' \in J$ and $v \in G$ be defined by $(\mu b)_{j'',j'''} = v$. Now, the $(j, 1)$ and the $(j'', 1)$ entries of $\mu b e_{11}$ are respectively equal to u and v since $\mu e_{1,1}$ has all its non zero entries equal to e (and located in its first column). On the other hand, if i'' is defined by $be_{1,1} \in R_{i''}$, these two entries are equal respectively to $\Gamma_{j,i}w$ and $\Gamma_{j'',i}w$ for some $w \in G$. Since $j, j'' \in J''$, and since the hypothesis that G is abelian implies $G' = \{e\}$ (because of 4.3), and consequently $\Gamma_{\bar{j},\bar{i}} = e$ for $\bar{j} \in J''$, $\bar{i} \in I$, we have $\Gamma_{j,i} = \Gamma_{j'',i} = e$. Consequently $u = v = w$. We set $\xi\varphi^{-1}b = u$.

Consider now an arbitrary $i \in I$ and define $i' \in I$ by $b\, e_{i,1} \in R_{i'}$. The same argument shows that the $(j, 1)$ entry, and the $(j'', 1)$ entry

of $\mu b\ e_{i,1}$ are respectively equal on the one hand to $u\Gamma_{j',i}$ and $v\Gamma_{j''',i}$ and on the other hand to $\Gamma_{j,i'}\ w'$ and $\Gamma_{j'',i'}\ w'$ for some $w' \in G$.

Again, $\Gamma_{j',i} = \Gamma_{j'',i} = \Gamma_{j',i'} = e$ and, using $u = v$ shows that $\Gamma_{j''',i} = e$. Since this is true for all $i \in I$, we conclude from 4.5 that $j''' \in J''$. Thus, we have proved that $\bar{B} = \{f \in F : L'' \cdot \varphi f \subset L''\}$.

It is classical (Dubreil, 1953) that this relation implies $\bar{B} = B^\dagger$ where B is a prefix code. Indeed, if $b, b', bb'' \in \varphi\bar{B}$, we have $L'' \cdot bb' = (L''b)b' \subset L''b' \subset L''$ (showing $bb' \in \bar{B}$, hence $\varphi\bar{B}\varphi\bar{B} \subset \varphi\bar{B}$) and $L''b'' \supset (L''b)b'' = L''\ bb'' \subset L''$ (showing $b'' \in \varphi\bar{B}$, hence that $\varphi\bar{B}$ satisfies $\mathfrak{U}_r$).

To complete the verification, we observe that $\varphi F \cdot e_{1,1} \subset \varphi\bar{B}$. Thus $\bar{B}$ is a.s. synchronizing.

Since $L'' \cdot \varphi\bar{B} \subset L''$ and since μ is a representation of F, we have $\xi bb' = \xi b \cdot \xi b'$ for any $b, b' \in \bar{B}$. Finally, $A \subset \bar{B} \cap \xi^{-1}e$ follows from 4.3, $G' = \{e\}$, and $J' \subset J''$.

Let now $A \in \mathbf{J}$. In order to be able to apply Property 2 and Remark 2, we need to show that φF satisfies $(\mathfrak{N}_k)$ and that G is abelian.

Recalling the notations introduced at the beginning of *Section* 2, we define a homomorphism φ' of F by the condition that, for any $f, f' \in F$, $\varphi' f = \varphi' f'$ iff $\tau tf = \tau tf'$ for each $t \in T$. Clearly, φ' is compatible with $A^\dagger$ and, consequently, φF is a homomorphic image of $\varphi' F$. Further, since Card $\tau Tf' \leqq$ Card τTf for any $f \in F$ and $f' \in FfF$ and since Card $\tau Ta \leqq$ deg a for any $a \in A$, the ideal $\varphi' FAF$ of $\varphi' F$ contains no infinite strictly decreasing sequence of one sided ideals. It follows immediately that φF satisfies $(\mathfrak{N}_k)$ and that any group in φFAF is the homomorphic image of at least one group in $\varphi' F$.

We show that any group H' in $\varphi' F$ is a finite cyclic group. Of course, this is equivalent to *Remark 1* but it can also be verified directly as follows.

Let $H = \varphi'^{-1}H'$. The hypothesis that H' is a group is equivalent to the existence of a subset $T' \subset T$ such that $\tau Th = \tau T'h = T'$ for any $h \in H$.

Let $\varphi' h'$ $(h' \in F)$ be the neutral element of H'. We have $t = \tau th'$ for every $t \in T'$. Thus $h' \in FAF$ and, by $\mathfrak{N}_j$, T' is a set of $r < \infty$ right factors of h'. Further $\tau T'h = T'$ for $h \in H$, implies that $r =$ Card $\tau T'f$ for each $f \in K = \{f' \in F : F'F \cap H \neq \emptyset\}$. Thus, for $f \in K$, we can index the r elements of T' and $\tau T'f$ by increasing degree and define a permutation $\gamma' f : i \to i'$ of $[1, r]$ by the identical relation $\tau t_i f = t'_{i'}$, $(t'_{i'} \in \tau T'f)$. Clearly, $\gamma' ff' = \gamma' f \gamma' f'$ when $ff' \in H$ and H' is isomorphic to $\gamma' H$. Since T' is a set of right factors of h', a straightforward application of $\mathfrak{N}_{r_j}$

shows that $\gamma' f$ is a cyclic permutation when $f \in X \cap K$ and the verification is concluded.

RECEIVED: June 7, 1963

REFERENCES

CHEN, K. T., FOX, R. H., AND LYNDON, R. C. (1958), Free differential calculus. *Ann. Math.* **68,** 82–86.

CLIFFORD, A. H., AND PRESTON, G. B. (1961), The algebraic theory of semi groups. Math. Surveys of the Am. Math. Soc., Providence, R. I.

DAVID, F. N., AND BARTON, R. A. (1962), "Combinatorial Chance." (London).

DUBREIL, P., (1953), Contributions à la théorie des demi-groupes III. *Bull. Soc. Math. France* **81,** 289–306.

FELLER, W., (1958), "An Introduction to Probability Theory and Its Applications," Chap. 13, sect. 7 and 8. Wiley, New York.

LUCAS, E. (1891), "Théorie des Nombres," pp. 501–503. Gauthiers Villars, Paris.

MANDELBROT, B., (1957), "Linguistique Statistique Macroscopique en Logique, Language et Théorie de l'Information," by L. Apostel, B. Mandelbrot, and A. Morf. P.U.F., Paris.

MANDELBROT, B., (1961), On the theory of word frequences and on related Markovian models of discourse, *in* "Structure of language and its mathematical aspects," *Twelfth Symp. Appl. Math.*, Am. Math. Soc., Providence, Rhode Island.

NEUMAN, P. G. (1962), Efficient error limiting codes. *IRE Trans. Inform. Theory* **8,** 292–304.

NEUMAN, P. G. (1962), On a class of efficient error limiting codes. *IRE Trans. Inform. Theory.* **8,** 260–266.

NEUMAN, P. G. (1963), On error limiting variable length codes. *IRE Trans. Inform. Theory* **9,** p. 209.

SUSCHKEWITSCH, A. (1928), Ueber die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit. *Math. Ann.* **99,** 30–50.

TEISSIER, M. (1951), Sur les équivalences régulières dans les demi groupes. *C. R. Acad. Sci.* **232,** 1987–1989.

WINOGRAD, S. (1962), Bounded transient automata. *Proc. A.I.E.C. 3rd Switching Theory and Logical Design*, pp. 138–141.

WINOGRAD, S. (1963), Input error limiting automata. IBM Res. Rept. RC 966.

SUR CERTAINES CHAINES DE MARKOV NON HOMOGÈNES

J. LARISSE et M. P. SCHÜTZENBERGER

Extrait de
PUBLICATIONS DE L'INSTITUT DE STATISTIQUE DE L'UNIVERSITÉ DE PARIS
Vol. XIII - fascicule 1 - 1964

SUR CERTAINES CHAINES DE MARKOV NON HOMOGÈNES

par J. LARISSE et M. P. SCHÜTZENBERGER

Soit donnée une chaîne de Markov non-homogène sur un ensemble *fini* d'états I, c'est-à-dire, soit donnée une représentation μ d'un monoïde libre F dans le monoïde M des I×I matrices stochastiques. Pour chaque $f \in F$, le sous-monoïde $\{ \mu f^n : n \in \underset{\sim}{N} \}$ de M est une chaîne de Markov finie au sens habituel ; si μf appartient au sous-ensemble M_r de M des I×I matrices stochastiques ayant exactement r racines caractéristiques de module unité, (c'est-à-dire si la chaîne de Markov $\{ \mu f^n : n \in \underset{\sim}{N} \}$ a exactement r classes ergodiques), la matrice $\mu f^{r!} = (\mu f)^{r!}$ est apériodique et, par conséquent, $\lim_{k \to \infty} \mu f^{kr!+1}$ existe. C'est une matrice stochastique que l'on désignera par $\bar{\mu} f$ et qui appartient au sous-ensemble $\overline{M}_r \subset M_r$ des matrices n'ayant que des racines nulles ou de module unité et dont les puissances successives forment un groupe fini.

D'autre part, la donnée de μ détermine de façon univoque un homomorphisme ω de F dans le groupe additif des réels tel que pour chaque générateur x de F on ait :
ωx = la borne inférieure des entrées positives de μx si celles-ci ne sont pas toutes égales à un et $\omega x = 0$ dans le cas contraire (c'est-à-dire si μx est un élément du sous-monoïde P de M constitué par les matrices représentant des applications de I dans lui-même).

Pour simplifier, on fera l'hypothèse qu'il existe une valeur *positive* $\bar{\omega}$ tel que $\omega x > \bar{\omega}$ ou $= 0$ pour tout générateur x et on po-

sera $F_z = \{ f \in F : \omega f > z \}$ pour chaque valeur réelle z (ce qui entraîne donc $\mu f \in P$ pour tout $f \in F \backslash F_o$). Avec ces notations, il résulte d'un théorème récent de J. Wolfowitz [1] (1) que si $\mu f \in M_1$ pour tout $f \in F_o$ on a : (W_1). $0 = \lim_{z \to \infty} \text{Max} \{ \| \mu f_1 f_2 - \bar{\mu} f_2 \| : f_1 \in F \ ; \ f_2 \in F_z \}$, où la norme $\| m \|$ d'une $I \times I$ matrice quelconque m est $\text{Max}_{i \in I} \sum_{i' \in I} | m_{i,i'} |$.

On se propose ici de vérifier en application de ce théorème que s'il existe un entier r tel que $\mu f \in M_r$ pour tout $f \in F_o$, on peut trouver une application π de F dans un sous-ensemble *fini* de M telle que l'on ait :

(W_r). $0 = \lim_{z \to \infty} \text{Max} \{ \| \mu f_1 f_2 f_3 - \bar{\mu} f_1 . \pi f_2 . \bar{\mu} f_3 \| : f_2 \in F \ ; \ f_1, f_3 \in F_z \}$.

Si toutes les matrices μf $(f \in F_o)$ satisfont la condition plus forte d'appartenir à M_r et d'avoir r racines égales à un, (c'est-à-dire si toutes les chaînes $\{ \mu f^n : n \in \underset{\sim}{N} \}$ $(f \in F_o)$ sont apéridiques), l'introduction de π est inutile et l'on peut écrire :

(W_r^*) : $0 = \lim_{z \to \infty} \text{Max} \{ \| \mu f_1 f_2 f_3 - \bar{\mu} f_1 . \bar{\mu} f_3 \| : f_2 \in F \ ; \ f_1, f_3 \in F \}$.

Nous ne sommes pas en mesure d'apprécier ici la signification éventuelle de ces relations dans la théorie générale des "automates probabilistes" de M. Rabin [2].

Vérification de la propriété

Nous supposons la représentation μ donnée et telle que $\{ \mu f : f \in F_o \} \subset M_r$. Le *support* (ou *type* [1]) d'une matrice $m \in M$ est l'ensemble $\beta m \in \mathfrak{P}(I \times I)$ des paires $(i, i') \in I \times I$ telles que $0 \neq m_{i,i'}$, le support de la i-ième ligne de m étant désigné par $\beta_i m = \{ i' \in I : (i, i') \in \beta m \}$. Pour $m, m' \in M$, le *produit* $\beta m . \beta m'$ des supports βm et $\beta m'$ est, comme d'usage (cf. [3]), l'ensemble des paires $(i, i'') \in I \times I$ telles que $(i, i') \in \beta m$ et $(i', i'') \in \beta m'$ pour au moins un $i' \in I$. Donc,

---

(1) Nous remercions le Professeur Wolfowitz d'avoir bien voulu nous communiquer son travail avant sa publication.

$\beta mm' = \beta m . \beta m'$ et on peut considérer β comme un homomorphisme du monoïde $\{ \mu f : f \in F \}$ dans le sous-monoïde de $\mathfrak{P}(I \times I)$ constitué par tous les supports βm tels que $\beta_i m \neq \emptyset$ pour chaque $i \in I$.

Il résulte immédiatement de ceci que pour $m, m' \in M$ et $i, i' \in I$ on a :

si $\beta_i m$ est un élément minimal de la famille $\{ \beta_j m : j \in I \}$ ordonnée par inclusion, $\beta_i mm'$ est un élément minimal de la famille $\{ \beta_j mm' : j \in I \}$;

si $\beta_i mm' \cap \beta_{i'} mm' = \emptyset$, alors, d'une part $\beta_i m \cap \beta_{i'} m = \emptyset$, d'autre part $\beta_j m' \cap \beta_{j'} m' = \emptyset$ pour tout $j \in \beta_i m$ et $j' \in \beta_{i'} m$.

Nous dirons que βm est *cyclique* si $\beta m = \beta m^{2+n}$ pour au moins un $n \in \mathbb{N}$ (et par conséquent pour une infinité de $n \in \mathbb{N}$). On sait que quelque soit $m \in M$, βm^n est cyclique pour $n \geqslant (\mathrm{Card}\ I)!$.

Il est clair que la propriété pour une matrice $m \in M$ d'avoir ou non r racines de modules unité, ainsi que la valeur de ces racines dépend exclusivement de son support βm. De la même façon si $m \in M_r$, et si $\overline{m} = \lim_{k \to \infty} m^{kr!+1}$, le support $\beta \overline{m}$ ne dépend que du support βm. Plus précisément, $\mu f \in M_r$ si la chaîne de Markov $\{ \mu f^n : n \in \mathbb{N} \}$ a exactement r classes ergodiques auxquelles on réservera la notation $I_1^*(f)$, $I_2^*(f)$, ..., $I_r^*(f)$ en posant $I^*(f) = \cup \{ I_j^*(f) : j \in [1,r] \}$. On sait que si $\mu f \in M_r$, la restriction à $I_j^*(f) \times I$ du support de μf est contenue dans un "rectangle" $I_j^*(f) \times I_{j'}^*(f)$ (Cf. [3]) et qu'elle est égale à ce rectangle si $\beta \mu f$ est cyclique. De même la restriction à $I \times I^*(f)$ du support de μf est contenue dans $\beta \bar{\mu} f$ et $\beta \bar{\mu} f$ est égale à la restriction à $I \times I^*(f)$ du support de μf quand $\beta \mu f$ est cyclique.

Ces notions étant rappelées, définissons R comme la fermeture convexe du sous-ensemble $P_r \subset P$ des matrices représentant une application $I \to I$ telle que l'image Ip de I ait au plus r éléments. A chaque $f \in F$ nous associons $\chi f \in [0,1]$, $\mu_R f \in R$ et $\mu_R' f \in M$ par les relations suivantes :

$\mu f = (1 - \chi f) . \mu_R f + \chi f . \mu'_R f$;

$\chi f = \text{Min} \{ \chi \in [0,1] : \mu f = (1 - \chi) . m + \chi . m' ; m \in R, m' \in M \}$.

Enfin, nous désignons par F_+ l'ensemble des $f \in F$ tel qu'il existe au moins un $g \in F_0$ de support cyclique et une paire $f', f'' \in F$ satisfaisant $\beta\mu f = \beta\mu f' g f''$.

REMARQUE 1. Pour chaque $f \in F_+$ *on a* $\chi f < 1$ *et* $\beta\mu_R f \subset \beta\bar{\mu} f$.

Vérification. Il est clair que $PP_r P \subset P_r$ et que le support de tout $m \in M$ est une union de supports d'applications $p' \in P$. Il en résulte immédiatement que $\chi ff' \leqslant \chi f . \chi f'$ pour tout $f, f' \in F$.

Considérons $g \in F_0$ de support cyclique. Si $I' \subset I$ a un et un seul élément en commun avec chacune des classes ergodiques $I_j^*(g)$, le fait que pour chaque $i \in I$ la ligne $\beta_i \mu g$ contienne au moins un $I_i(g)$ montre qu'il existe au moins un $p \in P_r$ tel que $I' = Ip$ et $\beta p \subset \beta\mu f$. Donc $\chi g < 1$ et par conséquent $\chi f' g f'' < 1$ pour tout $f', f'' \in F$. Comme la propriété $\chi m < 1$ ne dépend en fait que de βm, l'inégalité $\chi f < 1$ pour $f \in F_+$ est établie.

Soit maintenant $\beta p \subset \beta\mu f$ où $p \in P_r$ et $f \in F$. Si $I' = Ip$, l'union des supports des colonnes de μf d'indice $i \in I'$ est égale à I, et il en est de même pour toute matrice de la forme $\mu f' f$. Prenant $f' = f^n$ tel que $\beta\mu f' f$ soit cyclique, on en conclut que I' doit avoir un (et un seul) élément en commun avec chacune des classes ergodiques $I_j^*(f)$ et qu'en particulier $I' \in I^*(f)$. Comme $\beta p \subset \beta\mu f$ et comme la restriction de $\beta\mu f$ à $I \times I^*(f)$ est contenue dans $\beta\bar{\mu} f$, la remarque est entièrement vérifiée.

Il résulte de $\beta\mu f \subset \beta\bar{\mu} f$ que chaque classe $I_j^*(f)$ admet un sous-ensemble minimal $I_j'^*(f)$ tel que $I^*(f) \times I_j'^*(f)$ contienne la restriction à $I^*(f) \times I_j^*(f)$ du support de $\mu_R f$. De même, il existe un sous-ensemble maximal $I_j''^*(f)$ contenant tous les $i \in I$ tels que $\beta_i \mu_R f \subset I_j''^*(f)$.

REMARQUE 1 bis. *Si* $f, f' \in F_+$ *il correspond à chaque* $j \in [1,r]$ *un et un seul* $j' \in [1,r]$ *tel que* $I_j^{*}(f) \subset I_{j'}^{*}(f')$.

Vérification. Soit pour $m \in M$, $\Delta(m)$ la cardinalité maximale d'un ensemble de lignes de m ayant leurs supports deux à deux disjoints. On vérifie facilement que pour tout m, $m' \in M$ on a $\Delta(mm') \leqslant \Delta(m)$, $\Delta(m')$. Donc, si $f \in F_+$, on a $\Delta(\mu f) \leqslant r$ puisque $\beta\mu f$ admet $\beta\mu g$ comme facteur et $\Delta(\mu f) = r$ puisque $\Delta(\mu f) = r$ pour $n \geqslant (\underset{\sim}{\text{Card}}\ I)!$.

Considérons maintenant le cas particulier de l'énoncé où $\beta\mu f$ et $\beta\mu f'$ sont cycliques. La relation $\Delta(\mu ff') = r$ montre que pour chaque $i \in I_j^{*}(f)$, le support $\beta_i \mu f'$ doit avoir une intersection non vide avec une seulle classe $I_{j'}^{*}(f)$. Le cas général s'en déduit immédiatement : en effet, $I_j^{'*}(f) \subset I_j^{*}(f)$ et les seuls $i \in I$ tels que $\beta_i \mu f'$ n'intersecte qu'une seule classe $I_{j'}^{*}(f')$, appartiennent à l'union $I^{**}(f')$ des ensembles disjoints $I_j^{**}(f')$.

Nous écrivons désormais pour abréger Lim au lieu de $\lim_{z \to \infty}$ Max et nous désignons par f_z et f_z' des variables liées par la condition $f_z, f_z' \in F_z$.

REMARQUE 2. $\operatorname{Lim} \| \mu f_z - \mu_R f_z \| = 0$.

Vérification. Soit $B = \{ \beta\mu f : f \in F_o \}$. Si un élément $b \in B$ appartient à une $\mathcal{D}$-*classe régulière* ([4]), il existe un élément $b' \in B$ tel que $b'^2 = b'$ et $b'b = b$. Donc si B_+ est l'idéal de B engendré par les $\mathcal{D}$-classes régulières, l'image inverse de B par β^{-1} appartient à F_+.

Soit h le nombre des $\mathcal{D}$-classes de B. Nous montrons d'abord que tout produit $b_1 b_2 \ldots b_{\bar{h}}$ de $\bar{h} = 2^{h-1}$ éléments de B a au moins un facteur droit non vide $b_{k'} b_{k'+1} \ldots b_{\bar{h}}$ appartenant à une $\mathcal{D}$-classe régulière de B. Ceci est trivial pour $h = 1$ puisque dans ce cas B a une seule $\mathcal{D}$-classe qui est nécessairement régulière. On peut donc supposer le résultat vérifié quand B a moins de $h > 1$ $\mathcal{D}$-classes et, naturellement, on peut aussi supposer qu'aucun des $b_{k'}$ $(k' = 1, 2, \ldots, \bar{h} = 2^{h-1})$

n'appartient lui-même à une $\mathcal{D}$-classe régulière. Comme toutes les $\mathcal{D}$-classes considérées sont finies, ceci entraîne ([5]) que pour chaque $k' < \bar{h}$ les trois éléments $b_{k'}, b_{k'+1}$ et $b_{k'}b_{k'+1}$ n'appartiennent pas à la même $\mathcal{D}$-classe. Donc le sous-monoïde engendré par les 2^{h-2} produits $b_1b_2, b_3b_4, \ldots, b_{\bar{h}-1}\, b_{\bar{h}}$ a au plus h-1 $\mathcal{D}$-classes et le résultat découle de l'hypothèse d'induction.

Soit maintenant $F_+^! = F_+ \setminus (F_+)^2$. Le résultat qui vient d'être vérifié montre que tout $f \in (F_o)^{n\bar{h}}$ a au moins n facteurs dans $F_+^!$. En outre, faisant intervenir l'hypothèse selon laquelle $\omega x = 0$ ou $\omega x > \bar{\omega} > 0$ pour tout $x \in X$, on voit que $\omega f > 1 - \bar{\omega}^{\bar{h}}$ pour tout $f \in F_+^!$. Donc $\chi f < (1 - \bar{\omega}^{\bar{h}})^n$ pour chaque $f \in (F_o)^{n\bar{h}}$ ce qui entraîne $\operatorname{Lim} \chi f_z = 0$ et achève la vérification de la remarque 2.

Soit V l'ensemble des I-vecteurs v à coordonnées non négatives tels que $\sum_{i\in I} v_i = 1$. Pour $(v, v') \in V \times V$ et $m \in M$ nous posons : $\delta_{v,v'}.m = 1 - \sum_{i\in I} \operatorname{Min}\{(vm)_i, (v'm)_i\}$. D'après Hajnal ([6]), pour tout $m' \in M$ on a : $0 \leqslant \delta_{v,v'}.mm' \leqslant \delta_{v,v'}.m \leqslant 1$ avec $\delta_{v,v'}.m = 0$ (resp. = 1) si et seulement si $vm = v'm$ (resp. $\beta vm \cap \beta v'm = \phi$). Quand μ et μ' sont deux applications de F dans M telles que : $\operatorname{Lim} \| \mu f_z - \mu' f_z \| = 0$ on a évidemment $\operatorname{Lim} | \delta_{v,v'}.\mu f_z - \delta_{v,v'}\mu' f_z | = 0$.

Nous considérons maintenant un sous-ensemble fixe K de I ayant r éléments et nous définissons la I×I matrice e_K par $(e_K)_{i,i'} = 1$ si $i = i' \in K$; = 0, autrement. Pour abréger, nous écrivons $m' \in M'$ (resp. $m'' \in M''$) si $m' = m.e_K$ (resp. $m'' = e_K.m$ pour au moins un $m \in M$) et si m' contient r lignes ayant des supports disjoints telles que toute autre ligne soit une combinaison linéaire à coefficients non négatifs de ces dernières (resp. et si m'' a r lignes ayant des supports disjoints non vides.).

REMARQUE 3. Il existe deux applications $\mu' : F \to M'$ *et* $\mu'' : F \to M''$ *telles que* $\operatorname{Lim} \| \mu f_z - \mu' f_z . \mu'' f_z \| = 0$.

Vérification : Nous utilisons les notations de la Remarque 1 bis. Le support de la restriction de $\mu_R f_z$ à $I''^*(f_z)\times I$ est une union de r rectangles disjoints $I''_j(f_z)\times I'_{j'}(f_z)$. Comme $\mu_R f_z$ appartient à la fermeture convexe R de P_r ceci entraîne que deux lignes quelconques de cette matrice soient égales quand l'intersection de leurs supports n'est pas vide. Il existe donc une matrice $\mu''f_z \in M''$ dont les lignes non nulles sont égales aux r lignes distinctes de la restriction de $\mu_R f_z$ à $I''^*(f_z)\times I$.

Soit f'_z un autre élément de F_z. D'après la Remarque 1 bis, chacun des ensembles $I'^*_{j'}(f')$ est contenu dans un et un seul ensembles $I''^*_j(f_z)$ et $\mu_R f'_z$ est identique à la somme de ses restrictions à $I\times I'^*_{j'}(f_z)$ ($j' \in [1,r]$). Donc deux lignes quelconques non nulles de la restriction à $I\times I'_j(f_z)$ de $\mu_R f'_z . \mu_R f_z$ sont proportionnelles et l'on peut trouver une application $\upsilon' : F\times F \to M'$ telle que l'on ait $\mu_R f'_z . \mu_R f_z = \upsilon'(f'_z, f_z) . \mu' f_z$ identiquement. D'après la Remarque 2, $\operatorname{Lim} \| \mu f'_z f_z - \mu_R f'_z \| = 0$. Par conséquent, $\operatorname{Lim} \| \mu f'_z f_z - \upsilon'(f'_z, f_z).\mu' f_z \| = 0$ ce qui entraîne la validité de la Remarque 3.

REMARQUE 3 bis. Si les applications $\mu' : F \to M'$; $\upsilon : F\times F\times F \to M$ et $\mu'' : F \to M''$ *satisfont la relation* $\operatorname{Lim} \| \mu f_z f f'_z - \mu' f_z . \upsilon(f_z, f, f'_z) . \mu'' f'_z \| = 0$, *il existe trois applications* $\bar\mu' : F \to M'$; $\rho : F\times F\times F \to M''$ et $\bar\mu'' : F \to M''$ *telles que :*

$\operatorname{Lim} \| \mu' f_z - \bar\mu' f_z f f'_z \| = \operatorname{Lim} \| \upsilon(f_z, f, f'_z) - \rho(f_z, f, f'_z) \| =$

$\operatorname{Lim} \| e_K . \upsilon(f_z, f, f'_z) . \mu'' f_z - \bar\mu'' f_z f f'_z \| = 0$, *et qu'en outre, d'une part la restriction de* $\rho(f, f, f')$ à $K\times I$ *représente une permutation de* K, *d'autre part, pour tout* $f' \in F_o$, $\bar\mu f' = \bar\mu' f' . \bar\mu'' f'$.

Vérification. L'existence d'applications $\bar\mu' : F \to M'$ et $\bar\mu'' : F \to M''$ satisfaisant l'identité $\bar\mu f' = \bar\mu' f' . \bar\mu'' f'$ est triviale et il est clair que toutes les paires d'applications satisfaisant ces conditions sont équivalentes sur F_o à une permutation de K près.

Désignons maintenant par $\lambda^i m$ la plus grande entrée de la i-ème colonne de m. Il est bien connu que $\lambda^i m'm < \lambda^i m$ identiquement. Donc pour tout $i \in I$ et $(f_z, f, f'_z) \in F \times F \times F$ on a $\lambda^i \bar{\mu} f_z f f'_z = \lambda^i \bar{\mu}'' f_z f f'_z \leqslant \lambda^i \mu f_z f f'_z$ et

$\lambda^i(\mu' f_z . \upsilon(f_z, f, f'_z) . \mu'' f'_z) \leqslant \lambda^i(\upsilon'(f_z, f, f'_z) . \mu'' f'_z) \leqslant \lambda^i \mu'' f'_z$.

Les hypothèses impliquent

$$\text{Lim} \parallel \lambda^i(\mu' f_z . \upsilon(f_z, f, f'_z) . \mu'' f'_z) - \lambda^i \mu f_z f f'_z \parallel = 0$$

et, comme $\bar{\mu} f_z f f'_z$ et $\mu'' f'_z$ appartiennent à M'', on a $\sum_{i \in I} \lambda^i \bar{\mu}'' f_z f f'_z = \sum_{i \in I} \lambda^i \mu'' f'_z = r$. Donc, pour chaque $i \in I$, $\text{Lim} | \lambda^i \bar{\mu}'' f_z f f'_z - \lambda^i (\upsilon(f_z, f, f'_z) . \mu'' f') | = \text{Lim} | \lambda^i (\upsilon(f_z, f, f'_z) . \mu'' f'_z) - \lambda^i \mu'' f'_z | = 0$ et $\text{Lim} \sum_{i \in I} \lambda^i (\upsilon(f'_z, f, f'_z) . \mu'' f'_z) = r$ ce qui montre l'existence de $\rho : F \times F \times F \to M$, identique à υ sur $(I \backslash K) \times I$, se réduisant à une permutation de K sur $K \times I$ et satisfaisant $\text{Lim} \parallel \upsilon(f_z, f, f'_z) - \rho(f_z, f, f'_z) \parallel = 0$. D'après la première de ces relations on peut choisir $\bar{\mu}'' : F \to M''$ telle que $\text{Lim} \parallel e_K . \rho(f_z, f, f'_z) . \mu'' f'_z - \bar{\mu}'' f_z f f'_z \parallel = 0$. Ceci établit la partie de la remarque concernant les applications $\bar{\mu}''$ et ρ.

De façon analogue, pour tout $(v, v') \in V \times V$ on a :

$\delta_{v,v'} \bar{\mu}' f_z f f'_z = \delta_{v,v'} \bar{\mu} f_z f f'_z \leqslant \delta_{v,v'} \mu f_z f f'_z$ et $\text{Lim} \ \delta_{v,v'} \mu f f' < \text{Lim} \ \delta_{v,v} \mu f_z$.

Comme l'ensemble des $(v, v') \in V \times V$ telles que $\delta_{v,v'} \bar{\mu}' f_z f f'_z$ (resp. $\delta_{v,v'} \mu' f_z$) est 0 ou 1 détermine $\bar{\mu}'$ (resp. μ') à une permutation près de K et comme le support de la restriction de $\mu f_z f f'_z$ à $I \times I^*(f, f f'_z)$ est contenu dans $\beta \bar{\mu} f_z f f'_z$, la vérification est achevée.

PROPRIETE 1 : Si $\mu : F \to M$ est telle que pour chaque $f \in F_o$ la chaine de Markov $\{ \mu f^n : n \in N \}$ a exactement r classes ergodiques, il existe une application π de F dans un sous ensemble fini de M telle que :

$$(W_r) \ . \ \text{Lim} \parallel \mu f_z f f'_z - \bar{\mu} f_z . \pi f . \bar{\mu} f'_z \parallel = 0.$$

Si en outre toutes les chaines $\{ \mu f^n : n \in \underset{\sim}{N} \}$ $(f \in F_o)$ sont apériodiques, on peut écrire :

$$(W_r^*) . . \ \text{Lim} \parallel \mu f_z f f'_z - \bar{\mu} f_z . \bar{\mu} f'_z \parallel = 0.$$

Vérification. D'après la Remarque 3, il existe deux applications $\mu' : F \to M'$ et $\mu'' : F \to M''$ telles que $\mathrm{Lim} \| \mu f_z - \mu' f_z . \mu'' f_z \| = 0$.

Prenant une application υ de $F \times F \times F$ sur la matrice unité e_I et employant la Remarque 3 bis, ceci montre que $\mathrm{Lim} \| \bar{\mu} f_z - \mu f_z \| = 0$ et qu'il n'y a aucune diminution de généralité à supposer désormais que $\mu' = \bar{\mu}'$ et $\mu'' = \bar{\mu}''$, c'est-à-dire que $\mu' f . \mu'' f = \bar{\mu} f$ pour tout $f \in F_0$. Le premier de ces résultats donne

$$\mathrm{Lim} \| \mu f_z f f'_z - \bar{\mu} f_z . \mu f . \bar{\mu} f'_z \| = \mathrm{Lim} \| \bar{\mu} f_z f f'_z - \bar{\mu} f_z . \mu f . \bar{\mu} f'_z \| = 0 .$$

Comme $\bar{\mu} f_z . \mu f . \bar{\mu} f'_z = \mu' f_z . \upsilon(f_z, f, f'_z) . \mu'' f'_z$ où maintenant υ est une application quelconque de $F \times F \times F$ dans M telle que $e_K . \upsilon(f_z, f, f') = \mu'' f . \mu f . \mu' f'$, on peut appliquer de nouveau la Remarque 3 bis qui montre cette fois l'existence d'une application ρ de $F \times F \times F$ dans M telle que $e_K . \rho$ soit une permutation de K et que $\mathrm{Lim} \| \mu'' f_z . \mu f . \mu' f'_z - e_K . \rho(f_z, f, f'_z) \| = 0$. D'après l'hypothèse faite plus haut, $\mu' f_z . \mu'' f_z = \bar{\mu} f_z$ et $\mu' f'_z . \mu'' f'_z = \bar{\mu} f'_z$. On en conclut que $\mu'' f_z . \mu f . \mu' f'_z$ est elle-même, pour tout $(f_z, f, f'_z) \in F \times F \times F_0$, une matrice ayant son support contenu dans $K \times K$ et représentant une permutation de cet ensemble.

Puisque les matrices $\mu' f_z$, μf et $\mu' f'_z$ ont des entrées non négatives, ceci entraîne $\mu'' f_z . \mu f . \mu' f'_z = \mu' f_z . \pi f . \mu' f'_z$ quelque soit l'application $\pi : F \to M$ telle que $\beta \mu f = \beta \pi f$. Par conséquent, sous cette hypothèse $\bar{\mu} f_z . \mu f . \bar{\mu} f'_z = \bar{\mu} f_z . \pi f . \bar{\mu} f'_z$ ce qui achève la vérification de (W_r) puisque le monoïde $\{ \beta \mu f : f \in F \}$ est fini.

Supposons maintenant que toutes les chaînes $\{ \mu f^n : n \in \mathbb{N} \}$ soient apériodiques, c'est-à-dire que $\bar{\mu} f = \bar{\mu} f^2$ pour tout $f \in F_0$, c'est-à-dire encore, (dans les notations de la Remarque 2 bis) que $I'^*_j(f) \subset I^{**}_j(f)$ pour tout $j \in [1, r]$. La Remarque 2 bis montre que l'on peut choisir l'indexage des classes ergodiques des différentes chaînes $\{ \mu f^n : n \in \mathbb{N} \}$ $(f \in F_0)$ de telle sorte que $I^*_j(f) \subset I^{**}_j(f')$ pour tout $f, f' \in F_x$ et $j \in [1, r]$. Ceci entraîne que $\mu'' f_z . \mu' f'_z = e_K$ identiquement quand $f_z, f'_z \in F_+$. La propriété est entièrement vérifiée.

REFERENCES

[1]. J. WOLFOWITZ : Products of indecomposable, aperiodic stochastic matrices, Proc. Amer. Math. Soc. *14*, (1963) : 733-737.

[2]. M. O. RABIN : Probabilistic Automata, Information and Control *6*, (1963) : 230-245.

[3]. J. RIGUET : Relations binaires, fermetures, correspondances de Galois, Bull. Soc. Math. France, *76*, (1948) : 114-155.

[4]. D. D. MILLER and A. H. CLIFFORD : Regular $\mathcal{D}$-classes in semi-groups, Trans. Amer. Math. Soc., *82*, (1956) : 270-280.

[5]. J. A. GREEN : On the structure of semi-groups, Ann. of Math. *54*, (1951) : 163-172.

[6]. J. HAJNAL : Weak ergodicity in non-homogeneous Markov chains, Proc. Cambridge Philos. Soc., *54*, (1958) : 233-246.

Cetis Euratom (Ispra)

et Faculté des Sciences (Poitiers)

Reçu le 22 décembre 1963

Année 1965

Bibliographie

[1] Marcel-Paul Schützenberger. Sur certains sous-monoïdes libres. *Bull. Soc. Math. France*, 93 :209–223, 1965.

[2] Marcel-Paul Schützenberger. Sur les monoïdes finis n'ayant que des sous-groupes triviaux. In *Séminaire Dubreil-Pisot, année 1964-65*, Exposé 10, 6 pages. Inst. H. Poincaré, Paris, 1965.

[3] Marcel-Paul Schützenberger. Sur une question concernant certains sous-monoïdes libres. *C. R. Acad. Sci. Paris*, 261 :2419–2420, 1965.

[4] Marcel-Paul Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8 :190–194, 1965.

[5] Marcel-Paul Schützenberger. A remark on incompletely specified automata. *Information and Control*, 8 :373–376, 1965.

[6] Marcel-Paul Schützenberger. On a factorisation of free monoids. *Proc. Amer. Math. Soc.*, 16 :21–24, 1965.

[7] Luigi Petrone and Marcel-Paul Schützenberger. Sur un problème de McNaughton. manuscrit, 12 pages, 1965. Euratom.

[8] Marcel-Paul Schützenberger. Codes à longueur variable, 1965. Lecture held in 1965, at a seminar in Royan, also published in École de printemps "Théorie des codes", 1979, p. 247–271.

[9] Marcel-Paul Schützenberger. On the algebraic theory of automata. In Wayne A. Kalenich, editor, *Information Processing 65 : Proceedings of IFIP Congress 1965*, pages 27–29. Spartan Books, 1965.

Bull. Soc. math. France,
93, 1965, p. 209 à 223.

(Au Professeur A. D. Wallace, en hommage respectueux)

SUR CERTAINS SOUS-MONOÏDES LIBRES ;

PAR

Marcel Paul SCHÜTZENBERGER.

Soit A une partie finie non vide fixe du monoïde libre X^* engendré par l'ensemble fini X. Nous supposerons toujours que A satisfait les deux conditions suivantes :

($\mathfrak{U}'_d$). *A engendre librement un sous-monoïde de X^*.*
(C'est-à-dire qu'il existe un ensemble Y et une bijection de Y sur A pouvant être étendue à un monomorphisme dans X^* du monoïde libre engendré par Y.)

($\mathfrak{R}'_d$). *A est maximal parmi les parties de X^* qui satisfont* ($\mathfrak{U}'_d$).

La première condition équivaut à l'hypothèse que chaque mot de X^* a au plus une factorisation comme produit de mots de A, et nous aurons à considérer les conditions plus restrictives :

($\mathfrak{U}'_r$) [resp. ($\mathfrak{U}'_l$)]. *Chaque mot de X^* a au plus un facteur gauche* (resp. *droit*) *dans A.*

On verra plus loin que ($\mathfrak{U}'_d$) et ($\mathfrak{R}'_d$) entraînent l'existence d'un polynôme $T \in \mathbf{Z}[X]$ tel qu'on ait

$$(\bigstar) \qquad 1 - \sum_{a \in A} \alpha a = \left(1 - \sum_{x \in X} \alpha x\right) T,$$

où α dénote l'homomorphisme naturel de X^* dans le monoïde multiplicatif de l'anneau $\mathbf{Z}[X]$. On peut vérifier que l'ensemble $\mathfrak{S}$ des polynômes T associés aux parties finies A, qui satisfont ($\mathfrak{U}'_r$) [ou ($\mathfrak{U}'_l$)] et ($\mathfrak{R}'_d$), est la plus petite famille de polynômes contenant 1 qui soit telle que

$$\sum_{x \in X} \alpha x . T_x \in \mathfrak{S}$$

pour toute application $x \to T_x$ de X dans $\mathfrak{S} \cup \{0\}$. Ceci indique que les polynômes de $\mathfrak{S}$ n'ont « en général » aucune propriété remarquable de factorisation et motive la proposition suivante dont la vérification est le but de cette note :

PROPOSITION. — *Si le polynôme T défini par $(\bigstar)$ est irréductible sur $\mathbf{Z}[X]$, alors A satisfait $(\mathfrak{U}'_r)$ ou $(\mathfrak{U}'_l)$.*

Le lecteur pourra trouver dans [4] une étude des notions utilisées ici d'un point de vue qui donne une interprétation un peu différente de cette proposition.

Résultats préliminaires. — Soit

$$K = \{k_1, k_2, \ldots, k_n\} = \{f \in X^*; fXX^* \cap A \neq \emptyset\}$$

l'ensemble des facteurs propres gauches des mots de A, les indices étant choisis de telle sorte que k_i soit un facteur gauche de k_j seulement si $i \leqq j$, ce qui implique que k_1 soit l'élément neutre e de X^*.

(1). — *Il existe une représentation μ de X^* par des $n \times n$-matrices ayant les propriétés suivantes :*

(1.1) *Quel que soit $f \in X^*$, tous les éléments de μf appartiennent à $\{0, 1\}$ et*

$$A^* = \{f \in X^*; (\mu f)_{1,1} = 1\}.$$

(1.2) *Posant $M = \{\mu f; f \in X^*\}$ et $M' = \{\mu f; f \in A^*\}$, on a*

$(\mathfrak{U}_d)$ $$M' = \{m \in M; mM' \cap M'm \cap M' \neq \emptyset\}$$

et

$(\mathfrak{N}_d)$ $$\emptyset = \{m \in M; MmM \cap M' = \emptyset\}.$$

(1.3) $$1 - \sum_{a \in A} \alpha a = \det\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right), \quad \text{où la matrice } \sum_{x \in X} \alpha x . \mu x$$

appartient à l'anneau des $n \times n$ matrices ayant leurs éléments dans $\mathbf{Z}[X]$.

Preuve.

(1.1). — Nous prenons μe égale à la $n \times n$-matrice unité, et nous définissons μ par sa restriction à X en posant pour chaque $x \in X$ et $i, j \in [1, n]$:

$$(\mu x)_{i,j} = 1 \quad \text{si } j = 1 \text{ et } k_i x \in A \quad \text{ou si } j \neq 1 \text{ et } k_i x = k_j;$$
$$= 0 \quad \text{dans tous les autres cas.}$$

Donc, pour $f \in X$, nous avons, d'une part $(\mu f)_{1,j} \neq 0$ si et seulement si $f \in A^* k_j$ et, d'autre part, $(\mu f)_{1,j} \in \{0, 1\}$. Supposant que ceci est vrai pour $f \in X^*$, nous vérifions qu'il en est encore de même pour fx $(x \in X)$.

En effet, si $(\mu fx)_{1,j} \neq 0$, on doit avoir $(\mu f)_{1,i} \neq 0$ et $(\mu x)_{i,j} \neq 0$ pour au moins un $k_i \in K$. L'hypothèse d'induction montre que $f \in A^* k_i$ et que $k_i x \in A$ ou que $k_i x = k_j$ selon que $j = 1$ ou non, et l'on a donc encore

$$fx \in A^* k_i x \subset A^* A \subset A^* \qquad \text{ou} \qquad fx \in A^* k_i x = A^* k_j.$$

Réciproquement, si $fx \in A^* A$, l'hypothèse $(\mathfrak{U}'_d)$ implique l'existence d'un et d'un seul mot $a \in A$ tel que $fx \in A^* a$, et le mot a détermine univoquement un $k_i \in K$ tel que $a = k_i x$, ce qui entraîne

$$f \in A^* k_i \qquad \text{et} \qquad (\mu fx)_{1,1} = 1;$$

si $fx \in A^* k_j$ $(j \neq 1)$, il existe un et un seul $k_i \in K$ tel que $k_j = k_i x$, et l'on a encore

$$f \in A^* k_i \qquad \text{et} \qquad (\mu fx)_{1,j} = 1.$$

On a donc montré que

$$A^* = \{ f \in X^*;\ (\mu f)_{1,1} = 1 \}$$

et que tous les éléments des premières lignes des matrices μf $(f \in X^*)$ sont 0 ou 1.

Maintenant, par construction, $(\mu k_i)_{1,i} = 1$ quel que soit $k_i \in K$; donc, pour chaque $f \in X^*$, la première ligne de la matrice $\mu k_i f$ est la somme d'un vecteur non négatif et de la $i^{\text{ième}}$ ligne de μf; puisque $(\mu k_i f)_{1,j} \in \{ 0, 1 \}$, ceci montre que $(\mu f)_{i,j} \in \{ 0, 1 \}$ identiquement, et (1.1) est vérifiée.

Il est clair que si $K' = \{ k'_1, k'_2, \ldots, k'_{n'} \}$ est l'ensemble des facteurs droits propres des mots de A, il existe aussi une représentation μ' de X^* par des $n' \times n'$-matrices ayant les mêmes propriétés que μ; on peut vérifier que, pour tout $f \in X^*$, on a $\mu f . \nu = \nu . \mu' f$, où ν est la $n \times n'$-matrice à éléments dans $\{ 0, 1 \}$ telle que $\nu_{i,i'} = 1$ si et seulement si $k_i k'_{i'} \in \{ e \} \cup A$.

(1.2). — Si les éléments (1,1) des matrices μf et $\mu f'$ sont positifs, il en est de même pour la matrice $\mu ff'$; donc M' est un sous-monoïde de M et

$$M' \subset \{ m \in M;\ mM' \cap M'm \cap M' \neq \emptyset \}.$$

Réciproquement, si les éléments (1,1) de μa, $\mu a'$, μfa et $\mu a' f$ sont positifs, il doit exister deux indices i et i' tels que $(\mu f)_{1,i}$, $(\mu a)_{i,1}$, $(\mu f)_{i',1}$ et $(\mu a')_{1,i'}$ soient positifs et l'on ne peut avoir $(\mu a' fa)_{1,1} \leq 1$ que si $i = i' = 1$, c'est-à-dire que si $f \in A^*$; donc, *a fortiori*,

$$\{ m \in M;\ mM' \cap M'm \cap M' \neq \emptyset \} \subset M',$$

et $(\mathfrak{U}_d)$ est établie.

Pour vérifier $(\mathfrak{R}_d)$, on peut toujours supposer que X contient au moins deux lettres distinctes x et x' car, sinon, $A = \{ x^n \}$, et $(\mathfrak{R}_d)$ est trivialement vraie. Supposons qu'il existe un mot $f \in X^q x'$ qui soit tel

que $M.\mu f.M \cap M' = \emptyset$, et montrons qu'en posant $b = x^q f$, l'ensemble $A' = \{b\} \cup A$ engendre librement un sous-monoïde A'^*, en contradiction avec $(\mathcal{R}'_d)$. Pour cela, soit g le mot le plus court dont il n'a pas encore été établi que la factorisation comme produit de mots de A' est unique; puisque, d'une part A engendre librement A^* et que, d'autre part, $X^* b X^* \cap A^* = \emptyset$, le seul cas qui requiert une discussion est celui de deux factorisations de g contenant chacune, au moins une fois, le mot b, et l'on peut supposer que $g = a_1 b a'_1 = a_2 b a'_2$, où a_1, $a_2 \in A^*$; a'_1, $a'_2 \in A'^*$ et où $a_2 b$ est un facteur gauche de $a_1 b$. En raison de $X^* b X^* \cap A^* = \emptyset$, $a_2 b$ n'est pas un facteur gauche de a_1; comme la définition $b = x^q f$ ($f \in X^q x'$, $x \neq x'$) entraîne que e est le seul mot qui soit en même temps un facteur gauche et un facteur droit de b, on a donc $a_2 b = a_1 b$, et l'unicité de la factorisation de g résulte de l'hypothèse d'induction.

Ceci termine la vérification de (1.2) qui dépend donc seulement du fait que tous les éléments des matrices μf sont dans $\{0, 1\}$; si cette condition est satisfaite par une représentation ρ de X^*, on peut montrer que $F = \{f \in X^*;\ (\rho f)_{1,1} = 1\}$ est un sous-monoïde librement engendré par $F \cap XX^* \setminus (F \cap XX^*)^2$ et que, quand ρ est de dimension finie, $(\mathcal{R}_d)$ est équivalente à $(\mathcal{R}'_d)$ (*cf.* [4]).

(1.3). — Considérons la matrice

$$\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right)^{-1} = \mu e + \sum_{m>0} \left(\sum_{x \in X} \alpha x . \mu x\right)^m$$

dont les éléments appartiennent à l'algèbre large du monoïde commutatif libre engendré par les $\alpha x (x \in X)$. D'après (1.1) et $(\mathcal{U}'_d)$, l'élément (1,1) de cette matrice est égal à

$$1 + \sum \{\alpha f;\ f \in AA^*\} = 1 + \sum_{m>0} \left(\sum_{a \in A} \alpha a\right)^m = \left(1 - \sum_{a \in A} \alpha a\right)^{-1}$$

D'autre part, ce même élément est égal au produit de $\left(\det\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right)\right)^{-1}$ par l'élément (1,1), soit u, de la matrice adjointe de $\mu e - \sum_{x \in X} \alpha x . \mu x$; par construction, u est égal à 1, car tous les éléments non nuls de $\sum_{x \in X} \alpha x . \mu x$ sont dans la première colonne ou au-dessus de la diagonale principale. On a donc

$$\left(\det\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right)\right)^{-1} = \left(1 - \sum_{a \in A} \alpha a\right)^{-1}$$

et la vérification de la remarque (1) est achevée.

Le monoïde M ayant au plus 2^{n^2} éléments, nous pourrons utiliser le théorème suivant qui est dû à Suschkéwitsch, et que nous formulons dans des notations inspirées de Rees [6].

Théorème (Suschkéwitsch [5]). — *Soient M un monoïde fini et M' un sous-monoïde de M satisfaisant $(\mathcal{D}_d)$. M possède un idéal bilatère unique $D = MDM$ qui est à la fois l'union des idéaux à droite minimaux $R_i = R_i M$ $(i \in I)$ et des idéaux à gauche minimaux $L_j = ML_j$ $(j \in J)$ de M. Il existe un groupe fini G, une famille d'éléments $\{ g_{j,i} \}$ de G indexés par les paires $(j, i) \in J \times I$, deux sous-ensembles non vides d'indices $I' \subset I$ et $J' \subset J$, un sous-groupe G' de G et une bijection $\gamma : I \times G \times J \to D$ qui ont les propriétés suivantes :*

(S. 1) *Quels que soient (i, g, j) et $(i', g', j') \in I \times G \times J$, on a*

$$\gamma(i, g, j) . \gamma(i', g', j') = \gamma(i, g . g_{j,i'} . g', j') \in R_i \cap L_{j'};$$

(S. 2) *Pour chaque $(j, i) \in J' \times I'$, l'élément $g_{j,i}$ appartient à G' et*

$$M' \cap D = \{ \gamma(i, g, j) ; (i, g, j) \in I' \times G' \times J' \}.$$

Nous aurons aussi besoin de la conséquence très simple suivante du théorème de Suschkéwitsch :

(S. 3) *Il existe une représentation de M par des applications (notées multiplicativement) de I (resp. de J) dans lui-même telle que, pour chaque $m \in M$ et $i \in I$ (resp. $j \in J$), la restriction à R_i (resp. à L_j) de la translation $m' \to mm'$ (resp. $m' \to m'm$) soit une bijection de R_i (resp. de L_j) sur $R_{m.i}$ (resp. sur $L_{j.m}$).*

En effet, ceci résulte immédiatement de (S. 1) si $m \in D$. Soit $m \in M$ quelconque et pour chaque $i \in I$ prenons un $j \in J$ arbitraire. Posant

$$u = \gamma(i, (g_{j,i})^{-1}, j),$$

(S. 1) montre que $ur = r$ pour tout $r \in R_i$; d'autre part, puisque u appartient à l'idéal à gauche minimal $L_j = ML_j$, on peut écrire $mu = v = \gamma(i', g', j)$ pour une certaine paire $i' \in I$, $g' \in G$; quel que soit $r \in R_i$, on a donc $mr = mur = vr \in R_{i'}$ et l'indice i' ne dépend par conséquent que de m et de i; nous le désignerons par $m.i$. Le fait que la translation $r \to mr$ est une bijection résulte de ce qu'il en est de même pour la translation $r \to vr$, et un raisonnement symétrique s'applique aux idéaux à gauche minimaux.

Ceci étant rappelé, nous établissons les remarques suivantes :

(2). — *L'ensemble P' des $f \in X^*$ tels que $ff'X^* \cap A^* \neq \emptyset$ pour tout $f' \in X^*$ est identique à l'ensemble P des $f \in X^*$ tels que, pour tout $f' \in X^*$, on ait $A^*ff' \cap A^* \neq \emptyset$ si et seulement si $ff' \in A^*$.*

Preuve. — Puisque $A^\star = \mu^{-1}M' (= \{ f \in X^\star ; \mu f \in M' \})$, il suffit d'établir l'énoncé correspondant pour les sous-ensembles $\mu P' (= \{ \mu f ; f \in P' \})$ et μP de M.

Soient $p \in \mu P$ et $m \in M$ arbitraires, et prenons un élément m' de $M' \cap D$ quelconque; le produit $m'pm$ appartient au même idéal à droite minimal que m' et, d'après (S. 1) et (S. 2), nous pouvons trouver un $m'' \in M$ tel que $m'pmm'' \in M'$; comme $p \in \mu P$, cette dernière relation implique $pmm'' \in M'$, et nous avons montré que $pmM \cap M' \neq \emptyset$ quel que soit m, pour chaque $p \in \mu P$, c'est-à-dire que $\mu P \subset \mu P'$.

Soit maintenant $p \in \mu P'$. Nous allons montrer que si $m' \in M'$ et $m \in M$ satisfont $m'pm \in M'$, on a nécessairement $pm \in M'$, ce qui établira que $p \in \mu P$ et $\mu P' = \mu P$. Prenons $r \in M' \cap D$ quelconque; l'hypothèse $p \in \mu P'$ implique qu'on puisse trouver un $m'' \in M$ satisfaisant $pmrm'' \in M'$; de fait, puisque $r \in D$, le produit pmr appartient à un idéal à droite minimal, $R_{i''}$, contenant aussi $pmrm''$ et, comme ce dernier produit est dans M', l'indice i'' appartient à I'. Utilisant (S. 1), on voit que, sans perte de généralité, on peut prendre $m'' = \gamma(i'', g'', j'')$, où $(i'', j'') \in I' \times J'$. Vérifions qu'on doit avoir $g'' \in G'$; en effet, puisque $m'pm$ et r appartiennent à M', on peut écrire :

$$m'pmr = \gamma(i', g', j'),$$

où $(i', g', j') \in I' \times G' \times J'$ en vertu de (S. 2), donc, d'après (S. 1),

$$m'pmrm'' = \gamma(i', g' . g_{j'', i''} . g'', j'');$$

maintenant, comme m' et $pmrm''$ appartiennent à M', on a $g' . g_{j'', i''} . g'' \in G'$, où $g' \in G'$ en raison de $m' \in M'$ et $g_{j'', i''} \in G'$ en raison de $(j', i'') \in J' \times I'$ et $g'' \in G'$ est établi. Nous avons donc $m'' \in M'$. Le produit pm satisfait la double égalité

$$(pmrm''m')pm = pm(rm''m'pm) = (pmrm'')(m'pm),$$

où tous les termes entre parenthèses appartiennent à M' par hypothèse ou par construction ainsi qu'on vient de le voir. Faisant appel à $(\mathfrak{U}_d)$ on en conclut que $pm \in M'$, et la vérification de $P' = P$ est achevée.

(2 *bis*). — *Une condition nécessaire et suffisante pour que A satisfasse $(\mathfrak{U}'_r)$ est qu'il satisfasse :*

$(\mathfrak{R}_r)$ *Tout mot de $X^\star$ est facteur gauche d'au moins un mot de $A^\star$.*

Preuve. — La condition $(\mathfrak{R}_r)$ équivaut à $P' = X^\star$ (c'est-à-dire, dans la théorie de DUBREIL [1], à l'hypothèse que $A^\star$ est « net à droite ») donc, à $P = X^\star$, donc, enfin à l'hypothèse que $A^\star f \cap A^\star = \emptyset$ pour tout $f \notin A^\star$ (ce qui, selon [2], signifie que $A^\star$ est « unitaire à gauche »). Si cette dernière condition est satisfaite, il est clair qu'aucun mot de A n'est facteur gauche d'un autre mot de A et que, par conséquent, tout mot de $X^\star$

a au plus un facteur gauche dans A ; réciproquement, si A satisfait $(\mathfrak{U}'_r)$, et si a, $a' \in A^*$ et $f \in X^*$ sont tels que $af = a'$, on voit par induction sur le nombre des facteurs de a appartenant à A que f doit être un mot de A^* et que, par conséquent, $(\mathfrak{U}'_r)$ entraîne $P = X^*$.

Afin de pouvoir recourir à des résultats connus, nous faisons maintenant appel à des considérations un peu différentes. Soient désormais x_0 un élément distingué de X et π une bijection de $X \setminus \{x_0\}$ sur un nouvel ensemble Y ; π peut être prolongé en un homomorphisme de X^* dans la structure multiplicative de $Z[Y]$ en posant

$$\pi x_0 = 1 - \sum_{x \in X \setminus \{x_0\}} \pi x,$$

et il n'y aura pas d'inconvénient à désigner aussi par π l'homomorphisme naturel de l'algèbre large $\hat{Z}[X]$ du monoïde commutatif libre engendré par les αx $(x \in X)$ dans l'algèbre large $\hat{Z}[Y]$ du monoïde commutatif libre engendré par les $y \in Y$. De plus, nous définirons Λ comme l'ensemble des homomorphismes λ de X^* dans $]0, 1]$ qui ont la forme $\lambda = \lambda' \pi$, où λ' est un homomorphisme de $Z[Y]$ dans les réels. Finalement, pour tout sous-ensemble F de X^*, nous poserons

$$\lambda_n F = n^{-1} \sum \{ \lambda f ; f \in F \setminus X^n X^* \} \qquad \text{et} \qquad \lambda_\infty F = \limsup_{n \to \infty} \lambda_n F.$$

Il résulte immédiatement des définitions que $0 < \lambda f \leq 1$ pour tout $f \in X^*$, que $\lambda_n X^* = 1$ pour tout entier n et que $\lambda_\infty f X^* = \lambda f$ pour tout $f \in X^*$.

(3). — *L'application* $\lambda_\infty \mu^{-1}$ *(notée* $\bar{\lambda}$*, pour abréger) de* M *dans les réels définit une mesure de probabilité idempotente sur* M *qui a les propriétés suivantes :*

(3.1). *Quel que soit le sous-ensemble* M'' *de* M,

$$\bar{\lambda} M'' = \bar{\lambda}(M'' \cap D).$$

(3.2). *Quels que soient* $(i, j) \in I \times J$ et $m \in R_i \cap L_j$,

$$\bar{\lambda} m = (\mathrm{Card}(G))^{-1} . \bar{\lambda} R_i . \bar{\lambda} L_j > 0,$$

où

$$\sum_{i \in I} \bar{\lambda} R_i = \sum_{j \in J} \bar{\lambda} L_j = \bar{\lambda} D = 1.$$

Preuve. — Prenons M lui-même comme ensemble d'indices, et définissons, pour chaque $m \in M$, une $M \times M$ matrice ρm par la condition que, pour tout m', $m'' \in M$, l'élément (m', m'') de ρm soit égal à 1 ou

à o selon que $m'm = m''$ ou non; ρ est la représentation régulière droite de M et l'on a identiquement

$$\rho m_1 . \rho m_2 = \rho(m_1 m_2) \qquad \text{pour tout} \quad m_1, m_2 \in M.$$

Par construction, chacune des matrices ρm est une matrice stochastique; comme l'hypothèse $\lambda \in \Lambda$ implique $\sum_{x \in X} \lambda x = 1$, il en résulte que $\sum_{x \in X} \lambda x . \rho \mu x$ est une $M \times M$ matrice stochastique que nous désignerons par $\mathbf{X}$. Donc, d'après le théorème de Perron-Frobenius, la limite de $n^{-1} \sum_{0 \leq n' < n} \mathbf{X}^{n'}$, pour n tendant vers l'infini est une matrice stochastique idempotente que nous désignerons par $\overline{\mathbf{X}}$.

Maintenant, pour chaque n fini, on a

$$n^{-1} \sum_{0 \leq n' < n} \mathbf{X}^{n'} = n^{-1} \sum \{ \lambda f . \rho \mu f; f \in X^* \setminus X^n X^* \} = \sum_{m \in M} \lambda_n \mu^{-1} m . \rho m.$$

Comme, par définition, l'élément $(\mu e, m')$ de ρm est égal à 1 ou à o selon que $m' = m$ ou non, on en conclut que $\bar{\lambda} m$ est égal à l'élément $(\mu e, m)$ de $\overline{\mathbf{X}}$. Ceci suffit pour établir $\bar{\lambda} m > 0$ et $\sum_{m \in M} \bar{\lambda} m = 1$, et le fait que $\bar{\lambda}$ est une mesure idempotente résulte immédiatement de l'idempotence de la matrice $\overline{\mathbf{X}}$. Une fois ces propriétés établies, (3.1) et (3.2) sont, aux notations près, les théorèmes 2.3.2 (*a*) et 2.3.2 (*b*) de [3].

(4). — *Il existe deux polynômes* πH, $\pi H' \in Z[Y]$ *tels qu'en désignant par* q *l'indice du sous-groupe* G' *de* G, *et en posant*

$$\pi A^* = \sum_{a \in A^*} \pi a,$$

on ait $q . \pi H . \pi H' . \pi A^* = 1$ *et que* A *satisfasse* $(\mathfrak{U}'_r)$ [*resp.* $(\mathfrak{U}'_l)$] *si et seulement si* $\pi H = 1$ (*resp.* $\pi H' = 1$).

Preuve. — Prenons un mot $a \in A^*$ fixe, tel que $\mu a \in M' \cap D$, et posons $F = \{ f \in X^*; af \in A^* \}$. Les énoncés (S. 1) et (S. 2) montrent que pour chaque paire $(i, j) \in I \times J$, l'intersection de μF (resp. de M') avec $R_i \cap L_j$ contient exactement $\mathbf{Card}(G')$ ou zéro élément selon que $(i, j) \in I \times J'$ (resp. $\in I' \times J'$) ou non. Donc, utilisant (3.1) et (3.2), on a

$$\lambda_* F = \bar{\lambda}(D \cap \mu F) = q^{-1} . \bar{\lambda} L' \tag{4.1}$$

et

$$\lambda_* A^* = \bar{\lambda}(D \cap M') = q^{-1} . \bar{\lambda} L' . \bar{\lambda} R', \tag{4.2}$$

où

$$L' = \bigcup_{j \in J'} L_j \qquad \text{et} \qquad R' = \bigcup_{i \in I'} R_i.$$

Soit maintenant H l'ensemble des $f \in F$ qui n'admettent aucune factorisation de la forme $f = f'a'$, avec $f' \in F$ et $a' \in A$. Par définition, H est formé de facteurs droits de mots de A; donc H est fini, et $\pi H = \sum_{h \in H} \pi h$ est un polynôme de $Z[Y]$. De plus, tout $f \in F$ a au moins une factorisation de la forme $f = ha'$, où $h \in H$ et $a' \in A^*$; cette factorisation est unique car, sinon, le produit af aurait deux factorisations distinctes comme produit de mots de A en contradiction avec $(\mathfrak{U}'_d)$. On a donc

$$\lambda_n F = \sum_{h \in H} \left(\lambda h . n^{-1} \sum \{ \lambda a' ;\ a' \in A^* ;\ ha' \in X^* \setminus X^n X^* \} \right).$$

Comme H est fini, chacune des sommes

$$n^{-1} \sum \{ \lambda a' ;\ a' \in A^* ;\ ha' \in X^* \setminus X_n X^* \}$$

tend uniformément vers $\lambda_\infty A^*$ quand n tend vers l'infini, et l'on a donc

$$\lambda_\infty F = \lambda' \pi H . \lambda_\infty A^*,$$

c'est-à-dire, d'après (4.1) et (4.2),

$$\bar{\lambda} R' . \lambda' \pi H = 1 ;$$

il est clair qu'il existe aussi un polynôme $\pi H' \in Z[Y]$ tel que $\bar{\lambda} L' . \lambda' \pi H' = 1$, et la formule désirée résulte de (4.2) et du fait que toutes les égalités écrites sont identiquement vraies pour tous les $\lambda = \lambda' \pi \in \Lambda$.

Maintenant, comme $R' \subset D$, on a

$$(\lambda' \pi H)^{-1} = \bar{\lambda} R' \leqq \bar{\lambda} D = 1$$

avec égalité si et seulement si $R' = D$, c'est-à-dire $I' = I$, c'est-à-dire enfin, $P' = X^*$ et, d'après (2 *bis*), on a donc $\pi H = 1$ si et seulement si A satisfait $(\mathfrak{U}'_r)$; un raisonnement symétrique s'applique à $\pi H'$ et (4) est établie.

Fin de la vérification. — Soit maintenant $\mathbf{Q}(M)$ l'anneau engendré par les $n \times n$ matrices $m \in M$ sur le corps des nombres rationnels; pour chaque matrice $m \in \mathbf{Q}(M)$ nous désignons par $\overleftarrow{m}$ (resp. $\overrightarrow{m}$) le n-vecteur égal à la première colonne (resp. ligne) de m.

PROPOSITION. — *Il existe trois polynômes* T_1, T'_3 *et* $T_4 \in Z[X]$ *tels que*

$$1 - \sum_{a \in A} \alpha a = \left(1 - \sum_{x \in X} \alpha x\right).T_1.T_4.\left(q + \left(1 - \sum_{x \in X} \alpha x\right).T'_3\right)$$

et qu'en outre, T_1 *(resp.* T_4*) ne se réduise à* 1 *que si* A *satisfait* $(\mathfrak{U}'_r)$ *[resp.* $(\mathfrak{U}'_l)$*].*

Preuve. — Soit V l'espace vectoriel sous-tendu par tous les vecteurs $\overleftarrow{m}$ $[m \in \mathbf{Q}(M)]$, $\mathbf{Q}(M)$ opérant par multiplication à gauche sur V; pour chaque $i \in I$, nous posons $\overleftarrow{r}_i = \sum_{r \in R_i} \overleftarrow{r}$, et nous définissons les sous-espaces suivants de V :

V_1 : le sous-espace sous-tendu par toutes les différences

$$\overleftarrow{r}_i - \overleftarrow{r}_{i'} \qquad (i, i' \in I);$$

V_2 : le sous-espace sous-tendu par tous les

$$\overleftarrow{r}_i \quad (i \in I);$$

V_3 : le sous-espace formé de tous les $v \in V$ tels que

$$0 = \left(\sum_{m \in L_j} \overrightarrow{m} - \sum_{m \in L_{j'}} \overrightarrow{m}\right).v \text{ pour toutes les paires } j, j' \in J.$$

Comme la restriction de la translation $r \to mr$ $(m \in M)$ à chaque R_i est une bijection de cet ensemble sur $R_{m.i}$, ainsi qu'on l'a vu plus haut, les sous-espaces V_1 et V_2 sont invariants. D'après (S. 1), on a

$$\left(\sum_{m \in L_j} m\right)\left(\sum_{m \in R_i} m\right) = \mathbf{Card}(G).\left(\sum_{m \in D} m\right)$$

quels que soient $(i, j) \in I \times J$. Par conséquent,

$$\left(\sum_{m \in L_j} m - \sum_{m \in L_{j'}} m\right).r_i = 0 \quad \text{identiquement}$$

et $V_2 \subset V_3$; de plus, V_3 est invariant puisqu'il en est de même, par rapport à la multiplication à droite par les éléments de $\mathbf{Q}(M)$, de l'espace W sous-tendu par tous les vecteurs $\sum_{m \in L_j} \overrightarrow{m} - \sum_{m \in L_{j'}} \overrightarrow{m}$ $(j, j' \in J)$. Convenant que $V = V_4$, nous pouvons donc, pour $k = 1, 2, 3, 4$, définir μ_k comme la représentation de X^* induite par μ sur l'espace quotient V_k/V_{k-1} $(V_0 = \{0\})$, et poser

$$T_k = 1 \text{ ou } = \mathbf{det}\left(\mu_k e - \sum_{x \in X} \alpha x.\mu_k x\right)$$

selon que V_k/V_{k-1} a pour dimension zéro ou non. D'après (1.3), nous avons

$$1 - \sum_{a \in A} \alpha a = \mathbf{det}\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right) = T_1 T_2 T_3 T_4,$$

et il suffit de considérer l'homomorphisme de $\mathbf{Z}[X]$ dans $\mathbf{Z}$ qui envoie tous les $\alpha x (x \in X)$ sur zéro pour vérifier que chacun des polynômes T_k a un terme constant égal à 1; en vertu du lemme de Gauss, et du fait que le produit des T_k est dans $\mathbf{Z}[X]$, il en résulte que tous ces polynômes appartiennent à $\mathbf{Z}[X]$; nous discuterons successivement T_2, T_1, T_4 et T_3.

(T_2) *Le polynôme T_2 est égal à* $1 - \sum_{x \in X} \alpha x$.

En effet, d'après (S. 3), on a

$$m . \overleftarrow{r}_i = \overleftarrow{r}_{m.i} = \overleftarrow{r}_i - \left(\overleftarrow{r}_i - \overleftarrow{r}_{m.i}\right)$$

quels que soient $m \in M$ et $i \in I$; donc V_2/V_1 a pour dimension 1, et $\mu_2 f = 1$ pour tout $f \in X^*$, ce qui entraîne trivialement le résultat cherché.

(T_1) *Le polynôme T_1 est égal à 1 si et seulement si A satisfait* ($\mathfrak{U}'_r$)

D'après (S. 2), la première coordonnée de chaque vecteur $\overleftarrow{r}_i$ ($i \in I$) est égale à $\mathbf{Card}(G').\mathbf{Card}(J')$ ou a zéro selon que $i \in I'$ ou non. Donc, si μ'_2 est la représentation de X^* induite par μ sur V_2 et si i_1 est un indice fixe de I', il existe une matrice fixe $\mathbf{t}_1$ ayant ses éléments dans $\mathbf{Q}$ et satisfaisant la condition que, pour chaque $f \in X^*$, la trace $\mathbf{Tr}(\mathbf{t}_1 . \mu'_2 f)$ soit égale à 1 ou à 0 selon que $f \in F_1 = \{f' \in X^*; \mu f' . i_1 \in I'\}$ ou non.

Posant

$$\mathbf{X}'_2 = \sum_{x \in X} \alpha x . \mu'_2 x \qquad \text{et} \qquad T'_1 = \mathbf{Tr}(\mathbf{t}_1 . \mathbf{Adj}(\mu'_2 e - \mathbf{X}'_2)) \in \mathbf{Q}[X],$$

on a donc

$$\alpha F_1\left(= \sum_{f \in F_1} \alpha f\right) = \mathbf{Tr}(\mathbf{t}_1 . (\mu'_2 e - \mathbf{X}'_2)^{-1})$$

$$= T'_1 . \mathbf{det}(\mu'_2 e - \mathbf{X}'_2)^{-1} = T'_1 . \left(1 - \sum_{x \in X} \alpha x\right)^{-1} . (T_1)^{-1},$$

c'est-à-dire

$$T_1 . \alpha F_1 = T'_1 . \left(1 - \sum_{x \in X} \alpha x\right)^{-1}.$$

Comme $T_1 \in \mathbf{Z}[X]$ et comme tous les coefficients des séries infinies αF_1 et $\left(1 - \sum_{x \in X} \alpha x\right)^{-1}$ sont entiers, ceci montre que T'_1 appartient aussi à $\mathbf{Z}[X]$.

De plus, pour tout homomorphisme $\lambda = \lambda' \pi \in \Lambda$, on a

$$\lambda' \pi T_1 . \lambda_\infty F_1 = \lambda' \pi T'_1 .$$

Observons maintenant que $D \cap \mu F_1 = R'$; utilisant (3.1), et la vérification de (4), on trouve

$$\lambda_\infty F_1 = \bar{\lambda} R' = (\lambda' \pi H)^{-1},$$

d'où

$$\lambda' \pi T_1 = \lambda' \pi H . \lambda' \pi T'_1$$

et enfin

$$\pi T_1 = \pi H . \pi T'_1 .$$

Donc, si $T_1 = 1$, on a $\pi T_1 = 1$, et par conséquent, $\pi H = 1$ puisque tous ces polynômes ont des coefficients entiers. Ceci prouve que $T_1 = 1$ seulement si A satisfait $(\mathfrak{U}'_r)$.

Réciproquement, si cette dernière condition est satisfaite, chacune des matrices $\mu f (f \in X^*)$ possède un et un seul élément non nul par ligne; donc tous les vecteurs $\overleftarrow{r_i}$ $(i \in I)$ sont égaux à un même multiple du n-vecteur unité, donc enfin $V_1 = \{ 0 \}$ et $T_1 = 1$ par définition.

(T_4) *$T_4 = 1$ si, et seulement si A satisfait $(\mathfrak{U}'_l)$.*

Il suffit de répéter de façon symétrique la discussion précédente puisque par construction la représentation μ_4 est isomorphe à la représentation de X^* induite par μ (opérant à droite) sur l'espace W.

(T_3) *Il existe un polynôme $T'_3 \in \mathbf{Z}[X]$ tel que*

$$T_3 = q + \left(1 - \sum_{x \in X} \alpha x\right) . T'_3 .$$

D'après la formule (4.2), on a

$$\lambda_\infty A^* . \pi H . q . \pi H' = 1$$

et, d'après les résultats qui viennent d'être obtenus,

$$\lambda_\infty A^* . \pi T_1 . \pi T'_3 . \pi T_4 = 1$$

avec, en outre, $\pi T_1 = \pi H . \pi T'_1$ et $\pi T_4 = \pi H' . \pi T'_4$, où toutes les expressions de la forme πS sont des polynômes de $\mathbf{Z}[Y]$. Il en résulte immé-

diatement que $\pi T'_1 = \pi T'_4 = 1$ et que $\pi T_3 = q$, c'est-à-dire, puisque $T_3 \in Z[X]$, que

$$T_3 = q + \left(1 - \sum_{x \in X} \alpha x\right) T'_3, \qquad \text{avec} \quad T'_3 \in \mathbf{Z}[X].$$

La vérification est achevée. On peut noter que la condition $q = 1$ équivaut à la condition

$$\emptyset = \{ f \in X^* ;\ A^* f A^* \cap A^* = \emptyset \}$$

puisque, d'une part si $q = 1$, c'est-à-dire si $G' = G$, on a $m' m m' \in M'$ pour tout $m \in M$ et $m' \in M' \cap D$ et que, d'autre part, si $G' \neq G$, les énoncés (S. 1) et (S. 2) montrent que $M' m M' \cap M' = \emptyset$ pour tout $m \in (R_i \cap L_j) \setminus M'$ quand $(i, j) \in I' \times J'$. Par conséquent, $T = T_1 T_3 T_4$ a au moins *trois* facteurs $\neq 1$ dans $\mathbf{Z}[X]$ quand A ne satisfait ni $(\mathfrak{U}'_r)$, ni $(\mathfrak{U}'_l)$ ni la condition qui vient d'être écrite.

Observation. — Par définition, l'ensemble $P = P'$ de (2) est un idéal à droite de X^*; de fait, P est le plus grand idéal à droite de X^* tel que $R' = D \cap \mu P$. Soit $B = P \setminus PXX^*$ l'ensemble engendrant P en tant qu'idéal à droite. Par construction, $P = BX^*$, et chaque mot de X^* a au plus un facteur gauche dans B; donc,

$$\lambda_\infty P = \sum_{b \in B} \lambda' \pi b \quad (= \lambda' \pi B)$$

et, d'après (3.1) et les résultats de (4), on a

$$\lambda' \pi B = \bar{\lambda}(D \cap \mu P) = \bar{\lambda} R' = (\lambda' \pi H)^{-1},$$

d'où $1 = \pi B . \pi H$ et enfin la conclusion que B est un ensemble fini (c'est-à-dire $\pi B \in Z[Y]$) si et seulement si $H = 1$, c'est-à-dire si A satisfait $(\mathfrak{U}'_r)$. Il nous semble intéressant, en raison de la signification donnée dans [4] à la condition $\mathbf{Card}(B) < \infty$, de fournir une vérification strictement combinatoire de ce résultat. Nous supposons désormais que $B \neq \{ e \}$, [c'est-à-dire que $P = X^*$ et, d'après (2 *bis*), que A ne satisfait pas $(\mathfrak{U}'_r)$] et nous employons les notations introduites dans la discussion de (4). Nous avons d'abord :

Tout mot de X^* est facteur gauche d'au moins un mot de HBX^* et possède au plus un facteur gauche dans HB.

En effet, soit $f \in X^*$; comme par hypothèse $a \in \mu^{-1}(D \cap M') \subset P'$, il existe au moins un $f' \in X^*$ tel que $aff' \in A^*$, et l'on peut écrire $ff' = ha'$, avec $h \in H$ et $a' \in A^*$; considérons $ff'a$; comme $a \in \mu^{-1}(D \cap M')$ et

$a' \in A^*$, le mot $a'a$ appartient à P, et a donc un et un seul facteur gauche $b \in B$; nous avons donc $ff'a = hbf_1$ pour un certain $f_1 \in X^*$, et nous avons montré que tout mot de X^* est facteur gauche d'au moins un mot de HB. Gardons les mêmes notations et supposons que $ff'a = hbf_1$ est égal à $h'b'f_2$, où $h' \in H$, $b' \in B$, $f_2 \in X^*$ et où, par exemple, h' est un facteur gauche de h; nous avons $ahbf_1 = ah'b'f_2 \in A^*$; comme d'après $(\mathfrak{U}'_d)$, tout mot de X^* a au plus une factorisation comme produit de mots de A et comme $b'f_2 \in A^*$ en raison de $h' \in H$ qui entraîne $ah' \in A^*$ et de $b' \in B \subset P$, ceci n'est possible que si $h = h'a''$ pour un certain $a'' \in A^*$; en vertu de la définition de H, cette dernière relation entraîne $a'' = e$, c'est-à-dire $h = h'$, d'où $b = b'$ et la vérification de ce résultat intermédiaire est achevée.

Nous montrons maintenant que B est un ensemble infini en vérifiant que la longueur de ses mots n'est pas bornée. Comme H est un ensemble fini, nous pouvons prendre un mot $h \in H$ fixe qui ait la propriété de n'être facteur gauche d'aucun autre mot de H. Soit b un mot quelconque de $B \cap XX^*$; on a $b = fx$, où $f \in X^*$ et $x \in X$. Il existe au moins un mot $f' \in X^*$ tel que $ff'X^* \cap BX^* = \emptyset$ car, sinon, on aurait $ff'X^* \cap A^* = \emptyset$ pour tout $f'' \in X^*$, c'est-à-dire $f \in P'$ en contradiction avec la définition même de f.

On vient de voir que le mot hff' est facteur gauche d'au moins un mot de HBX^*; en prenant f' assez long, on peut faire en sorte qu'il existe $h' \in H$ et $b' \in B$ tels que $h'b'$ soit un facteur gauche de hff' et qu'on ait toujours $ff'X^* \cap BX^* = \emptyset$; on sait aussi que h' et b' sont déterminés de façon univoque par hff'. Maintenant, on ne peut pas avoir $h = h'$, car ceci entraînerait que b' soit un facteur gauche de ff' en contradiction avec $ff'X^* \cap BX^* = \emptyset$; donc h' est un facteur gauche propre de h. De plus, $h'b'$ ne peut pas être un facteur gauche de hf, car ceci entraînerait que $hfx = hb$ a deux facteurs gauches distincts dans HB; donc hf est un facteur gauche propre de $h'b'$, et nous avons obtenu la conclusion désirée que la longueur de b' est strictement plus grande que celle de b. Ceci termine la vérification du fait que si A ne satisfait pas $(\mathfrak{U}'_r)$ l'ensemble B, et par conséquent l'ensemble C, de ses facteurs gauches propres sont deux ensembles infinis.

BIBLIOGRAPHIE

[1] Dubreil (Paul). — *Contributions à la théorie des demi-groupes*, I. — Paris, Gauthier-Villars, 1941 (Mémoires de l'Académie des Sciences de l'Institut de France, série 2, t. 63, 51 pages).

[2] Dubreil (Paul). — Contribution à la théorie des demi-groupes, II, *Rendiconti di Matematica*, Roma, série 5, t. 10, 1951, p. 183-200.

[3] Grenander (Ulf). — *Probabilities on algebraic structures.* — New York, J. Wiley and Sons, 1963.

[4] Nivat (Maurice). — Éléments de la théorie générale des codes, *Cours de l'École d'été de Ravello*, 1964.

[5] Rees (D.). — On semi-groups, *Proc. Cambridge phil. Soc.*, t. 36, 1940, p. 387-400.

[6] Suschkéwitsch, A. — Ueber die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit, *Math. Annalen*, t. 99, 1928, p. 30-50.

(Manuscrit reçu le 24 janvier 1965.)

Marcel Paul Schützenberger,
Institut Blaise Pascal,
23, rue du Maroc, Paris, 19e.

SÉMINAIRE DUBREIL.
ALGÈBRE ET THÉORIE
DES NOMBRES

MARCEL-PAUL SCHÜTZENBERGER

Sur les monoïdes finis n'ayant que des sous-groupes triviaux

Séminaire Dubreil. Algèbre et théorie des nombres, tome 18, n° 1 (1964-1965), exp. n° 10, p. 1-6.

<http://www.numdam.org/item?id=SD_1964-1965__18_1_A9_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
18e année, 1964/65, n° 10

10-01

25 janvier 1965

SUR LES MONOÏDES FINIS N'AYANT QUE DES SOUS-GROUPES TRIVIAUX

par Marcel-Paul SCHÜTZENBERGER

Introduction.

Soit X^* le monoïde libre (demi-groupe libre avec élément neutre e) engendré par un ensemble fixe X . A chaque congruence sur X^* correspond l'algèbre de Boole des parties de X^* saturées par cette congruence ; réciproquement, à chaque algèbre de Boole de parties de X^* correspond de façon unique une congruence qui est la plus fine parmi toutes celles pour lesquelles chacune de ces parties est saturée. Un des problèmes de ce que l'on appelle parfois la théorie des langages formels consiste à étudier les rapports existant entre les familles de congruences sur X^* et les familles de parties de X^* (ou "familles de langages formels") qui leur sont ainsi associées. Soit en particulier $\mathfrak{G}$ une variété de groupes, c'est-à-dire une famille de groupes abstraits contenant tout sous-groupe et tout groupe quotient du produit direct de deux de ses membres. Nous désignerons toujours par $\mathfrak{M}(\mathfrak{G})$ la famille des monoïdes quotient de X^* qui, d'une part sont finis et, d'autre part, ont tous leurs sous-groupes dans $\mathfrak{G}$. On verra plus bas que, de fait, $\mathfrak{M}(\mathfrak{G})$ est une variété de monoïdes ; on l'appellera la variété de monoïdes finis induite par $\mathfrak{G}$.

De même, $\mathfrak{F}^*(\mathfrak{G})$ désignera la famille des parties de X^* saturées par au moins une congruence telle que le monoïde quotient associé appartienne à $\mathfrak{M}(\mathfrak{G})$. On a l'énoncé suivant :

1. - $\mathfrak{F}^*(\mathfrak{G})$ est un sous-gerbier complémenté du gerbier des parties de X^* .

En d'autres termes, si A et B sont deux parties de X^* appartenant à $\mathfrak{F}^*(\mathfrak{G})$, $\mathfrak{F}^*(\mathfrak{G})$ contient $A \cup B$, le complément $X^* \backslash A$ de A dans X^* et le produit $AB = \{ff' \in X^* : f \in A ; f' \in B\}$. Le résultat suivant constitue le théorème fondamental de ce que l'on appelle la théorie des automates finis.

2. THÉORÈME de Kleene. - Quand $\mathfrak{G}$ est la variété de tous les groupes, $\mathfrak{F}^*(\mathfrak{G})$ est le plus petit gerbier de parties de X^* qui contienne toutes les parties X' de X et qui contienne le sous-monoïde A^* engendré par l'un quelconque de ses membres A .

Je me propose ici de donner la vérification de la propriété suivante :

3. - Si $\mathfrak{G}_0$ est la variété de groupes consistant en le seul groupe trivial (c'est-à-dire réduit à un élément neutre), $\mathfrak{x}^*(\mathfrak{G}_0)$ est le plus petit gerbier complémenté contenant toutes les parties X' de X .

Il serait naturellement intéressant d'avoir des caractérisations analogues pour d'autres variétés de groupes que les deux cas extrêmes envisagés ici. Des progrès substantiels ont été réalisés dans cette direction par RHODES et KRON en faisant appel à certaines applications de X^* dans lui-même et à la notion de produit semi-direct (ou de produit en couronne) de monoïdes ; M. NIVAT a exposé ici même cette question et certains des résultats qu'il a obtenus. Je mentionne l'énoncé suivant qui appelle de nouvelles recherches :

4. - Si $\mathfrak{A}$ est la variété des groupes abéliens, $\mathfrak{x}^*(\mathfrak{A})$ contient en même temps que chacun de ses membres B le sous-monoïde engendré par $B \backslash BXX^*$ (ou symétriquement, $B \backslash X^*XB$).

J'ignore si cette propriété de fermeture suffit à caractériser $\mathfrak{x}^*(\mathfrak{A})$; en utilisant les opérations de RHODES et KRON, elle permet d'obtenir $\mathfrak{x}^*(\mathfrak{G}_{sol})$ à partir des parties de X , où $\mathfrak{G}_{sol}$ est la variété des groupes solvables. Dans tous ces cas, il est impossible de se dispenser d'une hypothèse de finitude (au moins sur les chaînes d'idéaux) sur les monoïdes-quotient envisagés. On peut par contre, compliquer les énoncés pour obtenir des résultats un peu plus généraux. Pour terminer cette introduction et motiver un peu mieux les objets considérés, je signale l'énoncé suivant, inspiré de ce que les ingénieurs appellent les "automates incomplètement spécifiés" :

5. - Soient A , $B \in \mathfrak{x}^*(\mathfrak{G})$ où $\mathfrak{G}$ est la variété de tous les groupes. Il existe une plus petite variété de groupes $\mathfrak{G}'$ telle que $\mathfrak{x}^*(\mathfrak{G}')$ contienne au moins un A' satisfaisant $A \subset A'$; $B \cap A' = \emptyset$.

(Il n'existe pas en général de congruence plus fine que toutes les autres parmi celles qui saturent au moins une partie A' séparant A et B comme ci-dessus.)

Enfin, soit $\mathfrak{x}^{\underset{\sim}{N}}$ l'ensemble des applications dans X de l'ensemble $\underset{\sim}{N}$ des entiers naturels. Pour $f \in \mathfrak{x}^{\underset{\sim}{N}}$ et n , $n' \in \underset{\sim}{N}$, on pose

$$f[n , n'] = e \in X^* \quad \text{si} \quad n \geqslant n' ,$$

et

$$f[n , n'] = f(n)\ f(n+1) \ldots f(n'-1) \in X^* \quad \text{si} \quad n < n' .$$

Si $\mathfrak{G}$ est une variété de groupes, $\mathfrak{x}^{\underset{\sim}{N}}(\mathfrak{G})$ sera la famille de toutes les parties de $\mathfrak{x}^{\underset{\sim}{N}}$ qui sont une union finie de parties élémentaires V_M de $\mathfrak{x}^{\underset{\sim}{N}}$ de la forme

10-03

$$V_M = \{f \in \mathfrak{X}^N \; ; \quad M = \bigcap_{n>0} \{\alpha f[0 \, , \, n'] : \; n' > n\}\}$$

où $M \subset \alpha X^*$ et où α est un homomorphisme de X^* dans un monoïde de la variété $\mathfrak{M}(\mathfrak{G})$.

Il est assez remarquable que chaque $A \in \mathfrak{X}^N(\mathfrak{G})$ définisse de façon unique une certaine congruence sur X^* d'une manière qui généralise la construction applicable aux parties de X^* . On a :

6. THÉORÈME de Büchi et McNaughton. - Pour chaque variété de groupe $\mathfrak{G}$, $\mathfrak{X}^N(\mathfrak{G})$ est une algèbre de Boole qui contient toutes les parties de $\mathfrak{X}^N$ de la forme

$$V'_M = \{f \in \mathfrak{X}^N \; ; \quad M = \bigcap_{n,m>0} \{\alpha f[n' \, , \, n' + m'] : \; n' > n \; ; \; m' > m\}\} \; .$$

où M et α sont pris comme plus haut.

1. Vérification de la propriété 1.

Si les monoïdes M et M' ont tous leurs sous-groupes dans $\mathfrak{G}$, il est clair que tout sous-groupe de tout sous-monoïde de $M \times M'$ est un sous-groupe du produit direct de deux sous-groupes de M et de M' . Pour vérifier que $\mathfrak{M}(\mathfrak{G})$ est une variété de monoïdes, il suffit donc de considérer $M \in \mathfrak{M}(\mathfrak{G})$, un épimorphisme $\alpha : M \to M''$ et de vérifier que si G'' est un sous-groupe de M'' , il existe au moins un sous-groupe G de M tel que $\alpha G = G''$. Soit donc P l'union de l'élément neutre de M et de $\{m \in M \; ; \; \alpha m \in G''\}$. Comme M est fini, le monoïde $P \subset M$ possède au moins un quasi-idéal minimal H , c'est-à-dire un sous-ensemble non vide H qui satisfait $PH \cap HP = PHP = H$, et H est un sous-groupe de P , donc de M . On a $G''.\alpha H.G'' = \alpha H$, c'est-à-dire $G'' = \alpha H$, et la remarque est établie.

Vérifions maintenant que $\mathfrak{M}(\mathfrak{G})$ est un gerbier complémenté, et pour cela considérons deux homomorphismes

$$\alpha_i : X^* \to M_i \quad \text{où} \quad i = 1 \, , \, 2 \qquad \text{et} \quad M_1 \, , \, M_2 \in \mathfrak{M}(\mathfrak{G}) \; .$$

Soit R l'ensemble des parties de $M_1 \times M_2$. Pour $m_1 \in M_1$, $m_2 \in M_2$ et

$$r = \{(m'_{1,j} \, , \, m'_{2,j}) \; ; \quad j \in J_r\} \in R \; ,$$

on pose

$$m_1 . r . m_2 = \{(m_1 \, m'_{1,j} \, , \, m'_{2,j} \, m_2) \; ; \quad j \in J_r\} \in R \; ,$$

et, e_i étant l'élément neutre de M_i , on définit une multiplication associative

sur $M_1 \times R \times M_2$ en posant, pour toute paire d'éléments de ce produit direct d'ensembles :

$$(m_1 , r , m_2)(m_1' , r' , m_2') = (m_1 m_1' , m_1 r' e_2 \cup e_1 r m_2' , m_2 m_2') .$$

Enfin on définit l'homomorphisme β de X^* sur un monoïde P contenu dans $M_1 \times R \times M_2$ en posant, pour tout $f \in X^*$:

$$\beta f = (\alpha_1 f , \{(\alpha_1 f' , \alpha_2 f'') ; f'f'' = f\} , \alpha_2 f) .$$

Il est clair que si les sous-ensembles A_i de X^* satisfont $\alpha_i^{-1} \alpha_i A_i = A_i$, $(i = 1 , 2)$, on a aussi $B = \beta^{-1} \beta B$ pour

$$B = A_1 \cup A_2 , \quad B = A_1 \backslash A_2 \quad \text{ou} \quad B = A_1 A_2 .$$

Il ne nous reste à vérifier que $P \in \mathfrak{M}(\mathfrak{G})$. Soit $G = \{(m_{1,j} , r_j , m_{2,j}) ; j \in J\}$ un sous-groupe de P . Les sous-ensembles $G_i = \{m_{i,j} ; j \in J\}$ de M_i $(i = 1 , 2)$ sont des images homomorphes de G ; ce sont donc des sous-groupes. Soit u_i l'idempotent contenu dans G_i et soit N l'intersection de G avec $\{(u_1 , r , u_2) ; r \in R\}$. N est un sous-groupe normal de G et le groupe quotient G/N est isomorphe à un sous-groupe du produit direct $G_1 \times G_2$. Il suffit donc de vérifier que N se réduit à l'idempotent $u = (u_1 , r , u_2)$ contenu dans G . Pour cela, prenons deux éléments

$$g = (u_1 , s , u_2) \qquad \text{et} \qquad \overline{g} = (u_1 , \overline{s} , u_2)$$

de N inverses l'un de l'autre. La relation $u = u^2$ donne

$$r = u_1 r \cup r u_2$$

et la relation $u = g\overline{g}$ donne

$$r = u_1 \overline{s} \cup s u_2 .$$

On a donc

$$u_1 r = u_1 \cup u_1 s u_2$$

et, puisque $u_1 r \subset r$, ceci entraîne

$$u_1 s u_2 \subset r .$$

Maintenant, on déduit de $g = ugu$ la relation

$$s = u_1 r \cup u_1 s u_2 \cup r u_2$$

c'est-à-dire $s = r \cup u_1 s u_2$ et enfin $s = r$ ce qui montre que $g = u$, $N = \{u\}$; G est donc isomorphe à un sous-groupe de $G_1 \times G_2$, et $P \in \mathfrak{M}(\mathfrak{G})$ est vérifié.

10-05

On peut noter que, de fait, P est un sous-monoïde du produit semi-direct de $M_1 \times M_2$ par le produit direct de $\mathrm{Card}(M_1) \times \mathrm{Card}(M_2)$ copies du monoïde $\{0 , 1\}$ à deux éléments booléens $(0 = 01 = 10 = 00 \; ; \; 1 = 11)$.

2. Vérification de la propriété 3.

Soit $\Gamma(n)$ la famille des homomorphismes de X^* dans des monoïdes ayant au plus n éléments et dont tous les sous-groupes sont triviaux. Il est clair que pour chaque partie X' de X , on peut trouver un $\gamma \in \Gamma(3)$ tel que $\gamma^{-1}\gamma X' = X'$. Tenant compte de la propriété 1, ceci montre que $\mathfrak{F}^*(\mathfrak{S}_0)$ contient $\mathfrak{F}$, le gerbier complémenté des parties de X^* qui est engendré par tous les $X' \subset X$.

Réciproquement, si $\gamma \in \Gamma(2)$ et si $A = \gamma^{-1}\gamma A$, on a $A = \emptyset$ ou $A = \{e\}$ ou $A = X^*$, et par conséquent, $A \in \mathfrak{F}$. Pour établir la propriété, il suffit donc de prendre $\gamma \in \Gamma(n)$ fixe et de vérifier que $\gamma^{-1}\gamma A = A$ entraîne $A \in \mathfrak{F}$ sous l'hypothèse d'induction que $A' \in \mathfrak{F}$ pour tous les A' tels que $\gamma'^{-1}\gamma' A' = A'$ pour au moins un $\gamma' \in \Gamma(n-1)$. De fait, comme $M = \gamma X^*$ est fini, il suffit même de vérifier ce résultat pour chaque sous-ensemble A de la forme $\gamma^{-1} m$ $(m \in M)$.

On a :

(i) $\gamma^{-1} m \in \mathfrak{F}$ si le résiduel $W_m = \{m' \in M \; ; \; m \notin Mm'M\}$ de m a deux éléments ou plus.

En effet, il existe un homomorphisme ρ de M sur un monoïde M' tel que ρW_m soit un zéro de M' et que la restriction de ρ à $M \setminus W_m$ soit bijective. On a $\gamma^{-1} m = (\rho\gamma)^{-1} m$ et $\rho\gamma \in \Gamma(n-1)$, et par conséquent, $(\rho\gamma)^{-1} m \in \mathfrak{F}$ résulte de l'hypothèse d'induction.

(ii) Quel que soit $m \in M$, $\gamma^{-1}(MmM) \in \mathfrak{F}$.

Soit $f \in \gamma^{-1}(MmM)$. Le mot f possède au moins un facteur g de longueur minimale tel que γg appartienne à la même $\mathfrak{D}$-classe que m . Si $g \notin \{e\} \cup X$, on peut écrire $g = xg'x'$ où $x , x' \in X$ et $g' \in X^*$. Comme M est un monoïde fini, la théorie de Green et l'hypothèse qu'aucun des facteurs propres de g n'appartient à la $\mathfrak{D}$-classe de γg impliquent que $\gamma x g'$, $\gamma g' x'$ et γg appartiennent au résiduel de $\gamma g'$ et qu'au moins deux de ces trois éléments sont distincts. D'après ce que l'on vient de voir, $\gamma^{-1} g'$ appartient donc à $\mathfrak{F}$. Il en résulte que $\gamma^{-1} MmM$ est une union finie d'ensembles de la forme $X^* X_1 \times \gamma^{-1} g' \times X_2 X^*$ où X_1 et X_2 sont des parties de X et où $\gamma^{-1} g' \in \mathfrak{F}$ pour chacun des g' .

(iii) Quel que soit $m \in M$, $\gamma^{-1}(mM)$ et $\gamma^{-1}(Mm)$ appartiennent à $\mathfrak{F}$.

Soit encore $f \in \gamma^{-1}(mM)$, et soit g le facteur gauche de longueur minimale de

f tel que γg et m appartiennent à la même $\mathcal{R}$-classe. On peut écrire $g = g'x$ où $x \in X$ et $g' \in X^*$, et tenant compte de ce que M est fini, on voit que, comme plus haut, la $\mathcal{Q}$-classe de m appartient au résiduel de $\gamma g'$. Utilisant encore (i), on en conclut que $\gamma^{-1} g' \in \mathfrak{F}$ quand la $\mathcal{Q}$-classe de m contient deux éléments ou plus (si cette $\mathcal{Q}$-classe ne contenait qu'un seul élément, et si le résiduel de m ne contenait pas deux éléments, on aurait $mM = MmM$). Le même raisonnement que dans (ii) achève la vérification de (iii).

Ceci termine aussi la vérification de la propriété 3, car l'hypothèse que tous les sous-groupes de M sont triviaux équivaut à l'identité

$$\{m\} = (mM \cap Mm) \backslash W_m \qquad \text{pour tout } m \in M .$$

BIBLIOGRAPHIE

[1] KLEENE (S. C.). - Representation of events in nerve nets and finite automata, Automata studies, p. 1-41. - Princeton, Princeton University Press, 1956 (Annals of Mathematics Studies, 34).

[2] McNAUGHTON (R.). - Symbolic logic and automata. - Washington, Wright Air Development Center, 1960 (W. A. D. C. Technical Report).

C. R. Acad. Sc. Paris, t. 261, p. 2419-2420 (27 septembre 1965). Groupe 1.

ALGÈBRE. — *Sur une question concernant certains sous-monoïdes libres.* Note (*) de M. **Marcel Paul Schützenberger**, présentée par M. Paul Montel.

On répond à une question posée par Golomb et Gordon (2), p. 370.

Soient X^* le monoïde libre engendré par un ensemble fixe fini $X \neq \emptyset$ et $X_1^* = X^* \setminus \{f^{2+n} : f \in XX^* ; n \in N\}$. Pour tout $A \subset X^*$, on note A^* le sous-monoïde engendré par A et si $f \in X^*$ on pose $\rho_A f = \{aa' : a, a' \in A^* ; f = a'a\}$. On considère les conditions suivantes sur A où $p < 0 < p'$ [*cf.* (1) et (2)] : $U_s(p, p')$. *Si les* $f_j \in XX^*$ $(p < j < j+1 < p')$ *sont tels que* $f_j f_{j+1} \in A^*$ *identiquement, alors* $f_0 \in A^*$.

U'_s. *Pour tout* $f \in X^*$, $\rho_X f \cap A^* = \rho_A f$.

U''_s. *Pour tout* $f \in X^* \setminus A^*$, $\{f\}^* \cap A^* \cap XX^* = \emptyset$.

Si $\overline{p} \leqq p$ et $p' \leqq \overline{p}'$ on a $U_s(p, p') \Rightarrow U_s(\overline{p}, \overline{p}') \Rightarrow U'_s \,\&\, U''_s$. Si $\alpha_A = (\alpha_{n+1})_{n \in N}$, où $\alpha_{n+1} = \mathrm{Card}(A \cap X^{n+1})$, $U'_s \,\&\, U''_s$ impliquent $\alpha_n \leqq P_n(\alpha_A)$, où, d'après (2), $nP_n(\alpha_A)$ est la fonction des $n-1$ premiers termes de α_A exprimant à l'aide de la formule de Moreau [(3) p. 501-503] le nombre des $f \in X_1^* \cap X^n$ tels que $\rho_X f \cap A^2 A^* = \emptyset$. La propriété suivante répond à une question de (2). La même construction, inspirée de Širšov (4) et Lazard (5), donne aussi les codes de W. L. Eastman cités dans (2).

Propriété. — *Soient* $\alpha' = (\alpha'_{n+1})_{n \in N}$ *une suite d'entiers telle que* $0 \leqq \alpha'_n \leqq P_n(\alpha')$ *identiquement et* $q = \sum_{n>0} (P_n(\alpha') - \alpha'_n)$. *Il existe un* $A \subset X^*$ *satisfaisant* $\alpha_A = \alpha'$ *et* $U_s(-q, 1)$ *(et, par conséquent,* $AXX^* \cap A) = \emptyset$.

Vérification. — Étant donnée une suite $(\varepsilon_i, B_i)_{i \in N}$ $(\varepsilon_i = \pm 1, B_i \subset X^*)$ on pose $A_0 = X$ et, inductivement,

$$A_{i+1} = (A_i \cap B_i)^* . (A_i \setminus B_i) \quad \text{ou} \quad = (A_i \setminus B_i) . (A_i \cap B_i)^*$$

selon que $\varepsilon_i = -1$ ou $+1$. Les A_i^* forment une suite non croissante, et en posant $A = \lim_{i \to \infty} \bigcap_{i' < i} A_{i'}$, on a $A^* = \lim_{i \to \infty} A_i^*$.

Considérons les énoncés suivants où, sans perte de généralité, on supposera $\varepsilon_0 = -1$ et $\emptyset \neq B_i = B_i \cap A_i \neq A_i$ $(0 \leqq i < k)$.

I. A_k *satisfait* $U_s(p_k, p'_k)$, où $p_k + p'_k = k + 2$ et $p_k + p'_k = \sum_{i<k} \varepsilon_i$.

II. *Pour tout* $f \in XX^*$, *un et un seul des sous-monoïdes* $B_0^*, B_1^*, \ldots, B_{k-1}^*, A_k^*$ *a une intersection non vide avec* $\rho_X f$.

III. $A_k^{p'_k - 1} X^* \cap X^* A_k^{-p_k - 1} \subset A_k^*$.

Les énoncés sont triviaux pour $j = 0, 1$ car $ff' \in A_1 A_1^* \Rightarrow f' \in A_1 A_1^*$. Donc A_1 satisfait U'_s & U''_s et l'on peut trouver un ensemble $\bar{X}$, des sous-ensembles $\bar{B}_i, \bar{A}_i \subset \bar{X}^*$ et un monomorphisme $\psi : \bar{X}^* \to X^*$ tels que $\psi \bar{B}_i = B_{i+1}$; $\psi \bar{A}_i = A_{i+1}$ identiquement.

Supposons I, II et III établis pour $k < i \geq 2$ et soit $k = i$.

Pour I. Pour $p_i + 1 < j < j + 1 < p'_i$, on a $f_j \in A_1^*$ et il existe donc des $\bar{f}_j \in \bar{X}^*$ tels que $\psi \bar{f}_j = f_j$ et $\bar{f}_j \bar{f}_{j+1} \in \bar{A}_{i-1}$. L'hypothèse d'induction donne $\bar{f}_0 \in \bar{A}_{i-1}^*$ ce qui établit $f_0 = \psi \bar{f}_0 \in A_i^*$.

Pour II. Comme $A_1 A_1^* \subset X^* \setminus B_0^*$, ou bien $\rho_X f \cap B_0^* \neq \emptyset$ et

$$\rho_X f \cap A_i^* \subset \rho_X f \cap A_i^* = \emptyset, \qquad \text{ou bien} \quad g \in \rho_X f \cap A_1^* \neq \emptyset.$$

Dans ce dernier cas $g = \psi \bar{g}$, où $\bar{g} \in \bar{X}^*$ et l'énoncé résulte de l'hypothèse d'induction.

Pour III. Soit $g = af = f'a'$, où $a \in A_i^{p'_i - 1}$, $f \in X^*$, $f' \in X^* A_i$, $a' \in A_i^{-p_i - 1}$. Comme $f, f' \in A_1^*$, on a $g = \psi \bar{g}$ où $\bar{g} = \bar{a}\bar{f} = \bar{f}'\bar{a}'$ avec $\bar{a} \in \bar{A}_{i-1}^{p'_i - 1}$, $\bar{f}, \bar{f}' \in \bar{X}^*$ et $\bar{a} \in \bar{A}_{i-1}^{-p_i - 1}$. Donc $\bar{g} \in \bar{A}_{i-1}^*$, d'après l'hypothèse d'induction, et $g = \psi \bar{g} \in A_i^*$.

Supposons maintenant que les mots $b_0, b_1, \ldots, b_{m-1} \in XX^* \setminus X^k X^*$ soient tels qu'en posant $B_i = \{b_i\}$ $(0 \leq i < m)$ on ait $\alpha'_n = \mathrm{Card}(A_m \cap X^n)$ pour $n \leq k$. Si $f \in X^{k+1}$ et $g \in \rho_X f \cap B_i^* \neq \emptyset$ $(0 \leq i < m)$, on a $g = b_i^{2+p}$ et donc $f \notin X_1^*$. Donc, d'après II, $f \in X_1^* \cap X^{k+1}$ entraîne $\rho_X f \cap A_m^* \neq \emptyset$ et d'après U'_s, si $\rho_X f \cap A_m^2 A_m^* = \emptyset$, $\rho_X f \cap A_m^*$ se réduit à un élément unique de A_m. Ceci montre que $\mathrm{Card}(A_m \cap X^{k+1}) = P_{k+1}(\alpha')$ et qu'on peut prendre $d = P_{k+1}(\alpha') - \alpha'_{k+1} > 0$ éléments distincts $b_m, b_{m+1}, \ldots, b_{m+d-1}$ dans $A_m \cap X^{k+1}$. Posant $B_{m'} = \{b_{m'}\}$, $(m - 1 \leq m' < m + d)$, on a $\mathrm{Card}(A_{m+d-1} \cap X^n) = \alpha'_n$ pour $n \leq k + 1$, ce qui établit la propriété par induction sur k et passage à la limite en observant que tous les ε_i peuvent être pris égaux à -1. On notera que si $q < \infty$ on a la relation $1 = \sum_{n>0} (\mathrm{Card}\, X)^{-n} \mathrm{Card}(A \cap X^n)$ qui se vérifie facilement par induction sur les A_i $(i \in N)$ en observant que $A_i^* = A_{i+1}^* . (A_i \cap B_i^*)^*$ ou $(A_i \cap B_i)^* . A_{i+1}^*$ selon le signe de ε_i.

(*) Séance du 20 septembre 1965.

(1) S. W. Golomb, B. Gordon et L. R. Welch, *Canadian J. Math.*, 10, 1958, p. 202-209.
(2) S. W. Golomb et B. Gordon, *Information and Control*, 8, 1965, p. 355-372.
(3) E. Lucas, *Théorie des Nombres*, Paris, 1891.
(4) A. I. Širšov, *Mat. Sbornik*, 33, (75), 1953, p. 441-452.
(5) M. Lazard, *Istituto Mat. dell'Universita*, Roma, 1960.

(*Institut Blaise Pascal*, 23, *rue du Maroc, Paris.*)

Reprinted from Information and Control, Volume 8, No. 2, April 1965

INFORMATION AND CONTROL **8**, 190–194 (1965)

On Finite Monoids Having Only Trivial Subgroups

M. P. Schützenberger

An alternative definition is given for a family of subsets of a free monoid that has been considered by Trahtenbrot and by McNaughton.

I. INTRODUCTION

Let X^* be the free monoid generated by a fixed set X and let $\mathbf{Q}$ be the least family of subsets of X^* that satisfies the following conditions (K1) and (K2):

(K1). $X^* \in \mathbf{Q}$; $\{e\} \in \mathbf{Q}$ (e is the neutral element of X^*); $X' \in \mathbf{Q}$ for any $X' \subset X$.

(K2). If A_1 and A_2 belong to $\mathbf{Q}$, then $A_1 \cup A_2$,

$$A_1 \backslash A_2 \ (= \{f \in A_1 : f \notin A_2\})$$

and $A_1 \cdot A_2 \ (= \{ff' \in X^* : f \in A_1 ; f' \in A_2\})$ belong to $\mathbf{Q}$.

With different notations, $\mathbf{Q}$ has been studied in Trahtenbrot (1958) and, within a wider context, in McNaughton (1960). According to Eggan (1963), $\mathbf{Q}$ contains, for suitable X, sets of arbitrarily large star-height (cf. Section IV below).

For each natural number n, let $\Gamma(n)$ denote the family of all epimorphisms γ of X^* such that **Card** $\gamma X^* \leqq n$ and that γX^* has only trivial subgroups (i.e., $\gamma f^n = \gamma f^{n+1}$ for all $f \in X^*$, cf. Miller and Clifford (1956)).

Main Property. $\mathbf{Q}$ *is identical with the union* $\mathbf{Q}'$ *over all* n *of the families*

$$\mathbf{Q}'(n) = \{A \subset X^* : \gamma^{-1}\gamma A = A ; \gamma \in \Gamma(n)\}$$
$$(= \{\gamma^{-1}M' : M' \subset \gamma X^* ; \gamma \in \Gamma(n)\}).$$

As an application, if $A, A' \subset X^*$ are such that for at least one triple $f, f', f'' \in X^*$, both $\{n \in \mathbf{N} : f'f^n f'' \in A\}$ and $\{n \in \mathbf{N} : f'f^n f'' \in A'\}$ are infinite sets of integers, we can conclude that no $B \in \mathbf{Q}$ satisfies $A \subset B$ and $A' \subset X^* \backslash B$.

II. VERIFICATION OF $\mathbf{Q} \subset \mathbf{Q}'$

The next two remarks are reproduced from Petrone and Schützenberger (1963) for the sake of completeness.

REMARK 1. $\mathbf{Q}'$ *satisfies* (K1).

Verification. Let the monoid $M = \{e', x', 0\}$ and the map $\gamma : X^* \to M$ be defined as follows: $\gamma e = e' = e'^2$; for each $x \in X'$, $\gamma x = x' = e'x' = x'e'$; for each $f \in X^* \backslash (\{e\} \cup X')$, $\gamma f = 0 = e'0 = 0e' = x'^2 = x'0 = 0x' = 0^2$.

It is clear that $\gamma \in \Gamma(3)$ and, since $X^* = \gamma^{-1}M$; $\{e\} = \gamma^{-1}e'$; $X' = \gamma^{-1}x'$, the remark is verified.

REMARK 2. $\mathbf{Q}'$ *satisfies* (K2).

Verification. For $j = 1, 2$ let $\gamma_j : X^* \to M_j$ and $M_j' \subset M_j$ satisfy $\gamma_j \in \Gamma(n_j)$ and $A_j = \gamma_j^{-1}M_j'$. We consider the family R of all sets of pairs $(m_1, m_2) \in M_1 \times M_2$ and for $m_1 \in M_1$, $m_2 \in M_2$, $r = \{(m_{1,i}, m_{2,i}) : i \in I_r\}$, we let $m_1 r = \{(m_1 m_{1,i}, m_{2,i}) : i \in I_r\}$ and $r m_2 = \{(m_{1,i}, m_{2,i} m_2) : i \in I_r\}$. Finally, letting $\bar{M}$ denote the direct product of sets $M_1 \times R \times M_2$, we define an associative product on $\bar{M}$ and an epimorphism γ of X^* onto a subset M of $\bar{M}$ by setting for all (m_1, r, m_2), $(m_1', r', m_2') \in \bar{M}$ and $f \in X^*$:

$$(n_1, r, m_2)(m_1', r', m_2') = (m_1 m_1', m_1 r' \cup r m_2', m_2 m_2');$$

$$\gamma f = (\gamma_1 f, \{(\gamma_1 f', \gamma_2 f'') : f', f'' \in X^*; f'f'' = f\}, \gamma_2 f).$$

It is clear that $A_1 \cup A_2$, $A_1 \backslash A_2$ and $A_1 \cdot A_2$ are images by γ^{-1} of suitable subsets of M. Since $\bar{M}$ is finite, the remark will follow from the fact that any subgroup $G = \{(m_{1,i}, r_i, m_{2,i}) : i \in I_G\}$ of $\bar{M}$ is isomorphic to a direct product $G_1 \times G_2$ where G_j is a suitable subgroup of M_j $(j = 1, 2)$.

Indeed, by construction $\{m_{j,i} : i \in I_G\}$ is a homomorphic image of G, hence a subgroup G_j of M_j. Let e_j denote the neutral element of G_j $(j = 1, 2)$ and let N be the intersection of G with the subset $\{(e_1, r, e_2) : r \in R\}$ of $\bar{M}$. Since G is finite N is a normal subgroup of G and G/N is isomorphic to a subgroup of $G_1 \times G_2$. Therefore it suffices to show that N reduces to the neutral element $e' = (e_1, r, e_2)$ of G. To see this, let $g = (e_1, s, e_2)$ and $h = (e_1, t, e_2)$ be elements of N inverse of each other. The relations $e' = e'^2$, $e' = gh$, and $g = e'ge'$ give, respectively, $r = e_1 r \cup r e_2$, $r = e_1 t \cup s e_2$, and $s = e_1 r \cup e_1 s e_2 \cup r e_2$. From the second and the first of these equations we get $e_1 t \cup e_1 s e_2 = e_1 r \subset r$. Thus, using the third equation, $s = r \cup e_1 s e_2$ where, as we have just seen, $e_1 s e_2 \subset r$. This gives $s = r$; hence $e' = g = h$, concluding the verification of the Remark

and of $\mathbf{Q} \subset \mathbf{Q}'$ since $\mathbf{Q}$ is defined as the least family to satisfy (K1) and (K2).

III. VERIFICATION OF $\mathbf{Q}' \subset \mathbf{Q}$

The family $\mathbf{Q}'(1)$ consists of X^* and of the empty set. Thus $\mathbf{Q}'(1) \subset \mathbf{Q}$ and it will suffice to consider an arbitrary fixed $\gamma \in \Gamma(n)$ and to show $\gamma^{-1}M' \in \mathbf{Q}$ for all $M' \subset M = \gamma X^*$ under the induction hypothesis $\mathbf{Q}'(n-1) \subset Q$.

REMARK 3. *If $W_{M'} = \{m \in M : MmM \cap M' = \emptyset\}$ contains two elements or more, then $\gamma^{-1}M' \in \mathbf{Q}$.*

Verification. Let β be a map of M onto a set $\bar{M}$ that has the following two properties: β sends $W_{M'}$ on a distinguished element 0 of $\bar{M}$; the restriction of β to $M \backslash W_{M'}$ is a bijection onto $\bar{M} \backslash \{0\}$.

Taking into account that, by definition, $W_{M'} = M \cdot W_{M'} \cdot M$, a structure of monoid is defined on $\bar{M}$ by letting $(\beta m)(\beta m') = \beta(mm')$ for all $m, m' \in M$. Then, if **Card** $W_{M'} \geqq 2$, we have $\beta\gamma \in \Gamma(n-1)$ and, since $\gamma^{-1}M' = (\beta\gamma)^{-1}\beta M'$, the Remark is verified.

REMARK 4. *If M' is an ideal (i.e., if $M' = M'M$ or $= MM'$), then $\gamma^{-1}M' \in \mathbf{Q}$.*

Verification. Because of left-right symmetry and of the finiteness of M, it suffices to consider the two cases of $M' = mM \neq MmM$ and of $M' = MmM \neq M$ where m is an arbitrary fixed element of M.

Let $A = \gamma^{-1}(mM)$ (resp. $= \gamma^{-1}(MmM)$) and $B = A \backslash A \cdot X \cdot X^*$ (resp. $= A \backslash (X^* \cdot X \cdot A \cup A \cdot X \cdot X^* \cup X^* \cdot X \cdot A \cdot X \cdot X^*)$). By construction B is the least subset of X^* such that $A = B \cdot X^*$ (resp. $= X^* \cdot B \cdot X^*$) and the hypothesis $M' \neq M$ is equivalent to $e \notin B$. Further, let $M'' = \{m' \in M : \gamma^{-1}m' \cdot X \cap B \neq \emptyset\}$ (resp. $= \{m' \in M : X \cdot \gamma^{-1}m' \cdot X \cap B \neq \emptyset\}$). Since $\gamma B \subset M' = M'M$ (resp. $= MM'M$) and $e \notin B$, we can find $X_0 \subset X$ and, for each $m' \in M''$, one subset $X_{m'}$ of X (resp. two subsets $X_{m'}$ and $X'_{m'}$ of X) in such a way that $A = X_0 \cdot X^* \cup \{\gamma^{-1}m' \cdot X_{m'} \cdot X^* : m' \in M''\}$ (resp. $= X^* \cdot X_0 \cdot X^* \cup \{X^* \cdot X'_{m'} \cdot \gamma^{-1}m' \cdot X_{m'} \cdot X^* : m' \in M''\}$) and we have only to check **Card** $W_{\{m'\}} \geqq 2$ for all $m' \in M''$.

First, let us recall the following consequence of Green (1951). *If P is a finite monoid and if $u, u' \in P$ satisfy $u' \in uP$ and either $u'P \neq uP$ or $Pu'P \neq PuP$, then $Pu'P \subset W_{\{u\}}$.*

Indeed, assume $u' \in uP$ and $Pu'P \not\subset W_{\{u\}}$, that is, assume $u' = ua''$ and $u = au'a'$ for some $a, a', a'' \in P$. We have $u = a^n u (a''a')^n$ for $n = 1$, hence for all $n \geqq 1$. Since P is finite there exist two positive integers r and

q such that $a^{rq} = a^q a^{rq}$. It follows that $u = a^{rq}u(a''a')^{rq} = a^q a^{rq}u \cdot (a''a')^{rq} = a^q u$ from which we deduce $u = a^{rq}u(a''a')^{rq} = u(a''a')^{rq} = u'a'(a''a')^{rq-1}$ showing $u \in u'P$, i.e., $uP \subset u'P$. Since by hypothesis $u'P \subset uP$ this gives the desired relations $u'P = uP$ and $Pu'P = PuP$. (For later reference we note that if P has only trivial subgroups, i.e., if $q = 1$, the same hypothesis give $u = au$ hence $au' = aua'' = ua'' = u'$ and, finally, $u = au'a' = u'a'$).

Consider now $m' \in M''$ and take $f \in \gamma^{-1}m'$ and $x \in X$ such that $fx \in B$ (resp. $x'fx \in B$ for some $x' \in X$). We have $\gamma fx = m'\gamma x \in m'M \cdot$ (resp. $\gamma fx \in m'M$ and $\gamma x'fx \in (\gamma x' \cdot m') \cdot M$). Because of the minimal character of B, $\gamma fx \cdot M$ $(= M' = M' \cdot M)$ is not equal to $m'M$ (resp. $M \cdot \gamma x'fx \cdot M$ $(= M' = M \cdot M' \cdot M)$ is not equal to $M \cdot \gamma x'f \cdot M$, a fact which implies that, also, $\gamma fx \cdot M \neq m'M$). Thus $M \cdot M' \cdot M \subset W_{\{m'\}}$ and **Card** $W_{\{m'\}} \geqq 2$ because of the hypothesis $M' \neq M \cdot M' \cdot M$ (resp $M \cdot \gamma fx \cdot M \subset W_{\{m'\}}$ and $M \cdot \gamma x'fx \cdot M \subset W_{\{\gamma x'f\}}$, hence, using symmetry, $\gamma x'fx, \gamma x'f, \gamma fx \in W_{\{m'\}}$ with $\gamma x'fx \neq \gamma x'f$).

REMARK 5. *For all $m \in M$, the set $(mM \cap Mm) \backslash W_{\{m\}}$ reduces to $\{m\}$.*

Verification. The hypothesis $m' \notin W_{\{m\}}$, $m' \in mM \cap Mm$ is equivalent to the existence of $a, a', a_1'', a_2'' \in M$ such that $m = am'a'$; $m' = ma_1''$; $m' = a_2''m$. As mentioned above the first two relations imply $m = m'a'$ and $m' = am'$. Thus, by symmetry, $m = am'$ and $m' = m'a'$ showing $m = m'$. This concludes the verification of Remark 5 and, in view of Remark 4, it also concludes the verification of $\mathbf{Q} = \mathbf{Q}'$.

IV. AN EXAMPLE OF EGGAN

Let $X = \{x_n\}_{n \in \mathbf{N}}$ and for each $k \in \mathbf{N}$ let λ_k be the endomorphism of X^* that sends each $x_n \in X$ onto $x_{n+n'}$ where $n' = 2^k - 1$ if $n < 2^k$ and $n' = 0$, otherwise. Setting $B_1 = \{x_1\}$, we define inductively for $k > 1$, $B_k = B_{k-1}^* \cdot (\lambda_k B_{k-1})^* \cdot \lambda_k x_0$ where for any $A \subset X^*$, A^* denotes the submonoid generated by A. In Eggan (1963), p. 389, it is shown that $B_k{}^*$ (denoted by $\mid \beta_k{}^* \mid$) has exactly star-height k.

It is clear that $B_1 \in \mathbf{Q}$ and, to verify $B_{k+1} \in \mathbf{Q}$, it suffices to verify $B_k{}^* \in \mathbf{Q}$ under the induction hypothesis that $\gamma^{-1}\gamma B_k = B_k$ for some epimorphism γ of X^* onto a finite monoid having only trivial subgroups. Consider any element $f \in X^* \cdot B_k$. Induction on the number of times $\lambda_k x_0$ appears in f shows that either $f \in B_k{}^* \cdot B_k$ or $f \in V_k = \{f' \in X^* : f'X^* \cap B_k{}^* = \emptyset\}$. Thus $B_k{}^* = \{e\} \cup X^* \cdot B_k \backslash V_k$ and since $V_k = \gamma^{-1}M'$ where $M' = \{m \in \gamma X^* : m \cdot \gamma X^* \cap \gamma B_k = \emptyset\}$ the result follows from the induction hypothesis.

It may not be too irrelevant to recall the following example which shows that sets of star-height one can have associated arbitrarily complex groups. Let x and y be two distinct elements of X and, for $n > 3$, let $C_n = \{x^n, x^{n-1}yx, x^{n-2}y, yx^{n-1}\} \cup \{x^iyx^{n-i-1} : 1 \leqq i \leqq n-3\}$. Applying the theorem of Teissier (1951) shows that if ρ is a homomorphism of X^* into a finite monoid such that the sets $\rho C_n{}^*$ and $\rho C_n{}^* \cdot \rho x$ are disjoint, then ρX^* contains at least one subgroup which admits the symmetric group $\mathfrak{S}_n$ as a quotient group.

RECEIVED: March 20, 1964

REFERENCES

EGGAN, L. C. (1963), Transition graphs and the star-height of regular events. *Michigan Math. J.* **10,** 385–397.

GREEN, J. A. (1951), On the structure of semi-groups. *Ann. Math.* **54,** 163–172.

MCNAUGHTON, R. (1960), Symbolic logic and automata. WADC Tech. Rept. 60–244.

MILLER, D. D., AND CLIFFORD, A. H. (1956), Regular D-classes in semigroups. *Trans. Am. Math. Soc.* **82,** 270–280.

PETRONE, L., AND SCHÜTZENBERGER, M. P. (1963), Sur un problème de McNaughton. Rapport CETIS·EURATOM.

TEISSIER, M. (1951), Sur les équivalences régulières dans les demi-groupes. *Compt. Rend. Acad. Sci. Paris* **232,** 1987–1989.

TRAHTENBROT, B. A. (1958), Sintes logiceskikh setei .... *Dokl. Akad. Nauk SSSR* **118,** 646–649.

Reprinted from INFORMATION AND CONTROL, Volume 8, No. 4, August 1965

INFORMATION AND CONTROL **8**, 373–376 (1965)

A Remark on Incompletely Specified Automata

M. P. SCHÜTZENBERGER

Institut Blaise Pascal, Paris, France

A remark is proved concerning certain groups associated with any finite automaton which satisfies a given incompletely specified auto-m aton.

INTRODUCTION

Let $X*$ (resp. $Y*$) denote the free monoid generated by a fixed input alphabet X (resp. output alphabet Y) and let $\bar{y}$ be an extra symbol not contained in Y. An *incompletely specified automaton* can be characterized formally by a map $\beta: X* \to Y \cup \{\bar{y}\}$ where for each input word $f \in X*$, $\beta f = y$ if the output at the end of f is $y \in Y$, and $\beta f = \bar{y}$ if the output at the end of f is not specified. A map $\beta': X* \to Y \cup \{\bar{y}\}$ will be said to *satisfy* β iff $\beta f = \beta' f$ for every $f \in X*$ such that $\beta f \neq \bar{y}$. The study of the automata such that their associated map satisfies a given β seems to be a standard topic in automata theory. The Property below is a side remark having its motivation in the point of view taken in (McNaughton, 1960) and in the theory developed in (Krohn and Rhodes, 1963). Further results along the present line have been obtained by L. Verbeek (to appear).

Let β be a fixed map of $X*$ into $Y \cup \{\bar{y}\}$ and, following (Teissier, 1951), let the quotient monoid M_β of $X*$ and the homomorphism $\gamma: X* \to M_\beta$ be defined by the following two conditions:

(i) For any $f, f' \in X*$, if $\beta f \neq \beta f'$ then $\gamma f \neq \gamma f'$.

(ii) If $\bar{\gamma}$ is another homomorphism of $X*$ that fulfils condition i, then M_β is a homomorphic image of $\bar{\gamma} X*$.

If β' is another map of $X*$ into $Y \cup \{\bar{y}\}$, we let the quotient monoid $M_{\beta'}$ and the homomorphism $\gamma': X* \to M_{\beta'}$ be defined in similar manner.

PROPERTY. *Assume that β' satisfies β and that any submonoid of $M_{\beta'}$ admits minimal quasi-ideals. To each subgroup G of M_β* (Miller and Clifford, 1956) *there correspond a subgroup G' of $M_{\beta'}$ and a normal subgroup H of G that satisfy the following two conditions: G/H is a homo-*

morphic image of G'; *for all* $f, f', f_1, f_2 \in X*$, *the relations* $\gamma f, \gamma f' \in H$ *and* $\beta f_1 f f_2 \in Y$ *imply that* $\beta f_1 f' f_2 = \bar{y}$ *or* $= \beta f_1 f f_2$.

The last condition above has been studied in (Elgot and Rutledge, 1962). Following these authors, we shall say that it expresses the statement that H is "*β-compatible.*"

VERIFICATION OF THE PROPERTY

We keep the notation and hypothesis already introduced and we let ρ denote the map $\gamma'\gamma^{-1}$ of $\mathfrak{P}(M_\beta)$ into $\mathfrak{P}(M_{\beta'})$ which sends each $A \subset M_\beta$ onto $\rho A = \{\gamma' f : f \in X*; \gamma f \in A\} \subset M_{\beta'}$. Thus, for any $A, B \subset M_\beta$ we have

$$\begin{aligned} \rho A \cdot \rho B &= \{\gamma' f f' : f, f' \in X*; \gamma f \in A; \gamma f' \in B\} \\ &\subset \{\gamma' f'' : f'' \in X*; \gamma f'' \in AB\} = \rho(AB). \end{aligned} \tag{1}$$

If G is a subgroup of M_β, we have $GG = G$ and (1) gives $\rho G \cdot \rho G \subset \rho(GG) = \rho G$ showing that the union of ρG with the neutral element of $M_{\beta'}$ is a submonoid of $M_{\beta'}$. By hypothesis this submonoid contains at least one subgroup G' which is a minimal quasi-ideal, i.e. which satisfies

$$G' = (G' \cdot \rho G) \cap (\rho G \cdot G') = G' \cdot \rho G \cdot G'. \tag{2}$$

G' is the desired group and, letting $\bar{\rho} A = G' \cap \rho A$ for any $A \subset G$, we show first that $\bar{\rho}\{g\} \neq \emptyset$ for any $g \in G$. Indeed, there is at least one element of G, say g_1, such that $\rho\{g_1\}$ contains at least one element of G', say g_1'. Let g_2 be the inverse of g_1 in G. We have $g_1 g_2 g g_2 g_1 = g$. Using (1), this shows that $\rho\{g\}$ contains the set $A' = g_1' \cdot \rho\{g_2 g g_2\} \cdot g_1'$, which, because of $g_1' \in G'$ and (2), is a subset of G'. Since $\rho\{g_2 g g_2\} \neq \emptyset$ this proves $\bar{\rho}\{g\} \neq \emptyset$ and the equivalent statement $G \subset \gamma\gamma'^{-1} G' (= \{\gamma f : f \in X*; \gamma' f \in G'\})$.

Let $H = \gamma\gamma'^{-1}\{g_0'\} \cap G$ and $H' = \bar{\rho}\{g_0\}$ where $g_0' = g_0'^2 \in G'$ and $g_0 = g_0^2 \in G$. It is well-known that H is a normal subgroup of G, H' a normal subgroup of G' and that the quotient groups G/H and G'/H' are isomorphic. We recall the proof for the sake of completeness. Indeed, from $g_0 = g_0^2$, $G' \cdot G' = G'$ and (1) we deduce that $H' \cdot H' \subset H'$. Since the union of G' with the neutral element of $M_{\beta'}$ admits minimal quasi-ideals, this shows that H' is a subgroup of G', hence that $g_0' \in H'$. Take an arbitrary element $g_1 \in G$. From $g_1 g_0 = g_0 g_1 = g_1$ and (1) we deduce that both $\bar{\rho}\{g_1\} \cdot H'$ and $H' \cdot \bar{\rho}\{g_1\}$ are contained in $\bar{\rho}\{g_1\}$ and, since $g_0' \in H'$ implies that each of these sets contains $\bar{\rho}\{g_1\}$, we can conclude that $\bar{\rho}\{g_1\} = \bar{\rho}\{g_1\} \cdot H' = H' \cdot \bar{\rho}\{g_1\}$. Now, if g_2 is the inverse of g_1 in G, applying (1) to

$g_1g_2 = g_0$ shows that $\rho\{g_1\}\cdot\rho\{g_2\}$ is contained in H'. It follows that if $h, h' \in \bar{p}\{g_1\}$ and $h'' \in \bar{p}\{g_2\}$, we have hh'', $h'h'' \in H'$ showing that $\bar{p}\{g_1\}$ is contained in a single right coset of H'. Using symmetry and $\bar{p}\{g_1\}\cdot H' = H'\cdot\bar{p}\{g_1\}$, it follows that H' is a normal subgroup of G'. Further, for any two elements $g_1, g_3 \in G$, relation (1) gives $\bar{p}\{g_1\}\cdot\bar{p}\{g_3\} \subset \bar{p}\{g_1g_3\}$ showing that the restriction of $\bar{p}$ to the one-element subsets of G can be considered as a homomorphism of G onto G'/H' and our partial result is proved since, by definition, $H = \gamma\gamma'^{-1}\{g_0'\} \cap G$ is the kernel of this homomorphism.

To conclude the verification it only remains to show that H is β-compatible. However, H is a subset of $\gamma\gamma'^{-1}\{g_0'\}$ and we have only to check that for any $f, f', f_1, f_2 \in X^*$ the relations $\gamma f, \gamma f' \in \gamma\gamma'^{-1}\{g_0'\}$ and $\beta f_1 f f_2 \in Y$ imply $\beta f_1 f' f_2 \in \{\beta f_1 f f_2\} \cup \{\bar{y}\}$. The first relation gives $\gamma' f = \gamma' f'$, hence $\beta' f_1 f f_2 = \beta' f_1 f' f_2$ according to the definition of $M_{\beta'}$ and γ'. Thus $\beta f_1 f f_2 = \beta' f_1 f' f_2 \in Y$ since $\beta f_1 f f_2 \in Y$ and since we have postulated that β' satisfies β. For the same reason we must have $\beta f_1 f' f_2 = \{\beta' f_1 f' f_2\} \cup \{\bar{y}\}$ and the verification of our property is completed.

EXAMPLES

1. The property is vacuous if it imposes no restriction upon the subgroups of the monoid $M_{\beta'}$. Assuming that M_β is finite we show that a necessary condition for this is the existence of a natural number p such that for all $f, f', f'' \in X^*$ the set $\{\beta f f'^n f'' : n \geqq p\}$ contains at most one letter from Y. Indeed, since M_β is assumed to be finite, there corresponds to each $m \in M_\beta$ a natural number p_m such that $\{m^n : n \geqq p_m\}$ is a cyclic subgroup of M_β. Taking $p = \max\{p_m : m \in M_\beta\}$, it follows that for each $f \in X^*$ the set $\{\gamma f^n : n \geqq p\}$ is a cyclic group and in order that the property be vacuous each of these groups must be β-compatible, which is precisely the condition given above.

2. Let x_1 and x_2 (resp. y_1 and y_2) be two distinct elements of X (resp. of Y) and let n be a fixed integer at least equal to 5. Further, let $\beta^{-1}y_1$ be the submonoid of X^* generated by the set

$$\{x_1^n, x_1^{n-1}x_2x_1, x_1^{n-2}x_2, x_2x_1^{n-1}\} \cup \{x_1^i x_2 x_1^{n-i} : 0 < i < n-2\}$$

and $\beta^{-1}y_2 = (\beta^{-1}y_1)\cdot x_1$. Computing the syntactic monoid M_β shows that it contains a subgroup G isomorphic to the symmetric group on n objects and that the subgroup of G corresponding to the alternating subgroup is not β-compatible. Thus, by our property, any β' with $M_{\beta'}$ finite which satisfies β must contain a subgroup G' which is isomorphic

with G (since for $n \geqq 5$ the symmetric group admits no proper non-trivial normal subgroup except the alternating group). This implies, for instance, that none of the sets $\beta'^{-1}y_i$ $(i = 1, 2)$ can be described within the "L_π-language" of (McNaughton, 1960) since, as it is known, this last requirement would imply that all the subgroups of $M_{\beta'}$ are abelian (for a formulation in the so called "algebraic terminology" of the relevant part of McNaughton's theory see (Petrone et Schützenberger, 1963)).

RECEIVED: October 19, 1964

REFERENCES

ELGOT, C. C. AND RUTLEDGE, J. D. (1962), Machine properties preserved under state minimisation. *Proc. AIEE 3rd Ann. Symp. Switching Theory.*

KROHN, K. B. AND RHODES, J. L. (1963), Algebraic theory of machines. *In* "Mathematical Theory of Automata," J. Fox, ed., pp. 341–384. Polytechnic Press of the Polytechnic Institute of Brooklyn.

MCNAUGHTON, R. (1960), "Symbolic Logic and Automata" (Wright Air Development Div. Techn. Note No 60. Cincinnati, Ohio, 1960).

MILLER, D. D. AND CLIFFORD, A. H. (1956), Regular D-classes in semigroups. *Trans. Am. Math. Soc.* **82,** 270–280.

PETRONE, L ET SCHÜTZENBERGER, M. P. (1963), Sur un problème de McNaughton. Rapport, Cetis Euratom.

TEISSER, M. (1951), Sur les équivalences régulières dans les demi-groupes. *Compt. Rendus Acad. Sci.* **232,** 1987–1989.

ON A FACTORISATION OF FREE MONOIDS

M. P. SCHÜTZENBERGER

A property is given which relates two results of Spitzer [6]; it also relates two results of Chen, Fox and Lyndon [1]; the same remark applies to work of Meyer-Wunderli [5] and M. Hall [3] and to its generalisation by Lazard [4]. These connections are indicated more fully below.

In what follows, F is the free monoid generated by a fixed set X and F^+ denotes the set of all words of positive length of F. If the words f and f' of F belong to a submonoid F' of F, the words ff' and $f'f$ are said to be F'-*conjugate*. We consider the following conditions, I, I′ and II, on a family $\{Y_j: j\in J\}$ of subsets of F^+ indexed by a totally ordered set J.

(I) (resp. (I′)). Each $f\in F^+$ has at most (resp. at least) one representation in the form $f=f_1f_2\cdots f_n$, $n>0$, where each $f_i\in Y_j$, and $j_1\geqq j_2\geqq\cdots\geqq j_n$.

(II) Each F-conjugate class C has nonempty intersection with the submonoid F_j generated by Y_j for exactly one $j\in J$; further, $C\cap F_j$ is an F_j-conjugate class.

PROPOSITION 1. *Any two of the three conditions* I, I′ *and* II *imply the third one.*

PROOF. Let $\mathfrak{A}$ be the large algebra of F over the real field R. If U is a subset of F, we write $\boldsymbol{U}=\sum\{f: f\in U\}\in\mathfrak{A}$. Since $(1-\boldsymbol{U})^{-1}=1+\sum\{U^m: m>0\}$, it follows that $(1-\boldsymbol{U})^{-1}=\boldsymbol{G}$ iff G is a submonoid freely generated by U.

Let us assume first that I and I′ are satisfied; it follows that each F_j, $j\in J$, is freely generated by Y_j and that $(1-\boldsymbol{X})^{-1}=\prod\{(1-\boldsymbol{Y}_j)^{-1}: j\in J\}$ where the product is taken according to the given ordering of J. Further, $\mathrm{Log}(1-\boldsymbol{X})^{-1}=\sum\{m^{-1}\boldsymbol{X}^m: m>0\}=\sum\{(\lambda f)^{-1}f: f\in F^+\}$ and $\mathrm{Log}(1-\boldsymbol{Y}_j)^{-1}=\sum\{(\lambda_j f)^{-1}f: f\in F^+\cap F_j\}$, where λf (resp. $\lambda_j f$) denotes the length of the word f with respect to the free basis X (resp. Y_j).

For each F-conjugate class C, let π_C denote the linear map of $\mathfrak{A}$ onto R that satisfies $\pi_C f=1$ if $f\in C$ and $\pi_C f=0$ if $f\in F\setminus C$. Since π_C is constant on conjugate classes, for all f', $f''\in F$ we have $\pi_C(f'f'')=\pi_C(f''f')$; it follows that if $\mathfrak{L}\subset\mathfrak{A}$ is the large Lie algebra over R generated by F, then $\pi_C\mathfrak{L}'=0$ for $\mathfrak{L}'=[\mathfrak{L},\mathfrak{L}]$. According to our hy-

Received by the editors April 22, 1963 and, in revised form, June 13, 1963 and September 3, 1963.

pothesis, $\mathrm{Log}(1-X)^{-1}=\mathrm{Log}\prod(1-Y_j)^{-1}$ whence, by the Campbell-Hausdorff formula $\mathrm{Log}(1-X)^{-1}=\sum\{\mathrm{Log}(1-Y_j)^{-1}: j\in J\}+K$ where $K\in\mathfrak{L}'$. Consequently,

$$(1)\qquad \pi_C\,\mathrm{Log}(1-X)^{-1}=\sum\{\pi_C\,\mathrm{Log}(1-Y_j)^{-1}: j\in J\}.$$

If $f\in C$ has the form $f=g^p$ with maximal positive p, it follows that p Card $C=\lambda C$ where λC is the common length of all $f\in C$; in particular, p is independent of the choice of $f\in C$. Now $\pi_C\,\mathrm{Log}(1-X)^{-1}=\sum\{(\lambda f)^{-1}: f\in C\}=(\lambda C)^{-1}$ Card $C=p^{-1}$. From (1) we conclude that

$$(2)\qquad p^{-1}=\sum\{(\lambda_j(C\cap F_j))^{-1}\,\mathrm{Card}\,(C\cap F_j): j\in J\}.$$

If $p=1$, the sum in (2) can have only one nonzero term and II is verified for C. If $p>1$, we conclude from the case $p=1$ that g has an F-conjugate $g'\in F_{j_0}$ for some $j_0\in J$. It follows that $f'=g'^p\in C\cap F_{j_0}$, that $C\cap F_{j_0}$ is an F_{j_0}-conjugate class and that $(\lambda_{j_0}(C\cap F_{j_0}))^{-1}$ Card $(C\cap F_{j_0})=p^{-1}$. It now follows from (2) that $C\cap F_j\neq\varnothing$ iff $j=j_0$, and the implication I & I′⇒II is verified.

Let us assume now that II is satisfied; it follows that for each $j\in J$ one has

$$(3)\qquad \text{for any } f,f'\in F, \text{ if } ff', f'f\in F_j, \text{ then } f,f'\in F_j.$$

Consequently (cf., e.g., [2]), each F_j is freely generated by Y_j and (2), whence (1), holds for every F-conjugate class C. Let α be the natural homomorphism of $\mathfrak{A}$ into the large algebra over R of the free commutative monoid generated by X. We deduce from (1) that $\alpha\,\mathrm{Log}(1-X)^{-1}=\sum\{\alpha\,\mathrm{Log}(1-Y_j)^{-1}: j\in J\}$, or, in equivalent fashion that $\alpha(1-X)^{-1}=\alpha\prod\{(1-Y_j)^{-1}: j\in J\}$. Now, I (resp. I′) is equivalent to $S+\prod(1-Y_j)^{-1}=(1-X)^{-1}$ where S (resp. $-S$) is an element of $\mathfrak{A}$ in which every $f\in F$ has non-negative coefficient. Since $\alpha S=0$ implies $S=0$, the implication I & II⇒I′ (resp. I′ & II⇒I) is verified.

Example 1. Let σ be a homomorphism of F into the additive group of R and identify J with R. For $r\in R$, let Y_r be the set of all $f\in F^+$ such that $\sigma f=r\lambda f$ and that $\sigma f'<r\lambda f'$ for every factorisation $f=f'f''$ $(f'\neq 1, f)$. The fact that $\{Y_r: r\in R\}$ satisfies I and I′ (resp. II) is proved by Spitzer in [6, p. 327] (resp. p. 324).

Example 2. Let $\leqq$ denote a lexicographic order on F and let J be the set H of all $f\in F^+$ such that $f=f'f''$ for $f', f''\in F^+$ implies $f<f''f'$. Let $Y_h=\{h\}$, for each $h\in H$. The fact that I, I′ and II are satisfied is due to Chen, Fox and Lyndon [1] (cf. also [7]). A similar result holds when H is replaced by the set obtained by "removing the brackets" from Hall's *basic commutators* ([5] and [3, Chapter 11]).

We conclude with the following application of the "elimination method" of Lazard [4].

PROPOSITION 2. *Let F be a free monoid, and P_1 and P_2 two subsets of F such that $F^+ = P_1 + P_2$. Then there exists a unique pair of subsets $Y_1 \subset P_1$ and $Y_2 \subset P_2$ such that*

$$F = (1 - Y_1)^{-1}(1 - Y_2)^{-1}. \tag{4}$$

PROOF. Let X be a free set of generators of F and let $X_{i,0} = X \cap P_i$ $(i = 1, 2)$. Then $W_0 = (1 - X_{2,0})^{-1} X_{2,0} X_{1,0} (1 - X_{1,0})^{-1}$ is the sum of all $f = f_2 f_1$ where f_1 is a nontrivial word in the elements of $X_{1,0}$ and f_2 in those of $X_{2,0}$. It follows that $F = (1 - X_{1,0})^{-1}(1 - W_0)^{-1}(1 - X_{2,0})^{-1}$. If we let $Y_{i,0} = X_{i,0}$ $(i = 1, 2)$ this establishes for $k = 0$ the inductive hypothesis that

$$X_{i,k} \subset Y_{i,k} \subset P_i \quad (i = 1, 2) \quad \text{and} \quad F = F_{1,k}(1 - W_k)^{-1} F_{2,k} \tag{5}$$

where

$$F_{i,k} = (1 - Y_{i,k})^{-1} \quad (i = 1, 2) \quad \text{and} \quad W_k = F_{2,k} X_{2,k} X_{1,k} F_{1,k}.$$

Suppose (5) is satisfied for some $k \geqq 0$. We construct inductively a sequence of subsets $W_{k,n}$ of W_k for all $n \geqq 0$. First we take $W_{k,0} = \varnothing$. Supposing $W_{k,n}$ given we define $W_{k,n+1}$ to be the union of $W_{k,n}$ with the set of all words of minimal length in the complement of $(W_{k,n} \cap P_1) F_{1,k} \cup F_{2,k}(W_{k,n} \cap P_2)$ in W_k. We now define

$$X_{i,k+1} = \bigcup_{n \geqq 0} (W_{k,n} \cap P_i); \qquad Y_{i,k+1} = Y_{i,k} \cup X_{i,k+1} \qquad (i = 1, 2).$$

Thus, $X_{i,k+1} \subset Y_{i,k+1} \subset P_i$ $(i = 1, 2)$. To complete the verification that (5) holds for $k+1$, we need to show first

$$W_k = X_{1,k+1} F_{1,k} + F_{2,k} X_{2,k+1}. \tag{6}$$

Indeed, by the inductive hypothesis each $f \in W_k$ has a unique representation in the form $f = f_2 f_1$, where $f_1 \in X_{1,k} F_{1,k}$ and $f_2 \in F_{2,k} X_{2,k}$. Taking $W_k = F_{2,k} W_k F_{1,k}$ into account, it follows that there exist two sets T_1 and T_2 such that $T_1 = X_{1,k+1} F_{1,k}$, $T_2 = F_{2,k} X_{2,k+1}$, and $W_k = T_1 \cup T_2$. Thus the proof of (6) needs only the verification that $T_1 \cap T_2 = \varnothing$.

Let $f \in T_2$. By definition $f = g_2 f_2 f_1$, where $g_2 \in F_{2,k}$, $f_2 \in F_{2,k} X_{2,k}$, $f_1 \in X_{1,k} F_{1,k}$, and $f_2 f_1 \in W_{k,n} \cap P_1$ for some $n \geqq 0$. The definition of $W_{k,n}$ implies that $f_2 f_1 \notin X_{1,k+1} F_{1,k}$. Thus, for each $n' \geqq 0$ and for each left factor $f_1' \in X_{1,k} F_{1,k}$ of f_1, we have $f_2 f_1' \notin W_{k,n'} \cap P_1$. It follows that for each such f_1' we have $f_2 f_1' \in T_2$, hence $g_2 f_2 f_1' \in T_2$, and finally $g_2 f_2 f_1' \notin W_{k,n''} \cap P_1$ for all $n'' \geqq 0$. This shows that $f = g_2 f_2 f_1 \notin T_1$ and $T_1 \cap T_2 = \varnothing$, hence (6) is proved.

For the rest, we compute as follows:

$$
\begin{aligned}
&(F_{1,k+1}(1 - W_{k+1})^{-1}F_{2,k+1})^{-1}\\
&= (1-Y_{2,k+1})(1-(1-Y_{2,k+1})^{-1}X_{2,k+1}X_{1,k+1}(1-Y_{1,k+1})^{-1})(1-Y_{1,k+1})\\
&= 1-Y_{2,k+1}-Y_{1,k+1}+Y_{2,k+1}Y_{1,k+1}-X_{2,k+1}X_{1,k+1}\\
&= 1-(Y_{2,k}+X_{2,k+1})-(Y_{1,k}+X_{1,k})+(Y_{2,k}+X_{2,k+1})(Y_{1,k}+X_{1,k+1})\\
&\quad -X_{2,k+1}X_{1,k+1}\\
&= 1-Y_{2,k}-Y_{1,k}+Y_{2,k}Y_{1,k}-(1-Y_{2,k})X_{1,k+1}-X_{2,k+1}(1-Y_{1,k})\\
&= (1-Y_{2,k})(1-X_{1,k+1}(1-Y_{1,k})^{-1}-(1-Y_{2,k})^{-1}X_{2,k+1})(1-Y_{1,k})\\
&= F_{2,k}^{-1}(1-W_k)F_{1,k}^{-1}=F^{-1}
\end{aligned}
$$

Finally, since $W_0 \subset FXXF$ and $W_{k+1} \subset FW_kW_kF$, each W_k $(k \geqq 0)$ contains no word of length less than 2^{k+1}. It follows that the same is true for the set complement of $(1-Y_{1,k})^{-1}(1-Y_{2,k})^{-1}$ in F. Thus, letting $Y_i = \bigcup_{k \geqq 0} Y_{i,k}$ $(i=1, 2)$, we have proved the existence of at least one pair of sets satisfying the conditions stated in Proposition 2.

To verify the uniqueness, let us consider any other pair of subsets Y_1' and Y_2' of F^+ that satisfies $F=(1-Y_1')^{-1}(1-Y_2')^{-1}$. We define the subsets U_i, V_i, V_i' $(i=1, 2)$ of F^+ by the relations $U_i = Y_i \cap Y_i'$; $V_i = Y_i - U_i$; $V_i' = Y_i' - U_i$ $(i=1, 2)$. From $F^{-1}=(1-Y_2)(1-Y_1)$ $=(1-Y_2')(1-Y_1')$ we deduce

$$(7) \qquad -V_2 - V_1 + U_2V_1 + V_2U_1 = -V_1' - V_2' + U_2V_1' + V_2'U_1.$$

Now, either $Y_1 = Y_1'$ and $Y_2 = Y_2'$ (i.e., $V_1 \cup V_2 \cup V_1' \cup V_2' = \varnothing$) or else $V_1 \cup V_2 \cup V_1' \cup V_2'$ contains some element f of minimal length. By construction $V_1 \cap V_1' = V_2 \cap V_2' = \varnothing$. Thus (7) shows that $f \in (V_1 \cap V_2') \cup (V_2 \cap V_1')$. Since this last set is empty if $Y_1' \subset P_1$ and $Y_2' \subset P_2$, the verification of Proposition 2 is concluded.

Acknowledgment. I gratefully acknowledge the help of the referee in improving the proofs.

References

1. K. T. Chen, R. H. Fox and R. C. Lyndon, *Free differential calculus*. IV, Ann. of Math. (2) **68** (1958), 81–95.

2. P. M. Cohn, *On subsemigroups of free semigroups*, Proc. Amer. Math. Soc. **13** (1962), 347–357.

3. Marshall Hall, *The theory of groups*, Macmillan, New York, 1959.

4. M. Lazard, *Groupes, anneaux de Lie et problème de Burnside*, Inst. Mat. dell-'Università, Roma, 1960.

5. H. Meyer-Wunderli, *Note on a basis of P. Hall for the higher commutators in free groups*, Comment. Math. Helv. **26** (1952), 1–5.

6. F. Spitzer, *A combinatorial lemma and its application to probability theory*. Trans. Amer. Math. Soc., **82** (1956), 323–339.

7. A. I. Širšov, *On free Lie rings*, Mat. Sb. (N.S.) **45** (**87**) (1958), 113–122.

Université de Poitiers, Poitiers, France

COMMUNAUTE EUROPEENNE DE L'ENERGIE ATOMIQUE - EURATOM

SUR UN PROBLEME DE McNAUGHTON

par

L. PETRONE (Università L. Bocconi, Milan)
M.P. SCHÜTZENBERGER (Université de Poitiers)

1965

Centre Commun de Recherche Nucléaire
Etablissement d'Ispra - Italie
Centre de Traitement de l'Information Scientifique - CETIS

Contrat EURATOM/UNIVERSITA L. BOCCONI N° 015-61-5 CETI

1. Cette note répond à une question posée par R. McNaughton à la fin de son memoire "Symbolic Logic and Automata" [4]. Dans ce travail McNaughton définit deux langages "L" et "L^{II}" pour décrire le "comportement" ("behaviour") d'une certaine famille d'automates (synchrones, déterministes, discrets, finis) et propose ([4] p. 28) le problème de construire explicitement un tel automate dont le "comportement" ne puisse pas être décrit dans "L^{II}" . L'automate B de l'Exemple 1 ci-dessous satisfait ces conditions. Pour vérifier ceci nous remplaçons les définitions de McNaughton par la Définition 1 ci-dessous qui n'a d'autre but que de contenir tous les automates (du type considéré par McNaughton) dont le "comportement" peut être décrit dans L^{II}
La Remarque 1 met en évidence que tous les automates visés par la Définition 1 ont une certaine proprieté abstraite et la vérification que B n'a pas cette propriété est entièrement triviale.

Toutefois la propriété utilisée est trop grossière pour permettre d'établir le même résultat en ce qui concerne l'automate donné par McNaughton à la page 29 de [4].

2. Comme les notations algébriquesne donnent pas la possibilité de réaliser l'économie conceptuelle et la simplicité de notations obtenues par les méthodes logiques de McNaughton, il n'y aurait aucun avantage ici à ne pas prendre pour l'"alphabet d'entrée" X_i (input alphabet) et pour l'"alphabet de sortie" X_u (output alphabet) deux ensembles quelconques. Soit $\underset{\sim}{N}$ l'ensemble des entiers naturels positifs; $\{J\}$ (resp. $\{V\}$), l'ensemble des applications de $\underset{\sim}{N}$ dans $X_i^{\underset{\sim}{N}}$ (resp. dans $X_v^{\underset{\sim}{N}}$).

Le "comportement" d'un automate $\mathcal{M}$ du type considéré peut être identifié à une application $\mu: \{J\} \to \{V\}$ telle que pour chaque $J \in \{J\}$ et $n \in N$ la restriction $(\mu J)_1^{n+1}$ de la "séquence de sortie" μJ à l'intervalle $[1,n]$ soit une fonction (d'une nature particulière discutée plus bas) de la restriction correspondante J_1^{n+1} de la "séquence d'entrée" $J \in \{J\}$. Introduisons selon la Théorie de A. Burks [1] l'ensemble $X = X_i \times X_u$. et considérons le monoide libre F engendré par X .

Il existe deux épimorphismes ρ_i et ρ_u de F sur les monoides libres F_i et F_u, engendrés par X_i et X_u respectivement, qui sont tels que pour tout $x = (x',x") \in X$ $(x' \in X_i , x" \in X_u)$ on ait $\rho_i x = x'$ et $\rho_u x = x"$. Ces conditions définissent ρ_i et ρ_u sans ambiguité.

Pour $\mu: \{J\} \to \{V\}$, $J \in \{J\}$ et $n,n' \in \mathbb{N}$, donnés, nous désignerons par $|\mu, J_n^{n+n'}|$ le mot $f \in F$ tel que $\rho_i f$ et $\rho_u f$ soient respectivement les images dans F_i et dans F_u des restrictions à l'intervalle $[n, n+n'-1]$ de J et de μJ.

Selon Burks [1], un automate $\mathcal{A}$, d'application associée μ, pourra donc être caractérisé par l'ensemble $\mathcal{A}(F)$ des "éléments de son comportement" c'est à dire par l'élément $\mathcal{A}(F) \in \mathcal{P}(F)$ défini par $\mathcal{A}(F) = \{f \in F : f = |\mu, J_1^{n+1}|, J \in \{J\} ; n \in \mathbb{N}\}$ de F Par abus de notation et en vertu de l'hypothèse sur μ impliquée par la notion d'automate séquentielle, $\mathcal{A}(F) = \{f \in F : \rho_u f = \mu \rho_i f\}$ D'autre part si $\mathcal{P}(F)$ (resp. $\mathcal{P}^2(F)$) est l'ensemble des partie de F (resp. de $\mathcal{P}(F)$) et si $P,P' \in \mathcal{P}(F)$, on écrira comme d'habitude $P \backslash P' = \{f \in F : f \in P , f \notin P'\}$, $PP' = \{f \in F : f = f'f" : f' \in P, f" \in P\}$ $P^0 = \{e\}$ où e est l'élément neutre de F. Si $\mathcal{Q} \in \mathcal{P}^2(F)$ on désignera par $\mathcal{Q}^\dagger$ le plus petit $\mathcal{Q}' \in \mathcal{P}^2(F)$ qui satisfasse les conditions suivantes.

(i) $\mathcal{Q} \subset \mathcal{Q}'$; $F \in \mathcal{Q}'$; si $X' \subset X$ alors $X' \in \mathcal{Q}$

(ii) Si $P,P' \in \mathcal{Q}'$ alors PUP' , $P \backslash P'$, $PP' \in \mathcal{Q}$

En particulier $\mathcal{Q}_0 = \{F\}^\dagger$ et, désignant par $X^{(n+1)*} \in \mathcal{P}(F)$ le sous-monoide de F engendré par X^{n+1} $(n \in \mathbb{N})$, on définira $\mathcal{Q}_\Pi$ comme $\mathcal{Q}'^\dagger_\Pi$ où $\mathcal{Q}'_\Pi = U\{X^{(n+1)*} : n \in \mathbb{N}\} \in \mathcal{P}^2(F)$.

3. Dans la famille $\{\mathcal{A}\}$ des automates considérés par McNaughton l'application $\mu: \{J_1^{n+1}\} \to \{V_1^{n+1}\}$ $(n \in \mathbb{N})$ satisfait des conditions très spéciales à la discussion desquelles McNaughton consacre de trop nombreuses pages pour que nous puissions songer à les

reproduire ici in extenso. La Définition 1 ci-dessous est donc à la fois une traduction algébrique et un résumé de la Théorie élaborée dans [4]. Par définition, pour tout $n \in N$ au moins égal à un certain "délai" $d \in N$ fixe (éventuellement égal à 1), la "n+1ième lettre" du "mot de sortie" (c'est à dire, $\rho_u \left| \mu, J_1^{n+1} \right|$) est une certaine fonction ψ' de la "n+1ième lettre" du "mot d'entrée" ($\rho_i \left| \mu, J_n^{n+1} \right|$), des n-premières lettres de "la séquence d'entrée" et de la "séquence de sortie" (c'est à dire, en définitive, de $\left| \mu, J_1^n \right|$).

Dans la Théorie de McNaughton la fonction ψ' ne dépend que des valeurs de vérité de $\underline{\text{Card}}\ X_u$ prédicats incompatibles deux à deux et dont la disjonction est toujours vraie. Chacun de ces prédicats est lui-même exprimable comme une "formule" du langage "L^{II}" (ou "L") . A leur tour ces "formules" de L^{II} et de L sont des formules particulières du calcul des prédicats du premier ordre avec des quantificateurs bornés ("restricted quantifiers").
Elles sont obtenues en composant par des opérations booléennes un nombre fini de prédicats spécifiques des types ci-dessous (1), (2), (3), (4) et (5). ([4] p.6). Comme il s'agit toujours d'une application $\mu = \{J\} \to \{V\}$ et d'un $J \in \{J\}$ donnés, nous pouvons utiliser pour la traduction les conventions faites en [1] sur l'ensemble des éléments du comportement de $\mathcal{M}$.

(1) Le "temps" $n \in N$ est (au moins) égal (au plus égal) à une valeur fixe $n_1 \in N$.

Ceci se traduit par $f \in FX^{n_1}$ ($f \in F \setminus FX^{n_1-1}$, $f \in X^{n_1}$).

(2) La "n-ième lettre du mot d'entrée (de sortie)" est une lettre déterminée $x' \in X_i$. ($\in X_u$).

Ceci se traduit par $f \in X^{n-1}X'F$ où $X' = \{x \in X : \rho_i x = x'\}$ ($\{x \in X' : \rho_u x = x'\}$).

(3) Pour $n_1 \in \mathbb{N}$ fixe, $n \in \mathbb{N}$ supérieur à n_1 et arbitraire, $x' \in X_i$ (resp. $\in X_u$) fixe, la $(n-n_1+1)$-ième lettre du mot d'entrée (de sortie) est x'.

Ceci se traduit par $f \in FX'X^{n_1-1}$ avec X' comme ci-dessus.

(4) Pour le langage L^{II}, le "temps" $n \in \mathbb{N}$ est congruent à n_2 modulo n_1+1 $(n_1, n_2 \in \mathbb{N})$.

La traduction est $f \in X^{(n_1+1)*} X^{n_2}$

Plus généralement nous associerons à L la famille $\mathcal{Q}_0 \in \mathcal{P}^2(F)$ et à L^{II} la famille $\mathcal{Q}_{II} \in \mathcal{P}^2(F)$ et il résulte de $\mathcal{Q}_0 = \mathcal{Q}_0^{\dagger}$ et de $\mathcal{Q}_{II} = \mathcal{Q}_{II}^{\dagger}$ que toutes les fonctions booléennes d'un nombre fini de formules des types qui viennent d'être décrits (c'est à dire toutes celles dont on aura besoin) peuvent être associés sans ambiguité à des prédicats de la forme "$f \in P$" où les P sont des éléments particuliers de $\mathcal{Q}_0$ ou de $\mathcal{Q}_{II}$ selon le langage considéré.

Le dernier prédicat spécifique ([1] p. 6) utilisé par McNaughton est défini par induction à l'aide des prédicats précédents.
Si ces derniers sont dits avoir "hauteur zéro" un prédicat de hauteur au plus $k+1$ est caractérisé par k' $(k' \in \mathbb{N})$ prédicats λ_i $(i=1,2,\ldots,k')$ de hauteur au plus k et exprime pour n arbitraire la propriété suivante:

(5) Il existe une séquence croissante de $k'+1$ entiers $n_1 = 1 < n_2 < \ldots < n_{k'+1} = n$ tels que les k' restrictions $(J_{n_i}^{n_{i+1}}, (\mu J)_{n_i}^{n_{i+1}})$ $(i=1,2,\ldots,k')$ satisfassent chacune le prédicat λ_i correspondant.

Ceci se traduit par $f \in P_1 . P_2 \ldots . P_{k'}$ où les P_i sont les

éléments de $\mathcal{P}(F)$ qui traduisent les prédicats λ_i . Donc, d'après la définition même de l'opération de fermeture †, on a encore $f \in P$ avec $P \in \mathcal{Q}_\Pi$ (ou $P \in \mathcal{Q}_0$).

Enfin, puisque McNaughton ne considère que des alphabets finis la fonction ψ' ne dépend que d'un système fini de prédicats de "L" ou de "L_Π". Il n'y a donc pas de perte de généralité du point de vue de la discussion de l'Exemple 1 à utiliser désormais la définition suivante où les alphabets X_i et X_u sont supposés donnés et où $\mathcal{Q} = \mathcal{Q}_0$ ou $\mathcal{Q}_\Pi$.

Définition 1: Un $\mathcal{Q}$-automate de McNaughton est un 5-tuple $\mathcal{M} = (d, \mu', m, \chi, \psi)$ où $d, m \in \mathbb{N}$, μ' est une application de $F_i \setminus F_i X_i^{d+1}$ dans $F_u \setminus F_u X_u^{d+1}$ préservant la longueur des mots; χ est une partition de F en m éléments $P_1, P_2, \ldots, P_m \in \mathcal{Q}^\dagger$; ψ est une application de $[1,m] \times X_i$ dans X_v .

Par définition: $\mathcal{M}(F) = F \setminus (\bar{M}' \cup \bar{M}'') F$ où $\bar{M}' = \{f \in F \setminus FX^{d+1} \; \rho_u f \neq \mu' \; \rho_i \; f\}$ et où, en posant pour $m' \in [1,m]$ et $x_i \in X_i$, $\bar{X}_{m'} = \{x \in X : \rho_u x \neq \psi(m' , \rho_i \; x)\}$, on a

$$\bar{M}'' = \bigcup_{1 \leq m' \leq m} \{f \in FX^{d+1} : f = f'x \; , \; f' \in FX^{d+1} \cap P_{m'} \; , \; x \in \bar{X}_{m'}\}$$

$$= \bigcup \{(FX^d \cap P_{m'}) \; \bar{X}_{m'} : 1 \leq m' \leq m\}$$

Puisque m est supposé fini, ceci implique donc que $\mathcal{M}(F) \subset \mathcal{Q}^\dagger$ pour tout $\mathcal{Q}$-automate.

Cette définition de l'ensemble $\mathcal{M}(F)$ des "éléments du comportement" de $\mathcal{M}$ traduit la condition que pour les mots d'entrée de longueur au plus de l'application μ est identique à une application μ' arbitraire (qui constitue la condition initiale de McNaughton) et que pour les autres mots, la n+1-ième lettre de sortie est fonction de la n+1 lettre d'entrée et d'un prédicat du type voulu sur les n-premières lettres des mots d'entrée et de sortie.

4. Nous introduisons encore quelques notations. Pour chaque $P \in \mathcal{P}(F)$, on sait [Teissier 1951] qu'il existe un homomorphisme unique φ_P de F dans un monoide quotient $\varphi_P F$ tel que $\varphi_P^{-1}\varphi_P\, P \subset P$ (c'est à dire, $P = \{f \in F : \varphi_P f\, \varphi_P\, P\}$) et que pour tout homomorphisme $\varphi: F \to \varphi F$ tel que $\varphi^{-1}\, \varphi P \subset P$, $\varphi_P\, F$ soit une image homomorphe de φP.

D'autre part, pour chaque monoide M, on peut définir l'ensemble $\underset{\sim}{G}(M)$ des sous-groupes abstraits de M c'est à dire l'ensemble des groupes abstraits G tel qu'il existe au moins un sous-ensemble $M' \subset M$ $(M' \neq \emptyset)$ ayant la propriété que $M'\, M' = M'$ et que la restriction à M' de la structure de monoide de M soit isomorphe à la structure de monoide de G. L'ensemble stable M' lui-même est un sous-groupe de M et la Théorie de ces objets a été établie par A.A. Miller et A.H. Clifford dans [5].

Soit maintenant $\mathcal{G}$ une famille quelconque de groupes abstraits et $\mathcal{G}^{(+)}$ la plus petite famille G' de groupes abstraits telle que $\mathcal{G} \subset \mathcal{G}'$, $G_0 \in \mathcal{G}$ (où G_0 désigne le groupe abstrait d'ordre un) et $G_3 \in \mathcal{G}$ pour toute image homomorphe G_3 de tout sous-groupe de tout produit direct $G_1 \times G_2$ où G_1 et G_2 sont deux éléments quelconques de G'. Nous définissons $\mathcal{Q}(\mathcal{G}) \in \mathcal{P}^2(F)$ comme la famille de tous les $P \in \mathcal{P}(F)$ tels que pour tout ensemble <u>fini</u> $X' \subset X$ l'image par φ_P du sous-monoide $F_{X'}$ de F, engendré par X', soit un monoide fini $\varphi_P F_{X'}$ satisfaisant $\underset{\sim}{G}(\varphi_P F_{X'}) \in G$.

Trois cas particuliers sont utilisés dans la Théorie de McNaughton:

(i) Pour $P = F$, $\varphi_P F$ se réduit à un élément neutre. Donc $\underset{\sim}{G}(\varphi_F F) = \{G_0\} \in \{G_0\}^{(+)}$.

(ii) Pour $P = X' \subset X$, $P \neq \emptyset$; la relation $FX^2F \cap P = \emptyset$ montre que pour tout $f \in FX$ on a $\varphi_P f^2 = u = u^2$ et que, par conséquent, $\underset{\sim}{G}(\varphi_{X'} F)$ $\{G_0\}^{(+)}$

(iii) Pour $P = X^{(n+1)*}$ $(n \in N)$, $\varphi_P F$ est isomorphe au groupe additif des entiers rationnels modulo $n+1$ et, par conséquent $\underset{\sim}{G}(\varphi_{X^{(n+1)*}} F) \in \mathcal{C}_{ab}$, où $\mathcal{C}_{ab}$ $(= \mathcal{C}_{ab}^{(\dagger)})$ est la famille des groupes abéliens.

La remarque suivante est une application triviale de résultats de (Clifford et Miller [5]) à un cas particulier du Théorème de Kleene sur les "événements réguliers" [3]. La vérification en est cependant donnée par souci d'être complet.

Remarque 1: $\mathcal{Q}_0 \subset \mathcal{Q}(\{G_0\}^{(\dagger)})$ et $\mathcal{C}_{II} \subset \mathcal{Q}(\mathcal{C}_{ab})$.

Vérification: Soient $P_1, P_2 \in \mathcal{C}(\mathcal{C})$. D'après la définition même des opérations de fermeture $\dagger$ et $(\dagger)$ et les cas particuliers (i) et (ii) ci-dessus il suffit de vérifier d'abord que pour $P = P_1 \cup P_2$, $= P_1 \setminus P_2$ ou $= P_1\, P_2$ il existe un homomorphisme φ de F sur un monoide M tel que $\varphi^{-1}\varphi P \subset P$ et que les conditions sont satisfaites. Ensuite on montrera que ces conditions sont encore satisfaites pour toute image homomorphe M' de M (donc en particulier pour $\varphi_P F$).

Nous construisons d'abord M. Soient $M_i = \varphi_{P_i} F$ $(i=1,2)$. Pour $m_1 \in M_1$, $m_2 \in M_2$, $r = \{(m_{1,j}, m_{2,j}) : j \in J_r\} \in \mathcal{P}(M_1 \times M_2)$ nous écrivons $m_1 r = \{(m_1\, m_{1,j}, m_{2,j}) : j \in J_r\}$ et $r\, m_2 = \{(m_{1,j}, m_{2,j}\, m_2) : j \in J_r\}$; pour (m_1, r, m_2), $(m_1', r', m_2') \in M_1 \times \mathcal{P}(M_1 \times M_2) \times M_2$ nous posons $(m_1, r, m_2)(m_1', r', m_2') = (m_1\, m_1', m_1\, r' \cup r\, m_2, m_2\, m_2')$ ce qui munit cet ensemble d'un produit associatif et permet de definir un homomorphisme φ de F sur $M \subset M_1 \times \mathcal{P}(M_1 \times M_2) \times M_2$ en posant pour tout $f \in F$ $\varphi f = (\varphi_{P_1} f, \{(\varphi_{P_1} f', \varphi_{P_2} f'') : f', f'' \in F, f'f'' = f\}, \varphi_{P_2} f)$. Il est immédiat que $\varphi^{-1}\varphi P \subset P$ pour $P = P_1 \cup P_1$, $= P_1 \setminus P_2$, $= P_1\, P_2$.

Soit $K = \{(m_{1,g}, r_g, m_{2,g}) : g \in G\}$ un sous-groupe de M. Cette hypothèse implique que, pour $i=1,2$, $\{m_{i,g} : g \in G\}$ est un

sous-groupe de M_i (isomorphe au groupe abstrait G_i) dont l'élément neutre est $m_{i,e}$ avec $m_{i,e}$ défini par la donnée de l'élément neutre $u = (m_{1,e}, r_e, m_{2,e})$ de K. Pour établir que K est isomorphe à un sous-groupe de $G_1 \times G_2$ il suffit de vérifier que si $a = (m_{1,g}, r_g, m_{2,g})$ et $a' = (m'_{1,g'}, r'_{g'}, m'_{2,g'})$ $(a, a' \in K)$ sont tels que $m_{1,g} = m'_{1,g'}$ et $m_{2,g} = m'_{2,g}$ on a $a = a'$, c'est à dire $r_g = r'_{g'}$. En considérant les produits $a\,\bar{a}$ et $a'\bar{a}$ où $\bar{a} \in K$ est défini par $a'\bar{a} = u$ on peut se ramener au cas de $a = u$. Soient donc $v' = (m_{1,e}, r', m_{1,e})$; $\bar{v} = (m_{1,e}, \bar{r}, m_{2,e})$ $(v', \bar{v} \in K)$. Les identités $u = u^2 = u^3$; $uvu = v$; $u\bar{v}u = \bar{v}$ donnent les relations $m_{1,e}\, r_e\, m_{2,e} \subset m_{1,e}\, r_e \cup r_e\, m_{2,e}$; $r = r_e \cup m_{1,e}\, r\, m_{2,e}$; $\bar{r} = r_e \cup m_{1,e}\, \bar{r}\, m_{2,e}$. Comme il résulte de $v\bar{v} = \bar{v}v = u$ que $r_e = m_{1,e}\, \bar{r} \cup r\, m_{2,e} = m_{1,e}\, r \cup \bar{r}\, m_{2,e}$ on en conclut que $r_e = m_{1,e}\, r_e \cup m_{1,e}\, r_e\, m_{2,e} \cup r_e\, m_{2,e} \cup m_{1,e}\, r\, m_{2,e}\, m_{1,e}\, \bar{r}\, m_{2,e}$ d'où $m_{1,e}(r \cup \bar{r}) m_{2,e} \subset r_e$ et, enfin $r_e = r = \bar{r}$ ce qui achève la vérification de ce point.

Finalement, il résulte immédiatement des définitions que $\varphi F_{X'}$, et, par conséquent, $\psi\varphi F_{X'}$, sont finis pour tout sous-monoide $F_{X'} \subset F$ engendré par un sous-ensemble <u>fini</u> $X' \subset X$ et tout homomorphisme $\psi : M \to M'$

Il reste seulement à vérifier que tout sous-groupe K' de $\psi\varphi F_{X'}$ est l'image homomorphe d'au moins un sous-groupe de $\varphi F_{X'}$.

Soit $A = \{\varphi e\} \cup \{m \in \varphi F_{X'} : \psi m \in K'\}$. Nous prenons un élément arbitraire $h \in A$ tel que <u>Card</u>$(h\,A\,h) \leqslant$ <u>Card</u>$(m'\,A\,m')$ pour tout $m' \in A$. Comme $h\,m'\,h\,A\,h\,m'\,h \subset h\,A\,h$, on a nécessairement $m'\,A\,m' = h\,A\,h$ pour tout $m' \in h\,A\,h$. En particulier $h^p\,A\,h^p = h\,A\,h$ pour tout $p \in N$, ce qui montre (puisque A est fini) que l'on peut choisir h tel que $h^2 = h$ et que, par conséquent, $h \in h\,A\,h$. Maintenant, si $m' \in h\,A\,h$ on a $m' = h\,m''\,h$ pour un certain $m'' \in A$ donc $m'h = h\,m'$ et $m'\,A\,m' = m'(h\,A\,h)m'$. Il en résulte que pour chaque $m' \in h\,A\,h$ on a:

Card(h A h) = Card(m' A m') ⩽ Card(m' h A h) ⩽ Card(m' A m' h A h) = Card(h A h A h) ⩽ Card(h A h) ce qui montre que $m'h \cap h = h \cap h m'$ pour tout $m' \in h \cap h$, donc que $h \cap h$ est isomorphe à un groupe, et ce qui achève la vérification de la Remarque 1.

5. Soient $X_i = \{x'_1, x'_2\}$; $X_u = \{x''_1, x''_2\}$ et $\mathfrak{B}$ un automate défini par un ensemble $S = \{s_k : (1 \leqslant k \leqslant 5)\}$ d'états et la table de transition suivante (dans les notations de Gill [2])

	x'_1	x'_2	x'_1	x'_2
s_1	s_1	s_2	x''_2	x''_1
s_2	s_3	s_1	x''_1	s''_1
s_3	s_4	s_4	x''_1	x''_1
s_4	s_5	s_5	x''_1	x''_1
s_5	s_2	s_3	x''_1	x''_1

L'état initial est s_1.

Soient $X = \{x_{j,j'} : j,j' = 1,2\}$ où pour abréger $x_{j,j'} = (x'_j, x''_{j'}) \in X_i \times X_u$ et $B = \mathfrak{B}(F)$ dans les notations de 3.

Considérons $S' = \{s_k : 0 \leqslant k \leqslant 5\}$ et la représentation ψ de F par des applications de S' dans lui-même qui est définie par le tableau suivant où pour chaque ligne k et chaque colonne j,j' l'entrée $(k,(j,j'))$ dénote l'élément $s_k \cdot \psi x_{j,j'} \in S'$

	$x_{1,1}$	$x_{1,2}$	$x_{2,1}$	$x_{2,2}$
s_0	s_0	s_0	s_0	s_0
s_1	s_0	s_1	s_2	s_0
s_2	s_3	s_3	s_1	s_0
s_3	s_4	s_4	s_4	s_0
s_4	s_5	s_5	s_5	s_0
s_5	s_2	s_2	s_3	s_0

Par construction [1] , $\varphi_B F$ est isomorphe à ψF . On vérifie facilement que si F' est le sous-monoide de F engendré par $x_{1,1}$ et $x_{1,1} x_{2,1} x_{2,1}$, $\psi F' \subset \psi F$ est isomorphe au groupe symétrique γ_4 qui n'est pas abélien. Donc $\varphi_B F \notin \mathfrak{Q}(\mathfrak{G}_{ab})$ et par conséquent $\mathfrak{B}_n$ n'est pas un $\mathfrak{Q}_\Pi$ -automate de McNaughton.

BIBLIOGRAPHIE

[1] BURKS A.W. and J.B. WRIGHT
Sequence Generators and Digital Computers
Proc. of Symp. on Recursive Function Theory, Amer. Math. Soc. (1961)

[2] GILL A.
Introduction to the theory of finite state machines
McGraw-Hill (1962)

[3] KLEENE S.C.
Representation of events in nerve nets and finite automata
Automata Studies. Princeton Univ. Press, (1956), 3-41.

[4] McNAUGHTON R.
Symbolic logic and automata
Wright Air Development Division Tech. Note No.60-214. Cincinnati Ohio, (1960).

[5] MILLER A.A. and R. CLIFFORD
Regular $\mathcal{D}$-classes in Semigroups
Trans. Am. Math. Soc., 82, 270-280 (1956)

[6] SCHEIBER M.
Sur les équivalences régulières dans les demigroupes.
C.R. Acad. Sci., 232, 1987-1989, (1951)

CODES A LONGUEUR VARIABLE

par

M.P. SCHUTZENBERGER

CODES A LONGUEUR VARIABLE

M.P. Schützenberger

I) Introduction.-

Les codes à longueur variable ont été considérés dès les premiers travaux de Shannon sur la théorie des communications. Cependant nous n'en savons guère plus à leur sujet maintenant qu'il y a dix ans. Ceci est d'autant plus remarquable que l'étude des codes équivaut à celle d'un objet mathématique assez naturel (les sous monoides libres d'un monoide libre) et que l'on peut formuler à ce propos des conjectures précises et d'un contenu apparemment élémentaire.

Le but de ces notes est de présenter quelques définitions et quelques arguments de plausibilité concernant l'une de ces conjectures. Dans ce qui suit, X dénote un ensemble (l"alphabet") d'éléments appelés lettres. X^* est le monoide libre engendré par X c'est-à-dire l'ensemble de tous les mots en les lettres de X muni de l'opération de concaténation ; e désigne l'élément neutre de X^* (c'est-à-dire le mot vide).

Définition 1.-

Un sous ensemble non vide A de X^* est un code s.s.i tout mot de X^* a au plus une factorisation comme produit de mots de A. Par exemple, pour $X = \{x, y\}$ l'ensemble $A = \{xx, yxx, yyx, yx, yy\}$ est un code (la vérification est laissée au lecteur); par contre $A' = \{xy, yx, y\}$ n'est pas un code parce que par exemple le mot yxy a deux factorisations distinctes $(y)(xy)$ et $(yx)(y)$ comme produit de mots de A.

Si A est un code, soit Y un alphabet et $\lambda : Y \to A$ une bijection; λ s'étend en un homomorphisme dans X^* un monoide libre Y^* engendré par Y. L'hypothèse que A est un code équivaut à l'hypothèse que λ est un monomorphisme etpar définition le sous monoïde A^* de X^* engendré par A est isomorphe à Y^*. A^* est donc un sous-monoïde libre de X^*. Réciproquement, soit B^* un sous-monoïde libre de A^*; B^* est librement engendré par l'ensemble $B = (B^* \setminus \{e\}) \setminus (B^* \setminus \{e\})^2$ qui est donc un code s'il est non vide. Ceci montre l'équivalence des notions de code et de sous monoide libre d'un monoide libre.

Il existe une catégorie de codes faciles à construire: les codes préfixes dont la définition est la suivante:

Définition 2.-

Un sous ensemble non vide A de X^* est un code préfixe s.s.i aucun des mots de A n'est facteur gauche propre d'un autre mot de A. (en symboles: $AXX^* \cap A = \emptyset$).

On vérifie sans peine qu'un code préfixe est un code. On appellera code préfixe gauche tout $A \subset X^*$ non vide satisfaisant la condition symétrique $X^*XA \cap A = \emptyset$ et bi préfixe tout code qui est à la fois préfixe et préfixe gauche.

Un exemple de code préfixe est: $\{x, yxx, yxy, yy\}$ (de code préfixe gauche: x, xxy, yxy, yy).

On doit à B. Mandelbrot l'observation que A est un code préfixe s.s.i A peut être considéré comme l'ensemble des suites de lettres définissant la première réalisation d'un évènement récurrent au sens de Feller. Aucune interprétation simple n'est connue pour les codes quelconques et de fait, il n'existe aucune méthode non triviale permettant de construire tous les codes ayant un nombre donné de mots. Cependant c'est un fait remarquable que tous les codes

(fini ou infini) que l'on connait peuvent être transformés en des codes préfixes par permutation des lettres de leurs mots.

Par exemple le code $A = \{xx, yxx, yyx, yx, yy\}$ n'est ni préfixe ni préfixe gauche, mais il se ramène au code préfixe $A' = \{xx, xyx, xyy, yx, yy\}$ par permutation des lettres des mots yxx et yyx . L'essentiel de ces notes consistera en la discussion de certaines propriétés se rattachant à la conjecture que la constatation empirique que l'on vient d'énoncer est vraie pour tous les codes.

Pour terminer cette introduction, il faut encore introduire la notion de paire synchronisante.

Définition 3.-

Soit A un code. Une paire $(f, f') \in X^* \times X^*$ est une paire synchronisante s.s.i quels que soient $g, g' \in X^*$ la relation $g f f' g' \in A^*$ entraine $gf, f'g' \in A^*$.

Le contenu intuitif de cette définition est simplement que le mot ff' détermine sans ambiguité une factorisation du message quel que soit le contexte dans lequel elle se trouve puisque la fin du mot f est nécessairement la fin d'1 mot de A . Il est clair qu'il existe de nombreux codes n'ayant aucune paire synchronisante: par exemple (pour $X = \{x, y\}$) le code $A = \{xx, xy, yx, yy\}$)
Il semble cependant que les codes n'ayant pas de paire synchronisante aient des propriétés très spéciales et l'étude de ces propriétés se rattache étroitement à la conjecture précédente.

II) Propriétés élémentaires des codes généraux.-

On garde les notations X , A , A^* , etc... introduites jusqu'ici et on rappelle qu'un sous ensemble B de X^* est dit stable si et seulement si $B^2 \subset B$.

.4.

Propriété 1.-

Deux conditions nécessaires et suffisantes équivalentes pour qu'un sous ensemble stable A^* de X^* soit un sous-monoide libre sont

(1) A^* satisfait la condition U_d

U_d : $A^* = \{ f \in X^* : A^* f \cap f A^* \cap A^* \neq \emptyset \}$.

(2) Il existe une représentation μ de X^* par des matrices à éléments 0 ou 1 telle que $A^* = \{ f \in X^* : (\mu f)_{1,1} = 1 \}$.

De plus, A^* est engendré par un code préfixe si et seulement si il satisfait l'une des deux conditions suivantes:

(3) U_r : $A^* = \{ f \in X^* : A^* f \cap A^* \neq \emptyset \}$

(4) La représentation μ peut être choisie de telle sorte que pour tout $f \in X^*$, μf ait au plus un élément non nul dans chaque ligne.

Vérification.-

Il est commode de noter d'abord qu'étant donné un sous ensemble stable A^* de X^*, un mot f satisfait $A^* f \cap f A^* \cap A^* \neq \emptyset$ s.s.i il satisfait $A^* f \cap A^* \neq \emptyset$ et $f A^* \cap A^* \neq \emptyset$. En effet, si $a_1, a_2, a_3 \in A^*$ sont tels que $a_1 f = f a_2 = a_3$ on a certainement $A^* f \cap A^* \supset \{a_3\} \neq \emptyset$.(1) Réciproquement, si $a_1, a_2, a_4, a_5 \in A^*$ sont tels que $a_1 f = a_4$ et $f a_2 = a_5$, on a $a_5 a_1 f = a_5 a_4 = f a_2 a_5$ et $A^* f \cap f A^* \cap A^* \supset \{a_5 a_4\} \neq \emptyset$ d'après l'hypothèse $A^{*2} \subset A^*$.

Montrons maintenant:

(α) $U_d \Rightarrow A^*$ libre; supposons que A^* est un sous ensemble stable non vide de X^* satisfaisant U_d. Comme $A^* e = e A^* = A^*$, on a $e \in A^*$. Posons $A = (A^* \setminus \{e\}) \setminus (A^* \setminus \{e\})^2$. Si $A^* \neq \{e\}$, ce que nous supposerons désormais, A est non vide et chaque mot $g \in A^* \setminus \{e\}$ a au moins une factorisation $g = a_1 a_2 \ldots a_m$ comme produit de mots $a_1, a_2, \ldots, a_m \in A$. Pour montrer que A est un code, il suffit de vérifier que cette factorisation est unique et,

---

1) et $f A^* \cap A^* \supset \{a_3\} \neq \emptyset$

procédant par induction sur la longueur de g, on peut supposer que ceci est déjà établi pour tous les mots de A^* qui sont strictement plus courts que g. Soit donc $g = a'_1 a'_2 \cdots a'_{m'}$ $(a'_1, a'_2, \ldots, a'_{m'} \in A)$ une autre factorisation de g. D'après l'hypothèse d'induction, cette factorisation est la même que la précédente si et seulement si $a_1 = a'_1$. Si a_1 était différent de a'_1 on pourrait supposer sans perte de généralité que a_1 est plus court que a'_1. On aurait donc $a'_1 = a_1 f$ pour un certain mot $f \in X^*$ et l'on aurait $f \in A^*$ d'après la définition de A. De plus, on aurait aussi $fa'_2 a'_3 \cdots a'_m = a_2 a_3 \cdots a_m$, c'est-à-dire $A^* f \cap A^* \neq \emptyset$ et $fA^* \cap A^* \neq \emptyset$ avec $f \neq 1$ ce qui est impossible d'après l'hypothèse que A^* satisfait U_d. L'implication " $U_d \Longrightarrow A^*$ libre" est établie.

(β) A^* libre $\Longrightarrow \mu$

Soit $H = \{ h \in X^* : hXX^* \cap A \neq \emptyset \}$ = l'ensemble des facteurs gauches propres des mots de A. Nous prenons H comme ensemble d'indices et nous définissons μe comme la $H \times H$ matrice unité. Pour chaque $f \in X^* \setminus \{e\}$, nous définissons la $H \times H$ matrice par la condition que pour chaque $h, h' \in H$ on ait : $(\mu f)_{h,h'} = 1$ si $hf = h'$ ou s'il existe $a \in A \cap hXX^*$ et $\bar{a} \in A^*$ tels que $hf = a\bar{a}h'$ $(\mu f)_{h,h'} = 0$ dans tous les autres cas. Par définition $e \in H$, $A^* = \{ f \in X^* : (\mu f)_{e,e} = 1 \}$ et tous les éléments des matrices μf sont 0 ou 1. Il suffit maintenant de vérifier sous l'hypothèse que A^* est libre que μ est bien une représentation de X^* c'est-à-dire que $\mu f \mu f' = \mu ff'$ identiquement pour $f, f' \in X^*$. Procédant par induction, on peut se limiter au cas où $f' = x \in X$ et la vérification découle de la définition de μ en considérant successivement les différents cas possibles. Je ne la reproduis pas ici.

.6.

(γ) $\mu \Rightarrow U_d$. Supposons maintenant que X^* possède une représentation μ par des matrices à éléments 0 ou 1 et, prenant un indice quelconque, disons 1 , posons $A^* = \{ f \in X^* : (\mu f)_{1,1} = 1 \}$. Il est clair que A^* est un sous monoïde de X^* . Soient $a, a' \in A^*$ et $f \in X^*$ tels que $af, fa' \in A^*$. D'après la définition de A^* ceci équivaut à l'existence d'indices i et j tels que $(\mu a)_{1,i} = (\mu f)_{i,1} = (\mu f)_{1,j} = (\mu a')_{j,1} = 1$. Comme $(\mu a)_{1,1} = (\mu a')_{1,1}$, on voit en calculant $(\mu afa')_{1,1}$ que cette dernière quantité ne peut être $\in 1$ que si $i = j = 1$ c'est-à-dire que si $f \in A^*$, ce qui montre que A^* satisfait U_d et achève la vérification de la première partie de la propriété.

La vérification de la deuxième partie est très simple. D'après la définition des codes préfixes, A est un tel code si et seulement si $A \cap H = \emptyset$ où A et H sont définis comme ci-dessus, c'est-à-dire encore, utilisant la représentation décrite dans (β) si et seulement si pour chaque $x \in X$ et $h \in H$ on a soit $hx \in H$ soit $hx \in A$ mais jamais les deux à la fois, c'est-à-dire enfin si et seulement si chaque matrice μx $(x \in X)$ a au plus une entrée non nulle par ligne, ce qui équivaut à la même condition pour chaque μf $(f \in X^*)$. Dans ce cas si $a, af \in A^*$ (c'est-à-dire $(\mu a)_{e,e} = (\mu af)_{e,e} = 1$) , on a certainement $(\mu f)_{e,e} = 1$ donc $f \in A^*$, ce qui montre que U_r est satisfaite pour tout code préfixe et pour tout code correspondant à une représentation par des matrices ayant au plus une entrée positive par ligne. Finalement, d'après la définition de A , on voit que U_r entraine en particulier que $aXX^* \cap A = \emptyset$ pour tout $a \in A$, ce qui achève la vérification de la propriété.

.7.

L'intérêt de la condition U_d est que son énoncé ne fait pas intervenir l'hypothèse que X^* est un monoide libre. Ainsi étant donné un monoide quelconque M, nous pouvons considérer la famille de tous les sous monoides M' de M tels que l'on ait U_d. $M' = \{m \in M : M'm \cap mM' \cap M' \neq \emptyset\}$ et l'on voit facilement que cette famille est un treillis complet.
En particulier, si M est un groupe, un sous ensemble stable non vide $M' \subset M$ satisfait U_d si et seulement s'il est un sous groupe. En effet, U_d entraine d'abord que $e \in M'$ où e est l'élément neutre de M ; ensuite $\bar{m}$ étant l'inverse d'un élément quelconque $m \in M'$, on a $\{e\} \in \bar{m}M' \cap M'\bar{m} \cap M'$ ce qui montre que $m \in M'$ implique $\bar{m} \in M'$.
Ceci permet très facilement de construire des exemples de sous monoides libres de X^* car, étant donné un épimorphisme φ de X^* sur M, l'image inverse $\varphi^{-1}M' = \{f \in X^* : \varphi f \in M'\}$ de M' satisfait U_d dans X^* quand M' satisfait U_d dans M.

CODES A LONGUEUR VARIABLE

M.P. SCHÜTZENBERGER

(s u i t e)

CODES A LONGUEUR VARIABLE (suite)

M.P. Schützenberger

La Proprieté 1 est purement formelle et n'implique aucune restriction sur la cardinalité des ensembles (X ou A) considérés. Nous introduisons maintenant la définition suivante:

Définition.- Le code A sera dit élémentaire s.s.i il existe un homomorphisme φ de X^* compatible avec A^* (c'est-à-dire tel que $A^* = \varphi^{-1}\varphi A^* = \{ f \in X^* : \varphi f \in \varphi A^* \}$) tel que le monoïde φX^* ait des quasi-idéaux minimaux (c'est-à-dire tel qu'il existe au moins un $u \in \varphi X^*$ satisfaisant $u \in u.m. \varphi X^* \cap X^*.m.u.$ pour tout $m \in \varphi X^*$) .

Ceci est certainement le cas quand $A^* = \varphi^{-1} G'$ où φX^* est un groupe. Un cas moins limité est le suivant :

Remarque : Une condition suffisante pour que A soit élémentaire est qu'il existe au moins un mot $b \in X^*$ qui n'est facteur d'aucun mot de A $(X^* b X^* \cap A = \emptyset)$, (ce qui est certainement le cas quand la longueur des mots de A est bornée) .

Vérification .- Définissons en effet un homomorphisme φ de X^* sur un monoïde quotient φX^* de X^* par la condition suivante :

pour tout $f, f' \in X^*$, $\varphi f = \varphi f'$

s.s.i quelques soient $g, g' \in X^*$ la relation $gfg' \in A^*$ équivaut à $gf'g' \in A^*$.

On sait (M. Teissier) que l'homomorphisme ainsi défini est compatible

avec A^* (puisque $efe \in A^*$ s.s.i $f \in A^*$) et que φX^* est une image homomorphe de tout monoïde $\varphi' X^*$ où φ' est compatible avec A^*. Nous appellerons φX^* le monoïde syntactique de A^*.

Si l'ensemble $W = \{ f \in X^* : X^* f X^* \cap A^* = \emptyset \}$ est vide, on voit facilement que $X^* W X^* = W^*$ et que φW est un élément unique u du monoïde syntactique satisfaisant

$u \in um\, \varphi X^* \cap \varphi X^* mu$ pour tout $m \in \varphi X^*$.

On peut donc supposer désormais que $W = \emptyset$. Pour chaque $b \in X^*$, il existe donc au moins une paire $g, g' \in X^*$ telle que $gbcbg' \in A^*$ et d'après l'hypothèse $X^* b X^* \cap A = \emptyset$ il existe deux factorisations $b = b_1 b_2$ et $b = b_3 b_4$ de b telles que gb_1, $b_2 c b_3$, $b_4 g' \in A^*$. Comme b n'a qu'un nombre fini de factorisations, on déduit facilement de la définition de φ que l'image par φ de l'ensemble $bX^* b^* = Q$ n'a qu'un nombre fini d'éléments et comme $QX^* Q \subset Q$ il en résulte que l'ensemble φQ contient un sous-ensemble $G \neq \emptyset$ satisfaisant $G . \varphi X^* . G = G$. D'après la théorie classique des monoïdes, ceci signifie que G est un quasi-idéal minimal de φX^*, ou, comme l'on dit aussi, un sous-groupe de SUSCHKEWITSCH de φX^*. La remarque est établie et l'on a même vérifié le résultat plus fort que l'existence de b entraîne que les sous-groupes de Suschkewitsch du monoïde syntactique soient finis.

Réciproquement, il est possible de vérifier que si A est un code tel que le monoïde syntactique associé soit fini, il existe au moins un $b \in X^*$ qui n'est facteur d'aucun mot de A. (Ceci résulte de théorèmes dûs à Shannon et à Feller, dont nous utiliserons par la suite d'autres cas particuliers).

. 3.

D'un point de vue technique, il est intéressant de noter que si A est élémentaire la condition U_d entraîne la propriété caractéristique suivante de son monoïde syntactique: quels que soient m , $m' \in \varphi X^*$ on a $m = m'$ s. s.i $um = um'$ et $mu = m'u$ pour chaque u appartenant à l'idéal bilatère minimal de φX^* . Nous n'utiliserons pas cette observation ici.

Propriété 2.-

Une condition nécessaire pour que le code A soit maximal est

N_d : $X^* = \{ f \in X^* : X^X f X^X \cap A^X \neq \emptyset \}$,

cette condition étant aussi suffisante quand A est élémentaire.

Quand A est un code préfixe, une condition nécessaire et suffisante pour qu'il soit maximal en tant que code préfixe est

N_r : $X^* = \{ f \in X^* : f X^* \cap A^* \neq 0 \}$.

Enfin, quand A est un code élémentaire maximal, N_r est une condition nécessaire et suffisante pour qu'il soit un code préfixe.

Vérification.- Je renvoie au cours de Nivat [ ] pour la preuve que si $f \in X^*$ est tel que $X^* f X^* \cap A^* = \emptyset$ l'on peut adjoindre à A un mot de la forme fx^m $(x \in X)$ de telle sorte que $A \cup \{fx^m\}$ soit encore un code ce qui montre que A n'est maximal que quand N_d est satisfaite.

Si A est un code élémentaire satisfaisant N_d soit D l'idéal bilatère minimal du monoïde syntactique $M = qX^*$ introduit plus haut. La condition N_d exprime que $D' = D \cap \varphi A^* \neq \emptyset$. Prenons $\bar{a} \in \varphi^{-1} D'$ et supposons que A ne soit pas maximal, c'est-à-dire qu'il existe un $g \in X^*$ tel que $\{g\} \cup A = B \neq A$ soit un code.

Ceci implique $\bar{a}g\bar{a} \notin A^*$ car autrement ce mot aurait deux factorisations en produit de mots de B. Cependant, comme $\varphi\bar{a} \in D$, $\varphi\bar{a}g\bar{a}$ appartient au sous groupe $\varphi(\bar{a}X^*\bar{a})$ de M et il existe un mot $g' \in \bar{a}\,X^*\,\bar{a}$ tel que $\varphi(g'\,\bar{a}\,g\,\bar{a}) = \varphi(\bar{a}\,g\,\bar{a}\,g') = \varphi\bar{a}$, ce qui entraîne $g'\,\bar{a}\,g\,\bar{a}$, $\bar{a}\,g\,\bar{a}\,g' \in A^* \subset B^*$ et $g' \in B^*$ puisque par hypothèse B^* satisfait U_d.

Le mot g' a donc au moins une factorisation comme produit de mots de B et par conséquent $g'\,\bar{a}\,g\,\bar{a}$ admet au moins une factorisation en produit de mots de B dans laquelle un au moins des facteurs est g. Comme d'autre part on a vu que $g'\,\bar{a}\,g\,\bar{a} \in A^*$, tout ceci implique que $g'\,\bar{a}\,g\,\bar{a}$ ait deux factorisations distinctes en contradiction avec l'hypothèse initiale que B était un code;.
On a donc établi que N_d est une condition suffisante pour la maximalité de A quand A est élémentaire.

Considérons maintenant un code préfixe A.
Si b $(\neq e)$ n'est pas un mot de A et si A satisfait N_r il existe au moins un $f \in X^*$ tel que $bf \in A^*$ donc b est facteur gauche d'un mot de A ou admet un mot de A comme facteur gauche. Ceci montre que A est maximal en tant que code préfixe s'il satisfait N_r.

Réciproquement, si $F = \{f \in X^X : f\,X^* \cap A^* = \emptyset\}$ n'est pas l'ensemble vide, on peut écrire $F = F'\,X^*$ où $F' = F \setminus X\,X^*$ (= l'ensemble des mots de F n'ayant aucun facteur gauche propre dans F) et l'on vérifie sans peine que $A \cup F'$ est un code préfixe satisfaisant N_r.

Pour achever la vérification de la propriété 2 il reste seulement à vérifier l'équivalence de U_2 et de N_2 sous les hypothèses indiquées, ce qui est un simple exercice sur les monoïdes ayant des quasi-idéaux minimaux et est laissé au lecteur.

On notera que la Propriété 2 entraîne qu'un code préfixe élémentaire maximal soit bi-préfixe si et seulement s'il satisfait N_k : $X^* = \{ f \in X^* : X^* f \cap f X^* \cap A^* \neq \emptyset \}$. La condition restrictive que A soit élémentaire peut sembler extrêmement artificielle et n'est pas la meilleure possible. Il est cependant impossible de se dispenser entièrement d'une hypothèse de cette nature et ceci suggère le:

Problème.- Trouver des conditions intéressantes définissant des familles de codes pour lesquelles N_d est équivalent à la maximalité du code, pour lesquelles $U_d \& N \iff U_r \& N_d$ ou pour lesquelles $U_r \& N_\ell \iff U_\ell \& N_r$.

De façon plus restreinte et plus précise, il semble possible de proposer la conjecture suivante dont la preuve permettrait celle de la conjecture 1 pour les codes finis.

Comme plus haut, α désigne l'homomorphisme naturel de X^* dans le monoïde abélien libre engendré par X.

Conjecture 2.-

Soit $\alpha b = x_1^{n_1} x_2^{n_2} \dots x_r^{n_r}$ un mot fixe d monoïde abélien αX^* et soit $\bar{A}$ un code tel que pour chaque $a \in \bar{A}$, αa soit un facteur de αb. Posant pour chaque $a \in \bar{A}$: $\delta a = (\sum_i (n_i - m_i))\,! \;(\prod_i (n_i - m_i)\,!)^{-1}$ où les entiers positifs $m_i \leq n_i$ sont définis par $\alpha a = x_1^{m_1} x_2^{m_2} \dots x_r^{m_r}$, on a l'inégalité:

$$\sum_{a \in \bar{A}} \delta a \leq (\sum_i n_i)\,! \;(\prod_i n_i\,!)^{-1} \quad (= \delta e).$$

L'énoncé est trivial quand $\bar{A}$ est un code préfixe. En effet dans ce cas, $\delta a = \mathrm{Card}\{a X^* \cap \bar{\alpha}^{-1} b\}$ et le nombre des $f \in X^*$ tels que $\alpha f = \alpha b$ qui admettent a comme facteur gauche est $\delta e = \mathrm{Card}(\bar{\alpha}^{-1} b)$.

Donc pour $\bar{A}$ préfixe $\sum_{a \in \bar{A}} \delta a = \delta e$ est une condition

nécessaire et suffisante pour que $\bar{A}$ soit l'intersection avec $\alpha^{-1}b$ d'un code préfixe maximal. Cependant même pour $\bar{A}$ préfixe satisfaisant $\sum \delta a = \delta e$, je suis incapable de prouver sans hypothèses supplémentaires que si $c \notin \bar{A}$ est tel que c est un facteur de αb, l'ensemble $\bar{A} \cup \{c\}$ n'est pas un code.

L'une de ces hypothèses est $\alpha b = x_1^{n_1} x_2$ et il me parait intéressant de signaler qu'un des obstacles préliminaires pour passer au cas de mots b moins spéciaux est l'absence d'énoncés concernant la factorisation des groupes cycliques. En effet, étant donné un groupe cyclique G d'ordre n on ne connait pas sauf pour des classes très particulières d'entiers n la forme générale des sous ensembles H, $H' \subset G$ tels que chaque $g \in G$ ait une et une seule factorisation $g = h\,h'$ avec $h \in H$, $h' \in H'$.

Une autre hypothèse est que $\bar{A}$ est bi-préfixe comme le montre l'exemple suivant:

Exemple.-

Soit A un code préfixe satisfaisant N_r et $b = B_1 = x_1 x_2 \dots x_n$ $(x_1, x_2, \dots, x_n \doteq X)$ un mot tel qu'aucun de ses mots conjugués $b_i = x_i x_{i+1} \dots x_n x_1 x_2 \dots x_{i-1}$ $(i = 1, 2, \dots n)$ ne soit facteur de mots de A, $(X^* b_i X^* \cap A = \emptyset$ pour $i = 1, 2, \dots n)$. Un tel mot b existe toujours s'il existe au moins un $f \in X^x$ tel que $X^* f X^* \cap A = \emptyset$ car on peut prendre alors $b = ff$.

La condition N_r implique que quel que soit $j \in [1, m]$ il existe au moins un $f \in X^x$ pour lequel $x_j x_{j+1} \dots x_n\, bf \in A^*$ et comme $X^* b_j X^* \cap A = \emptyset$, il existe un indice $\bar{j}$ tel que $a_j \in A$ avec $a_j = x_j x_{j+1} \dots x_{\bar{j}}$ (si $j \leq \bar{j} \leq n$) ou $= x_j x_{j+1} \dots x_n x_1 \dots x_{\bar{j}}$ (si $1 \leq \bar{j} < j$).

L'hypothèse que A est un code préfixe implique que a_j est déterminé de façon unique donc que la correspondance

.7.

$j \to \bar{j}$ est une application de $[1, n]$ dans lui-même et l'ensemble $\bar{A}$ des mots a_j $(j = 1, 2, \ldots n)$ constitue la totalité des mots de A qui sont facteurs d'un mot du monoide $\{b\}^*$ engendré par b ou d'un mot quelconque des monoides $\{b_i\}^*$.

Maintenant deux cas sont possibles:

1) $j \to \bar{j}$ n'est pas une bijection, c'est-à-dire qu'il existe au moins deux indices différents j et j' tels que $\bar{j} = \bar{j}'$. Dans ce cas l'un des deux mots a_j et $a_{j'}$ est facteur droit de l'autre et $\bar{A}$ (donc A) n'est pas bi préfixe. De plus, il existe au moins un indice, disons j^* tel que $j^* \neq \bar{j}$ pour tout $j \in [1, n]$. Il en résulte que $b\, x_1\, x_2 \ldots x_{j^*} = g$ n'a aucun facteur droit dans $\bar{A}$ donc dans A, ce qui prouve $X^* g \cap A^* \neq \emptyset$ et enfin que A^* ne satisfait pas N_ℓ $\left(X^* = \{ f \in X^* : X^* f \cap A^* \neq \emptyset \} \right)$.

2) $j \to \bar{j}$ est une bijection. Il est clair que maintenant $\bar{A}$ est bi préfixe et que chaque b_i a un facteur droit $a_j \in A$ où $i-1 = \bar{j}$. Comme $b_{j-1} = a_j c_j$ où $c_j a_j = b_i$, il en résulte par induction que pour tout facteur g d'un mot du monoide $\{b\}^*$ on a $X^* g \cap \bar{A}^* \neq \emptyset$. Dans ce cas $\bar{A}$ peut donc être considéré aussi comme un sous-ensemble d'un code préfixe gauche fini satisfaisant N_ℓ.

Montrons pour finir que $\bar{A} \cup \{c\}$ ne peut pas être un code quand $c \notin \bar{A}$ est un facteur de $\{b\}^*$. Considérons la suite $j_1, j_2, j_3, \ldots, j_q, \ldots$ où $j_{i+1} = \dot{\bar{j}}_i$ identiquement. Comme $j \to \bar{j}$ est une bijection, il existe un q tel que $j_q = j_i$ ce qui montre que pour chaque $j \in [1, n]$ il existe un entier positif q_j tel que $b_j^{q_j} \in \bar{A}^*$. Prenons le plus petit commun multiple r des q_j, on a $b_j^r \in \bar{A}^*$ pour tout j. Maintenant on peut sans perte de généralité, supposer que $c = b_1^s x_1 x_2 \ldots x_j$ $(s \geq 0)$ et on a évidemment

$c\, b_j^r = b_1^r\, c$ ce qui montre que ce mot a deux factorisations distinctes en produit de mots de $X \cup \{c\}$ et achève la discussion de l'exemple.

Propriété 3.-

Soit A un code satisfaisant N_1. Une condition nécessaire pour qu'il admette des paires synchronisantes est N_s : $X^* = \{f \in X^* : A^X f A^* \cap A^X \neq \emptyset\}$.

Si A est élémentaire, la condition N_s est suffisante et elle équivaut à la condition que si φ est un homomorphisme compatible avec A^* tel que φX^* ait des quasi-idéaux minimaux, et A^* contienne au moins l'un des derniers.

Soit (g , g') une paire synchronisante. Quels que soient $g_1 , g'_1 \in X^*$, $(g_1 g , g' g'_1)$ est aussi une paire synchronisante car $f g_1 g g' g'_1 f' \in A^*$ implique $f g_1 g , g' g'_1 f' \in A^*$. Donc, quand A satisfait N_d, on peut toujours supposer que $g , g' \in A^*$. En vertu de N_d on peut trouver pour chaque $h \in X^*$ au moins une paire (f , f') telle que $f g g' h g g' \in A^*$ et puisque (g , g') est une paire synchronisante, il en résulte que les mots $f g , g' h g g' f'$, $f g g' h g$ et $g' f'$ appartiennent à A^*. Observant que $g' h g g' f' f g g' h g \in A^*$ on voit que $A^* g' h g \cap g' h g A^* \cap A^X \neq \emptyset$ et enfin, d'après U_d, que $g' h g \in A^*$ ce qui établit la nécessité de N_s.

Supposons maintenant que φ est un homomorphisme compatible avec A^* tel que φX^* admette des quasi-idéaux minimaux. En vertu de N_d, l'un de ceux-ci, disons G, a une intersection G' non vide avec φA^* et utilisant U_d, on montre que G' est un sous groupe de G. Soient $f \in \varphi^{-1} G$ et $a , a' \in A^*$ tels que $afa' \in A^*$.

.9.

Prenant $\bar{a} \in \bar{A}$ tel que $\varphi \bar{a} = \varphi \bar{a}\bar{a}$ = l'idempotent contenu dans G, on a $\bar{a} \propto f\ a'\ \bar{a} \in A^*$ et $\varphi f = \varphi(\bar{a}\ f\ \bar{a})$ donc $\varphi(\bar{a}\ a\ f\ a'\ \bar{a}) = \varphi(\bar{a}\ a\ \bar{a}\ f\ \bar{a}\ a'\ \bar{a}) = \varphi(\bar{a}\ a\ \bar{a}).\ \varphi f\ .\varphi \bar{a}\ a'\ \bar{a} \in G'$ avec $\varphi(\bar{a}\ a\ \bar{a})$, $\varphi(\bar{a}\ a'\ \bar{a}) \in G'$ et enfin, puisque G' est un sous groupe, $\varphi f \in G'$, ce qui entraîne $f \in A^*$ puisque φ est compatible avec A^*. Ceci établit que N_s entraine $G' = G$.

Réciproquement, si $G = G'$, l'intersection de φA^* avec l'idéal bilatère minimal D de X^* est le quasi idéal $R' \cap L'$ où $R' = D\ \varphi A^* = \{m = D : m.\varphi X^* \cap A^* \neq \emptyset\}$ et $L' = \varphi A^*\ D = \{m \in D : \varphi X^*.m \cap \varphi A^* \neq \emptyset\}$. Prenons $\bar{a} \in A^* \cap \bar{\varphi}^1 D$. Si $f\ \bar{a}\ \bar{a}\ f' \in A^*$ le mot $f\ \bar{a}$ appartient à la fois à $\varphi^{-1}L'$ (puisque $\varphi \bar{a} \in \varphi A^* \cap D$) et à $\varphi^{-1}R'$ puisque $\varphi f\ \bar{a} \in D$ et $\varphi f\ \bar{a}.\varphi \bar{a}\ f \in A^*$. Donc $f\ \bar{a} \in A^*$ et de façon symétrique $\bar{a}\ f \in A^*$, ce qui prouve que $(\bar{a}, \bar{a})$ est une paire synchronisante et achève la vérification.

On peut noter que la condition $G = G'$, c'est-à-dire N_s, équivaut à l'hypothèse que les quasi-idéaux minimaux du monoïde syntactique sont triviaux.

III) Quelques questions particulières concernant les codes maximaux finis.

Afin de simplifier la discussion (et surtout les notations), nous supposons désormais que l'alphabet X est fini, ce qui n'a que peu d'importance pour les questions discutées ici. Par contre, l'hypothèse qu'un code maximal A est fini entraine qu'il ait des propriétés algébriques que ne possèdent pas les codes maximaux satisfaisant seulement la condition plus faible mais encore très restrictive d'avoir un monoïde syntactique associé fini. Par exemple, il n'y a aucun code maximal fini A ($\neq X$) pour lequel on puisse trouver un entier fini m tel que toutes les paires (a^m, a^m) $(a \in A)$ soient synchronisantes alors que

ceci est vrai (avec $n = 1$) pour le cas très simple de $X = \{x , y\}$ et de $A = \{x^n y^{n'} : n . n' > 0\}$ = un code maximal infini dont le monoïde syntactique associé à 6 éléments! (dont un système représentatif dans X^* est e , x , y , xy , yx , xyx) .

Ceci pose donc le problème de trouver une méthode de construction pour ces codes.

Il sera commode de désigner désormais par α l'homomorphisme naturel de X^* dans l'anneau $Z[X]$ des polynomes à coefficients entiers en les variables $x \in X$ et pour tout sous-ensemble fini $F \subset X^*$ de poser $\alpha F = \sum_{f \in F} \alpha f$ ($\in Z[X]$). Donc, si F' est un autre ensemble de mots, $\alpha F = \alpha F'$ signifie que F et F' sont équivalents à des permutations près des lettres de leurs mots.

Il est facile de construire systématiquement la famille C_0 des codes préfixes maximaux finis. En effet, quelque soit $A \in C_0$ ($A \neq \emptyset$) , il existe au moins un $h \in \{f \in X^* : f X X^* \cap A \neq \emptyset\}$ tel que $h X \subset A$ et l'on voit que $(A \setminus hX) \cup \{h\} = A'$ appartient aussi à C_0 . Par conséquent, tenant compte de $X \in C_0$, tous les membres de C_0 peuvent être obtenus par itération de la construction $A' \to (A' \setminus \{a'\}) \cup a'X$ ($a' \in A'$) inverse de la précédente.

Rien de semblable n'existe pour les codes maximaux finis non préfixes. Par contre, tous ceux que je connaïs peuvent être obtenus à partir des codes préfixes et préfixes gauches par itération de la construction suivante:

Construction 1.-

Soient B un code sur X; Y un alphabet; $\theta : Y \to B$ une bijection et C un code sur Y . Etendant θ à un homomorphisme $\theta : Y^* \to X^*$, l'hypothèse que B est un code implique que θ est un homomorphisme et que θC^* est un sous monoide libre de X^*. Donc $\theta C = A$ est un code sur X . Quand B et C satisfont N_d il en est de même de A .

Toutefois, quand ni B ni C ne sont triviaux, A^* n'est pas maximal en tant que sous monoide libre de X^* (bien que A puisse être maximal en tant que code) puisque $A^* \not\subset B^* \not\subset X^*$.

De plus, comme il est facile d'associer à tout code préfixe gauche D un code préfixe D' tel que $\mathfrak{A}D = \mathfrak{A}D'$, on voit que tous les codes maximaux finis A obtenus par itération de cette construction sont tels que $\mathfrak{A}A = \mathfrak{A}A'$ pour au moins un code préfixe maximal A'. Ceci suggère la conjecture suivante qui signifie simplement que l'itération de la construction 1 livre tous les codes cherchés et qui, comme on le vérifie aisément, est plus forte que la Conjecture 2.

Conjecture 3.-

Si A^* est un sous monoide libre maximal engendré par un code fini A, alors A est préfixe ou préfixe gauche.

Nivat a formulé la conjecture supplémentaire que pour chacun de ces codes il existe deux mots a, $a' \in A$ tels que pour $f \in X^*$ l'une quelconque des relations $af \in A^*$ ou $fa' \in A^*$ entraine $f \in A^*$.

D'autre part, les seuls codes minimaux finis sans paire synchronisante que je sache construire sont les codes bi préfixes et tous les codes obtenus par une itération de la construction 1 dans laquelle apparait au moins un code préfixe. Ceci suggère l'énoncé suivant (qui est faux quand A n'est pas fini et dont j'avais à tort annoncé la validité il y a quelques années).

Conjecture 4.-

Si A^* est un sous monoide libre maximal engendré par un code fini non bi préfixe A, alors A^* possède au moins une paire synchronisante.

.12.

Je présente maintenant quelques conséquences des Conjectures 1,2,3 et 4 et tout d'abord le théorème suivant qui est un cas particulier de théorèmes plus puissants dus à Shannon et dont nous extrairons d'ailleurs plus tard un autre énoncé :

Théorème 1.- (Shannon)

Soit A un code fini. Une condition nécessaire et suffisante pour que A soit maximal est qu'il existe un polynôme $T \in Z\langle\langle X \rangle\rangle$ tel que $1 - \alpha A = (1 - \alpha X)T$. Quand A est préfixe, $T = \alpha H$ où H est l'ensemble des facteurs gauches propres des mots de A . Réciproquement, une condition nécessaire et suffisante pour qu'un polynôme $T \in Z\langle\langle X \rangle\rangle$ à coefficients non négatifs soit tel que $1 - (1-\alpha X)T$ ait la forme αA pour au moins un code préfixe maximal fini A est que $1 - (1-\alpha X)T$ ait un terme constant nul et des coefficients non négatifs.

Sous les hypothèses de finitude des codes considérés ici, la validité de la Conjecture 3 entrainerait celle des Conjectures 1 et 2 et en particulier que $(1-\alpha A)(1-\alpha X)^{-1} = T$ soit un polynôme à coefficients non négatifs pour tout code maximal fini A . En effet, si A est obtenu en composant B et C comme indiqué dans la construction 1 et si $1 - \alpha B = (1-\alpha X)S$; $1 - \alpha C = (1-\alpha Y)V$ on a (avec des notations évidentes) : $1 - \alpha A = \theta[1 - \alpha C] = (1 - \alpha\theta Y).\ \theta V = (1 - \alpha B).\ \theta V = (1 - \alpha X).\ S.\ V.$

Réciproquement, si le code maximal fini A est tel que l'inégalité de la Conjecture 2 est vérifiée pour tout αb où $b \in X^{*}$ est assez long , un calcul simple montre que $(1-\alpha A)(1-\alpha X)^{-1}$ n'a pas de coefficients négatifs et, d'après le théorème, on a $\alpha A = \alpha A'$ pour au moins un code préfixe maximal fini A' .

Maintenant, en utilisant les propriétés de réductibilité de la représentation μ de X^{*} introduite à la fin de la

.13.

vérification de la Propriété 1, et en observant que $1-\alpha A$ est égal au déterminant de la matrice $I - \sum_{x \in X} \alpha x . \mu x$ on peut vérifier la

Propriété 4.-

Soit A un code maximal fini. On a $(1-\alpha A)(1-\alpha X)^{-1} = P_r \cdot P_s \cdot (k + (1-\alpha X) P_s)$ où P_r (resp. P_ℓ) est un polynôme $\in Z[X]$ se réduisant à 1 s.s.i A est préfixe (resp. préfixe gauche), où $P_s \in Z[X]$ et où k est un entier positif qui est égal à 1 s.s.i A admet des paires synchronisantes.

Ainsi, par exemple pour $X = \{x, y\}$; $Y = \{u, v, w\}$; $B = \Theta Y = \{\Theta u = x ; \Theta v = yx ; \Theta w = yy\}$ (= un code préfixe maximal) $C = \{u, uv, vv, wv, w\}$ (= un code préfixe gauche maximal), on trouve $A = \{x, xyx, yxyx, yyyx, yy\}$. $1-\alpha A = (1-\alpha X)(1+x+xy+xy^2)(1-X)(1+y)(1+xy)$ et on a bien $\alpha A = \alpha A'$ où $A' = \{x, yxx, yxyx, yxyy, yy\}$ est un code préfixe. Comme $T = 1 + x + xy + y^2$ n'a pas de facteur de la forme $k + (1-\alpha X)P$ (avec $k \geq 1$), on peut noter que tout code A'' tel que $\alpha A'' = \alpha A$ possède des paires synchronisantes.

Par contre, pour X, Y, et B comme plus haut et $D = Y^2 = \{uu, uv, uw, vu, vv, vw, wu, wv, ww^2\}$ = un code bi-préfixe, le code $\bar{A} = \Theta D$ n'a pas de paire synchronisante et l'on trouve bien $1-\alpha\bar{A} = (1-\alpha X).(1+y)(2-(1-\alpha X)(1+y))$.

La Propriété 4 me parait donner un certain poids aux Conjectures 2 et 3 (qui auraient cette Propriété pour conséquence immédiate si elles pouvaient être prouvées directement). En effet, pour les codes préfixes maximaux finis, le polynôme T ne semble avoir "en général" aucune propriété particulière de factorisation puisque la famille $\mathcal{C}$ de tous ces polynômes est définie de la façon très simple suivante:

$\mathcal{C}$ est la plus petite famille de polynômes de $Z[X]$ qui contienne 1 et qui soit telle que $\sum_{x \in X} x\, T_x \in \mathcal{C}$ pour toute application $x \to T_x$ de X dans $\mathcal{C} \cup \{0\}$.

.14.

(Ceci résulte immédiatement de la construction des codes préfixes finis rappelée au début de cette section).
Des arguments supplémentaires sont fournis par le cas particulier que nous rappelons maintenant des théorèmes généraux de Shannon et de Feller.

Soit π un homomorphisme multiplicatif de $Z[X]$ dans les réels tel que $\sum_{x\in X} \pi x = 1$ et $\pi x \geq 0$ pour tout $x\in X$. On peut interpréter $\pi\alpha f$ comme la mesure de l'ensemble des séquences infinies de lettres de X commençant par le mot f sous l'hypothèse que les lettres $x\in X$ sont produites indépendamment avec les probabilités πx. Naturellement du point de vue algébrique, toute cette machinerie équivaut au calcul dans le quotient de l'anneau $Z[X]$ par son idéal engendré par $1-\alpha X$. Introduisant une nouvelle variable s et notant $|f|$ la longueur de $f\in X^*$, on a:

Théorème 2.-(Shannon, Feller)
Soit A un code fini et $Q(s) = \sum_{a\in A} s^{|a|}.\pi\alpha a$. Les modules des racines de l'équation en s $1 = Q(s)$ sont au plus égaux à 1 et $Q(1) = 1$ s.s.i. A est maximal. Si cette condition est satisfaite, on a $[(1-s)^{-1}(1-Q(s))]_{s=1}$ $= \pi T = \sum_{a\in A} |a|.\pi\alpha a$ = la longueur moyenne des mots de A. Enfin, quand A est maximal et quand toutes les probabilités πx $(x\in X)$ sont égales, on peut trouver un code préfixe A' tel que $Q(s)$ soit égal au polynôme en s correspondant $Q'(s) = \sum_{a\in A'} |s|^{a}.\pi\alpha a$.

La dernière assertion du Théorème possède une formulation équivalente (à vrai dire assez compliquée) permettant de généraliser l'hypothèse d'égalité des probabilités πx. Cette partie du Théorème montre que pour tout code maximal fini A, le polynôme obtenu en remplaçant chaque $x\in X$ par la même variable s dans αA est égal au polynôme correspondant relatif à un code préfixe A'.

Comme la conjecture 1 pour les codes maximaux finis est équivalente à l'hypothèse que le polynôme T n'a pas de coefficients négatifs , nous avons ici encore la preuve de la validité d'une conséquence particulière de cette conjecture.

La même observation s'applique à la conjecture 3. En effet : d'une part, on peut démontrer directement qu'il existe toujours deux sous-ensembles K_r ,K_ℓ de X^* tels que les polynômes P_r et P_ℓ de la Propriété 4 satisfassent

$$\pi P_r = \pi \alpha K_r \geq 1 \quad \text{et} \quad \pi P_\ell = \pi \alpha K_\ell \geq 1$$

quelque soit la distribution de probabilité π ;

d'autre part, la conjecture 3 entraîne l'hypothèse que l'on peut choisir ces deux ensembles de telle sorte que l'on ait les relations plus fortes $P_r = \alpha K_r$ et $P_\ell = \alpha K_\ell$.

Enfin, pour conclure cette section, il faut mentionner que la Propriété 4 entraîne la validité de la conjecture 4 sous l'hypothèse restrictive supplémentaire que 1 est le plus grand commun diviseur des longueurs des mots de A de la forme x^n $(x \in X)$. Cette même conjecture est établie aussi en ce qui concerne la famille des codes préfixes satisfaisant la relation supplémentaire $X^*A \subset AX^*$ plus restrictive que N_r . Chaque code A de cette famille peut être obtenu en prenant un sous-ensemble $F \subset XX^*$ et en posant

$A = X^*F \setminus X^*FXX^*$.

Par exemple le code $\theta D = \theta y^2$ construit plus haut est obtenu ainsi avec l'ensemble

$$F = \{xx, xyx, xyy, yyx, yyyy\} .$$

Cette vérification partielle de la conjecture 4 se généralise d'ailleurs au cas où A est élémentaire et où le sous-groupe de Suschkewitsch de monoïde syntactique est abélien, une hypothèse dont je suis malheureusement incapable de donner une interprétation utile en termes de codes.

Codes bipréfixes maximaux finis

Soit A un tel code. D'après la propriété 4, on a $1-\alpha A = (1-\alpha X)(k+(1-\alpha X)P_s)$ avec $P_s \in Z[X]$ et d'après le cas particulier des théorèmes de Shannon et Feller rappelé plus haut, l'entier k est la longueur moyenne des longueurs des mots de A quelque soit la distribution de probabilité π. Moyennant une extension des notations introduites ici, il découle des théorèmes évoqués plus haut que ce dernier résultat se généralise au cas où A est un code bipréfixe maximal infini dont le monoïde syntactique associé est fini. Il me parait assez significatif qu'il soit possible de vérifier que pour chaque $k \geq 3$ il n'éxiste qu'un nombre fini de codes bipréfixes maximaux finis sur l'alphabet fini X ayant k pour longueur moyenne de leurs mots alors que le contraire est vrai quand la clause restrictive "fini" est remplacée par la clause "de monoïde syntactique associé fini". Ceci propose le problème de trouver une technique pour construire systématiquement tous les codes bipréfixes maximaux, dont la longueur moyenne des mots est un entier naturel n donné.

Il est clair que l'ensemble X^n de tous les mots de longueur n est un tel code et il me paraît remarquable que si $A^* = \varphi^{-1}G'$ où G' est un sous-groupe d'indice n d'un

groupe $G = \varphi X^{*}$ (ce qui d'après le théorème 2 assure que A^{*} est bipréfixe maximal de longueur moyenne de mots n) le seul cas où A^{*} soit engendré par un code fini soit précisément celui où $A = X^{n}$ (la vérification est laissée au lecteur) .

Considérons maintenant la construction suivante :

Construction 2. Soient A un code bipréfixe maximal et $h \notin A$ un mot fixe, facteur gauche d'au moins un mot de A et facteur droit d'au moins un autre mot de A. Posant

$$B_h = \{f \in X^{*} : hf \in A\} , \quad B'_h = \{f \in X^{*} : fh \in A\}$$

et supposant que $hB_h \cap B'_h h = \emptyset$, l'ensemble

$$\bar{A} = (A \setminus (hB_h \cup B'_h h)) \cup \{h\} \cup B'_h h B_h$$

est un code bipréfixe maximal .

En effet, soit A'' un code préfixe satisfaisant N_r et h un facteur propre d'un mot de A'' . Il est facile de montrer que l'ensemble A''_1 obtenu en remplaçant par h tous les mots de A'' ayant h comme facteur gauche est encore un code préfixe satisfaisant N_r et que la même chose est vraie pour l'ensemble A''_2 , obtenu en remplaçant dans A''_1 chaque mot a ayant h comme facteur droit par l'ensemble aB_h où $B_h = \{f \in X^{*} : hf \in A''\}$ puisque l'ensemble B_h est lui-même un code préfixe satisfaisant N_r. Dans le cas où $A'' = A$ l'ensemble A''_2 est précisément l'ensemble $\bar{A}$ de la construction 2. Donc, $\bar{A}$ est un code préfixe, et en raison de la symétrie de la construction on a établi que $\bar{A}$ est un code bipréfixe maximal .

.18.

Quand la valeur moyenne de la longueur des mots de A est finie, elle est égale à celle de $\bar{A}$.

En effet, comme B_h (resp. B') est un code préfixe (resp. préfixe gauche) maximal fini, il existe un ensemble fini $S \in X^{\#}$ (resp. $S' \in X^{\#}$) tel que $1 - \alpha B_h = (1-\alpha X).\alpha S$ (resp. $1 - \alpha B'_h = (1-\alpha X).\alpha S'$) . Comme d'autre part

$$\alpha \bar{A} = \alpha A - \alpha h.\alpha B_h - \alpha h.\alpha B'_h + \alpha h + \alpha h.\alpha B_h.\alpha B'_h =$$

$$= \alpha A + \alpha h(1-\alpha B_h)(1-\alpha B'_h)$$

on a donc bien

$$(1-\alpha \bar{A})(1-\alpha X)^{-1} = (1-\alpha A)(1-\alpha X)^{-1} + \alpha h.\alpha S.\alpha S'.(1-\alpha X)$$

- - - - - - - - - - - - - - -

QUESTION :

Est-il possible d'obtenir tous les codes bipréfixes maximaux finis par itération de la construction 2 à partir des codes X^n ($n>0$) ?

Une étape possible vers la reponse à cette question serait la solution du problème strictement algébrique suivant : (où comme toujours $\alpha X = \sum_{x \in X} x$) .

Quelle est pour n entier positif donné la forme générale des polynômes $V \in \underline{Z}[X]$ tels que $(\alpha X)^n + (\alpha X-1)^2 V$ et $1 + \alpha X + (\alpha X)^2 \ldots + (\alpha X)^{n-1} + (\alpha X-1)V$ n'aient pas de coefficients négatifs ?

ON THE ALGEBRAIC THEORY OF AUTOMATA

M. P. SCHUTZENBERGER
Institut Blaise Pascal
Paris, France

A serious bibliography of automata theory (even algebraic) contains some few hundred titles which might explain my not attempting to record all the progress that has been accomplished; the quality of these works either published or awaiting publication is, as a matter of fact, an excuse to leave this task to others better qualified than myself. I believe, also, that this congress may accomplish as useful a function by profiting from the reunion to confront various opinions on the role of mathematical disciplines in the art of non-numeric information processing. Indeed, there is room on this wagon for the most varied topics and, also, for the same topic in the most diverse dress. However, in the names *cybernetics*, *information theory*, *automata theory* (or the *theory of algorithms*), the *theory of formal languages* (*grammars*) related to so many others in the titles of books and conferences, one may distinguish a common core unified, at least, by the researchers who study its multiple facets one after another. This core, it seems to me, is that part of mathematics which applies to T. I. n. N. and it is of this that I shall speak from now on, begging pardon if I should go beyond the prescribed frame. I know— must one say it?— the emptiness of pompous generalities and the ridicule of prophecies, but teaching and research forces one to adopt options which are not individual and which it is better to state explicitly. If that, which the schematism imposed by time of that which I shall attempt, provokes enough discussion, and if we learn from so many experts the hopes which make one way preferable to another, this exposé, as I would wish it, will not have been just an interlude between the conferences of high technical value enriching this congress.

Like all applications of mathematics, the theory being considered has tasks which may be regrouped as follows: to orient research by classifying the problems, by extracting the proper concepts and by unifying the arguments; to put to use the essential results accumulated by the relevant branches of mathematics; and to allow the latter to profit from a restated problematics and from intuition born of experience and of the thorough study of special cases it requires.

I doubt that there would be any disagreement on these banalities, though one may imagine many shadings in the optimism implied by the first remarks and many degrees of fervor in the pursuit of the last one. To illustrate, I shall take the theory of Krohn and Rhodes on the simulation of a finite automaton given by a cascade of elementary organs. The authors have established that the basic concept is that of the variety of monoids (more exactly, of the subgroup of the finite monoid, the automaton model). This has allowed them to use deep theorems on simple groups to characterize the modular elements necessary to such a synthesis and has led them to that which is today the best adaptation to monoids of the "set extension theorems." No one here will dispute the interest of this last result, but one will ask in what way the notion of variety of subgroups is a "good concept" and in what way this would not hold also for more tangible notions; one may even state that the theory of Krohn and Rhodes is "a fine algebraic result devoid of practical significance," since it gives no explicit detail on this last parameter. I think there is one simple answer to these two objections: the notion of minimal number of states is not a good concept because no one has yet been able to say something non-trivial about it; the notion of variety has a practical importance because it allows the formulation of non-trivial relations between describable objects in

the most naive vocabulary. What is more, it is the algebraic concept which, it seems, leads in vitality and the little we know of this minimal number of states derives in a natural way from the consideration of certain varieties. Two examples: the remarkable study by Elgot and Rutledge on the minimization of incompletely specified automata is based implicitly on the discussion of *Abelian* subgroups; the theory of Trachtenbrot and McNaughton on regular expressions with no Kleene stars, blends itself with that of finite monoids whose subgroups are degenerate. The detour which has led us away from the obvious has not only revealed the underlying unity but it has, I believe, allowed a collection of substantial new results, illustrated by the work of Verbeek, Beatty or Pappert. One may ask then, if it is not rather intuitions of this sort which should be awakened in young researchers and if, without abandoning more concrete goals, one should not recognize the deplorable existence of apparently simple and ostensibly useful problems which will not submit to a head-on attack with home-made arms. True, a certain vertigo of abstraction seizes all too often those among us who prefer mathematics to its applications (the others also, as a matter of fact). Why cite those articles in which the reader must ascend pyramids of *n*-tuples to attain a few dozen "theorems" each of which could be verified in two lines if one didn't have to translate and retranslate a pile of definitions? It seems to me that there is, however, a criterion to test the validity of a problem from the point of view which concerns us here, namely, its application: it is the one I made use of above: to show non-trivial relations between objects described in a reasonably simple manner by a change of notation. For the rest, that is, the interest claimed to be practical by some or by many, let me recall, according to Moore, the history of chemistry and ask in turn whether Priestly's experiences or Lavoisier's would have attracted the attention of alchemists working on the *GREAT WORK?*

I now come to that common mathematical core which has been successfully applied to T. I. n. N. Its negative characteristics keep us from the richest provinces of analysis and arithmetic. The only instance where classical methods could have been used is that of correcting codes: the existence of module structures shown by Slepian has allowed Hocquenghem, Bose and Chaudhury to establish through galois fields the theory we know. One must then go toward fresher territory, algebra after Glushkov and his school, mathematical logic with Myhill, Wang, Medveev, Kalmar and Rabin to find ways in which to study that which seems to us as the main problems:

1. Establishing a hierarchy for questions of information processing in terms of permissible modular elements and their rules of usage.
2. The optimization in terms of the material, time or feasibility.

There is, therefore, no break: the first topic was that of classical geometry. As for the second, we should like it to encompass numerical problems and the intermediate mode of Boolean algebra studied extensively by Kuntzmann and the Grenoble group that, like circuit theory, I shall not embark on here for lack of space; after all, the considerable work of Ardeen, Rabin and Winograd leave one with the hope that selective natural hypotheses will be found to avoid the difficulties revealed by Shannon in the general instance. Therefore, if a detailed analysis is conducted of this or that problem of reliability by McCulloch or Cowan, or of sorting by Schensted, Picard or Nelson, of unusual dynamics by Holland or Arbib, by Eastman or by Neuman or A. A. Markov according to Sardinas and Patterson, subtle Gödelization by Minsky, Böhm or Manuel Blum, of complexity measure by Hartmanis, Stearns or Eggan, it is certainly for the merit of the question itself but also, as Rabin has shown, in the hope of creating from a sample case these general principles which one suspects from the positive characteristics which our common mathematical core contains:—for want of topology, the hypothesis given by usage is the finiteness of a generative or referential system. This is sufficient to escape the dull formalism of a too universal algebra and does not exclude (on the contrary, I would say, at the risk of seeming old-fashioned) that as for Buchi's fine work, concrete reality be illuminated by denying what seemed its most essential trait.

For want of geometry, what machines universally propose is the finite sequence structure of discrete elements; therefore, still, N, then free monoids. Moreover, N is a Procrustean bed to which graphs and tables must conform before being manipulated. This is the interest in setting up correlations intelligently between the most varied structures and the words and operations that combine them (see Foata's original algebras with probabilistic resonances and the generating functions of Sherman, Raney, Gross and Harrison which have us revisiting, as algebraists, chapters of classical analysis and leave us hoping to extend its methods in the manner of Magnus Fox or Lyndon to commutative cases).

That is stating also the value of these procedures for cutting and retranscription of words developed by Nivat to build a theory of compilers completing the work of Bauer and Samelson.

Finally, if I knew how to do it, I should state a third character, very manifestly linked to the non-negativeness and which sustains also other close areas of application of mathematics. Maybe there shall be a theory compensating for our present inability in spite of the works of Nerode and of Gill to act like everyone and to use widely the apparatus of linear methods and vector spaces. It is, however, questions of formal languages (another name for the parts of a free monoid) which occupy the greatest number of people and which, owing to the attention of Backus, Naur or Vauqois, Hayes or Ravzin, Markus or Benzecri, confer on our small domain a trust we should not like to fail. One must first establish the equivalences of the definitions of a family of formal languages. Mathematical logic has provided the fundamental concept of recursive insolvability which, brandished vigorously by Bar-Hillel, Ginsburg and their groups, mark for all time the boundary of certain algorithmic dreams. Even though the theorems of Markov or Lecerf have a more classical twist, no one maintains that today algebra would be anything better than a convenient formalism for families of formal languages or algebras as general as those of Yamada, Ritchie, Shepherdson and Sturgis or Kuroda; the same reason dispenses us from speaking of automatic demonstrations. It is impossible to set a precise limit but it seems not to be so for languages and systems such as those studied by Shamir, Fisher, Stahl, Hennie, Cole or Evey. At this level, the typical problem is to build an algorithm (the automaton) capable of recognizing by sequential examination of its letters if a word belongs to the given formal language; owing to Gorn, Floyd, Burks and Wright, we know how to treat similarly many other problems of ambiguity and transformation. Besides, and this is the main fact, it is generally possible to compress effectively the information accumulated during the reading of the word, therefore to identify the *states* of the automaton to classes of a regular equivalence. As Rabin, Scott and Shepherdson were first to show, the problem is only one of representative monoids and one knows the advantage that authors like Culik, Mezei, Laemmel, Deussen, Giveon or Paz have derived from that model; more complicated cases (*non-deterministic* or *probabilistic*) first require monoids with binary relations elaborated by Riguet, then by Sain and Zaretskii.

Thus, we find ourselves rich with formal languages; a remarkable ingenuity was necessary to establish radical differences between procedures to which a superficial examination would have attributed an identical power, and, to conclude, I might refer to Rado who has demonstrated so well all the benefits which the art of programming extracts from such precise and difficult problems.

But, since I want to speak for theory and for algebra, I must submit that the chance for counter examples to remain put, like that for conjectures not to remain riddles, is a function of a parameter other than non-triviality, the contingency of which is smaller than that of our efforts: the richness of their relations with the center of mathematics. It is the special merit of the structures discovered by Kleene and of those discovered by Chomsky that, having been found at so many cross-roads, they are the object of so many theorems. If the most serious authos only see the utensil virtues of finite automata and of cell memories, I must remind you that their definition, as we now know it, could be the same one as for finite monoids and free groups and I thank you for allowing me to repeat after Siger: "esse autem essentiae dicit totum quod pertinet ad entitatem eius, sive potentia, sive actus, indicatum per definitionem."

Année 1966

Bibliographie

[1] Jean Larisse and Marcel-Paul Schützenberger. Sur certaines chaînes de Markov non homogènes. In *Automata Theory, Ravello 1964*, pages 239–250. Academic Press, New York, 1966.

[2] Marcel-Paul Schützenberger. Sur certaines variétés de monoïdes finis. In *Automata Theory, Ravello 1964*, pages 314–319. Academic Press, New York, 1966.

[3] Marcel-Paul Schützenberger. On a family of sets related to McNaughton's *L*-language. In *Automata Theory, Ravello 1964*, pages 320–324. Academic Press, New York, 1966.

[4] Michel Coudrain and Marcel-Paul Schützenberger. Une condition de finitude des monoïdes finiment engendrés. *C. R. Acad. Sci. Paris Sér. A-B*, 262 :A1149–A1151, 1966.

[5] Maurice Nivat and Marcel-Paul Schützenberger. Sur les produits semi-directs droits de monoïdes. *C. R. Acad. Sci. Paris Sér. A-B*, 263 :A659–A660, 1966.

[6] Françoise Dejean and Marcel-Paul Schützenberger. On a question of Eggan. *Information and Control*, 9 :23–25, 1966.

[7] Marcel-Paul Schützenberger. On a question concerning certain free submonoids. *J. Combinatorial Theory*, 1 :437–442, 1966.

[8] Marcel-Paul Schützenberger. Le dialogue homme-machine à l'ère de l'ordinateur. *Les cahiers de l'institut de la vie*, 10 :43–44, octobre 1966.

[9] Marcel-Paul Schützenberger. Classification of Chomsky languages. In *Formal Language Description Languages for Computer Programming*, pages 100–104. North-Holland Publ. Co., 1966.

Sur Certaines Chaines de Markov Nonhomogènes

J. Larisse

CETIS–EURATOM
Ispra, Italy

et M. P. Schützenberger

Institut Blaise Pascal
Paris, France

Considérons un ensemble $\{m_1 m_2 \cdots m_k\}$ $(k \leqslant \infty)$ de matrices stochastiques $I \times I$. Une séquence infinie arbitraire $m_{i_1} m_{i_2} \cdots$ constitue une chaîne de Markov nonhomogène sur les états I. D'une manière équivalente nous pouvons définir cette chaîne comme une représentation μ du monoïde libre F [1] dans le monoïde M des $I \times I$ matrices stochastiques. Soit $X = \{x_1 x_2 \cdots x_k\}$ $(k \leqslant \infty)$ l'ensemble générateur de F, nous nous proposons dans cet exposé d'étudier les propriétés limites de $\mu f = \mu x_{i_1} \cdot \mu x_{i_2} \cdots \mu x_{i_n}$ pour $n \to \infty$; le cas homogène se ramenant à celui du sous-monoïde engendré par l'élément unique μf, nous aurions alors à étudier les propriétés asymptotiques de μf_n pour $n \to \infty$.

Un résultat de J. Wolfowitz [2] montre que si $\{A_1, A_2, \ldots, A_k\}$ est un ensemble fini ou infini de matrices stochastiques carrées de même ordre tel que tout produit B de la forme $A_{i_1} A_{i_2} \cdots A_{i_n}$ est apériodique et indécomposable, c'est-à-dire que

$$\lim_{n \to \infty} B^n = Q$$

où Q a toutes ses lignes égales, alors en définissant

$$\delta(B) = \max_j \max_{i_1 i_2} |b_{i_1 j} - b_{i_2 j}|$$

nous pouvons pour ϵ arbitrairement petit donné trouver $n(\epsilon)$ tel que

$$\delta(B) < \epsilon \text{ dès que } |B| = n > n(\epsilon) \qquad (1)$$

En d'autres termes soit M_1 l'ensemble des matrices stochastiques ayant une racine simple de module un (ce qui est équivalent à l'hypothèse d'apériodicité et d'indécomposabilité), définissant

$$\text{norme } \mu f = \|\mu f\| = \max_{i \in I} \sum_{j \in I} |\mu f|_{ij}$$

$$\bar{\mu} f = \lim_{n \to \infty} \mu f^n \qquad \text{pour } \mu f \in M_1$$

On a

$$\|\mu f_1 f_2 - \bar{\mu} f_2\| < \epsilon \text{ dès que } |f_2| > n(\epsilon) \text{ et quel que soit } f_1$$

En effet, pour $|f_2| > n(\epsilon)$ on peut écrire

$$\mu f_2 = m + E$$

où $m \in M_1$ a toutes ses lignes égales, E est une matrice quelconque avec $|\epsilon_{ij}| < \epsilon$ pour $i, j \in I$. Dès lors,

$$|(\mu f f_2)_{ij} - (\mu f_2)_{ij}| = |\sum_{k \in I} (\mu f)_{ik}(m_{\cdot j} + \epsilon_{kj}) - m_{\cdot j} - \epsilon_{ij}|$$

$$= |\sum_{k \in I} (\mu f)_{ik} \epsilon_{kj} - \epsilon_{ij}| < 2\epsilon$$

$$\|\mu f f_2 - \mu f_2\| < 2I\epsilon$$

ceci étant vérifié pour μf stochastique quelconque, faisons $\mu f = \mu f_1$ et $\mu f = \bar{\mu} f_2$ on a

$$\|\mu f_1 f_2 - \bar{\mu} f_2\| \leqslant \|\mu f_1 f_2 - \mu f_2\| + \|\mu f_2 - \bar{\mu} f_2\|$$
$$= \|\mu f_1 f_2 - \mu f_2\| + \|\bar{\mu} f_2 \cdot \mu f_2 - \mu f_2\| \leqslant 4I\epsilon$$

d'où

$$\lim_{|f_2| \to \infty} \|\mu f_1 f_2 - \bar{\mu} f_2\| = 0 \tag{2}$$

Pour assurer dans la suite de l'exposé (Remarque 2) une convergence uniforme nous imposerons à la plus petite entrée positive ωx des μx, $x \in X$ la condition suffisante qu'il existe $\bar{\omega} > 0$ tel que $\omega x > \bar{\omega}$, $x \in X$. Nous poserons $\omega x = 0$ si les éléments positifs de μx sont tous égaux à 1. La donnée de μ déterminant d'une façon univoque l'homomorphisme ω de F dans le groupe additif des réels nous définirons

$$F_z = \{f \in F;\ \omega f > z\}$$

ce qui entrainera en particulier que $\mu f \in P$ (sous-monoïde des matrices d'application de I dans I) pour tout $f \in F \setminus F_0$. Avec ces notations (1) s'écrit donc

$$(W_1) \cdot \lim_{z \to \infty} \{\|\mu f_1 f_2 - \bar{\mu} f_2\| : f_1 \in F, f_2 \in F_z\} = 0$$

Considérons maintenant le cas où les $\mu f \in M_r$ (ensemble des matrices stochastiques $I \times I$ ayant r classes ergodiques). La forme la plus générale de telles matrices est (Fig. 1; [3])

$g_i\, i \in [1, m]$: blocs indécomposables de classes ergodiques cycliques r_{ik}
$t_j\, j \in [1, p]$: groupements transitoires

Il est clair que la propriété pour une matrice μf d'avoir r classes ergodiques ne dépend pas de la valeur particulière des entrées mais de la

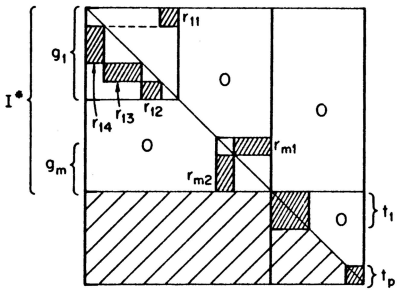


FIG. 1

distribution des éléments nuls. Nous associerons donc à chaque μf sa matrice de support $\beta\mu f$ définie de la manière suivante:

$$(\beta\mu f)_{ij} = 1 \qquad \text{si } (\mu f)_{ij} \neq 0$$
$$= 0 \qquad \text{si } (\mu f)_{ij} = 0$$

Avec les lois d'addition et de multiplication booléennes on voit aisément que β est un homomorphisme du monoïde $\{\mu f; f \in F\}$ dans le sous-monoïde des matrices de support:

$$\beta(\mu f_1) \cdot \beta(\mu f_2) = \beta(\mu f_1 \cdot \mu f_2) = \beta(\mu f_1 f_2)$$

En remarquant, d'autre part que

$$\text{La } i\text{ème ligne de } \beta(\mu f_1 f_2) = \bigcup_k \{k\text{ième ligne de } \beta\mu f_2;\ k \in \beta\mu f_1\}$$

on vérifie immédiatement que:

$$\text{Si } \beta_i \mu f_1 \text{ est un élément minimal de la famille } \{\beta_j \mu f_1; j \in I\}$$

ordonnée par inclusion, $\beta_i \mu f_1 f_2$ est un élément minimal de la famille $\{\beta_j \mu f_1 f_2; j \in I\}$.

Si $\beta_i \mu f_1 f_2 \cap \beta_{i'} \mu f_1 f_2 = \phi$ alors, d'une part $\beta_i \mu f_1 \cap \beta_{i'} \mu f_1 = \phi$, d'autre part $\beta_j \mu f_2 \cap \beta_{j'} \mu f_2 = \phi$ pour tout $j \in \beta_i \mu f_1$ et $j' \in \beta_{i'} \mu f_1$. Il découle de ces

dernières relations que si $\Delta(\mu f)$ est la cardinalité maximale d'un ensemble de lignes de μf ayant leurs supports deux à deux disjoints, on a pour tout $\mu f_1, \mu f_2 \in M$.

$$\Delta(\mu f_1 f_2) \leqslant \{\Delta(\mu f_1), \Delta(\mu f_2)\}$$

Le sous-monoïde des supports étant fini il existe un $n \geqslant$ (**Card I**)! et un q tels que

$$(\beta\mu f)^n = (\beta\mu f)^{n+q}$$

La propriété est alors vraie pour une infinité de n et nous dirons que $(\beta\mu f)^n$ est cyclique.

En réservant la notation $I_j^*(f)$ ($j \in [1,r]$) à la $j$ième classe ergodique et en posant $I^*(f) = \cup\{I_j^*(f); j \in [1,r]\}$ la restriction à $I_j^*(f) \times I$ de $\beta\mu f$ est contenue dans un "rectangle" $I_j^*(f) \times I_j^*(f)$ et elle est égale à ce rectangle si $\beta\mu f$ est cyclique, parce qu'alors les sous-matrices r_{ij} (Fig. 1) n'ont que des éléments différents de zéro.

D'autre part, le groupement cyclique g_i possédant r_i classes ergodiques est isomorphe au groupe cyclique d'ordre r_i [4], et $r!$ étant divisible par $r_1 r_2 \cdots r_m$ ($r = r_1 + \cdots r_m$) il s'ensuit que $(\mu f)^{r!}$ est apériodique et la limite $\bar{\mu} f = \lim_{k \to \infty} \mu f^{kr!+1}$ existe.

$\bar{\mu} f$ est une matrice stochastique dont toutes les lignes dans $I^*(f) \times I$ ayant même support sont égales et dont les autres lignes sont des combinaisons linéaires à coefficients nonnégatifs des premières [3]. Il s'ensuit que la restriction à $I \times I^*(f)$ du support de μf est contenue dans $\beta\bar{\mu} f$ et $\beta\bar{\mu} f$ est égale à la restriction à $I \times I^*(f)$ du support de μf quand $\beta\mu f$ est cyclique.

Ces notions étant rappelées, définissons R comme la fermeture convexe du sous-ensemble $P_r \subset P$ des matrices représentant une application $I \to I$ telle que l'image I_p de I ait au plus r éléments. A chaque $f \in F$ nous associons $\chi f \in [0,1]$, $\mu_R f \in R$ et $m \in M$ par les relations suivantes:

$$\mu f = (1 - \chi f)\,\mu_R f + \chi f m$$
$$\chi f = \min\{\chi \in [0,1]: \mu f = (1-\chi)\,m + \chi m';\ m \in R,\ m' \in M\}$$

Enfin soit F_+ l'ensemble des $f \in F$ tel qu'il existe au moins un $g \in F_0$ de support cyclique et une paire $f', f'' \in F$ satisfaisant $\beta\mu f = \beta\mu f' g f''$.

Remarque 1. Pour chaque $f \in F_+$ on a $\chi f < 1$ et $\beta\mu_R f \subset \beta\bar{\mu} f$.

Vérification. Il est clair que $PP_r P \subset P_r$ et que le support de tout $m \in M$ est

une union de supports d'applications $p' \in P$. Il en résulte immédiatement que $\chi ff' \leqslant \chi f \cdot \chi f'$ pour tout $f,f' \in F$. En effet,

$$\begin{aligned} \mu f &= (1-\chi f)\mu_R f + \chi f m \\ \mu f' &= (1-\chi f')\mu_R f' + \chi f' m' \\ \mu f \cdot \mu f' = \mu f f' &= (1-\chi f)(1-\chi f')\mu_R f \cdot \mu_R f' + \chi f'(1-\chi f)\mu_R f m' \\ &\quad + \chi f(1-\chi f') m \cdot \mu_R f' + \chi f \cdot \chi f' m m' \end{aligned}$$

Etudions les produits $\mu_R f \cdot \mu_R f'$, $\mu_R f \cdot m'$, $m\mu_R f'$, et mm'. La fermeture convexe de l'ensemble P_r étant égale à l'ensemble des combinaisons linéaires convexes de P_r on a

$$\mu_R f \cdot \mu_R f' \in R$$

D'autre part,

$$m \cdot \mu_R f' = \sum_{k=1}^{n} \alpha'_k m r'_k \qquad \mu_R f \cdot m' = \sum_{k=1}^{n'} \alpha_k r_k m'$$

$$\sum_{k=1}^{n} \alpha'_k = \sum_{k=1}^{h'} \alpha_k = 1$$

On vérifie aisément que $mr'_k \in R$, et que $r_k m'$ est une matrice stochastique dont toutes les lignes de même support dans $I^* \times I$ sont identiques, les autres étant des combinaisons linéaires à coefficients nonnégatives des premières, donc $r_k m' \in R$. Comme $mm' \in M$ on peut écrire:

$$\begin{aligned} (1-\chi f)(1-\chi f')\mu_R f \cdot \mu_R f' + \chi f'(1-\chi f)\mu_R f \cdot m' + \chi f(1-\chi f') m \cdot \mu_R f' \\ = (1-\chi f \cdot \chi f')\mu_R f f' \qquad \text{avec } \mu_R f f' \in R \end{aligned}$$

puis

$$\mu f f' = (1-\chi f \cdot \chi f')\mu_R f f' + \chi f \cdot \chi f' m''$$

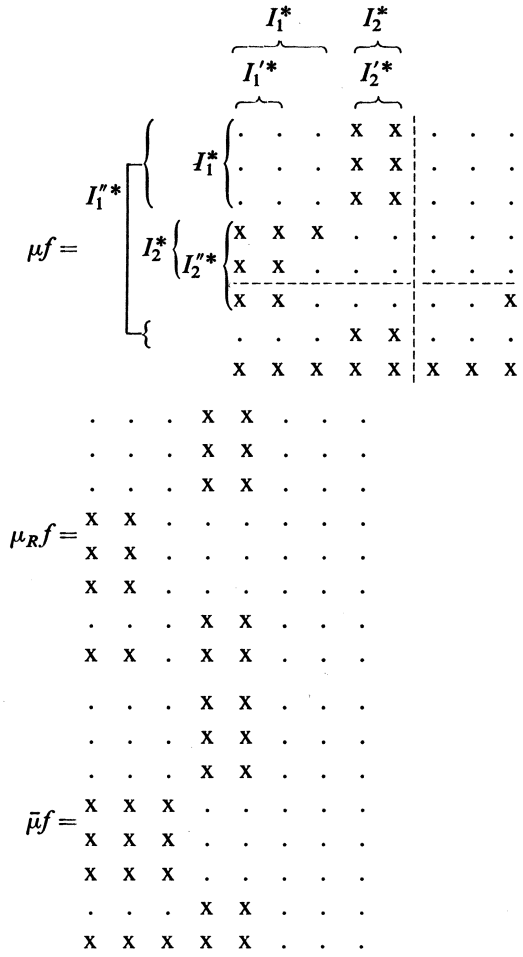
ce qui montre que $\chi ff' \leqslant \chi f \cdot \chi f'$.

Considérons $g \in F_0$ de support cyclique. Si $I' \subset I$ a un et un seul élément en commun avec chacune des classes ergodiques $I_j^*(g)$, le fait que pour chaque $i \in I$ la ligne $\beta_i \mu g$ contienne au moins un $I_j(g)$ montre qu'il existe au moins un $p \in P_r$ tel que $I' = Ip$ et $\beta p \subset \beta \mu g$. Donc $\chi g < 1$ et par conséquent $\chi f' g f'' < 1$ pour tout $f',f'' \in F$. Comme la propriété $\chi m < 1$ ne dépend en fait que de βm, l'inégalité $\chi f < 1$ pour $f \in F_+$, est établie.

Soit maintenant $\beta p \subset \beta \mu f$ où $p \in P_r$ et $f \in F_+$. Si $I' = Ip$, l'union des supports des colonnes de μf d'indice $i \in I'$ est égale à I, et il en est de même pour toute matrice de la forme $\mu f' f$. Prenant $f' = f^n$ tel que $\beta \mu f' f$ soit cyclique, on en conclut que I' doit avoir un (et un seul) élément en commun avec chacune des classes ergodiques $I_j^*(f)$ et qu'en particulier $I' \in I^*(f)$. Comme $\beta p \subset \beta \mu f$ et comme la restriction de $\beta \mu f$ à $I \times I^*(f)$ est contenue dans $\beta \bar{\mu} f$, la remarque est entièrement vérifiée.

Il résulte de $\beta\mu\ \ f \subset \beta\bar{\mu}f$ que chaque classe $I_j^*(f)$ admet un sous-ensemble minimal $I_j'^*(f)$ tel que $I^*(f) \times I_j'^*(f)$ contienne la restriction à $I^*(f) \times I_j^*(f)$ du support de $\mu_R f$. De même, il existe un sous-ensemble maximal $I_j''^*(f)$ contenant tous les $i \in I$ tels que $\beta_i \mu_R f \subset I_j'^*(f)$.

Exemple



Remarque 1'. Si $f, f' \in F_+$ il correspond à chaque $j \in [1,r]$ un et un seul $j' \in [1,r]$ tel que $I_j'^*(f) \subset I_{j'}''^*(f')$.

Vérification. Soit $f \in F_+$ on a $\Delta(\mu f) \leqslant \Delta(\mu g) = r$ puisque f admet g comme facteur. D'autre part nous savons que pour $n \geqslant$ (**Card I**)! μf^n est cyclique donc $r = \Delta(\mu f^n) \leqslant \Delta(\mu f)$, il s'ensuit que $\Delta(\mu f) = r$.

Considérons maintenant le cas particulier de l'énoncé où $\beta\mu f$ et $\beta\mu f'$ sont cycliques. La relation $\Delta(\mu ff') = r$ montre que pour chaque $i \in I_j^*(f)$, le support $\beta_i \mu f'$ doit avoir une intersection nonvide avec une seule classe $I_{j'}^*(f)$. Le cas général s'en déduit immédiatement: en effet, $I_j'^*(f) \subset I_j^*(f)$ et les seuls $i \in I$ tels que $\beta_i \mu f'$ n'intersecte qu'une seule classe $I_{j'}^*(f')$, appartiennent à l'union $I''^*(f')$ des ensembles disjoints $I_j''^*(f')$.

Nous écrivons désormais pour abréger lim au lieu de $\lim_{z\to\infty}$ max et nous désignons par f_z et f'_z des variables liées par la condition $f_z, f'_z \in F_z$.

Remarque 2. $\mathrm{Lim}\|\mu f_z - \mu_R f_z\| = 0$.

Vérification. Soit $B = \{\beta\mu f; f \in F_0\}$. Si un élément $b \in B$ appartient à une $\mathscr{D}$-classe régulière [5], il existe un élément $b' \in B$ tel que $b'^2 = b'$ et $b'b = b$. Donc si B_+ est l'idéal de B engendré par les D-classes régulières, l'image inverse de B_+ par β^{-1} appartient à F_+.

Soit h le nombre des $\mathscr{D}$-classes de B, B étant fini on a $\mathscr{D} = \mathscr{J}$ et dans le monoïde $B^1 = B \cup e$ la relation d'inclusion sur les idéaux bilatères principaux $B^1 a B^1 \subseteq B^1 b B^1$, $a, b \in B^1$ induit une relation d'ordre partiel sur les $\mathscr{J}$-classes donc sur les $\mathscr{D}$-classes. Autrement dit les idéaux bilatères principaux forment un semi-treillis dont l'élément minimal, idéal minimum de B, est une $\mathscr{D}$-classe régulière (plus précisément un sous-demi-groupe complètement simple). Or nous savons [6] que si b', b'' et $b'b''$ appartiennent à la même $\mathscr{D}$-classe celle-ci est régulière, autrement la $\mathscr{D}$-classe de $b'b''$ est telle que

$$\mathscr{D}_{b'b''} \leqslant \mathscr{D}_{b'} \qquad \mathscr{D}_{b'b''} \leqslant \mathscr{D}_{b''}$$

On peut alors montrer que tout produit $b_1 b_2 \cdots b_{\bar{h}}$ de $\bar{h} = 2^{h-1}$ éléments de B a au moins un facteur nonvide appartenant à une $\mathscr{D}$-classe régulière de B donc appartient lui-même à βF_+. Ceci est trivial pour $h = 1$ puisque dans ce cas B a une seule $\mathscr{D}$-classe qui est nécessairement régulière. On peut donc supposer le résultat vérifié quand B a moins de $h > 1$ $\mathscr{D}$-classes, et naturellement, on peut aussi supposer qu'aucun des $b_{k'}$ $(k' = 1, 2\ldots, \bar{h} = 2^{h-1})$ n'appartient lui-même à une $\mathscr{D}$-classe régulière. Le sous-monoïde engendré par les 2^{h-2} produits $b_1 b_2, b_3 b_4, \ldots, b_{\bar{h}-1} b_{\bar{h}}$ a au plus $h-1$ $\mathscr{D}$-classes et le résultat découle de l'hypothèse d'induction.

Soit maintenant $F'_+ = F_+ \backslash F \times F_+ \times F$. Le résultat qui vient d'être vérifié montre que tout $f \in (F_0)^{n\bar{h}}$ a au moins n facteurs dans F'_+. Faisant intervenir l'hypothèse selon laquelle $\omega x = 0$ ou $\omega x > \bar{\omega} > 0$ pour tout $x \in X$ on voit que $\omega f > \bar{\omega}^{\bar{h}}$, $\chi f < 1 - \omega f < 1 - \bar{\omega}^{\bar{h}}$ pour tout $f \in F'_+$ et par

suite $\chi f < (1-\bar{\omega}^{\bar{h}})^n$ pour tout $f \in (F_0)^{n\bar{h}}$ ce qui entraine $\lim \chi f_z = 0$.

Soit $m \in M$ et définissons [7]

$$\lambda(m) = 1 - \min_{i_1 i_2} \sum_j \min(m_{i_1 j}, m_{i_2 j})$$

on a $0 \leqslant \lambda(m) \leqslant 1$ avec

$\lambda(m) = 0$ si et seulement si m a toutes ses lignes égales
$\lambda(m) = 1$ si et seulement si βm a deux lignes disjointes

$0 < \lambda(m) < 1$ définiera une "scrambling matrix," c'est-à-dire que quelles que soient les deux lignes $i_1 i_2$ il existe une colonne j telle que $m_{i_1 j}, m_{i_2 j} > 0$.

On démontre que $\delta(m_1 m_2) \leqslant \delta(m_1)$ et qu'un produit de matrices stochastiques dont un facteur est "scrambling" est lui-même scrambling. Cette propriété est identique à celle des matrices positives ayant une colonne d'éléments nonnuls et aux matrices $\mu f \in F_+$.

Soit V l'ensemble des I-vecteurs v à coordonnées nonnégatives tels que $\Sigma_{i \in I} v_i = 1$. Pour $(v, v') \in V \times V$ et $m \in M$ nous pouvons poser

$$\delta_{vv'} m = 1 - \sum_{i \in I} \min\{(vm)_i, (v'm)_{i'}\}$$

Par définition: $\delta_{vv'} m = \lambda(m_v m')$ où m_v est une matrice stochastique dont les deux premières lignes sont identiques aux vecteurs v et v', les autres étant, par exemple, identique à v (ou v'). On a donc pour tout $m' \in M$

$$0 = \delta_{vv'} mm' \leqslant \delta_{vv'} m \leqslant 1 \qquad \text{avec } \delta_{vv'} m = 0 \text{ (resp. } = 1)$$

si et seulement si $vm = vm'$ (resp. $\beta vm \cap \beta v' m = \phi$). Quand μ et μ' sont deux applications de F dans M telles que $\lim \|\mu f_z - \mu' f_z\| = 0$ on a évidemment $\lim |\delta_{vv'} \mu f_z - \delta_{vv'} \mu' f_z| = 0$.

Nous considérons maintenant un sous-ensemble fixe K de I ayant r éléments et nous définissons la $I \times I$ matrice e_k par $(e_k)_{i,i'} = 1$ si $i = i' \in K$; $= 0$, autrement. Pour abréger, nous écrivons $m' \in M'$ (resp. $m'' \in M''$) si $m' = m \cdot e_k$ (resp. $m'' = e_k \cdot m$ pour au moins un $m \in M$) et si m' contient r lignes ayant des supports disjoints telles que toute autre ligne soit une combinaison linéaire à coefficients nonnégatifs de ces dernières (resp. et si m'' a r lignes ayant des supports disjoints nonvides).

Remarque 3. Il existe deux applications $\mu' : F \to M'$ et $\mu'' : F \to M''$ telles que $\lim \|\mu f_z - \mu' f_z \cdot \mu'' f_z\| = 0$.

Vérification. Nous utilisons les notations de la Remarque 1'. Le support de la restriction de $\mu_R f_z$ à $I''^*(f_z) \times I$ est une union de r rectangles disjoints

$I''_j(f_z) \times I'_{j'}(f_z)$. Comme $\mu_R f_z$ appartient à la fermeture convexe R de Pr ceci entraîne que deux lignes quelconques de cette matrice soient égales quand leurs supports sont identiques. Il existe donc une matrice $\mu'' f_z \in M''$ dont les lignes nonnulles sont égales aux r lignes distinctes de la restriction de $\mu_R f_z$ à $I''^*(f_z) \times I$.

Soit f'_z un autre élément de F_z. D'après la Remarque 1', chacun des ensembles $I'^*_{j'}(f'_z)$ est contenu dans un et un seul ensemble $I''_j(f_z)$ et $\mu_R f'_z$ est identique à la somme de ses restrictions à $I \times I'^*_{j'}(f_z)(j' \in [1,r])$. Donc deux lignes quelconques nonnulles de la restriction à $I \times I'_j(f_z)$ de $\mu_R f'_z \cdot \mu_R f_z$ sont proportionnelles et l'on peut trouver une application $\nu' = F \times F \to M'$ telle que l'on ait $\mu_R f'_z \cdot \mu_R f_z = \nu'(f'_z, f_z) \cdot \mu'' f_z$ identiquement. D'après la Remarque 2,

$$\lim \|\mu f'_z f_z - \mu_R f'_z f_z\| = 0$$

Par conséquent,

$$\lim \|\mu f'_z f_z - \nu'(f'_z, f_z)\, \mu'' f_z\| = 0$$

ce qui entraîne la validité de la Remarque 3.

Remarque 3'. Si les applications $\mu' : F \to M'$; $\nu = F \times F \times F \to M$ et $\mu'' : F \to M''$ satisfont la relation $\lim \|\mu f_z f f'_z - \mu' f_z \nu(f_z, f, f'_z) \cdot \mu'' f'_z\| = 0$, il existe trois applications $\bar{\mu}' = F \to M'$; $\rho : F \times F \times F \to M$ et $\bar{\mu}'' : F \to M''$ telles que

$$\lim \|\mu' f_z - \bar{\mu}' f_z f f'_z\| = \lim \|\nu(f_z, f, f'_z) - \rho(f_z, f, f'_z\|$$
$$= \lim \|e_k \nu(f_z, f, f'_z)\, \mu'' f'_z - \bar{\mu}'' f_z f f'_z\| = 0$$

et qu'en outre, d'une part la restriction de $\rho(f_z, f, f'_z)$ à $K \times I$ représente une permutation de K, d'autre part, pour tout $f' \in F_0$, $\bar{\mu} f' = \bar{\mu}' f' \cdot \bar{\mu}'' f'$.

Vérification. Deux lignes de même support de la restriction à $I^*(f) \times I$ de $\bar{\mu} f'$ étant égales, les autres étant des combinaisons linéaires à coefficients nonnégatifs des précédentes, il est clair que l'existence d'applications $\bar{\mu}' : F \to M'$ et $\bar{\mu}'' : F \to M''$ satisfaisant $\bar{\mu} f' = \bar{\mu}' f' \cdot \bar{\mu}'' f'$ est triviale et que toutes les paires d'applications satisfaisant ces conditions sont équivalentes sur F_0 à une permutation de K près.

Désignons maintenant par $\lambda^i m$ la plus grande entrée de la $i$ème colonne de m. Il est bien connu que $\lambda^i m' m < \lambda^i m$ identiquement. Donc pour tout $i \in I$ et $(f_z, f, f'_z) \in F \times F \times F$ on a

$$\lambda^i \bar{\mu} f_z f f'_z = \lambda^i \bar{\mu}'' f_z f f'_z \leqslant \lambda^i \mu f_z f f'_z$$

et

$$\lambda^i [\mu' f_z \cdot \nu(f_z f f'_z) \cdot \mu'' f'_z] \leqslant \lambda^i [\nu(f_z f f'_z) \cdot \mu'' f'_z] \leqslant \lambda^i \mu'' f'_z$$

Les hypothèses impliquent que

$$\lim\|\lambda^i(\mu' f_z \cdot \nu(f_z,f,f'_z)\cdot\mu'' f'_z) - \lambda^i \mu f_z f f'_z\| = 0$$

et comme $\bar{\mu}'' f_z f f'_z$ et $\mu'' f'_z$ appartiennent à M'', on a

$$\sum_{i\in I} \lambda^i \bar{\mu}'' f_z f f'_z = \sum_{i\in I} \lambda^i \mu'' f'_z = r$$

Donc, pour chaque $i \in I$

$$\lim|\lambda^i \bar{\mu}'' f_z f f'_z - \lambda^i(\nu(f_z f f'_z)\cdot\mu'' f'_z| = \lim|\lambda^i(\nu(f_z f f'_z)\cdot\mu'' f'_z) - \lambda^i \mu'' f'_z = 0$$

et

$$\lim \sum_{i\in I} \lambda^i(\nu(f_z,f,f'_z)\cdot\mu'' f'_z) = r$$

ce qui montre l'existence de $\rho\colon F\times F\times F \to M$, identique à ν sur $(I\setminus K)\times I$ se réduisant à une permutation de K sur $K\times I$ et satisfaisant

$$\lim\|\nu(f_z f f'_z) - \rho(f_z f f'_z)\| = 0$$

D'après la première de ces relations on peut choisir $\bar{\mu}''\colon F \to M''$ telle que

$$\lim\|e_k \cdot \rho(f_z f f'_z)\,\mu'' f'_z - \bar{\mu}'' f_z f f'_z\| = 0$$

De façon analogue, pour tout $(v,v') \in V\times V$ on a

$$\delta_{v,v'}\,\bar{\mu}' f_z f f'_z = \delta_{v,v'}\,\bar{\mu} f_z f f'_z \leqslant \delta_{v,v'}\,\mu f_z f f'_z$$

et

$$\lim \delta_{v,v'}\,\mu f_z f f'_z < \lim \delta_{v,v'}\,\mu' f_z$$

Comme l'ensemble des $(v,v') \in V\times V$ telles que $\delta_{v,v'}\bar{\mu}' f_z f f'_z$ (resp. $\delta_{v,v'}\mu' f_z$) est 0 ou 1 détermine $\bar{\mu}'$ (resp. μ') à une permutation près de K et comme le support de la restriction de $\mu f_z f f'_z$ à $I\times I^*(f_z f f'_z)$ est contenu dans $\beta\bar{\mu} f_z f f'_z$, la vérification est achevée.

Propriété 1. Si $\mu\colon F \to M$ est telle que pour chaque $f \in F_0$ la chaine de Markov $\{\mu f^n\colon n \in N\}$ a exactement r classes ergodiques, il existe une application π de F dans un sous-ensemble fini de M telle que

$$(W_r)\cdot\lim\|\mu f_z f f'_z - \bar{\mu} f_z \cdot \pi f \cdot \mu f'_z\| = 0$$

Si en outre toutes les chaines $\{\mu f^n\colon n \in \mathbf{N}\}$ $(f \in F_0)$ sont apériodiques, on peut écrire

$$(W_r^*)\cdot\lim\|\mu f_z f f'_z - \bar{\mu} f_z \cdot \bar{\mu} f'_z\| = 0$$

Vérification. D'après la Remarque 3, il existe deux applications $\mu'\colon F \to M'$ et $\mu''\colon F \to M''$ telle que $\lim\|\mu f_z - \mu' f_z \cdot \mu'' f_z\| = 0$. Prenant une

application ν de $F \times F \times F$ sur la matrice unité e_I et employant la Remarque 3' on a $\lim\|\mu f_z - f_z - \mu' f_z \cdot \mu'' f_z\| = 0$, ceci montre que $\lim\|\bar{\mu} f_z - \mu f_z\| = 0$. En effet, quel que soit ϵ petit on peut trouver $z(\epsilon)$ tel que pour tout $z > z(\epsilon)$ on a

$$\|\mu f_z - \mu' f_z \cdot \mu'' f_z\| < \epsilon \qquad \text{et} \qquad \|\mu f_z \cdot \mu f_z - \mu' f_z \cdot \mu'' f_z\| < \epsilon$$

d'où

$$\|\mu f_z \cdot f_z - \mu f_z\| \leqslant \|\mu f_z \cdot f_z - \mu' f_z \cdot \mu'' f_z\| + \|\mu' f_z \cdot \mu'' f_z - \mu f_z\| < 2\epsilon$$

D'autre part on voit par récurrence que

$$\|\mu f_z^{p+1} - \mu f_z^p\| \leqslant \|\mu f_z\| \|\mu f_z^p - \mu f_z^{p-1}\| \leqslant 2\epsilon$$

et en particulier,

$$\|\mu f_z^{kr!+1} - (\mu f_z)^{kr!}\| < 2\epsilon$$

donc en sommant

$$\|\mu f_z^{kr!+1} - \mu f_z\| < \sum_{p=1}^{kr!} \|\mu f_z^{p+1} - \mu f_z^p\| < kr!\,2\epsilon$$

De plus,

$$\|\bar{\mu} f_z - \mu f_z\| \leqslant \|\bar{\mu} f_z - \mu f_z^{kr!+1}\| + \|\mu f_z^{kr!+1} - \mu f_z\|$$

et on sait que si on se donne ϵ' petit on peut trouver $k(\epsilon')$ tel que pour $k > k(\epsilon')$ on aura

$$\|\bar{\mu} f_z - \mu f_z\| \leqslant 2r!\,k\epsilon + \epsilon'$$

On peut donc se donner $\epsilon, \epsilon', \epsilon'', k(\epsilon')$ tels que pour tout $z > z(\epsilon)$ on aura

$$\|\bar{\mu} f_z - \mu f_z\| \leqslant \epsilon'' \text{ par suite } \lim\|\bar{\mu} f_z - \mu f_z\| = 0$$

Il n'y aura donc aucune diminution de généralité à supposer désormais que $\mu' = \bar{\mu}'$ et $\mu'' = \bar{\mu}''$, c'est à dire que $\mu' f \cdot \mu'' f = \bar{\mu} f$ pour tout $f \in F_0$.

Le premier de ces résultats donne

$$\lim\|\mu f_z f f'_z - \bar{\mu} f_z \cdot \mu f \cdot \bar{\mu} f'_z\| = \lim\|\bar{\mu} f_z f f'_z - \bar{\mu} f_z \cdot \mu f \cdot \bar{\mu} f'_z\| = 0$$

Comme

$$\bar{\mu} f_z \cdot \mu f \cdot \bar{\mu} f'_z = \mu' f_z \cdot \nu(f_z, f, f'_z) \cdot \mu'' f'_z$$

où maintenant ν est une application quelconque de $F \times F \times F$ dans M telle que $e_K \cdot \nu(f_z, f, f'_z) = \mu'' f_z \cdot \mu f \cdot \mu' f'_z$, on peut appliquer de nouveau la Remarque 3' qui montre cette fois l'existence d'une application ρ de $F \times F \times F$ dans M telle que $e_K \cdot \rho$ soit une permutation de K et que

$$\lim\|\mu'' f_z \cdot \mu f \cdot \mu' f'_z - e_K \cdot \rho(f_z, f, f'_z)\| = 0$$

D'après l'hypothèse faite plus haut,

$$\mu' f_z \cdot \mu'' f_z = \bar{\mu} f_z \qquad \text{et} \qquad \mu' f'_z \cdot \mu'' f'_z = \bar{\mu} f'_z$$

On en conclut que $\mu'' f_z \cdot \mu f \cdot \mu' f'_z$ est elle-même, pour tout $(f_z, f, f'_z) \in F \times F \times F_0$, une matrice ayant son support contenu dans $K \times K$ et représentant une permutation de cet ensemble.

Puisque les matrices $\mu' f_z$, μf, et $\mu' f'_z$ ont des entrées nonnégatives, ceci entraîne $\mu'' f_z \cdot \mu f \cdot \mu' f'_z = \mu'' f_z \cdot \pi f \cdot \mu' f'_z$ quelque soit l'application $\pi: F \to M$ telle que $\beta\mu f = \beta\pi f$. Par conséquent, sous cette hypothèse $\bar{\mu} f_z \cdot \mu f \cdot \bar{\mu} f'_z = \bar{\mu} f_z \cdot \pi f \cdot \bar{\mu} f'_z$ ce qui achève la vérification de (W_r) puisque le monoïde $\{\beta\mu f: f \in F\}$ est fini.

Supposons maintenant que toutes les chaînes $\{\mu f^n: n \in \mathbf{N}\}$ soient apériodiques, c'est-à-dire que $\bar{\mu} f = \bar{\mu} f^2$ pour tout $f \in F_0$, c'est-à-dire encore (dans les notations de la Remarque 2′) que $I'_j{}^*(f) \subset I''_j{}^*(f)$ pour tout $j \in [1, r]$. La Remarque 1′ montre que l'on peut choisir l'indexage des classes ergodiques des différentes chaînes $\{\mu f^n: n \in \mathbf{N}\}$ $(f \in F_0)$ de telle sorte que $I'_j{}^*(f) \subset I''_j{}^*(f')$ pour tout $f, f' \in F_+$ et $j \in [1, r]$. Ceci entraîne que $\mu'' f_z \cdot \mu' f'_z = e_K$ identiquement quand $f_z, f'_z \in F_+$. La propriété est entièrement vérifiée.

Note: Cet exposé est un développement de l'article "Sur certaines chaînes de Markov non-homogènes" par J. Larisse et M. P. Schützenberger, Publications de l'Institut de Statistique de l'Université de Paris, Vol. XIII, fasc. 1, 1964.

Références

1. C. Chevalley, *Fundamental Concepts of Algebra*, Academic Press, New York, 1956.
2. J. Wolfowitz, Products of indecomposable, aperiodic stochastic matrices, *Proc. Am. Math. Soc.* **14**, 733–737 (1963).
3. J. L. Doob, *Stochastic Processes*, Wiley, 1953.
4. M. Hall, Jr., *The Theory of Groups*, Macmillan, 1959.
5. A. H. Clifford et G. B. Preston, *Algebraic Theory of Semi-Groups*, Vol. 1, Am. Math. Soc., 1961.
6. J. A. Green, On the structure of semi-groups, *Ann. Math.* **54**, 163–172 (1951).
7. J. Hajnal, Weak ergodicity in non-homogeneous Markov chains, *Proc. Cambridge Phil. Soc.* **54**, 233–246 (1958).

Sur Certaines Variétés de Monoïdes Finis

M. P. Schützenberger

Institut Blaise Pascal
Paris, France

Le but de cet exposé est de rassembler un certain nombre d'énoncés de la théorie des monoïdes finis qui semblent pouvoir présenter des applications à l'étude des automates finis et des langages de Kleene.

Nous commencerons par rappeler le résultat suivant de Clifford et de Miller (1956).

Théorème 1. *Soit u un élément idempotent d'un monoïde M et soit*

$$G_u = \{m \in Mu \cap uM : u \in Mm \cap mM\} \tag{1}$$

L'ensemble G_u est un sous groupe de M qui contient tous les sous groupes de M admettant u pour élemént neutre.

Démonstration. Soit $u = u^2 \in M$. Par définition un élément $m \in M$ appartient à G_u si et seulement si il existe $m_1, m_2, m_3, m_4 \in M$ satisfaisant:

$$m = m_1 u = u m_2 \qquad u = m_3 m = m m_4$$

Donc en particulier $u \in G_u$. Les deux premières relations donnent

$$mu = m_1 uu = m_1 u = m \qquad um = uum_2 = um_2 = m$$

Donc u est un élément neutre pour tous les éléments de G_u.

Soit $m' = m'_1 u = u m'_2$ tel que $u = m'_3 m' = m' m'_4$ un autre élément de G_u. On a

$$mm' = mm' u = umm' \qquad m'_3 m_3 mm' = m'_3 um' = m'_3 m' = u$$
$$mm' m'_4 m_4 = mum_4 = mm_4 = u$$

Donc G_u est un sous ensemble stable de M (c'est à dire $G_u G_u \subset G_u$). Enfin, d'après $u^2 = u = m_3 m$ et $m = um$, on voit que $u = um_3 um$ et il n'y a donc pas de perte de généralité à supposer désormais que $um_3 = m_3 u = m_3$.

Considérons le produit mm_3. En utilisant successivement les hypothèses $m_3 = m_3 u$, $u = mm_4$, $m_3 m = u$, $mu = m$, $mm_4 = u$ on obtient:

$$mm_3 = mm_3 u = mm_3 mm_4 = mum_4 = mm_4 = u$$

Nous avons établi que G_u est un sous ensemble stable admettant un élément neutre u et ayant la propriété qu'à tout $m \in G_u$ correspond un élément $m_3 = um_3u$ qui satisfait $u = um_3u.m = mum_3u$.

Ceci montre d'abord que $um_3u \in G_u$ et que l'ensemble G_u muni du produit de M est isomorphe à un groupe puisque chaque élément possède un inverse. Enfin le groupe G_u est maximal car si les éléments m_5 et m_6 de M sont invariant par multiplication par u et satisfont $u = m_5m_6 = m_6m_5$ ils appartiennent à G_u d'après la définition même de cet ensemble. Ceci terminé la démonstration du théorème.

Rappelons maintenant qu'une famille **V** de groupes (monoïdes) est une *pseudo variété de groupes* (*monoïdes*) si elle contient tout sous groupe (sous monoïde) tout groupe (monoïde) quotient, et tout produit direct de deux membres quelconques de ses membres.

Par exemple, les groupes (monoïdes) finis forment une variété de même que les groupes (monoïdes) commutatifs; par contre les groupes cycliques ne forment pas une variété puisque le produit direct de deux groupes cycliques n'est plus nécessairement cyclique. On a

Proposition 1. *Soit* **V** *une variété de groupes et soit* **V′** *la famille de tous les monoïdes finis dont tout les sous groupes appartiennent à* **V**. **V′** *est une pseudo variété de monoïdes que l'on appelara la pseudo variété de monoïdes finis induite par la variété de groupe* **V**.

Démonstration. Soit M un monoïde fini dont tout les sous groupes appartiennent à la variété de group V. Si M' est un sous monoïde de M et G' un sous groupe de M', G' contient un et un seul idempotent u et il résulte immédiatement de (1) que G' est contenu dans $M' \cap G_u$. Donc M' appartient à la variété **V′** de monoïde fini induite par **V**.

De même, si $M_1, M_2 \in \mathbf{V}'$, tout sous groupe de produit direct $M_1 \times M_2$ est le produit direct d'un sous groupe de M_1 et d'un sous groupe de M_2 et par conséquent $M_1 \times M_2 \in \mathbf{V}'$.

Il reste seulement à établir $M' \in V'$ quand $M \in V'$ et quand $M' = \alpha M$ où α est un épimorphisme.

Dans ces conditions soit u' un idempotent de M' et soit $G_{u'}$ le sous groupe maximal de M' qui contient u'. Soit $P = \{m \in M : \alpha m \in G_{u'}\}$ d'après $G'_uG'_u = G'_u \neq \phi$ on a $PP \subset P \neq \phi$.

Considérons un élément $m \in P$ tel que l'ensemble $mP \cap Pm$ ait le plus petit nombre possible d'élément. Cette hypothèse a un sens puisque M est fini. Quelque soit $k > 0$ $m^kP \cap Pm^k = mP \cap Pm$ et en vertu de l'hypothèse de minimalité $m^kP \cap Pm^k = mP \cap Pm$.

De plus comme M est fini l'ensemble $m, m^2, m^3, \ldots, m^k, \ldots$ ne contient qu'un nombre fini de termes, donc $m^{k_1} = k m^{k_1 k'_1}$ pour au moins une paire k_1, k'_1 d'entiers positifs et par consequent toutes les paires k_2, k'_2 où $k_2 \geqslant k_1$ et $k'_2 = k_3 k_1$; donc enfin en prenant $k = k_1 k'_1$ on obtient $m^k = m^{2k}$ et l'on peut supposer désormais que $m = u = u^2$ est un idempotent.

Montrons que $uP \cap Pu = G_u$ est bien un sous groupe de P contenant u. En effet la relation $m \in uP \cap Pu$ signifie que $m = um_1 = m_2 u$ pour au moins une paire $m_1, m_2 \in M$; par conséquent

$$m \in mP \cap Pm = um_1 P \cap Pm_2 u \subset uP \cap Pu$$

ce qui, d'après l'hypothèse de minimalité, entraine $mP \cap Pm = uP \cap Pu$, donc $u \in mP \cap Pm$ puisque $u \in uP \cap Pu$ d'après (1) ceci établit le résultat cherché.

Maintenant la relation $G_u = uG_u = G_u u$ donne $G_u = uG_u u = u(uP \cap Pu)u = uPu$, donc en prenant les images par α et en rappelant que $\alpha P = G'$ on obtient

$$\alpha G_u = \alpha u \,.\, \alpha P \,.\, \alpha u = \alpha u \,.\, G' \,.\, \alpha u = G'$$

et nous avons établi que le sous groupe G' de M' est une image homomorphe du sous groupe G_u de M. Ceci termine la preuve de la Proposition 2.

Il y a évidemment bien des manières d'affaiblir la condition de finitude de M; il est toutefois impossible de se dispenser entièrement d'hypothèses de ce type puisqu'un sous groupe G' d'un monoïde $M' = \alpha M$ peut, pour M infini, être l'image d'un sous ensemble $P \subset M$ ne contenant aucun sous groupe G tel que $\alpha G = G'$. Ceci est illustré par l'exemple où M est un monoïde libre puisque dans ces conditions M n'a qu'un seul sous groupe—à savoir le sous groupe trivial formé par l'élément neutre de M.

On se propose maintenant de définir une opération de composition entre monoïdes. Pour faciliter l'écriture on considère deux monoïdes fixes M_1 et M_2 et l'on désigne par R la famille de tous les ensembles de paires d'éléments $(m_1, m_2) \in M_1 \times M_2$. Etant donnés des éléments quelconques $r = \{(m_{1,i}, m_{2,i}) : i \in I_r\} \in R$; $m_1 \in M_1$ et $m_2 \in M_2$ on définit les éléments $m_1 r$ et $r m_2$ de R par les relations

$$m_1 r = \{(m_1 m_{1,i}, m_{2,i}) : i \in I_r\} \in R$$
$$r m_2 = \{(m_{1,i}, m_{2,i} m_2) : i \in I_r\} \in R$$

Définition 1. *On appelera produit semi direct, booléen $M_1 \circledast M_2$ l'ensemble $M = M_1 \times R \times M_2$ muni de la loi de composition qui associe à tout $m = (m_1, r, m_2)$, $m' = (m'_1, r', m'_2) \in M$ l'élément*

$$mm' = (m_1 m'_1, m_1 r' \cup r m'_2, m_2 m'_2) \in M$$

Il est facile de voir que l'opération $m \times m' \to mm'$ est associative.

En effet, si $m'' = (m_1'', r'', m_2'') \in M$, on a

$$\begin{aligned}(mm')\,m'' &= (m_1 m_1' m_1'', (m_1 m_1')\,r'' \cup (m_1 r' \cup r m_2)\,m_2'', m_2 m_2' m_2'')\\ &= (m_1 m_1' m_1'', m_1 m_1' r'' \cup m_1 r' m_2'' \cup r m_2 m_2'', m_2 m_2' m_2'')\\ &= m(m'\,m'')\end{aligned}$$

De plus M a un élément neutre [à savoir (e_1, ϕ, e_2) où e_1 et e_2 sont des éléments neutres de M_1 et de M_2 et où $\phi \in R$ est l'ensemble vide] et par conséquent M est un monoïde.

Proposition 2. *Soit* **V** *une variété de groupe. Si* M_1 *et* M_2 *appartiennent à la pseudo variété de monoïde finis induite par* **V** *il en est de même de leur produit semi-direct booléen* $M = M_1 \circledast M_2$.

Démonstration. Soit $u = (u_1, r, u_2) \in M$ un idempotent de M et soit G_u le sous groupe maximal de M qui le contient. Il est clair que $u_1 = u_1^2$, $u_2 = u_2^2$, et que l'application qui envoie tout $g = (r_1, r_g, m_2) \in G_u$ sur la paire $(m_1, m_2) \in M_1 \times M_2$ est un homomorphisme γ de G_u dans le produit direct $G_{u_1} \times G_{u_2}$ des sous groupes maximaux $G_{u_1} \in M_1$ et $G_{u_2} \in M_2$. Par construction, le noyeau de γ est l'ensemble N des éléments de M de la forme (u_1, s, u_2) qui appartiennent à G_u. Donc si nous pouvons prouver que N se réduit à $\{u\}$ nous aurons établi que γ est un monomorphisme, c'est à dire que G_u est isomorphe à un sous groupe de $G_{u_1} \times G_{u_2}$. Soit donc $m = (u_1, s, u_2) \in N$. Puisque $m \in G_u$, m possède un inverse $\bar{m}$ (relativement à u) c'est à dire qu'il existe un élément $\bar{m} = u\bar{m} = \bar{m}u$ tel que $u = m\bar{m} = \bar{m}m$. Il est clair que $\bar{m}$ a la forme $\bar{m} = (u_1, \bar{s}, u_2)$ pour un certain $\bar{s} \in R$. Nous avons les relations suivantes:

$$\begin{aligned} r &= u_1 r \cup r u_2 && \text{(d'après } u = u^2\text{)}\\ r &= u_1 \bar{s} \cup s u_2 && \text{(d'après } u = m\bar{m}\text{)}\\ s &= u_1 r \cup u_1 s u_2 \cup u_2 && \text{(d'après } m = umu\text{)}\end{aligned}$$

La première relation montre que $u_1 r \subset r$; par conséquent $u_1 r = u_1 u_1 \bar{s} \cup u_1 s u_2 \subset r$ d'après la seconde relation et, a fortiori $u_1 s u_2 \subset r$. Or la troisième relation s'écrit aussi $s = r \cup u_1 s u_2$ et, par conséquent, on a établi $s = r$, c'est à dire $m = u$ pour tout $m \in N$. Ceci achève la vérification que tous les sous groupes du produit semi direct M appartiennent à **V**.

Afin de rattacher les sonsidérations précédentes à la théorie des langages formels nous considérons maintenant un ensemble fixe X et le monoïde libre X^* engendré par cet ensemble. Les éléments de X^* sont appelés "*mots*" et nous appelerons "*langages formels sur* X" tout sous ensemble de

X^*. Enfin étant donnée une *pseudo* variété $\mathbf{V}'$ de monoïdes finis induites par une variété de group $\mathbf{V}$ nous dirons qu'un langage formel $F \subset X^*$ est un $\mathbf{V}'$-langage si et seulement si il existe un monoïde quotient $M \in V'$ et un homomorphisme $\alpha: X^* \to M$ tel que l'ensemble F soit précisèment égal à l'image inverse $\overset{-1}{\alpha}\alpha F$ de son image αF dans M par α. Formellement,

$$F = \{f' \in X^* : \exists_F f : \alpha f' = \alpha f\}$$

Proposition 3. *Si F_1 et F_2 sont deux $\mathbf{V}'$-langages sur X il en est de même de leur union $F_1 \cup F_2$, du complément relatif $F_1 \backslash F_2$ et du produit $F_1 F_2$*

$$F_1 F_2 = \{ff' \in X^* : f \in F_1, f' \in F_2\}.$$

Démonstration. Soient $\alpha_1: X^* \to M_1$ et $\alpha_2: X^* \to M_2$ tels que $M_1, M_2 \in \mathbf{V}'$ $\overset{-1}{\alpha_1}\alpha_1 F_1 = F_1$; $\overset{-1}{\alpha_1}\alpha_2 F_2 = F_2$. Nous considérerons le produit semi-direct $M = M_1 \oplus M_2$ et nous définissons une application $\alpha: X^* \to M$ en posant $\alpha e = (\alpha_1 e, \{(\alpha_1 e, \alpha_2 e)\}, \alpha_2 e)$ et pour tout $f \in X^*$

$$\alpha f = (\alpha_1 f, \{(\alpha_1 f', \alpha_2 f'') : f', f'' \in X^*; f' f'' = f\}, \alpha_2 f)$$

Il est clair que α est un homomorphisme de X^* sur un certain sous monoïde $\bar{M}$ de M. De plus si $f \in X^*$ on peut savoir en connaissant seulement son image $\alpha f \in \bar{M}$ si $f \in F_1 \cup F_1$ ou $f \in F_1 \backslash F_2$ ou $f \in F_1 F_2$. Donc $\overset{-1}{\alpha}\alpha F = F$ pour $F = F \cup F_1, = F_1 \backslash F_2$ ou $= F_1 F_2$ et la validité l'énoncé résulte de la Proposition 4.

Si la variété de groupe $\mathbf{V}$ est la variété $\mathbf{V}_1$ des groupes triviaux (c'est à dire des groupes réduits à leurs éléments neutres) la famille correspondantes de langage a été étudiée par McNaughton et Trachtenbrot et c'est la plus petite famille fermée par les opérations d'union de complémtement relatif et de produit qui contienne tous les sous ensembles de X. On sait aussi que quand $\mathbf{V}$ contient tous les groupes *abeliens* et que F est un $\mathbf{V}$ langage il en est de même du sous monoïde de X^* engendré par le langage $F' = X^* F \backslash X^* F X X^*$ formé de tous les mots de l'idéal $X^* F$ qui n'ont aucun facteur propre gauche dans $X^* F$. Cette deuxième forme de langage a aussi été étudiée par McNaughton (1960). Nous ne reproduirons par les démonstrations ici et nous terminerons en proposant le problème de prouver (ou de refuter) l'hypothèse selon laquelle les opérations d'union, complémentation produits et la formation de sous monoïdes du type qui vient d'être décrit permet d'engendrer tout les V'_{ab}-langages (à partir des $X' \subset X$) où V_{ab} est la *pseudo* variété de monoïdes finis induite par la variété des groupes abéliens.

BIBLIOGRAPHIE

McNaughton, R. (1960). Symbolic logic and automata, *Wright Air Development Div. Tech. Note* 60–244, Cincinnati, Ohio.

Miller, D. D., et Clifford, A. H. (1956). Regular D-classes in semigroups, *Trans. Am. Math. Soc.* **82**, 270–280.

Petrone, L., et Schützenberger, M. P. *Sur un problème de McNaughton* (à paraître).

On a Family of Sets Related to McNaughton's L-Language

M. P. Schützenberger

Institut Blaise Pascal
Paris, France

I. Introduction

Let F be the free monoid generated by a fixed set X containing at least two elements and let Q_1 be the least family Q of subsets of F that satisfies the conditions (K1) and (K2) below where, as always in this paper, e denotes the neutral element of F.

(K1). $F \in Q$; $\{e\} \in Q$; $X' \in Q$ for any subset X' of X.

(K2). If Q contains A_1 and A_2, it also contains $A_1 \cup A_2$ $A_1 \setminus A_2$ $(=\{f \in F : f \in A_1, f \in A_2\})$ and $A_1 \cdot A_2$ $(=\{ff' \in F : f \in A_1, f' \in A_2\})$.

The study of Q_1 is motivated by the fact (discussed in [5]) that Q_1 is closely related to the family of the subsets of F that can be described within the "L-language" of McNaughton ([3]). The object of the present paper is to verify the *main property* below, which gives for certain subsets of F the possibility of deciding if they belong to Q_1. Finally, as a direct application of Eggan's theory ([1]), we show that for suitable X, Q_1 contains sets of arbitrarily large "star height."

For each positive natural number n, let $M_1(n)$ denote the family of all monoids having at most n elements and admitting only trivial subgroups ([4]); that is, let the monoid M belong to $M_1(n)$ if and only if it has $n' \leqslant n$ elements and if $m^n = m^{n+1}$ for each $m \in M$. Further, for $A \subset F$, let $A \subset Q_1'$ if and only if there exist a monoid $M \in \cup\, M_1(n)$, a subset M' of M and a homomorphism γ of F into M that satisfy $A = \{f \in F : \gamma f \in M'\}$. We have

Main Property

The families Q_1 and Q_1' of subsets of F are identical.

As an illustration, let us consider two disjoint subsets A_1 and A_2 of F and assume that we know three elements f, f', and f'' of F for which both $A_1 \cap \{f' f^n f'' : n \in N\}$ and $A_2 \cap \{f' f^n f'' : n \in N\}$ are infinite sets. Using the

relation $Q_1 \subset Q_1'$, we can conclude that it is impossible to find a set $B \in Q_1$ satisfying $A_1 \subset B$ and $A_2 \subset F \setminus B$. Indeed, according to the definition of Q_1', $B \in Q_1'$ would imply the existence of a finite integer n such that the set $\{f' f^{n'} f'' : n' \in N, n' > n\}$ is entirely contained in B or in $F \setminus B$.

II. Verification of $Q_1 \subset Q_1'$

Since Q_1 is defined as the least family which satisfies (K1) and (K2), $Q_1 \subset Q_1'$ follows instantly from the following two remarks from ([5]), which are reproduced here for the sake of completeness.

Remark 1. Q_1' satisfies condition (K1).

Verification. Let the monoid $M = \{e', x', 0\} \in M_1(3)$ and the map $\gamma : F \to M$ be defined as follows:

$$\gamma e = e' = e'^2 \begin{cases} \text{for each } x \in X', \gamma x = x' = e' x' = x' e' \\ \text{for each } f \in F \setminus (\{e\} \cup X'), \gamma f = 0 = e' 0 = 0 e' = x'^2 = x' 0 \\ \qquad\qquad = 0 x' = 0^2. \end{cases}$$

Thus $F = \gamma^{-1} M$, $X' = \gamma^{-1} x'$, $\{e\} = \gamma^{-1} e'$. It is clear that γ is a homomorphism and Remark 1 is verified.

Remark 2. Q_1' satisfies condition (K2).

Verification. Let for $j = 1, 2$ the homomorphism $\gamma_j : F \to M_j$, the monoid M_j, and the subset M_j' of M_j satisfy $M_j \in M_1(n_j)$ and $A_j = \{f \in F ; \gamma_j f \in M_j'\}$.

We consider the family R of all sets of pairs $(m_1, m_2) \in M_1 \times M_2$ and for $m_1 \in M_1$, $m_2 \in M_2$, $r = \{(m_{1,i}, m_{2,i}) : i \in I_r\} \in R$, we let

$$m_1 r = \{(m_1 m_{1,i}, m_{2,i}) : i \in I_r\} \qquad r m_2 = \{(m_{1,i}, m_{2,i} m_2) : i \in I_r\}$$

Further, denoting by $\bar{M}$ the direct product (of sets) $M_1 \times R \times M_2$, we define the product for any two elements (m_1, r, m_2) and (m_1', r', m_2') of $\bar{M}$ by the formula

$$(m_1, r, m_2)(m_1', r', m_2') = (m_1 m_1', m_1 r' \cup r m_2', m_2 m_2') \in \bar{M}$$

Finally for $f \in F$, we let

$$\gamma f = (\gamma_1 f, \{(\gamma_1 f', \gamma_2 f'') : f', f'' \in F ; f = f' f''\}, \gamma_2 f) \in \bar{M}$$

The verification that we have defined an associative product and a homomorphism γ of F onto a finite monoid $M \subset \bar{M}$ is straightforward and

it is omitted. The same applies to the verification that $A_1 \cup A_2$, $A_1 \setminus A_2$, and $A_1 \cdot A_2$ are images by γ^{-1} of suitable subsets of M. Thus the remark will follow from the fact that any subgroup $G = \{(m_{1,i}, r_i, m_{2,i}) : i \in I_G\}$ of M is isomorphic to a direct product $G_1 \times G_2$, where G_j is a subgroup of M_j $(j = 1, 2)$.

Indeed, by construction, $\{m_{j,i} : i \in I_G\} \subset M_j$ is a homomorphic image of G, hence a group G_j. Let e_j be its neutral element and let N be the intersection of G with the subset $\{(e_1, r, e_2) : r \in R\}$ of $\bar{M}$; N is a normal subgroup of G and G/N is isomorphic to a submonoid of $G_1 \times G_2$.

Therefore, for verifying $M \in \bigcup_{n>0} M_1(n)$, it suffices to show that N reduces to the neutral element $e' (= (e_1, r, e_2))$ of G. To see this, let $g (= (e_1, s, e_2))$ and $g (= (e_1, \bar{s}, e_2))$ be inverse elements of N. The equation $e' = e'^2$ gives $r = e_1 r \cup r e_2$ and the equation $e' = g\bar{g}$ gives $r = e_1 \bar{s} \cup s e_2$. Therefore, $e_1 r = e_1 \bar{s} \cup e_1 s e_2$ and, since $e_1 r \subset r$, we have $e_1 s e_2 \subset r$. However, the equation $g = e' g e'$ gives $s = e_1 r \cup e_1 s e_2 \cup r e_2$; that is, $s = r \cup e_1 s e_2$ and therefore, $s = r$. This shows that $e' = g$, hence that $N = \{e\}'$, and the verification is concluded.

III. Verification of $Q_1' \subset Q_1$

For each positive natural number n let $Q_1(n)$ denote the least family of subsets of F that satisfies the conditions (K1) and (K2) and that contains every set of the form $\gamma^{-1} M'$ if $M' \subset \gamma F$ and if $\gamma : F \to \gamma F$ is a homomorphism of F onto a member of $M_1(n)$. Thus $Q_1(1) = Q_1$, since for $M' \subset \gamma F$ and $\gamma F \in M_1(1)$, we have either $\gamma^{-1} M' = \phi$ or $\gamma^{-1} M' = F$. Thus the relation $Q_1' \subset Q_1$ will follow instantly from Remarks 3, 5, and 6, which show that for each $n > 0$ one has $Q_1(n+1) \subset Q_1(n)$ and, therefore, that $Q_1' = \bigcup_{n>0} Q_1(n)$ is a subfamily of Q_1. The cores of the arguments below are elementary special cases of well-known theorems of Green ([2]) and of Miller and Clifford ([4]) concerning the $\mathscr{D}$-classes and the $\mathscr{H}$-classes of monoids.

To simplify notations, we assume henceforth that $M = \gamma F \in M_1(n+1)$.

Remark 3. To show $\gamma^{-1} M' \in Q_1(n)$ for all subsets M' of M, it suffices to verify the same property for $M' = MmM$, $M' = Mm$, and $M' = mM$, where m is an arbitrary element of M.

Verification. Consider $a_1, a_2, a_3, a_4, b, b' \in M$ and assume that $b = a_1 b' a_2$, $b' = a_3 b$. This implies $b' = a_3 a_1 b' a_2 = (a_3 a_1)^n b' a_2^n$ for all positive n. Since M has only trivial subgroups we can take n so large that $a_2^n = a_2^{n+1}$. Then

$b' = (a_3 a_1)^n b' a_2^n = (a_3 a_1)^n b' a_2^{n+1} = b' a_2$. From this we conclude that $b = a_1 b' a_2 = a_1 b'$. Assume further that $b' = b a_4$. By a symmetric argument we obtain $b' = a_1 b'$ (and $b = b' a_2$), showing that $b = b'$ under this supplementary condition.

For any $m \in M$, let $W_m = \{m' \in M : m \in M \setminus Mm'M\}$ and $H_m = (mM \setminus W_m) \cap (Mm \setminus W_m)$. It is clear that W_m is a finite union of sets having the form $Mm''M$ and that $\gamma^{-1} H_m \in Q_1(n)$ if the same is true for Mm, mM, and W_m. We show that in fact $H_m = \{m\}$. Indeed, let $m' \in H_m$. We must have $m = a_1 m' a_2$ (since $m' \notin W_m$), $m' = a_3 m$, and $m' = m a_4$ for some elements $a_i \in M$. The computations made above show that $m = m'$, and Remark 3 is verified.

Remark 4. If $m \in M$ is such that W_m has two elements or more, then $A = \gamma^{-1} m$ belongs to $Q_1(n)$.

Verification. Let $\beta : M \to \bar{M}$ be a surjection of M onto a set $\bar{M}$ that has the following properties: for each $m' \in W_m$, $\beta m'$ is a distinguished element 0, of $\bar{M}$; the restriction of β to $M \setminus W_m$ is a bijection of this set onto $\bar{M} \setminus \{0\}$. Since $M . W_m . M = W_m$, we can define a structure of monoid on $\bar{M}$ by letting $(\beta m')(\beta m'') = \beta(m' m'')$ if $m' m'' \in M \setminus W_m$ and $= 0$ if $m' m'' \in W_m$. It is clear that $\bar{M}$ has only trivial subgroups and $\bar{M} \in M_1(n)$ follows from the hypothesis that W_m has two elements or more. Since $A = \{f \in F : \beta \gamma f = \beta m\}$ the remark is verified.

Remark 5. If $m \in M$, $M' = MmM$, and $A = \gamma^{-1} M'$, then $A \in Q_1(n)$.

Verification. Since $\gamma e \in M'$ implies $M' = M$ and $A = F$, we can assume $\gamma e \notin M'$. Let $X' = X \cap \gamma^{-1} m$. We have $F . X' . F \subset A$ and $F . X' . F \in Q_1(1)$. Thus, either $\gamma^{-1} m \subset F . X' . F$ and the result is already proved, or there exists at least one $f \subset \gamma^{-1} m \setminus F . X . F$. We consider this last case. The element f admits at least one minimal factor f'' such that $M . \gamma f'' . M = MmM$, that is, $f = g x f' x' g'$ $(g, f', g' \in F; x, x' \in X; f'' = x f' x')$, where letting $m_1 = x$, $m' = f'$, $m_2 = x'$, we have $Mm_1 m' m_2 M = MmM$, $MmM \neq Mm_1 m' M$, $MmM \neq Mm' m_2 M$. Thus A contains $F . X_1 . A' . X_2 . F$, where $X_1 = X \cap \gamma^{-1} m_1$, $A' = \gamma^{-1} m'$, $X_2 = X \cap \gamma^{-1} m_2$, and, since M is finite, it is clear that $A \setminus F . X' . F$ is a finite union of such sets. Therefore, using Remark 4, the result will follow from the verification that W_m contains at least two distinct elements.

To see this, assume for the sake of contradiction that $m_1 m'$ does not belong to $W_{m'}$, that is, assume that $m' = a_1 m_1 m' a_2$ for some $a_1, a_2 \in M$. According to the computations made at the beginning of the verification of

Remark 3, this implies $m' = a_1 m_1 m'$, hence $Mm'm_2 = Ma_1 m_1 m' m_2 M \subset Mm_1 m' m_2 M = MmM$. Since by construction $Mm_1 m' m_2 M \subset Mm' m_2 M$, this relation is excluded by the hypothesis $MmM \neq Mm' m_2 M$. Thus $m_1 m' \subset W_{m'}$, and by a symmetric argument, $m' m_2 \subset W_{m'}$, are proved. This implies $m_1 m' m_2 \subset w_{m'}$. Since it is clear that $m_1 m' m_2 = m_1 m' = m' m_2$ is impossible, the verification is concluded.

Remark 6. If $m \in M$, $M' = Mm$ or $= mM$ and $A = \gamma^{-1} M'$, then $A \subset Q_1(n)$.

Verification. It suffices to consider the case of $M' = Mm$. Moreover, because of Remark 5, we can assume $Mm \neq MmM$, that is $Mm \neq F$ and $m_0 \subset MmM \setminus Mm$ for at least one $m_0 \in M$.

Let $f \in \gamma^{-1} m$. As above, f has a minimal right factor $f'' = xf' \in A$ ($x \in X$, $f' \in F$), that is, letting $m_1 = \gamma x$, $m' = \gamma f'$, $Mm = Mm_1 m'$ and $Mm \neq Mm'$. We have $F.(X \cap \gamma^{-1} m_1) \,.\gamma^{-1} m' \subset A$ and A is a finite union of such sets. As above, we have only to show that W_m contains at least two elements. That $m \in W_{m'}$ follows from the argument developed in the verification of the last remark, and if $m_0 \in W_m$ we conclude that $W_{m'}$ contains m and m_0. If $m_0 \notin W_m$, we have $m \in Mm_0 M$, hence $MmM = Mm_0 M$ (since $m_0 \in MmM$) and therefore also $m_0 \in W_{m'}$. This concludes the verification.

References

1. L. C. Eggan, Transition graphs and the star-height of regular events, *Mich. Math. J.* **10**, 385–397 (1963).
2. J. A. Green, On the structure of semigroups, *Ann. Math.* **54**, 163–172 (1951).
3. R. McNaughton, Symbolic logic and automata, *Wright Air Development Div. Tech. Rept.* 60–244, Cincinnati, Ohio, 1960.
4. D. D. Miller and A. H. Clifford, Regular D-classes in semigroups, *Trans. Am. Math. Soc.* **82**, 270–280 (1956).
5. L. Petrone and M. P. Schützenberger, *Sur un problème de McNaughton* (submitted for publication).
6. M. Teissier, Sur les équivalences régulières dans les demi-groupes, *Comp. Rend.* **232**, 1987–1989 (1951).

C. R. Acad. Sc. Paris, t. 262, p. 1149-1151 (23 mai 1966). Série A

ALGÈBRE. — *Une condition de finitude des monoïdes finiment engendrés.* Note (*) de MM. **Michel Coudrain** et **Marcel Paul Schützenberger**, présentée par M. Henri Villat.

On donne des conditions nécessaires et suffisantes pour qu'un monoïde soit fini, ce qui permet, en particulier, de simplifier certains raisonnements de (1).

Rappelons qu'un *bi-idéal principal* d'un monoïde M est une partie de celui-ci ayant la forme $a\mathrm{M}\,a$, où a est un élément quelconque de M.

Propriété. — *Un monoïde* M *est fini si (et seulement si) il satisfait les trois conditions suivantes :*

(1) M *est engendré par un ensemble fini;*

(2) *Toutes les chaînes strictement décroissantes de bi-idéaux principaux de* M *ont une longueur finie;*

(3) *Tous les sous-groupes de* M *sont finis.*

Deux quelconques de ces conditions ne suffisent pas pour assurer la finitude de M ainsi que le montrent les exemples suivants :

(2) et (3) : M formé d'un élément neutre, e, d'un zéro, o, et d'un ensemble infini M′ tel que $\mathrm{M}'^2 = \{\mathrm{o}\}$;

(1) et (3) : M = le monoïde additif des entiers naturels;

(1) et (2) : M = le groupe additif des entiers rationnels.

Notons (2′) [resp. (2″)] la condition obtenue en remplaçant dans (2) le terme « bi-idéal » par « idéal bilatère » (resp. « idéal à droite ») et disons que M est un *monoïde* de Green si et seulement si [*cf.* (2)] :

(G) *Pour tout* $a,\ b \in \mathrm{M}$, $\{a, b\} \subset \mathrm{M}\,a \cap b\mathrm{M}$ *implique* $\{a, b\} \subset a\,\mathrm{M} \cap \mathrm{M}b$.

On sait que (2) entraîne (G). Comme réciproquement (G) et (2′) entraînent (2), la propriété équivaut à l'assertion que *tout monoïde de Green satisfaisant* (1), (2′) *et* (3) *est fini.* Par contre, le problème reste posé de savoir s'il existe ou non des monoïdes infinis satisfaisant (1), (2″) et (3).

Pour établir la Propriété il suffit de considérer un monoïde *infini* M, image homomorphe par μ du monoïde libre $\mathrm{X}^\star$ engendré par un ensemble *fini* X et, supposant que M satisfait (2), de montrer qu'il contient un sous-groupe infini.

Soit $\overline{\mathrm{X}}^\star$ l'ensemble des mots généralisés, c'est-à-dire des suites $\mathbf{s} = (s_n)_{n \in \mathbf{N}}$ de mots $s_n \in \mathrm{X}^\star$ telles que $s_0 = e$ et $s_{n+1} \in s_n \mathrm{X}$ pour tout $n \in \mathbf{N}$. Si F_n désigne l'ensemble des $f \in \mathrm{X}^n$ tels que $\mu f' \neq \mu f$ pour tout $f' \in \mathrm{X}^\star \setminus \mathrm{X}^n \mathrm{X}^\star$, l'hypothèse que M est infini entraîne qu'il en soit de même de $\mathrm{F} = \bigcup_{0 \leq n} \mathrm{F}_n$. Comme chacun des ensembles X^n est fini et comme F contient les facteurs gauches de tous ses membres, on peut trouver un élément $\mathbf{s}$ de $\overline{\mathrm{X}}^\star$ pour lequel $\{s_n\}_{n \in \mathbf{N}}$ soit contenu dans F, ce que nous noterons $\mathbf{s} \in \overline{\mathrm{F}}$. Soit τs le

translaté de $\mathbf{s}$, c'est-à-dire le mot généralisé $\mathbf{s}'$ tel qu'on ait identiquement $\mathbf{s}_{1+n} = \mathbf{s}_1 \mathbf{s}'_n$. Puisque F contient tous les facteurs droits de chacun de ses membres, on a encore $\tau\mathbf{s} \in \mathrm{F}$.

Désignons maintenant par K l'ensemble des suites $\mathbf{k} = (k_n)_{n\in\mathbf{N}}$ de mots de X^* tels qu'on ait $k_1 \in \mathrm{X}$ et, pour tout $n > 0$, $k_{n+1} \in \mathrm{X}^* \setminus \mathrm{X}^{c_1}\mathrm{X}^*$ où $c_1 = 1 + \mathbf{Card}\,\mathrm{X}$ et inductivement, $c_{n+1} = c_n(1 + (\mathbf{Card}\,\mathrm{X})^{c_n})$. A une telle suite $\mathbf{k}$ nous attachons une autre suite $\tilde{\mathbf{k}} = (\tilde{k}_n)_{n\in\mathbf{N}}$ en posant $\tilde{k}_0 = e$, $\tilde{k}_1 = k_1$ et, inductivement, $\tilde{k}_{n+1} = \tilde{k}_n k_{n+1} \tilde{k}_n$.

Si $\mathbf{s} \in \overline{\mathrm{X}}^*$ nous écrivons $\mathbf{s} \in k_n \overline{\mathrm{X}}^*$ si $k_n = s_{n'}$ pour l'un des mots $s_{n'}$ de $\mathbf{s}$ et $\mathbf{s} = \tilde{\mathbf{k}}$ si $\mathbf{s} \in \tilde{k}_n \overline{\mathrm{X}}^*$ pour tout $n \in \mathbf{N}$. Nous montrons qu'il existe au moins un $\mathbf{k} \in \mathrm{K}$ tel que $\tilde{\mathbf{k}} \in \overline{\mathrm{F}}$.

Pour cela observons d'abord que, d'après la définition de c_{n+1}, tout $f \in \mathrm{X}^{c_{n+1}}$ factorise en un produit de $1 + (\mathbf{Card}\,\mathrm{X})^{c_n}$ mots de X^{c_n} et que, par conséquent, deux au moins de ces mots sont identiques. Donc $f = f'gg'gf''$, où f', $f'' \in \mathrm{X}^*$, $g \in \mathrm{X}^c$, $g' \in \mathrm{X}^* \setminus \mathrm{X}^{c_{n+1}-2c_n}\mathrm{X}^*$. Par induction sur n, on en déduit :

Quel que soit le mot, $f \in \mathrm{X}^{c_{n+1}}\mathrm{X}^*$ *on peut trouver au moins une suite* $\mathbf{k} \in \mathrm{K}$ *telle que* $\tilde{k}_{n+1}$ *soit un facteur de* f.

Puisque $\overline{\mathrm{F}}$ est non vide et fermée par translation, ceci assure qu'à tout $n \in \mathbf{N}$ correspondent au moins un $\mathbf{k}^{(n)} \in \mathrm{K}$ et une suite $\mathbf{s}^{(n)} \in \overline{\mathrm{F}}$ tels que $\mathbf{s}^{(n)} \in \tilde{k}_n^{(n)} \overline{\mathrm{X}}^*$. Comme chacun des ensembles $\{\tilde{k}_n : \mathbf{k} \in \mathrm{K}\}$ est fini, d'après la définition même de K, on peut donc trouver un $\mathbf{k} \in \mathrm{K}$ tel que pour chaque $n \in \mathbf{N}$ il existe au moins une suite $\mathbf{s}^{(n)} \in \overline{\mathrm{F}}$ satisfaisant $\mathbf{s}^{(n)} \in \tilde{k}_n \overline{\mathrm{X}}^*$ et puisque la famille $\{\mathbf{s}^{(n)}\}_{n\in\mathbf{N}} \subset \overline{\mathrm{F}}$ converge en un sens évident, la suite $\tilde{\mathbf{k}} = \lim_{n\to\infty} \mathbf{s}^{(n)}$ appartient encore à $\overline{\mathrm{F}}$.

Considérons maintenant les bi-idéaux principaux $\mathrm{B}_n = \mu\tilde{k}_n . \mathrm{M} . \mu\tilde{k}_n$ de M. Par construction on a identiquement $\mathrm{B}_{n+1} \subset \mathrm{B}_n$. La condition (2), affirme l'existence d'un entier naturel q tel que pour tout $n > q$ on ait $\mathrm{B}_q = \mathrm{B}_n$, donc en particulier $\mu\tilde{k}_{q+1} . \mu\tilde{k}_{q+1} \in \mathrm{B}_n$, c'est-à-dire, enfin,

$$\mu\tilde{k}_{q+1} . \mu\tilde{k}_{q+1} = \mu\tilde{k}_n . m_n . \mu\tilde{k}_n$$

pour au moins un $m_n \in \mathrm{M}$. Il en résulte que

$$\mu\tilde{k}_{q+1} \in \mu\tilde{k}_n . \mathrm{M} \cap \mathrm{M} . \mu\tilde{k}_n$$

et comme $\mu\tilde{k}_n \in \mu k_{q+1} . \mathrm{M} \cap \mathrm{M} . \mu\tilde{k}_{q+1}$ de par la définition même des $\tilde{k}_{n'}$ on a vérifié que tous les $\mu\tilde{k}_n (n > q)$ appartiennent à la même $\mathcal{J}$-classe H de M qui est donc infinie puisque $\mathrm{H} \in \mu\mathrm{F} . \mathrm{M}$ étant un monoïde de Green, ceci suffit pour prouver qu'il possède un sous-groupe infini [*cf.* (2), (3)]. Plus directement, la relation

$$\mu\tilde{k}_{q+1} = \mu\tilde{k}_{q+1} . m_{q+1} . \mu\tilde{k}_{q+1}$$

montre que $u = \mu\tilde{k}_{q+1}.m_{q+1}$ est un idempotent appartenant à la même $\mathcal{D}$-classe que $\mu\tilde{k}_{q+1}$ et la $\mathcal{H}$-classe de u est donc un sous-groupe équipotent avec H, ce qui achève la vérification de la propriété.

Remarque. — La suite $(c_n)_{n\in\mathbf{N}}$ utilisée ici n'est pas la meilleure possible. Par exemple, dans le cas où **Card** X = 2, on peut prendre $c_2 = 13$ (et non 27 comme plus haut).

(*) Séance du 16 mai 1966.

(1) J. A. Green et D. Rees, *Proc. Camb. Phil. Soc.*, 48, 1952, p. 35-40.
(2) J. A. Green, *Ann. Math.*, 54, 1951, p. 163 172.
(3) D. D. Miller et A. H. Clifford, *Trans. Amer. Math. Soc.*, 82, 1956, p. 270-280

(*Institut de Programmation*, 23, *rue du Maroc*, *Paris*, 19e.)

C. R. Acad. Sc. Paris, t. 263 (7 novembre 1966). Série A — 659

ALGÈBRE. — *Sur les produits semi-directs droits de monoïdes.* Note (*) de MM. **Maurice Nivat** et **Marcel Paul Schützenberger**, présentée par M. Henri Villat.

On précise deux propriétés des produits directs droits de monoïdes utilisées dans (1).

Dans cette Note, C désigne un produit *semi-direct droit* fixe de deux monoïdes A et B, c'est-à-dire que C est isomorphe à l'ensemble $B\times A$ muni de la loi de composition $(b, a)(b', a') = (b\zeta^a b', aa')$, où ${}^a b$ désigne une application $A\times B \to B$ satisfaisant les identités ${}^e A\, b = b$; ${}^{a'}({}^a b) = {}^{a'a} b$; ${}^a e_B = e_B$; ${}^a(bb') = {}^a b\zeta^a b'$. Pour $\mathfrak{X} = \mathcal{H}$, $\mathcal{R}$, $\mathcal{L}$ ou $\mathcal{D}$, on note $\mathfrak{X}(m)$ la $\mathfrak{X}$-classe d'un élément m (2).

Propriété 1. — *Tout sous-groupe maximal* $\mathcal{H}(w)$ *de* C *est extension d'un sous-groupe de* B *par un sous-groupe de* A.

Preuve. — Soit $w = (\rho, u)$ l'idempotent de $\mathcal{H}(w)$. La relation $w = w^2$ donne $\rho = \rho.{}^u\rho$ et $u = u^2$, ${}^u\rho = {}^u\rho.{}^u\rho$ et en posant $w' = ({}^u\rho, u)$ on trouve $w' = w'^2 = w'w$; $w = ww'$. Cela montre que $w' \in \mathcal{L}(w)$ et que, par conséquent, les sous-groupes $\mathcal{H}(w)$ et $\mathcal{H}(w')$ sont isomorphes. On pourra donc supposer désormais que $w = w'$, c'est-à-dire que $\rho = \rho^2 = {}^u\rho$.

Pour chaque $a \in A$, soit $K'_a = \{b \in B : (b, a) \in \mathcal{H}(w)\}$ et soit $H' = \{a \in A : K'_a \neq \emptyset\}$. Prenant un élément $c = (b, a) \in \mathcal{H}(w)$ et son inverse $c = (\bar b, \bar a)$ dans $\mathcal{H}(w)$, les relations $c = wc = cw$ et $w = cc = \bar c c$ donnent d'abord $a = ua = au$ et $u = a\bar a = \bar a a$, ce qui montre que H′ est un sous-groupe de $\mathcal{H}(u)$. La relation $b = \rho\, {}^u b$ donne ${}^u b = {}^u\rho.{}^{u^2} b = \rho.{}^u b = b$ et les relations $b = \rho.{}^a b$; $\rho = b.{}^a\bar b$ établissent $b \in \mathcal{R}(\rho)$. Enfin, la relation $\rho = \bar b.{}^{\bar a} b$ implique ${}^a\rho = {}^a\bar b.{}^{a\bar a} b = {}^a\bar b.b$ et, comme $b = b.{}^a\rho$ d'après $c = cw$, on conclut que ${}^a\rho \in \mathcal{L}(b)$, donc ${}^a\rho \in \mathcal{D}(\rho)$ et H′ est donc un sous-groupe de $H = \{a \in \mathcal{H}(u) : {}^a\rho \in \mathcal{D}(\rho)\}$. De même,

$$K'_a \subseteq K_a = \{b \in B : b = {}^u b;\ b \in \mathcal{R}(\rho) \cap \mathcal{L}({}^a\rho)\}$$

et, en particulier, K'_u est contenu dans le sous-groupe K_u de $\mathcal{H}(\rho)$.

Choisissons pour chaque $a \in H$ un élément $b_a \in K_a$. La correspondance associant à chaque paire $(k, a) \in K_u \times H$ l'élément $k.b_a \in \mathcal{R}(\rho) \cap \mathcal{L}({}^a\rho)$ est une surjection $K_u \times H \to U\{K_a : a \in H\}$. Comme ${}^{a'} b_a \in \mathcal{R}({}^{a'}\rho) \cap \mathcal{L}({}^{a'a}\rho)$ identiquement et comme chaque ensemble $\mathcal{R}({}^a\rho) \cap \mathcal{L}(\rho)$ contient un et un seul élément $\bar b_a$ tel que $b_a.\bar b_a = \rho$, l'ensemble $K_u \times H$ muni de la loi de composition $(k, a)(k', a') = (kb_a.{}^a k'.{}^a b_{a'}.\bar b_{a'a}, aa')$ est un groupe d'élément neutre (ρ, u) qui est une extension de K_u par H et qui est isomorphe à la partie $G = \{(b, a) : b \in K_a;\ a \in H\}$ de C. Par construction, $\mathcal{H}(w)$ est contenu dans G et, par conséquent, $\mathcal{H}(w) = G$.

660 — Série A C. R. Acad. Sc. Paris, t. 263 (7 novembre 1966).

La propriété est vérifiée. Disons maintenant qu'un monoïde M est un $\mathcal{R}_1$ (resp. $\mathcal{R}_0$) monoïde si aucune de ses $\mathcal{R}$-classes régulières ne contient plus d'un seul idempotent (resp. élément), c'est-à-dire si pour tout $p, q \in M$ les relations

$$(1) \qquad p = p^2 = qp; \qquad q = q^2 = pq \quad (\text{resp. } p = pqp;\ q = qpq)$$

impliquent

$$(2) \qquad p = pq, \quad \text{donc} \quad p = q \quad (\text{resp. donc } p = p^2 = pq;\ q = q^2 = qp).$$

Propriété 2. — *Si* A *et* B *sont des* $\mathcal{R}_1$ (resp. $\mathcal{R}_0$) monoïdes, *il en est de même de* C.

Preuve. — Supposons que les éléments $p = (b, a)$ et $q = (y, x)$ de C satisfont (1). Les éléments a et x de A satisfont les mêmes relations, donc les relations (2) puisque A est un $\mathcal{R}_1$ (resp. $\mathcal{R}_0$) monoïde. De plus, $b = b.^a b = y.^x b$; $y = y.^x y = b.^a y$ (resp. $b = b.^a y.^{ax} b$; $y = y.^x b.^{xa} y$). Compte tenu de $a = ax = a^2$, cela entraîne que $^a b$ et $^a y$ satisfassent (1), donc (2) puisque B est un $\mathcal{R}_1$ (resp. $\mathcal{R}_0$) monoïde. Par conséquent, $b = b.^a y$ et l'on a bien

$$p = (b, a) = (b, {}^a y, ax) = (b, a)(y, x) = pq,$$

ce qui achève la vérification.

Remarque. — *Soit* M *un monoïde dont tous les éléments sont d'ordre fini. Si* M *est un* $\mathcal{R}_1$ *(resp.* $\mathcal{R}_0$*) monoïde il en est de même de chaque monoïde qui le divise (c'est-à-dire qui est image homomorphe d'une partie stable de* M).

Preuve. — Il suffit de vérifier que si les parties non vides P et Q de M satisfont $P^2 \cup QP \subset P$; $Q^2 \cup PQ \subset Q$ (resp. $PQP \subset P$; $QPQ \subset Q$), on peut trouver $p \in P$ et $q \in Q$ satisfaisant (1).

Prenons $p' \in P$ et $q'' \in Q$ quelconques. Comme tous les éléments de M sont d'ordre fini on peut déterminer des entiers positifs n'', n' et n et des éléments q', $q \in Q$ et $p \in P$ par les conditions

$$q''^{n''} = q' = q'^2; \qquad (q'p')^{n'} = p = p^2;$$
$$(pq')^n = q = q^2 \quad (\text{resp. } p = p'(q''p')^n;\ q = q''(p'q'')^n;\ pqp = p'(q''p')^{3n+2} = p)$$

et l'on peut vérifier facilement que

$$p = qp; \qquad q = pq \quad (\text{resp. } q = qpq).$$

(*) Séance du 2 novembre 1966.

(1) K. Krohn et J. Rhodes, *Trans. Amer. Math. Soc.*, 116, 1965, p. 450-464.

(2) A. H. Clifford et G. R. Preston, *The algebraic theory of semi-groups*, 1; Math. Survey n° 7, American Math. Soc., Providence, R. I., 1962.

(*Institut de Programmation, 23, rue du Maroc, Paris, 19e.*)

Reprinted from INFORMATION AND CONTROL, Volume 9, No. 1, February 1966

INFORMATION AND CONTROL **9**, 23–25 (1966)

On a Question of Eggan

F. DEJEAN AND M. P. SCHÜTZENBERGER

Laboratoire de Cacul Numérique, 23, Rue du Maroc, Paris 19e, France

An elementary answer is given to a question raised by Eggan

In (Eggan, 1963), it is asked among other questions whether a free monoid X^* generated by a set X consisting of two distinct elements x and y contains subsets of arbitrary star height. McNaughton (unpublished Lecture Notes M.I.T., 1963–1964) has proved, as an application of very powerful and general methods, that it is so. The present note is devoted to the following more elementary example which answers directly Eggan's question.

EXAMPLE. *Let q be any fixed positive natural number and let γ be a homomorphism of X^* into the additive group $\{0, 1, \cdots, 2^q - 1\}$ of the integers modulo 2^q that satisfies $\gamma x = -\gamma y = 1$. The set*

$$\gamma^{-1}0 \ (= \{f \in X^* : \gamma f = 0\})$$

has star height q.

It is clear that $\gamma^{-1}0$ is a submonoid of X^* that is freely generated by $K = (\gamma^{-1}0 \cap XX^*) \setminus (\gamma^{-1}0 \cap XX^*)^2$ $(= \{f \in XX^* : \gamma f = 0;\ f \notin (\gamma^{-1}0 \cap XX^*)XX^*\})$. For $q = 1$, one has $K = X^2$, $\gamma^{-1}0 (= K^*) = (X^2)^*$ and the example is trivial. Thus we can assume henceforth that $q > 1$. For each natural number m we set:

$$\bar{L}_m = \{f \in XX^* : \gamma f = \pm 2^{m+1}\};$$

$$L_m = (\bar{L}_m \cap xX^*) \setminus (\bar{L}_m XX^* \cup KXX^*);$$

$$L_m' = (\bar{L}_m \cap yX^*) \setminus (\bar{L}_m XX^* \cup KXX^*);$$

$$K_m' = K \setminus \bar{L}_m XX^*.$$

Thus, e.g., $L_0 = \{x^2\}$; $L_0' = \{y^2\}$; $K_0' = \{xy \cup yx\}$; $L_1 = x^2(xy \cup yx)^*x^2$; $L_1' = y^2(xy \cup yx)^*y^2$; $K_1' = K_0' \cup x^2(xy \cup yx)^*y^2 \cup y^2(xy \cup yx)^*x^2$; $\cdots \bar{L}_{q-1} = \gamma^{-1}0 \cap XX^*$; $K_{q-1}' = K$.

Let P_m denote any of the sets L_m, L_m' or $K_m' \setminus K_{m-1}'$ where $m \in [1, q-2]$ and let $f \in P_m$. Considering the left factor f_1 (resp. $f_1 f_2$) of minimal degree (or "length") (resp. of maximal degree) of f that satisfies

γf_1 (resp. $\gamma f_1 f_2$) $= \pm 2^m$ shows that f has one and only one factorization of the form $f = f_1 f_2 f_3$ where, on the one hand, $f_2 \in K'^*_{m-1}$ and on the other hand:
if $P_m = L_m$ (resp. $L_m{}'$), both f_1 and f_3 belong to L_{m-1} (resp. to L'_{m-1});
if $P_m = K_m{}' \setminus K'_{m-1}$, either $f_1 \in L_{m-1}$ and $f_3 \in L'_{m-1}$ or $f_1 \in L'_{m-1}$ and $f_3 \in L_{m-1}$.
Accordingly, one has the recurrence relations:

$$L_m = L_{m-1}K'^*_{m-1}L_{m-1}\,; \qquad L_m{}' = L'_{m-1}K'^*_{m-1}L'_{m-1}\,;$$

$$K_m{}' = K'_{m-1} \cup L_{m-1}K'^*_{m-1}L'_{m-1} \cup L'_{m-1}K'^*_{m-1}L_{m-1}$$

which show that P_m has star height at most m. Thus $K = K'_{q-1}$ has star height at most $q - 1$.

This concludes the verification that $\gamma^{-1}0 = K^*$ has star height at most q and we proceed to the verification that $\gamma^{-1}0$ has star height at least q.

Consider for each natural number $n > 1$ the sequence of words $w_{0,n}$, $w_{1,n}$, $w_{2,n}$, $\cdots$, $w_{q-1,n} \in \gamma^{-1}0$ defined recursively by the equations:

$$w_{0,n} = xy;\ w_{1,n} = x^2(xy)^n y^2 (xy)^n;\ \cdots$$

$$w_{k,n} = x^{2^k}(w_{k-1,n})^n y^{2^k}(w_{k-1,n})^n;\ \cdots$$

$$w_{q-1,n} = x^{2^{q-1}}(w_{q-2,n})^n y^{2^{q-1}}(w_{q-2,n})^n.$$

For $k = 0, 1, \cdots, q - 1$, let $\mathfrak{W}_k$ denote the family of all subsets F of X^* of minimal star height that satisfy the following two conditions:
(γ). $\gamma f = \gamma f'$ *for any two* $f, f' \in F$.
(ω_k). *There exist infinitely many values of* n *such that* $(w_{k,n})^n$ *is a factor of at least one word of* F.

If h_k is the common value of the star height of the members of $\mathfrak{W}_k$, it is clear that

$$0 < h_0 \leqq h_1 \leqq \cdots \leqq h_{q-1} \leqq q$$

the first (resp. last) of these inequalities resulting trivially from the fact that any member of $\mathfrak{W}_0$ contains an infinity of words (resp. that $\gamma^{-1}0$ itself satisfies (γ) and (ω_{q-1})). Thus, to prove that $\gamma^{-1}0$ has exactly star height q we have only to show that $h_{k-1} < h_k$ for $k = 1, 2, \cdots, q - 1$. To do this, consider any $F \in \mathfrak{W}_k$. By definition, the hypothesis that F has star height at most h_k is equivalent to the hypothesis that F is the union of a finite number of sets F_j each of which is a finite product of the form $A_1 A_2{}^* A_3 A_4{}^* \cdots A_{2i'-1}A^*_{2i'} \cdots A_{2m-1}A^*_{2m}$ where all the A_i's ($i = 1, 2, \cdots, 2m$) are subsets of X^* having star height

at most $h_k - 1$ (A_{2m} may be empty). The hypothesis that F satisfies (γ) and (ω_k) implies that all the F_j's satisfy (γ) and that at least one of them satisfies (ω_k). Thus we can assume henceforth that F itself is the finite product $A_1A_2^* \cdots A_{2m-1}A_{2m}^*$. Now for each $i \in [1, 2m]$, there exist at least two words $f_1, f_2 \in X^*$ such that $f_1ff_2 \in F$ for all $f \in A_i$ (or, even, $\in A_i^*$ when i is even). Thus the hypothesis that F satisfies (γ) implies that each of the A_i's satisfies the same condition and in fact, since any submonoid of X^* contains the neutral element of X^*, we know that $A_i \subset \gamma^{-1}0$ when i is even. Owing to the hypothesis that F has minimal star height, this remark implies in turn that none of the sets A_i $(i \in [1, 2m])$ satisfies (ω_k).

However, since X is finite and since F has finite star height, Kleene's theorem asserts the existence of a homomorphism μ of X^* into a finite monoid M and of a subset M' of M such that $F = \{f \in X^* : \mu f \in M'\}$. Because of the finiteness of M, there exists a natural number p such that $u^{p'} = u^{p'+p}$ for all $p' \geqq p$ and all $u \in M$, and accordingly, the hypothesis that F satisfies (ω_k) implies here the formally stronger condition that there exist infinitely many values of n such that for infinitely many values of n', $(w_{k,n})^{n'}$ is a factor of at least one word of F. Since none of the A_i's satisfies (ω_k), this shows that at least one of the submonoids $A_{2i'}^*$ $(i' = 1, 2, \cdots, m)$, say $A_{2i_1}^*$, satisfies (ω_k). From this remark let us deduce that A_{2i_1} satisfies (ω_{k-1}) (which, together with the fact that $A_{2i_1} \subset \gamma^{-1}0$ has star height at most $h_k - 1$, will show that $h_k - 1 \geqq h_{k-1}$).

To see this, write $(w_{k,n})^2$ in the form $z_1w_1z_2w_2z_3w_3z_4w_4$ where $w_i = (w_{k-1,n})^n$ for $i = 1, 2, 3, 4$, and $z_i = x^{2^k}$ or y^{2^k} depending upon $i = 1, 3$ or $2, 4$. Taking into account that γf (resp. $-\gamma f$) is contained in $\{0, 1, \cdots, 2^k - 1\}$ for any left (resp. right) factor f of $(w_{k-1,n})^n$, direct examination shows that any factor $a \in K$ of $(w_{k,n})^2$ which is not a factor of one of the w_i's $(i = 1, 2, 3, 4)$ has the form $z_i'w_iz_{i+1}''$ where $i = 1, 2, 3$, $\gamma z_i' = -\gamma z_{i+1}''$ and where z_i' (resp. z_{i+1}'') is a nonempty right (resp. left) factor of z_i (resp. of z_{i+1}). Since $A_{2i_1} \subset \gamma^{-1}0 = K^*$, it follows that for infinitely many values of n, A_{2i_1} contains at least one word admitting a factor of the form $z_i'(w_{k-1,n})^nz_{i+1}''$. The verification that $\gamma^{-1}0$ has exactly star height q is concluded.

RECEIVED: March 30, 1965

REFERENCE

EGGAN, L. C. (1963), Transition graphs and the star height of regular events. *Michigan Math. J.* **10**, 385–395.

Reprinted from JOURNAL OF COMBINATORIAL THEORY Vol. 1, No. 4, December 1966
All Rights Reserved by Academic Press, New York and London *Printed in Italy*

On a Question Concerning Certain Free Submonoids*

M. P. SCHÜTZENBERGER

Faculté des Sciences,
La Sorbonne, Paris, France

Communicated by S. M. Ulam

ABSTRACT

A negative answer is given to a question of Gilbert and Moore concerning the existence of certain type of free submonoids of a free monoid.

Let X^* denote the free monoid (with neutral element e) generated by a fixed set $X \neq \emptyset$ and, for $F \subset X^*$, let F^* denote the submonoid of X^* generated by F. We intend to verify the following property which answers negatively a question raised by Gilbert and Moore in [2, p. 966, line 28] (see [3] for a more complete discussion of this issue).

PROPERTY. *Let A be a subset of X^* that satisfies the following three conditions*:

$U_r(d)$. *There exists a natural number d such that if $a \in A^d$ and $a_1, a_1' \in A$, one has $a_1 a X^* \cap a_1' A^* \neq \emptyset$ only if $a_1 = a_1'$.*

$N''(d)$. *A is maximal among the subsets of X^* that satisfy $U_r(d)$.*

F''. *There is no infinite sequence $a_1, a_2, \ldots, a_n, \ldots$ of elements of A such that each term is a proper left factor of the next one and for each $f \in XX^*$ there exists a natural number m such that $S^m X^* \cap A = \emptyset$ where $S = \{f' \in XX^* : f \in X^* f'\}$.*

* This research was supported in part by the Air Force Office of Scientific Research [AF 61(052)–945].

Then, no $a \in A$ is a proper left factor of another element of A; i.e., A satisfies $\mathbf{U}_r(0)$.

Let $a_1, a_2, \ldots, a_m, a_1', \ldots, a'_{m'} \in A$ be such that $a_1 a_2 \ldots a_m = a_1' a_2' \ldots a'_{m'}$. Multiplying on the right by any $a \in A^d$ and using repeatedly $\mathbf{U}_r(d)$ shows that $a_1 = a_1'$, $a_2 = a_2'$, ..., $m = m'$ and $a_m = a'_{m'}$. Thus $\mathbf{U}_r(d)$ implies that A freely generates A^*; i.e., that A is an "encoding" in the terminology of [2]. For $d = 0$, the condition becomes $a_1 X^* \cap a_1' A^* \neq \emptyset$ only if $a_1 = a_1'$ since $A^0 = \{e\}$, as usual. Because $e \in A^*$, it is equivalent to the hypothesis that A has the so called "prefix property," i.e., that for all $a_1, a_1' \in A$ one has $a_1' \in a_1 X^*$ only if $a_1 = a_1'$. If there exists a natural number n such that $A \cap X^n X^* = \emptyset$, $\mathbf{U}_r(d)$ becomes equivalent to the "finite delay property" of [2]; if, further, $X = \{x, y\}$, $\mathbf{F}''$ is trivially satisfied and $\mathbf{N}''(d)$ is just another way of expressing the condition (9) of [2], that is,

$$1 = \sum_{m>0} 2^{-m} \cdot Card(A \cap X^m).$$

Thus, in this set-up we can state that *no encoding satisfying* (9) *has the finite delay property without having the prefix property*. However, for positive d, the set $A_d = \{x\} \cup (x^d X^* \setminus X^* X x^d X^*)$ satifies $\mathbf{U}_r(d)$ and $\mathbf{N}''(d)$ but not $\mathbf{U}_r(d-1)$ nor $\mathbf{F}''$. The set $\{x, xyx\}$ satisfies $\mathbf{U}_r(1)$ and $\mathbf{F}''$ but not $\mathbf{U}_r(0)$ nor $\mathbf{N}''(1)$. The set $\{x, xy, yy\}$ does not satisfy $\mathbf{U}_r(d)$ for any finite d but it satisfies $\mathbf{F}''$ and it is maximal among the sets which freely generate a submonoid of X^*. Finally, letting F denote the set of all left factors of the infinite sequence $xyx^2y^2x^3y^3 \ldots x^n y^n \ldots$, the set $FX \setminus F$ satisfies $\mathbf{U}_r(0)$, $\mathbf{N}''(0)$ and $\mathbf{F}''$.

VERIFICATION OF THE PROPERTY. We assume henceforth that A is a non-empty subset of X^* that satisfies $\mathbf{U}_r(d)$, $\mathbf{N}''(d)$, and $\mathbf{F}''$.

REMARK 1. Consider the two sets:

P = the set of all $g \in X^*$ such that for each $f' \in X^*$ one has $A^* g f' \cap A^* \neq \emptyset$ only if $g f' \in A^*$;

P' = the set of all $g' \in X^*$ such that $g' f' X^* \cap A^* \neq \emptyset$ for each $f' \in X^*$.

One has $A^d \subset P = PX^* = P'$.

PROOF. Let $g \in A^d$, $a \in A^*$, and $f' \in X^*$ satisfy $agf' \in A^*$ and show that it implies $gf' \in A^*$. Indeed, a, $agf' \in A^*$ imply $a = a_1 a_2 \ldots a_m$;

$agf' = a_1'a_2' \ldots a'_{m'}$ where $a_1a_2, \ldots, a_m, a_1', \ldots, a'_{m'} \in A$; since $g \in A^d$, the relation $a_1a_2 \ldots a_mgf' = a_1'a_2' \ldots a'_{m'}$ gives successively $a_1 = a_1'$, $a_2 = a_2', \ldots, a_m = a_{m'}$ by repeated application of $\mathbf{U}_r(d)$. Thus $gf' = a'_{m+1}a'_{m+2} \ldots a'_{m'} \in A^*$ and $A^d \subset P$ is proved. The fact that $P = PX^*$ follows instantly from the very definition of P because for $g \in P$, $a \in A^*$, and $f' = f_1f'' \in X^*$ the relations $agf' \in A^*$ and $gf' \in A^*$ are equivalent, respectively, to $ag_1f'' \in A^*$ and $g_1f'' \in A^*$, where $g_1 = gf_1'$.

Keeping the same notations, assume that $P' \neq \emptyset$ and $g' \in P'$. It implies the existence of at least one $g'' \in X^*$ such that $g'g'' \in A^*$ and, for each $f' \in X^*$, of at least one $f'' \in X^*$ such that $g'g''gf'f'' \in A^*$; however, because of $g \in P$ and $g'g'' \in A^*$, this last relation implies $gf'f'' \in A^*$ and we have proved $P \subset P'$ (under the hypothesis $P' \neq \emptyset$). Assume now that $a \in A$ and $f' \in X^*$ satisfy $ag'f' \in A^*$. Because of $g \in P \subset P'$ we can find $h \in X^*$ such that $gh \in A^*$ and, because of $P = PX^*$ we know that $gh \in P$. Because of $g' \in P'$ we can find $h' \in X^*$ such that $g'f'ghh' \in A^*$. Thus $ag'f'ghh' \in A^*$, where $ag'f' \in A^*$ and $gh \in P$, from which we conclude that, in fact, $ghh' \in A^*$. Bringing together these results we see that $A^*g'f' \cap A^* \neq \emptyset$ (since $ag'f' \in A^*$) and $g'f'A^* \cap A^* \neq \emptyset$ (since $g'f'ghh' \in A^*$). Owing to the fact that A freely generates A^*, it is known [1] that these two relations imply $g'f' \in A^*$, and $P' = P$ is proved under the hypothesis $P' \neq \emptyset$.

To end the proof, we assume that A satisfies $\mathbf{U}_r(d)$ only and we show that if $A^d \not\subset P'$ we can find an element $u \in A^dX^*$ such that $B = A \cup \{u\} \neq A$ satisfies $\mathbf{U}_r(d)$ in contradiction with $\mathbf{N}''(d)$.

Let $u \in A^dX^*$ be such that $uX^* \cap A^* = \emptyset$; since $u = au'$ for $a \in A^*$ implies $u'X^* \cap A^* = \emptyset$, we can also assume that $u \not\in a^{d+1}X^*$. Suppose that $b_1, b_1' \in B$, $b \in B^d$, and $f' \in X^*$ satisfy $b_1bf' \cap b_1'B^* \neq \emptyset$ (i.e., $b_1bf' = b_1'b'$ for some $b' \in B^*$) and show that $b_1 = b_1'$ by considering successively the two cases of $b_1 = u$ and $b_1 \neq u$.

In the first case, $uX^* \cap A^* = \emptyset$ shows that $b_1'b' \in A^*$ is not possible. Let $b' = b_2'b_3' \ldots b'_{m'}$ $(b_2', b_3', \ldots, b'_{m'} \in B)$ and let j be the least index such that $b_j' = u$. If $j = 1$ we have already the desired conclusion $b_1 = b_1'$. If $j > 1$, the hypothesis $u \in A^dX^*$ implies that $b_1'b_2' \ldots b_j'$ has a left factor $a' \in A^{d+1}$; however, a' cannot be a left factor of u since $u \notin A^{d+1}X^*$ nor can it have u as a left factor since $uX^* \cap A^* = \emptyset$. Thus $j > 1$ is impossible and $b_1 = u$ only if $b_1' = b_1$.

In the second case, $b_1 \in A$ and, as above, b_1b has a left factor $a \in A^{d+1}$. Thus $b_1 = b_1'$ follows from $\mathbf{U}_r(d)$ if $b_1'b' \in A^*$. If not, using the same notation and the same reasoning as in the first case, we can exclude

$b_1' = u$ because a cannot have u as a left factor nor be one of its left factors. Finally, for $j > 1$, $b_1'b'$ has a left factor $a' \in A^{d+1}$. Since one of a and a' is a left factor of the other, $b_1 = b_1'$ follows from $\mathbf{U}_r(d)$ and the verification of Remark 1 is concluded.

REMARK 2. Let $Q = P \setminus PXX^*$ $(= \{f \in P;\ f \notin PXX^*\})$ and, taking a fixed element $r \in A^d$, let $H' = \{f \in X^* : rf \in A^*\}$ and $H = H' \setminus H'AA^*$. One has $fX^* \cap HQX^* \neq \emptyset$ for each $f \in X^*$ and, for $h, h' \in H$ and $q, q' \in Q$, one has $hqX^* \cap h'q'X^* \neq \emptyset$ only if $h = h'$ and $q = q'$.

PROOF. The condition $\mathbf{U}_r(0)$ is equivalent to $P = X^*$, that is, $Q = \{e\}$, and also to $H' = \{e\}$ and, in this case, the remark is trivially true. Thus we can assume that $d > 0$ and $Q \neq \{e\}$.

Let $f \in X^*$. Because of the hypothesis $r \in A^d$ and of $A^d \subset P = P'$ there exists at least one $f' \in X$ such that $rff' \in A^*$ and we can write $ff' = ha'$ with $h \in H'$ and $a' \in A^*$; in fact if $h = h''a''$ where $h'' \in H'$ and $a'' \in A^*$ we have $ff' = h''a''a' \in H'A^*$ and, consequently, we can assume henceforth that $h \in H$. Now, because of $A^d \subset P$, $ff'r = ha'r = hr'$ where $r' \in P$ and, by the very definition of Q, we have $ff'r = hqf_1$ for some $q \in Q$ and $f_1 \in X^*$. This proves that every $f \in X^*$ is a left factor of at least one element of HQX^*.

Keeping the same notation, assume now that $ff'r$ is equal to $h'q'f_2$ where $h' \in H$, $q' \in Q$, and $f_2 \in X^*$. Without loss of generality we can also assume that h' is a left factor of h, i.e., $h = h'f_3$. By construction, $rhqf_1 = rh'q'f_2 \in A^*$ where, on the one hand, $rh' \in A^*$ because of $h' \in H$ and, on the other, $q' \in P$. Thus, $q'f_2 \in A^*$ and f_3 satisfies $A^*f_3 \cap A^* \neq \emptyset$ (since $rh = rh'f_3$) and $f_3A^* \cap A^* \neq \emptyset$ (since $q'f_2 = f_3qf_1$). As above it implies $f_3 \in A^*$ but, since h and h' belong to $H = H' \setminus H'AA^*$, this is possible only if $f_3 \notin AA^*$, i.e., if $f_3 = e$ and, accordingly, $h = h'$ and $qf_1 = q'f_2$. Since $Q = P \setminus PXX^*$ satisfies $Q \cap QXX^* = \emptyset$, we conclude that $q = q'$, and Remark 2 is verified. In fact, what we have shown is that $H \times Q \to HQ$ is a bijection and that HQ satisfies $\mathbf{U}_r(0)$ and $\mathbf{N}''(0)$.

We now come to the verification of the property itself. Letting r and H as above, let $h_1, h_2, \ldots, h_n \ldots$ be an infinite sequence of (not necessarily distinct) elements of H such that each term is a left factor of the next one. By the definition of H, there corresponds to each h_n a right factor k_n of r such that $k_nh_n \in A$. Thus only finitely many of the k_n's are different and, because of the first part of $\mathbf{F}''$, we deduce that the same

is true for the h_n's. It follows that we can select a fixed $h \in H$ such that $hXX^* \cap H = \emptyset$. Let $S = \{f \in XX^* : h \in X^*f\}$ and $\bar{Q} = \{f \in X^* : fXX^* \cap Q \neq \emptyset\}$. If and only if A satisfies $\mathbf{U}_r(0)$, we have $Q = H = \{e\}$, that is, $S = \bar{Q} = \emptyset$. We show that $\bar{Q} \neq \emptyset$ leads to a contradiction with the second part of $\mathbf{F}''$ by proving first that for any $f \in \bar{Q}$ there exists at least one $s \in S$ such that $sf \in \bar{Q}$.

Indeed, let $f \in \bar{Q}$. Because of $Q = P \setminus PXX^*$ and $P = P'$ we have $f \notin P'$ and, accordingly, there exists at least one $f' \in X^*$ such that $ff'X^* \cap A^* = \emptyset$; since $Q \subset P'$, we have, *a fortiori*, $ff'X^* \cap QX^* = \emptyset$. However, by Remark 2 we know that $hff'X^* \cap HQX^* \neq \emptyset$ and, more accurately that there ex istsone and only one pair $(h', q') \in H \times Q$ such that $hff'X^* \cap h'q'X^* \neq \emptyset$. Because of our choice of h, h' is a left factor of h, i.e. $h = h's$ and $s \neq e$ because otherwise we would have $ff'X^* \cap q'Q \neq \emptyset$ in contradiction with our choice of f'. Thus we have $sff'X^* \cap q'X^* \neq \emptyset$ where $s \in S$. Now q' cannot be a left factor of sf because, taking any $f'' \in X^*$ such that $ff'' \in Q$, it would imply that $hff'' \in HQ$ has a second factor $h'q' \neq hff''$ in HQ. Thus sf is a proper left factor of q' and $sf \in \bar{Q}$ is proved.

Now, since $Q \subset \bar{Q}X^*$, $A^d \subset QX^*$, and $A^d \cap \bar{Q} = \emptyset$, any $f \in \bar{Q}$ is a proper left factor of at least one $a \in A^d$ and we have proved that if $\bar{Q} \neq \emptyset$ one has $A^d \cap S^mX^* \neq \emptyset$ for every natural number m. Recalling that S consists of all the right factors $\neq e$ of h, we see that any factor of any $s \in S^m$ belongs itself to S^*X^*. Since S is a finite set it follows that the relation $A^d \cap S^mX^* \neq \emptyset$ for all m implies that $A \cap S^mX^* \neq \emptyset$ for all m. Since this is excluded by the second part of $\mathbf{F}''$, we must have $\bar{Q} = \emptyset$, that is, $Q = \{e\}$, that is, $P = X^*$, and we have established the conclusion that A satisfies $\mathbf{U}_r(0)$.

OBSERVATION. Using published results on the theory of free monoids one can give to our proposition the following weaker alternative form:

Let A^* be any submonoid of X^* that satisfies the following two conditions:

$\mathbf{U}_d$: $\{f \in X^* : fA^* \cap A^*f \cap A^* \neq \emptyset\} = A^*$.

$\mathbf{N}_d$: $\{f \in X^* : X^*fX^* \cap A^* \neq \emptyset\} = X^*$.

If there exists a natural number n such that

$$X^nX^* \cap (A^* / (A^* \cap XX^*)^2) = X^nX^* \cap \{f \in X^* \setminus A^* : fA^* \cap X^*f \cap A^* \neq \emptyset\} = \emptyset,$$

then A^* *satisfies*:

$\mathbf{U}_r$: $\{f \in X^* : A^*f \cap A^* \neq \emptyset\} = A^*$ *and*

$\mathbf{N}_r$: $\{f \in X^* : fX^* \cap A^* \neq \emptyset\} = X^*$.

Indeed, $\mathbf{U}_d$ is a necessary and sufficient condition that A^* be freely generated by

$$A = (A^* \cap XX^*) \setminus (A^* \cap XX^*)^2$$

and, if $X^nX^* \cap A = \emptyset$ for large enough n, $\mathbf{N}_d$ is a necessary and sufficient condition that A be a maximal set among the subsets of X^* which freely generate a submonoid of X^* (see [3]). Let us assume

$$\mathbf{U}_d, \mathbf{N}_d, \ X^nX^* \cap A = \emptyset, \text{ and } \ X^nX^* \cap C = \emptyset,$$

where

$$C = \{f \in X^* / A^* : A^*f \cap fX^* \cap A^* \neq \emptyset\}$$

and let F denote the set of all the left factors of the elements of A^*. Suppose that $F \cap X^{2n}X^*$ contains a f such that $aff' \in A^*$ and $ff' \notin A^*$ for at least one pair $(a, f') \in A^*xX^*$. Because of $A \cap X^nX^* = \emptyset$ and $f \in X^{2n}X^*$, we can find $g \in X^{n+1}X^*$ and $g' \in X^*$ such that $f = gg'$, $ag = a_1 \in A^*$, and $g'f' \in A^*$. Because of $ff' = gg'f' \in A^*$ we know that $g \notin A^*$ and, because of $g \in F$ we can find $f'' \in X^*$ such that $gf'' = a_2 \in A^*$. Thus $a_2ag = gf''a_1 = a_2a_1 \in A^*$, i.e., $g \in C$ in contradiction with $X^nX^* \cap C = \emptyset$, and we can conclude that $F \cap X^{2n}X^* \subset P$ in the notations of Remark 1. It follows that $A^{2n} \subset P$, and we have proved that A satisfies $\mathbf{U}_r(2n)$. Since A is maximal among the subsets of X^* that freely generate a submonoid of X^*, it is a fortiori maximal among the subsets of X^* that satisfy $\mathbf{U}_r(2n)$ and, since $A \cap X^nX^* = \emptyset$, the condition $\mathbf{F}''$ is trivially verified. Now we can apply our proposition. $\mathbf{U}_r$ is obviously equivalent to $\mathbf{U}_r(0)$ and $\mathbf{N}_r$ is satisfied because it expresses that $P' = X^*$.

References

1. P. M. Cohn, On Subsemigroups of Free Semigroups, *Proc. Amer. Math. Soc.* **13** (1962), 347–351.

2. E. N. Gilbert and E. F. Moore, Variable-Length Binary Encodings, *Bell System Tech. J.* **38** (1959), 933–967.

3. M. Nivat, Théorie générale des Codes, in *Automata Theory* (E. Caianiello, Ed.), Academic Press, New York, 1966.

Printed in Italy by - I.T.E.C. Milan

LES CAHIERS DE L'INSTITUT DE LA VIE

OCTOBRE 1966
N° 10

M. SCHUTZENBERGER

Que deviendra alors le programmeur professionnel ? Il y a quelques années, les usagers le considéraient généralement comme l'intermédiaire nécessaire entre eux-mêmes et la machine. Ils lui expliquaient leur problème ou plutôt, ils s'y efforçaient avec plus ou moins de bonheur, et s'en remettaient à lui pour l'écriture des programmes. Cette conception n'était pas viable car elle exigeait beaucoup trop du programmeur : qui donc, s'il est capable de comprendre le langage d'un ingénieur, celui d'un chimiste, d'un physicien ou d'un médecin, se contenterait d'un rôle considéré comme subalterne ?

Et d'ailleurs, seul le praticien qui connaît ses propres problèmes est en mesure de les résoudre. Le nouveau système d'accès aux ordinateurs, en levant les obstacles majeurs qui décourageaient jusqu'ici certains usagers d'écrire eux-mêmes leurs programmes amènera ceux-ci à une vision plus saine des choses. Bien sûr, ils seront embarrassés de temps à autre, soit par des questions de méthode mathématique, soit par des problèmes relevant de la programmation pure. Il leur faudra alors faire appel à des spécialistes et c'est vers de telles spécialisations que doit évoluer la profession de programmeur.

M. YANOWSKI.

Monsieur Schutzenberger voudra-t-il revenir à ce qui était un des principaux thèmes de ce débat : « la place de la machine et l'obligation faite à l'homme de mathématiser de plus en plus un grand nombre de données et d'épurer de ses automatismes les composantes de la décision ».

M. SCHUTZENBERGER, Professeur à la Faculté des Sciences de Paris.

Il me reste à exprimer les réflexions que me suggèrent les discussions précédentes.

Il faut, en somme, distinguer deux plans.

1°) Un plan abstrait sur lequel on avance deux affirmations nullement contradictoires :

La première c'est que les machines à calculer peuvent faire énormément pour aider les expérimentateurs dans les sciences naturelles et les gestionnaires dans les domaines de la décision et du calcul. Au point de vue du mathématicien, des calculs sont maintenant possibles qui auraient pris, il y a seulement 50 ans, des centaines d'années à des équipes de centaines d'hommes.

La seconde proposition affirmée en même temps, peut-être un peu moins fortement, c'est que toutes ces réalisations extraordinaires de la machine sont relativement peu importantes par rapport au sujet dont il s'agit. Dans les sciences naturelles, il existe mille et un domaines qui ne sont pas concernés par ce qui peut résulter de

l'enregistrement électrique tant réel que potentiel. Les processus de décision dépassent, transcendent les détails de la gestion, nous a-t-on dit de façon très éloquente; j'y souscris. En mathématiques, je ne crois pas trahir l'opinion de mes collègues en soutenant que les découvertes par le calcul sont préliminaires et que les mathématiques commencent là où le calcul finit.
Tel est le plan abstrait.
2°) D'autres orateurs se sont exprimés sur un autre plan, et en se fondant soit sur l'une soit sur l'autre des deux assertions précédentes. Sait-on ce qui se passera ? Il pourrait se passer que les ordinateurs soient effectivement utilisés pour diminuer la peine des hommes, qu'ils jouent en quelque sorte le rôle des microscopes dans les sciences naturelles et qu'ils rendent aux mathématiques les mêmes services que l'invention de la numération arabe. C'est très important mais cela n'a pas bouleversé la pensée mathématique. De même dans le domaine de la gestion, on conçoit parfaitement que les ordinateurs rendent des services émérites. C'est une possibilité. Il en est une autre, et il me semble qu'un certain nombre des interventions du début de cette table ronde en ont exprimé la crainte : bien que ces machines ne puissent rien faire d'essentiel ou d'important, la vogue dont elles jouissent, le fait qu'on y voit une nouvelle révolution technologique, le fait qu'on parle de dialoguer avec elles, leur attribuent des pouvoirs qu'elles n'ont pas et permettent à d'autres pouvoirs d'agir derrière elles.

LES DÉBATS

FORMAL LANGUAGE DESCRIPTION LANGUAGES FOR COMPUTER PROGRAMMING

Proceedings of the
IFIP Working Conference on
Formal Language Description Languages

Edited by
T. B. STEEL, Jr.

1966

NORTH-HOLLAND PUBLISHING COMPANY – AMSTERDAM

CLASSIFICATION OF CHOMSKY LANGUAGES*

M. P. SCHÜTZENBERGER
France

Since our friend Dr. Ginsburg has already succeeded in defining our present knowledge of Chomsky languages (or context-free languages), I am dispensed from giving detailed exposition of the motives justifying several remarks I should like to develop in this paper on the classification of these languages.

We know that all languages L of the Chomsky type are languages that are accepted by a nondeterministic pushdown automaton. Formally, this means that if L is a Chomsky language on the alphabet X, another alphabet Y (X and Y are, of course, finite) and the following objects can be associated with L:

1. A homomorphism φ of the free monoid Y^* generated by Y in the free monoid X^* of which L is a subset.
2. A homomorphism μ of Y^* in a *finite* monoid M, and a proper, distinguished subset M' of M.
3. A homomorphism γ of Y^* in a free group G, and a finite, proper, distinguished subset G' of G.

By definition, $L = \{\varphi g \in X^* : g \in Y\ ;\ \mu g \in M'\ ;\ \gamma g \in G'\}$ and the ambiguity of a word f on X^* is the cardinal number of the set of g's, $g \in Y^x\ n\ \mu^{-1}M'\ n\ \gamma^{-1}G'$, that are mapped on f by φ.

The proof that this construction is possible results simply from the rewriting of the grammar producing L in a canonic form (with the help of the homomorphism φ); the proof that, conversely, every language defined in this manner is in fact a Chomsky language is a trivial consequence of elementary properties of these languages. In an intuitive way, μ symbolizes the finite part of the pushdown automaton, γ its pushdown store, and the homomorphism φ in a certain sense represents the "nondeterministic" character of the automaton.

Given a language L, it is clear that there generally exists an infinity of ways to find φ, μ, and γ that will satisfy the desired conditions, even when we fix the degree of ambiguity of every word. Nevertheless - and this is the point on which I should like to insist - a specific L imposes certain rather strong restrictions on each element of the triple (φ, μ, γ), which, in turn, implies the possibility of using these properties as classificatory principles for Chomsky languages.

* Dr. Zemanek was kind enough to furnish a translation of my original french text.

1. CLASSIFICATION BASED ON THE HOMOMORPHISM φ

In cases where φ is a monomorphism, every word of L has ambiguity one, i. e. according to the usual terminology L is "without ambiguity". Well-known counterexamples show that there are Chomsky languages possessing an essential ambiguity (for instance, $\{x^n y^m z^p\}$ with n, m, and p positive integers and $n=m$ or $m=p$) and that, consequently, there is a subfamily of Chomsky languages for which φ cannot be a monomorphism. On the other hand, I do not know any example of a language such that the minimum ambiguity increases exponentially with the word length, altough, in an intuitive way, it seems that this would constitute the general case. If one has such a counterexample, one could also separate the languages having an essential ambiguity from those which are the union of a finite number of languages corresponding to the monomorphisms, and those whose ambiguity increases like a polynomial in the word length.

Whenever φ is a monomorphism, it is possible to introduce new distinctions. Let us suppose that the set of words of the form φy ($y \in Y$) constitutes a prefix code. In this case, one can find for every word $f \in X^*$, read from left to right, the unique word $g \in Y^*$ of which it is the image by φ; with the help of a finite automaton one can verify whether g belongs to Kleene language $\mu^{-1}M'$. Using these finite devices, which either write sequentially or write just one symbol (marking the membership to M'), it is possible to verify the membership in L of a word f $\in X^*$ with a deterministic pushdown automaton only. To verify that these conditions define a *proper* subclass of Chomsky languages without ambiguity, it suffices to consider the counterexample of $L = \{\varphi g \tilde{g} : g \in Y^*\}$, where $\{g\tilde{g} : g \in Y^*\}$ is the set of "reflected words, and where φ is a monomorphism, such that $\{\varphi y : y \in Y\}$ is a generic code (i. e., with an unlimited delay). Another counterexample would be given by the reflected image of a *generic* language if it were accepted by a deterministic pushdown automaton.

2. CLASSIFICATION BASED ON THE HOMOMORPHISM μ

Classification by μ is, in fact, the most frequently utilized. One knows that it is always possible to choose μ and M' in such a way that the Kleene language $\mu^{-1}M'$ has the very particular form $M' = Y_1 Y^* \backslash Y^* V Y^*$, where Y_1 is a subset of Y, and V a subset of YY. Under these conditions, the metalinear Chomsky languages are characterized by the fact that M' has the form $Y^*_1 Y^*_2 \ldots Y^*_k$, where the Y_j's are disjoint subsets of Y and where, in addition, one supposes that the homomorphism γ is a monomorphism. If one does not make this last restriction, but supposes that each one of the Y_j's is reduced to a unique letter, one obtains languages that are very close to the "*bounded*" languages of Ginsburg. It is clear that a Chomsky language is generally neither metalinear nor "bounded", the simplest counterexample being, obviously, the reflected image by γ of a finite subset of the free group G.

In fact, the specification of V is equivalent to the specification of a relation on the alphabet Y, and it would be interesting to use the numerous results of the theory of relations to make the classification of Chomsky languages precise. As far as I know, not very much has been done in this direction, except for Ginsburg's theory of sequential languages.

3. CLASSIFICATION BASED ON THE HOMOMORPHISM γ

It is not difficult to show that, given L, one can choose (φ, μ, γ) in such a way that Y is an alphabet of four letters (i. e., G is a free group with two generators, because every generator of G corresponds to a pair of letters of Y). It seems interesting to me to emphasize that, in general, it is not possible to reduce Y and γ in such a way that F is a free group with a single generator. The counterexample is given by the language $\{x^n_1 x^m_2 x^m_3 x^n_4\}$ (with n and m two arbitrary integers) on an alphabet X formed by four letters x_i. The verification that this language (even with arbitrary ambiguities) cannot be produced by a triple (φ, μ, γ), where γ is a homomorphism in a free group with a single generator, does not present any difficulty at all. As usual, however, it implies the discussion of a considerable number of particular special cases. On the other hand, although it seems to be evident *a priori*, I have not succeeded in verifying the same result concerning the language constituted by the inverse image of a finite subset of a free group with several generators.

Intuitively, the hypothesis that G has a single generator is equivalent to the hypothesis that the pushdown store of the automaton is an (unlimited) counter, since G is isomorphic to the additive group of the integers. The "write" and "clear" operations now correspond to addition and subtraction. With the additional hypothesis that L is accepted by a nondeterministic pushdown automaton, it is easy to use ordinary considerations about the quantity of stored information to discuss the possibility of reducing the pushdown store to a counter. In the case where this additional hypothesis is not made, the nondeterministic character of the automaton is equivalent, in a certain sense, to the possibility of storing a quantity of an information that increases linearly with the length of the examined word under these conditions, however, it is no longer possible to use this shorter procedure to verify that the language has the desired properties. It seems, therefore, that the fact of admitting or not admitting a language into a group with a single generator is a rather profound property of a given Chomsky language, and I believe that this question deserves closer study.

DISCUSSION

DIJKSTRA
I gather that you are talking about finite alphabets defining words in terms of concatenation of characters of this alphabet, asking yourself whether there exist algorithms

to determine whether a given word is part of this language. Now, what I am thinking of is a very simple language, but here the decidability question poses great problems. The alphabet consists of a finite set of characters and the only words I should like to admit are words consisting of a single character. Clear? There are 26 letters, and my language consists of 26 words, a, b, c, etc. Do you consider a language of this nature as one where I can decide whether a given sequence of characters represents the word in the language or not? Do you regard this as decidable - or can we conceive an algorithm that does it?

SCHÜTZENBERGER
Insofar as the question is a catch, I will answer that I cannot answer it. I mean I am not dealing with interpretation and I don't understand it. The only problem with interpretation is that you give up on the words. If I ask you if it is decidable what is the value of the integer nearest to the value of the Bessel function of the square of 2 to the 2 to the 2, is this number odd or even? Is it decidable on that question? If I answer you "No" you tell me it can be done by a Turing machine. If I answer you "Yes" you will tell me do it and of course it will not be finished before you are all dead. [Laughter] So I suppose this is the same type of question, and I will very carefully say that I was entirely incompetent for dealing with interpretation.

DIJKSTRA
I think you misunderstood my question. You're talking about certain sequences of characters.

SCHÜTZENBERGER
No.

DIJKSTRA
People are talking about algorithms which can inspect a given sequence of elements of the alphabet, etc. You talk about scanning in sequence, thereby describing the way you are allowed to have access to the given sequence. If I give a sequence as I give a word, is it (at its expense) implied or not? I am trying to use your terminology; I gather that people talk about finite alphabets - alphabets of, let's say, 26 distinguishable characters.

DUNCAN
For example, the letters, a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, that is an example. Is this a set?

SCHÜTZENBERGER
Well, I'm no logician. I think that all these are interesting questions. The only thing is, I am entirely incompetent to answer them. I admit it frankly. I also admit that as a mathematician I have no involvement with objects that appeal to the intuition. I am involved with mathematics. The definition of mathematics is a matter of ideology.

GORN
Maybe I can help Dr. Dijkstra on this. If somebody gives an abstract theory and somebody else says "I think I have a fine application of your theory, don't you agree"? The theorist has to be very careful in answering because there may be considerations outside his theory that may arise in his answer. [Schützenberger] did not want to commit himself as to whether the alphabet, for instance, was a concrete application of a base of his monoid, because he didn't know how you were going to use the alphabet. So I think he was justifiably careful. I think it very likely that the alphabet of distinguishable letters would be an application of a base of a monoid. But there are things you might do. For instance, suppose the alphabet you chose was already a composite language over another alphabet.

ELGOT
I would like to have the question clarified. I think there is a serious question here for which he would like an answer. I'm not sure that everyone is clear on what the question is.

DIJKSTRA
I thought that one of the major concerns of people interested in the subject for today - I may be completely wrong - was that given a finite alphabet of distinguishable marks, and given rules about how to build up sequences of such marks, you can ask the inverse question about whether a given sequence of marks belongs to the set of sequences which can be constructed by the rules mentioned half a minute earlier. That's all. We take a very simple alphabet of 26 letters and the only sequences we wish to consider are those consisting of single letters. So I have a finite alphabet and even a finite number of words. Now I give you the sequence "ab". You can react to this in two ways. You can say "Now, this ab is not one of the basic characters, so it is not an element of the language". On the other hand, if I have a machine which can recognize the 26 letters, I give it the sequence "ab", so it looks at the first one and sees "a" and says "Well, it's a word". For instance, when you talk about a given sequence, is its length implied in what you give? If so, then you have apparently two other distinguishable marks you haven't said a word about, indicating where it begins and where it stops. Then I say what a curious restriction it is that you allow these marks only at the beginning and the end. Is my question now clear?

SCHÜTZENBERGER
I suppose I can answer that, in a sense. [Laughter] I very carefully said at the beginning that what you people were dealing with were mostly sequences and that I would be dealing with an almost equivalent concept, namely the elements of a free monoid. Now, insofar as you are dealing with sequences that you have any standard definition for, you are given the length. Insofar as you are dealing with elements of a free monoid you construe your hypotheses and assertions in such a way that this question is not a question. That is to say, this is a valid question but only at the level of the interpretation. When you study arithmetic you may ask all sorts of questions, such as "Are three apples the same as three Elgot's", or "Do four letters in this word have the same meaning as four letters in another word". Now when you do arithmetic you have certain definitions, which means that these questions are irrelevant. What I said mathematically does not pertain to the type of question you are raising. Whatever I say about a free monoid, it does not matter if it has a beginning or an end. It has a left factor, a right factor, and an intermediate factor which may be the empty word. By definition, there is something which we call the empty word which you can eventually interpret as the empty sequence, but it is not the same thing as the empty sequence; it's another concept entirely. I tried to go at a rarified level where these questions don't bother me anymore.

Année 1967

Bibliographie

[1] Maurice Nivat and Marcel-Paul Schützenberger. Errata : "Sur les produits semi-directs droits de monoïdes". *C. R. Acad. Sci. Paris Sér. A-B*, 264 :A383, 1967.

[2] Marcel-Paul Schützenberger. Algorithms and the neo-darwinian theory of evolution, preliminary working paper. In *Mathematical Challenge to the Neodarwinian Theory of Evolution, Wistar Institute Symposium*, page 121. 1967. Extended abstract.

[3] Marcel-Paul Schützenberger. Algorithms and the neo-darwinian theory of evolution. In *Mathematical Challenge to the Neodarwinian Theory of Evolution, Wistar Institute Symposium*, pages 73–80. 1967. Full paper.

[4] Marcel-Paul Schützenberger. On products of finite dimensional stochastic matrices. *Proc. Amer. Math. Soc.*, 18 :850–853, 1967.

[5] Marcel-Paul Schützenberger. On synchronizing prefix codes. *Information and Control*, 11 :396–401, 1967.

C. R. Acad. Sc. Paris, t. 264 (20 février 1967). **Série A — 383**

ERRATUMS

(*Comptes rendus* du 7 novembre 1966.)

Note présentée le 2 novembre 1966, de MM. *Maurice Nivat* et *Marcel Paul Schützenberger*, Sur les produits semi-directs droits de monoïdes :

Page 659, 20e ligne, *au lieu de* $K'_a \neq \emptyset$, *lire* $K'_a \neq \emptyset$.
» » 32e ligne, *au lieu de* $U\{K_a : a \in H\}$, *lire* $U\{K_a : a \in H\}$ (symbole de réunion).

Page 660, 1re ligne, 2e phrase, *au lieu de* Disons maintenant qu'un monoïde M est un $\mathcal{R}_1$ (resp. $\mathcal{R}_0$) monoïde si aucune de ses $\mathcal{R}$-classes régulières ne contient plus d'un seul idempotent (resp. élément), c'est-à-dire si pour tout p, $q \in M$ les relations, *lire* Disons maintenant qu'un monoïde M est un $\mathcal{R}_1$ (resp. $\mathcal{R}_0$) monoïde si aucune de ses $\mathcal{R}$-classes (resp. $\mathcal{H}$-classes) régulières ne contient plus d'un seul idempotent (resp. élément), c'est-à-dire si pour tout p, $q \in M$ les relations...

17e ligne, *au lieu de* $(b, a) = (b, {}^a y, ax)$, *lire* $(b, a) = (b\, {}^a y, ax)$.

Reprinted from MATHEMATICAL CHALLENGES TO THE NEO-DARWINIAN INTERPRETATION OF EVOLUTION
The Wistar Symposium Monograph No. 5, June, 1967

PRELIMINARY WORKING PAPER

Algorithms and the Neo-Darwinian Theory of Evolution

DR. MARCEL P. SCHÜTZENBERGER
University of Paris, France

According to the "dogma" the whole of genetic information should consist of a rather limited set of words in an alphabet of 20-odd letters. Then the only evolutive mechanisms which are ever mentioned are what might be called "typographic changes," i.e., suppression, duplication, transposition, and substitution of letters or blocks of letters, subject to short-range and eventually periodic constraints. Thus there is a striking similarity between these assumed blueprints of living organisms and the formal systems which underlie both programming languages and the simplest non-trivial models of natural ones. It must be emphasized that this framework implies an extremely special net of proximity (of derivability) relations on the set of all words considered. This we may call the "syntactic topology."

From another point of view, organisms are related by another topology which simply results from their being physical objects in space-time. Although this second topology is far harder to formalize, it is the basis of systematics, and it is objectively studied when observing the developmental effects of variations in the milieu. We call it "phenotypic topology."

In my view, we are faced in biology with the same crucial difficulties as in theoretical programming:

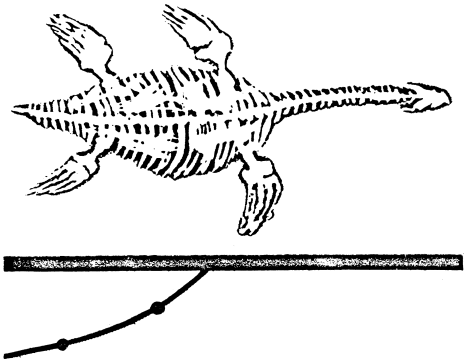
1) With respect to the problem of origins, the impossibility of sifting (within less than 10^{100} cycles, say, for non-trivial cases) from mere typographic variants the ones which are syntactically correct, except by using algorithms in which the very concept of syntactic correctness has been incorporated.

2) Granted such a syntactic device, the present lack of a conceivable mechanism which would insure within an interesting range the faintest amount of matching between the two above mentioned topologies (this is said notwithstanding claims to the contrary of some "artificial intelligence" teams).

In other words, I believe that an entirely new set of rules is needed to obtain the sort of correspondence which is assumed to hold (one way—Darwin, or the other—Lamarck) between neighboring phenotypes and which is needed in similar theories of evolutions. If these new principles, or deductions from old ones, were to be postulated, it would seem then a subsidiary point to discuss how much of random mutations and selections are at work in conjunction with them.

Mathematical Challenges to the Neo-Darwinian Interpretation of Evolution

Edited by
PAUL S. MOORHEAD
MARTIN M. KAPLAN



THE
WISTAR INSTITUTE
SYMPOSIUM MONOGRAPH
No. 5

Published by THE WISTAR INSTITUTE PRESS

Algorithms and the Neo-Darwinian Theory of Evolution

Dr. Marcel P. Schützenberger
University of Paris, France

Dr. Marcel Schutzenberger: Our thesis is that neo-Darwinism cannot explain the main phenomena of evolution on the basis of standard physico-chemistry. Here we stress two points. First that the physical concepts used by biologists are generally more classical (or less imaginative) than the ones occurring in such domains as, say, cosmology. Second that we are not trying to smuggle in extra scientific principles. Thus if we claim that radically new principles are needed we also believe that these have to be found within physics. The nature of the inability of biology to provide a coherent explanation of evolution is best seen when contrasting it with geology. It is certain that no one can work out mathematically every detail of the geological history of the earth. However, for each of the most important phenomena, there exists a simplified model which accounts for it, without mysterious forces, and there is no doubt that this chain of models could be refined *ad infinitum* without gaps and without requiring the verbal argument so often met here that new qualitative effects arise because of the enormous number of small quantitative variations. At no point does geology need to use such phrases as "creation of information", "increase of efficiency", "self-organization", and the like. (My examples are chosen so as to offend no one here, I hope). I intend to restrict my argument to show the existence of a serious gap in the current theory of evolution. The next question (which I will not discuss here) would be to ask how much random mutation and selection would be needed once this gap is filled.

My colleagues this morning have been doing their share of sand reckoning in the manner of Archimedes. From their talks it is clear that even on the most schematic models the number of cycles involved is truly enormous. Thus, when we reach the level of 10^{1000}, whether or not we take a few square roots makes little difference in this cosmos. A second point to which I would like to draw your attention is the fact that nowadays computers are operating within a range which is not entirely incommensurate with that dealt with in actual evolution theories. If a species breeds once a year, the number of cycles in a million years is about the same as that which one would obtain in a ten day computation which iterates a program whose duration is a hundredth of a second. Our ability to play with iteration of this magnitude is quite a new thing, and we can begin to develop some concrete experience with this type of process. It was not so in the time of Fisher and *mon bon Maître* Haldane, and now we have less excuse for explaining away difficulties by invoking the unobservable effect of astronomical numbers of small variations.

To present my argument I need to introduce a schematization of current ideas based on the introduction of three spaces, each endowed with a specific net of proximity relations, or as I shall say for short, a topology—if you forgive my using mathematical jargon.

According to the "dogma" of molecular biology the first level we start with is, ideally, something like a big book written in an alphabet of 20 odd letters. This is the blueprint of an individual, a genotype. Further we have a genic pool, i.e., a collection of such books which are variants of each other. For many clusters of species this collection is not much bigger than the Widener Library; for others, it is at most millions or billions of times larger. I shall

take those books as the elements of the first space, and, since we are not in any way Lamarckian, we have to admit that the proximity relations in this space are of a strictly typographic nature: omission, addition, duplication, transposition, or change of letters, pages, or of chapters—but irrespective of context, or if you allow me, of meaning. This topology, insofar as molecular biology is concerned, is of the same nature as the one which would represent the relations between several copies of the same manuscript typed and bound by a very careful assistant totally ignorant of the language in which it was written. Typically, in the typographic topology, two editions of the same textbook of botany differing only in the fact that one contains the common name of species wherever the other has the Latin name, would be further apart than two editions differing by replacement (or deletion, or duplication . . . etc . . .) by another word or jumble of letters perpetrated in a systematically random manner, of one or two words in each page.

At the opposite end we have the individuals who react to the environment in accordance with their being physico-chemical systems with a given size and configuration. Admittedly, it may be hard to give an abstract formulation of the fact that two trees (or two winged animals, or two protozoa) are "closer" to each other in the topology of phenotypes than are, say, a bush and a bird. However, this system of closeness relations is the one on which we base most of our taxonomy and physiology. It is with reference to this topology that one tries to account for the similarity of the selective effects of the milieu when discussing phenomena of convergence.

In the middle, neo-Darwinism introduces a third space consisting of vectors (i.e. finite sets of numerical parameters) with its usual topology. The coordinates of these vectors are such things as mutation rates, coefficients of viability, etc. Because this is a theoretical object, it is not dramatically surprising that one can predict or simulate Darwinian effects within it. One might question the adequacy of using the parameter space as a model for the phenotypic space and the validity of the reasonings based on it because in almost every case, both the parameters and the relations between them are strictly hypothetical constructs for which no conceivable direct or indirect cross measure exists. We shall not do it here because we believe that the crucial difficulty is not in relating this theoretical parameter space to the real phenotypic space but in providing a link, however tenuous, between either of them and the space of the chains of amino acids (or the space of genic pools, it does not make much difference) endowed with its specific typographic topology.

Indeed, what we have at each of the two extremes is not even chaos out of which one might believe that a certain regularity could emerge, as it may do in thermodynamic processes, but two systems having structures (topologies) which *a priori* are not more in agreement than in conflict. Now some modicum of agreement is needed if one wants the selection pressure to have the nice effects we are told it has. Otherwise, there is no reasonable probability (say more than 10^{-1000}) that variations in the milieu operate without the genotype having entered a *cul-de-sac* out of which no evolution is possible.

I apologize for being so assertive but here is the point where experience with computers (more seriously, of course, a few mathematical results) comes in. According to molecular biology, we have a space of objects (genotypes) endowed with nothing more than typographic topology. These objects correspond (by individual development) with the members of a second space having another topology (that of concrete physico-chemical systems in the real world). Neo-Darwinism asserts that it is conceivable that without anything further, selection based upon the structure of the second space brings a statistically adapted drift when random changes are performed in the first space in accordance with its own structure.

We believe that it is not conceivable. In fact if we try to simulate such a situation by making changes randomly at the typographic level (by letters or by blocks, the size of the unit does not really matter), on computer programs we find that we have no chance (i.e. less than $1/10^{1000}$) even to see

what the modified program would compute: it just jams. We can specify what it would take to have the random modifications introduced so that a sizable fraction of all programs start working: It is a self-correcting mechanism which must incorporate something like a symbolic formulation of what "computing" means. Thus no selection effected on the final output (if any!) would induce a drift, however slow, of the system toward the production of this mechanism if it were not already present in some form. Further, there is no chance ($<10^{-1000}$) to see this mechanism appear spontaneously and, if it did, even less for it to remain. Finally, we can predict what would happen if such a mechanism had been installed: for almost all the mutations the computation performed would have no relationship to the ones executed before: hence, no relationship to the selective pressure exercized on the output. All this, I repeat, is a simple consequence of the lack of matching between the space of the outputs and the space of the programs. This, of course, does not apply to the relationship between the space of parameters and adequate simplified models of the space of genotypes: They are theoretical constructs which have been specifically designed to fit. However, the question remains with respect to the relationships between the space of the chains of amino acids and the space of the organisms (or just as much, the parameter space studied by Sewall Wright). We do not know any general principle which would explain how to match blueprints viewed as typographic objects and the things they are supposed to control. The only example we have of such a situation (apart from the evolution of life itself) is the attempt to build self-adapting programs by workers in the field of artificial intelligence. Their experience is quite conclusive to most of the observers: without some built-in matching, nothing interesting can occur.

Thus, to conclude, we believe that there is a considerable gap in the neo-Darwinian theory of evolution, and we believe this gap to be of such a nature that it cannot be bridged within the current conception of biology.

Discussion

PAPER BY DR. SCHÜTZENBERGER

DR. ULAM: My impression is that what you have said so far is that one does not understand now how the blueprint determines the existing physical objects. That, of course, the Darwinians or neo-Darwinians would readily admit. Now, the assertion that such blueprints exist and are important is made much clearer through the discovery of the genetic chains as codes. Nobody in the 19th century or even now would profess to understand the details of how, from the code, an actual organism is produced.

DR. SCHUTZENBERGER: We are not worried with the details. The only thing is that I would need an example where such a correspondence would exist or could exist, even in the simpler case.

The Chairman, DR. WADDINGTON: You have confronted us again, you have made the gap because you have left out the middle space, the epigenetic space.

DR. WALD: What is epigenetics? What does the word mean?

The Chairman, DR. WADDINGTON: It is a derivative of an old Aristotelian word and means the study of the causal mechanisms of development. "Epigenesis" was used by Aristotle to mean that new things appear during development. Epigenetics is the name for the study of the causal interactions between the genes in the blueprint and the way they work together to produce first proteins, and then cells and membranes, myosin fibrils and God knows what. It is the causal study of the way the genotype space is translated into the phenotype and if you leave it out, of course there is a gap. Unfortunately, however, we can't yet put it

on computers! We really have got no analog of development. This is why the whole application of information theory to biology breaks down; because what biological organisms do is to treat information as axioms and then develop theorems from them, and this is something which isn't included in information theory, as it is normally understood. Information theory is a conservative theory, in which information can't be increased. But biology, as it were, starts with Euclidian axioms and proceeds to write a five-volume treatise on Euclidian geometry, and it is that process which goes on in this middle space of epigenetics and leads you into the space of phenotypes. But nobody has yet found how to do it on computers and therefore, it tends to get left out.

DR. SCHUTZENBERGER: I repeat, in order to mediate between the space of chains of amino acids and the real world of organisms, some new construct has to be introduced, and principles have to be stated explicitly explaining how this mediation is conceivable.

At the level of molecular biology, we are told that we have a reasonably complete description of the mechanisms. Also, physiology is providing us with an understanding of organs. However, everybody seems to take for granted that there is no gap in between. I am not discussing the adequacy of each of the two extremes. I just point out that nobody seems to be able to give reasons why they have anything to do with each other. If there were explicit general principles relating them, then we should be able to simulate something analogous, and we would have a lot of fun studying mathematical models showing the passage from disorder to order.

DR. ULAM: What you are saying, it seems to me, is that the Darwinian and neo-Darwinian theories are not complete, and everybody agrees with that; but it is not an objection to the scheme of things, which is sort of lost sight of.

DR. RICHARD C. LEWONTIN: Can we give you a practical experience where there is no gap? Will that suffice? Suppose I tell you that I know exactly the typographical change involved in a mutation of the enzyme tryptophane synthetase. I know what that change is and I know many such changes cause an inactive enzyme to be formed.

I know that an organism which is not fed tryptophane, if it is an organism that requires tryptophane in its proteins, will not succeed in dividing and reproducing if it has that typographic change. Therefore, the frequency of such organisms will decrease in the population and be replaced by those that can synthesize tryptophane.

Excuse me, but what step is missing in this argument?

DR. SCHUTZENBERGER: It is missing the decisive step. Maybe I have too ambitious a goal with respect to evolution theory; but it seems to me that if its principles were valid, we should then obtain on simplified models the same type of correlation which you claim to obtain. However, what we know is that when we make changes of a typographic nature, most of them are meaningless from any respect, and when I say "most of them," I mean less than one out of 10^{100}.

DR. LEWONTIN: No, that is not true.

DR. ULAM: Tell him, Dr. Schutzenberger, *where* his model fails.

DR. LERNER: Would you answer Dr. Lewontin's question?

DR. SCHUTZENBERGER: It is very intriguing, but if you tell me that the coding is such that this type of change induces meaningful changes—what I mean by "meaningful" is that they are related in one way or another to external individual characteristics—you already express a very strong hypothesis on the living system. I say this is not included in molecular biology as it is described now.

DR. LEWONTIN: If the speaker objects to a case in which the enzyme has been destroyed in its action, then I can give him known cases where the enzyme, far from being destroyed, is changed in its pH optimum, changed in its isoelectric points, changed in a number of aspects of its physiological function by single substitutions of single amino acids. We know exactly where in the phenotypic topology of the protein these amino acids have been substituted, and we can specify exactly in what way they change the physiology of the organism, changing its fitness in the write-in space.

If you want, I can give you reference after reference.

Dr. Schutzenberger: Yes, I can also give you references.

Dr. Lewontin: As in hemoglobin.

Dr. Schutzenberger: I can also give you a lot of anecdotes on typographic changes of books which transform some perfectly decent sentences into ones which are very funny to read in French.

Dr. Lewontin: But, sir, I have said that they are not meaningless changes; they are changes that change the organism in its phenotypic optimum from one set of environments to another one.

Dr. Weisskopf: I think the point Dr. Schutzenberger makes is the following: Dr. Lewontin is talking about changes in the enzyme by faults of reproduction; but Dr. Schutzenberger says that this is only a very, very small part of the typographic space and most of the changes seem to take place somewhere else in this space.

Dr. Schutzenberger: I want to say that it is an observed fact that life works.

Dr. Weisskopf: No, no, let's speak to the tryptophane!

Dr. Schutzenberger: I want to know how I can build, on computers, programs in which —

The Chairman, Dr. Waddington: We are not interested in your computers!

Dr. Schutzenberger: I am!

Dr. Bossert: Perhaps I misunderstood, but I thought yesterday there was some discussion about a point quite in line with what you are saying. You have mentioned variation several times, and you require that a small variation at one level translate into a small, meaningful variation at the other. In fact, I think it came up several times yesterday that those instances where a small variation in the program space translates into a large variation in the phenotype space or output space, are usually of no interest.

Dr. Shahn: My understanding is that the problem involved is how you get from a lower organism to a higher organism; or at a different level, perhaps, what is it about the genetic material which is going to differentiate a horse from a pig; not how one bacterial strain will die due to the deficiency of one enzyme.

However, the argument as it is presented, I think, could probably be leveled against all of biology in that, insofar as I know, there is not one mechanism which is completely understood. Any time there is a difficulty in getting from one step to another, an enzyme is introduced which often can be isolated, its properties in many ways expounded; but the mechanism is still left in a "black box". Using this terminology, one might be tempted to say that organisms have built in a "selectase," perhaps a "fitnessase," and these are part of an operon which is governed by "evolutionase." This now reduces all of evolution to the same state that most of molecular biology has been reduced to, and since molecular biology is today fashionable, I might claim to have solved all of evolution at the same level. I just have to isolate the enzymes.

Dr. Schutzenberger: I want to make clear that my point is methodological, strictly methodological, and now we are just discussing facts. I am asking the question, How can you devise a program (or a book) such that typographic changes are meaningful? You are not interested in computers; I'm sorry. I am not very much interested in computers either, but here is an instance of a problem of order-disorder, and I am speaking of computers just to follow the *Zeit-Geist.*

How come that a system, which is not the type of system imbedded in the usual space-time topology, has the property that small changes within this typographic topology are meaningful? I could be specific here; I could document it with theorems.

Dr. Lewontin: I gave you an example.

Dr. Schutzenberger: I am not asking for examples. I believe you! But, I say, How come these changes are meaningful?

The Chairman, Dr. Waddington: He asked a methodological question. You have to answer it as a methodological question. He has asked, How do you arrange that typographical errors, changing letters and so on, have meaning when translated into this space? Surely, the way you do it is to have the typographic script set up as paragraphs with logical structure in the para-

graph. Most typographical errors will then be absorbed by the logic. You will see that there is a misprint and go on reading, understanding perfectly well what is happening. Occasionally, a misprint will change a key word into some other key word, and actually change the logical structure, but very rarely.

The main point is that your typographic space contains meaningful blocks. It is not a set of isolated individual words. It has meaningful blocks of connected connotations and this can absorb a great deal of typographical error but can occasionally have its meaning changed.

The very simplest case is where the epigenetic space is very reduced and you are just producing an enzyme; Dick Lewontin has pointed this out. In more complicated cases, like the mouse, where the development from the genes to a front leg is much more complicated, you have much longer blocks.

DR. SCHUTZENBERGER: I am sorry, I want to challenge you somewhat. I am sorry to disagree flatly with the Chair. This is not an explanation but a postulate.

When you have said that there are meaningful paragraphs, you have already postulated the simplest thing, which is to make a computer program work at the paragraph level. For the time being there is no such possibility except by introducing beforehand the concept of meaning into it. There is dramatic change at the algorithmic level (that is the first time I have used the word but let it come now) between typographic errors of any sort and the ones which would preserve meaning. Taking paragraphs instead of letters is immaterial; it makes the case worse, that is all. So, what you say is all right except that what you propose is exactly the mechanism for which I am asking.

DR. BARRICELLI: The speakers seemed to stress very much the point that every step from one genetic pattern to another should be meaningful, but I think there is absolutely no requirement that every step should be meaningful. First, you have many examples of changes indicating that often a large part of a protein molecule can be unimportant or play no role in its function. You can lose a piece, you can add a piece, you can shift the reading frame in a segment of the RNA-molecule coding for the proteins, and so forth, and still leave the wild type function intact. That is one part of it.

Secondly, everybody can tell that by typographic change of the various types which have been mentioned today, you can change "Hamlet" of Shakespeare into Dante's "Divine Comedy," just by adding and subtracting pieces and changing one letter to another. So, if you don't require that every step in every place should be meaningful, you can make any large change you want.

DR. SCHUTZENBERGER: I think there are two points here. First, it seems to me that this reckoning activity has some merit in that it shows that the matter is not that all changes must be meaningful. Only a reasonable proportion has to be. By "reasonable proportion," I would mean 1 10^{100}. It is not the case. We have a conflicting experience. You can quote me experiences where things work in life, but we have a conflicting experience in the computer. Although our processes are based on the same principles as the ones you state explicitly and the probability of a meaningful change is not one in 10^{100}, it is entirely negligible.

The second point has no relationship to the present discussion, but it has a more general bearing on these two days' discussion. It seems to me that it is a nice intellectual game to try to find that there is some path from A to B, but the problem is not to discover *if* there is at least one path. The problem is to decide if there is any reasonable chance of *finding* such a path; it is an entirely different question.

DR. LEWONTIN: I think I understand finally what Dr. Schutzenberger is getting at, and that is that the difficulty (and I agree entirely) is that most of the changes in a given environment would seem to alter the function in a way which is not, as you put it, meaningful. I think the thing that has been left out is the fact that we agree with this point, and it certainly is true, but that in a new environment the old messages, which had meaning in the old environment, now can no longer be called "correct" and changes can no longer be called "errors." On the contrary, as environment changes,

the present messages are no longer in a meaningful language and, therefore, new changes that occur are more likely to produce a real meaning in the new context.

That is the one point which I think all evolutionists are agreed upon, that it is virtually impossible to do a better job than an organism is doing in its given environment.

Dr. Schutzenberger: I suppose we are getting nearer to an exchange of messages, but I was making a stronger point. When I said "meaningful," I was meaning meaningful in sort of an absolute sense. I say that all systems, similar systems that I know about, become meaningless in a radical fashion, when I make these sorts of changes.

Dr. Weisskopf: In any environment?

Dr. Schutzenberger: Yes, in any environment.

The Chairman, Dr. Waddington: This is not the case with the biological aspects.

Dr. Schutzenberger: O.K. I have also the idea that something more must exist in biological systems, but the problem is to find the recipe so that we can simulate it on a different material.

Dr. Lewontin: I think the answer is that you have over-estimated the number of absolutely meaningless changes that occur when you change a single nucleotide. If we list all single nucleotide changes and the known translation vocabulary between nucleotide triplets and insertion of amino acids, and then we list for a given protein all the results on that protein of changing amino acids all over the molecule, we will find, in fact, that a very large proportion of those do not render the molecule meaningless in an absolute context.

Dr. Schutzenberger: You tell me it is factually all right. I ask you, What is the mechanism which makes it so, or what sort of conceptual mechanism could make it so? I don't know of any general principle or of any trick which in any other circumstances could produce this effect.

The Chairman, Dr. Waddington: Before we go any further, I think that, first of all, we should agree how we are using the word "meaningful." I think Schutzenberger means that when he changes something in program space, nothing comes out at all.

Dr. Schutzenberger: It doesn't give support to any epigenetic effects.

The Chairman, Dr. Waddington: But actually when we change something, *some* protein does come out; it may not be a very good protein, but some protein comes out. All proteins do something, so all changes in the program level have meaning, in the sense that they produce a protein, except for some full stop marks, and so on.

Dr. Mayr: Are you basically asking, why do molecules have such-and-such properties? Why are molecules the way they are? Is that really, basically, what you are asking?

Dr. Schutzenberger: That's a good question. I don't think I have time to answer it now.

Dr. Levins: I think the missing ingredient in this analysis is that you have left out evolution. The error of the reductionist methodology is to start out with a lower level and attempt to derive a higher level from it without considering the reciprocal relation. In fact, its topology is, itself, a product of evolution and we can start out with a given topology and describe how natural selection will modify this without knowing about the original underpinnings, especially as you get further and further away from the site of gene action to the interactions of these gene products. This is something which, in your library, would have to be described by 10^{10} simultaneous partial differential equations.

On an evolutionary level, in terms of some epigenetic parameters involving elasticity, the rigidness of the terrain and other things can tell us how the evolution is going to change it, the direction of homeostasis, of epistatic interactions, so that, in fact, the topology is the result of evolution.

Dr. Schutzenberger: O.K., This is far easier to answer. You are falling into what I might call the Ashby trap. You only make the case worse by supposing that the mechanism which induces an agreement between the topologies has been produced also by random changes. That is to say, this sort of fallacy has been used a lot of times in "artificial intelligence" to pretend that one could write programs by machines which would learn how to tell themselves how to improve programs.

Still, then, at this level, the probability of meaningfulness is still slimmer by orders of magnitude which are 10^{100}.

If I had had more time, I could have dissected the typographic changes into three levels, each corresponding to a type of algorithm; each of them is practically irreducible to the previous one.

The Chairman, DR. WADDINGTON: Your argument is simply that life must have come about by special creation.

DR. SCHUTZENBERGER: No!

VOICES: No!

DR. FRASER: Can I contrast one computer with another? You have a computer programmed to examine the statement, "All I am allowed to do is change letters and I hope I produce a program. Any kind of program will do." This doesn't work. We now turn around and set up another computer, and we tell it a basic genetic system of plus-minus alleles in which we are saying, "Can it produce information?" The decision on whether the information is useful will be a selective one of "survive or not survive." This is the same kind of decision-making; the programs look very similar to those which are being constructed to try to produce information-containing programs. The principles are very similar.

However, in the genetic one, the system is that there are multiplicities of pathways to suitable answers. The machine can gradually, step by step, get there; each step takes it toward the answers, and it produces them when all we have fed into the machine is a genetic system of essentially complete simplicity. What is surprising is how fast rational information is produced by the machine within the meaning of the original context.

So, if you are going to take a program space and say, "We cannot transform it," but leave out of it the means of combination and recombination in between and of evolution by selection, I am certain that your program will not produce sense; but if you put it in there the machine gets there so fast it is surprising.

DR. SCHUTZENBERGER: What I have said is that insofar as principles have been explicitly stated, I have to deal with the whole space. To answer your question, one might believe that, in fact, life is using only extremely restricted subspaces of both spaces. What I am asking you, in all humility, is to provide me with a formal principle which would define those spaces, or to provide me with conceptual examples in which such spaces could be defined, even at the very modest level where they would have all the nice properties of matching. This has been done in a sense, at the Sewall Wright level: that is, on the space of parameters which by construction is correlated with the real world space. What I say is that such a type of restriction needs new conceptual tools, or principle, or what-have-you.

The Chairman, DR. WADDINGTON: I want Dr. Weisskopf to speak, but may I recommend that you have a talk in private with Alex Comfort; you can do it on his computer.

DR. WEISSKOPF: I want to analyze the difference of opinion between Schutzenberger and the rest of the world. This is, I think, the following: Schutzenberger says that in the typographical space, the overwhelming number of changes that can be done at random have absolutely no meaning, and he puts in support of it the fact that if you have a computer, and you change the program at random, it always is destroyed.

The other side says that that isn't so. The kind of program which genetics has produced with the 3-letter code is such that it isn't so. I think that is what Lewontin says, that a lot of changes, maybe not an overwhelming number but a large percentage, do make sense in the biochemical sense of the word, and here I think is the discrepancy.

DR. SCHUTZENBERGER: There is no discrepancy. I am asking for you to tell me what principle to use.

The Chairman, DR. WADDINGTON: I regret we will have to leave this discussion at the moment; I think Dick Lewontin's is the next paper.

ON PRODUCTS OF FINITE DIMENSIONAL STOCHASTIC MATRICES[1]

M. P. SCHÜTZENBERGER

1. In what follows, P is the monoid of all $p \times p$ stochastic matrices where p is a fixed natural number. For $a, a' \in P$, we let βa denote the "type" of a [1], i.e. the set of all pairs of indices (j, j') such that the element $a_{j,j'}$ of a is positive and we set $\|a - a'\| = \mathrm{Max}_j \sum_{j'} |a_{j,j'} - a'_{j,j'}|$. Letting ϵ and ω be two fixed positive quantities and $P(\omega)$ be the subset of all $a \in P$ having no positive element less than ω, we intend to verify the following partial generalization of a theorem of Wolfowitz [1].

PROPERTY. *There exists a natural number ν_* such that any product of more than ν_* matrices of $P(\omega)$ admits at least one nontrivial subproduct a which satisfies*

$$\beta a = \beta a^2 \quad \textit{and} \quad \operatorname*{Sup}_{n,n' \in N} \|a^{1+n} - a^{1+n'}\| \leqq \epsilon.$$

Our number ν_* is quite extravagant and examples such as $\lim_{n \to \infty} \prod_{0 \leq i < n} (x^{m_i} y)$ where the integers m_i grow fast enough,

$$x = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

indicate that little information on an infinite product of stochastic matrices is gained when knowing that for each positive ϵ it admits an infinity of subproducts a $(= x^{m_i})$ satisfying the relations stated in the Property (cf. [2]).

I am most indebted to Professor J. Wolfowitz for many suggestions and advice which have led to the writing of this note.

2. **Verification of the property.** We say that two products $x_1 x_2 \cdots x_n$ and $x'_1 x'_2 \cdots x'_{n'}$ of matrices x_i, x'_i are *β-equivalent* iff $n = n'$ and $\beta x_i = \beta x'_i$ for $i = 1, 2, \cdots, n$. They are *nontrivial* iff $n > 0$.

Let $q = (2^p - 1)^p$ $(= \mathrm{Card}\ \beta P)$ and define inductively a map

Received by the editors September 9, 1966.

[1] Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of the RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors.

This paper has been sponsored in part by the U. S. Air Force under contract AF61(052)-945.

ν: $\boldsymbol{N}\to\boldsymbol{N}$ and a sequence $(n_0, n_1, \cdots, n_q)$ of natural numbers by the following conditions:

$\nu(0)=1$; for each $n\in\boldsymbol{N}$, $\nu(n+1)=(1+q^{\nu(n)})\cdot\nu(n)$.

$n_0=1$; for each $i\in N$, $n_{i+1}=1+n_i+$the least positive number m such that $1-\omega^{\nu(ni)}$ to the power 2^m-1 is $\leqq\epsilon/20$.

REMARK 1. *Any product of $\nu_*=\nu(n_q)$ matrices of $P(\omega)$ admits a subproduct $a=h_1h_1'h_2h_2'h_3\cdots h_{2s+1}h_{2s+1}'$ where*

(i) *all the $2s+1$ subproducts h_i are β-equivalent products of s' matrices of $P(\omega)$ and $(1-\omega^{s'})^s\leqq\epsilon/20$;*

(ii) *$\beta h_1=\beta a\cdot\beta h_1$ and $\beta a=\beta a^2$.*

PROOF. Call 0-*sesquipower* any nontrivial product and, inductively, say that a product is a $(n+1)$-*sesquipower* iff it has the form $hh'h''$ where h' is arbitrary and where h and h'' are β-equivalent n-sesquipowers.

We verify first that any product of $\nu(n)$ matrices admits at least one n-sesquipower as a subproduct.

Indeed, it is trivial for $n=0$ since $\nu(0)=1$. If it is true for n and if f is a product of $\nu(n+1)$ matrices, the definition of ν implies that $f=f_1f_2\cdots f_{\bar q}$ $(\bar q=1+q^{\nu(n)})$ where each f_i is a product of $\nu(n)$ matrices. Since $q^{\nu(n)}$ is precisely the number of classes of β-equivalent product of $\nu(n)$ matrices, at least two of these subproducts (say f_j and $f_{j'}$) are β-equivalent. By the induction hypothesis we have $f_j=g_jhg_j'$; $f_{j'}=g_{j'}h''g_{j'}'$ where h and h'' are β-equivalent n-sesquipower and the statement is verified since f admits the subproduct $hh'h''$ where $h'=g_j'f_{j+1}f_{j+2}\cdots f_{j'-1}g_j'$.

In particular, if f is a product of ν_* matrices it admits a n_q-sesquipower k_q as a subproduct and for $j=q-1, q-2, \cdots, 0$; k_q admits a n_j-sesquipower k_j as a right subproduct. Again because of $q=\mathrm{Card}\,\beta P$, at least two of these products (say $k_{j'}$ and k_j) have the same type. We can write $k_{j'}=h_1h_1'h_2\cdots h_{2s+1}h_{2s+1}'k_j$ where $2s+2=2^nj'-^nj$ and where all the subproducts h_i are β-equivalent to k_j. The conditions (i) of the Remark are automatically satisfied because of our choice of the subsequence (n_j) when we take $a=h_1h_1'h_2\cdots h_{2s+1}h_{2s+1}'$ and we have $\beta h_1=\beta a\cdot\beta h_1$ since h_1, k_j and $k_{j'}=ak_j$ have the same image by β. The equation $\beta a=\beta a^2$ follows instantly from $\beta k_{j'}=\beta k_j=\beta h_1$ when multiplying on the right $k_{j'}=ak_j$ by $h_1'h_2\cdots h_{2s+1}h_{2s+1}'$. The remark is verified.

REMARK 2. *For each given natural number n there exist a nonnegative quantity $\epsilon'\leqq\epsilon/10$ and two matrices d, $d'\in P$ that satisfy $a^{1+n}=(1-\epsilon')\cdot d+\epsilon'\cdot d'$ and $d=d\bar a d$ where $\bar a=\lim_{m\to\infty}a^m$.*

PROOF. We identify the indices $1, 2, \cdots, p$ with the states of the

Markov chain defined by the matrix a and we suppose that it has r ergodic classes $E_1, E_2, \cdots, E_r$.

For each $x \in P$, let

$$\pi x = \mathrm{Inf}\{\eta \in [0, 1] : x = (1-\eta)\cdot x_r + \eta \cdot x_p ; x_r \in \overline{P}_r ; x_p \in P\}$$

where $\overline{P}_r$ (resp. $\overline{P}_p$) denotes the convex closure of the set P_r (resp. P_p) of all matrices $y \in P$ having entries 0 or 1 only and at most r (resp. p) nonzero columns. Thus, unless $\pi x = 1$, we have $1 - \pi x \geqq$ the least positive entry of x. Further, $\pi(xx') \leqq \pi x \cdot \pi x'$ for any x, $x' \in P$ since $P = \overline{P}_p$ and $P_r \subseteq P_p P_r P_p$ (cf. [3]).

In particular, $\pi a < 1$ because the relation $\beta a = \beta a^2$ implies that the type of any row of a contains at least one of the r ergodic classes. Taking $\beta k_{j'} = \beta k_j = \beta a \cdot \beta k_j$ into account, we deduce $\pi k_j < 1$, hence $\pi h_i < 1 - \omega^{s'}$ $(i = 1, 2, \cdots, 2s+1)$ since each h_i is a product of s' matrices of $P(\omega)$ that is β-equivalent to k_j.

Let us now define $b = a^n h_1 h_1' \cdots h_s h_s'$; $c = h_{s+1} h_{s+1}' \cdots h_{2s+1} h_{2s+1}'$; $d = b_r c_r$ $(b_r, c_r \in \overline{P}_r)$; $\epsilon' = \pi b + \pi c - \pi b \cdot \pi c$. Because of the submultiplicative character of the map π and $(1-\omega^{s'})^s \leqq \epsilon/20$, we have $\pi b, \pi c \leqq \epsilon/20$, hence $\epsilon' \leqq \epsilon/10$ and $a^{1+n} = (1-\epsilon')\cdot d + \epsilon' \cdot d'$ for a suitable $d' \in P$. Further, $\beta d \subseteq \beta a^{1+n} = \beta a$ and $\beta(d\bar{a}d) \subseteq \beta a$ because of $\beta \bar{a} \subseteq \beta a$. Since d and $d\bar{a}d$ are stochastic matrices, this shows that they have at least r characteristic roots equal to 1. To verify $d = d\bar{a}d$ we have only to check that the dimension of the null space of d has its maximal value $p-r$, since then it will follow that d and $d\bar{a}d$ are two commuting idempotent matrices having the same rank.

Consider any index i belonging to some ergodic class $E_{r'}$ $(1 \leqq r' \leqq r)$. Since $\beta(b_r c_r) \subseteq \beta a$ and since $E_{r'}$ is precisely the type of the ith row of a, we see that the type of the ith row of b_r must be contained in the set $E'_{r'}$ of the indices i' such that the type of the i'th row of c_r is contained in $E_{r'}$. The r sets $E'_{r'}$ are pairwise disjoint. Thus, since $b_r, c_r \in \overline{P}_r$, on the one hand the index of any nonzero column of b_r belongs to $\bigcup\{E'_{r'} : 1 \leqq r' \leqq r\}$ and, on the other hand, the type of any nonzero column of each $y \in P_r$ satisfying $\beta y \subseteq \beta c_r$ contains one (and only one) of the sets $E'_{r'}$.

Let $e'_{r'}$ be the diagonal matrix such that for any $j, j' = 1, 2, \cdots, p$, its (j, j') entry is equal to 1 or to 0 depending upon $j = j' \in E'_{r'}$ or not and $e' = e'_1 + e'_2 + \cdots + e'_r$. The first statement above implies that $d = b_r c_r = b_r e' c_r$ while the second one shows that all the nonzero rows of each matrix $e'_{r'} c_r$ are equal, hence that the null space of $e' c_r$ has dimension at least $p-r$. Remark 2 is verified.

Substituting $(1-\epsilon')\cdot d + \epsilon' \cdot d'$ for a^{1+n} in the right member of

$a^{1+n}-\bar{a}=a^{1+n}-a^{1+n}\bar{a}a^{1+n}$ and recalling that $\|x\|=1$ for any $x\in P$, we obtain

$$\begin{aligned}\|a^{1+n}-\bar{a}\| &= \epsilon'\cdot\|(1-\epsilon')(d-d\bar{a}d'-d'\bar{a}d)+d'-\epsilon'\cdot d'\bar{a}d'\| \\ &\leqq 5\epsilon' \leqq \epsilon/2.\end{aligned}$$

In view of the triangular inequality, this concludes the verification of the Property.

References

1. J. Wolfowitz, *Products of indecomposable aperiodic stochastic matrices*, Proc. Amer. Math. Soc. **14** (1963), 733–737.

2. N. J. Pullman, *Infinite products of substochastic matrices*, Pacific J. Math. **16** (1966), 536–544.

3. J. Larisse et M. P. Schützenberger, *Sur certaines chaines de Markov non homogènes*, Publ. Inst. Statist. Univ. Paris **13** (1964), 57–66.

Faculté des Sciences, Paris and
RAND Corporation

Reprinted from INFORMATION AND CONTROL, Volume 11, No. 4, October 1967

INFORMATION AND CONTROL **11**, 396–401 (1967)

On Synchronizing Prefix Codes

MARCEL PAUL SCHÜTZENBERGER

Faculté de Sciences, Paris

A study is made of the possible distribution of the word lengths in a synchronizing prefix code.

INTRODUCTION

Let X^* be the free monoid generated by a fixed finite alphabet X of $k > 1$ elements. A non-empty subset A of XX^* is a *prefix code* iff every word of X^* has at most one left factor in A, i.e. iff $A \cap AXX^* = \emptyset$. It is *synchronizing* iff $X^*\bar{a} \subset A^*$ for some $\bar{a} \in A^*$ where A^* denotes the submonoid generated by A. (See references).

Consider the enumerating sequence $\alpha = (\alpha_n = \textbf{\textit{Card}}\,(A \cap X^n))_{n\in\mathbf{N}}$ of a prefix code A and set $\sigma_n = k^n - \sum_{0<m\leqq n} \alpha_m k^{n-m} = \sigma_{n-1}k - \alpha_n$. We have $\alpha_0 = 0$ and $\sigma_0 = 1$ because of $A \subset XX^*$. Further, X^n is the disjoint union of the sets $S \cap X^n$ and $(A \cap X^m)X^{n-m} (m = 1, 2, \cdots, n)$ where $S = X^*\backslash AX^*$. It follows that $\textbf{\textit{Card}}\,(S \cap X^n) = \textbf{\textit{Card}}\,(X^n) - \sum_{0<m\leqq n} \textbf{\textit{Card}}\,(A \cap X^m).\ \textbf{\textit{Card}}\,(X^{n-m}) = \sigma_n$ showing

$$\sigma_n \geqq 0 \textit{ for all } n \in \mathbf{N}. \tag{1}$$

Assume that A is synchronizing and $\bar{a} \in X^p$. S contains the left factors of its members and no word having $\bar{a}$ as a right factor. Thus $S \cap X^{n+p}$ is a subset of $(S \cap X^n)(X^p\backslash\{a\})$ and

$$\sigma_{n+p} \leqq \sigma_n \,.\, (k^p - 1) \textit{ for some fixed positive } p \textit{ and all } n \in \mathbf{N}. \tag{2}$$

Finally, let d be the greatest common divisor of the elements of $N_\alpha = \{n \in \mathbf{N}: \alpha_n \neq 0\}$, i.e., let $A \subset (X^d)^*$. Since $A^* \subset (X^d)^*$, $f\bar{a} \subset A^* (f \in X^*)$ is possible only if $f \in (X^d)^*$. Thus

$$1 \textit{ is the g.c.d. of the elements of } N_\alpha\,. \tag{3}$$

We intend to verify the following converse property.

PROPERTY. *Let $\alpha = (\alpha_n)_{n\in\mathbf{N}}$ be a sequence of non-negative integers that*

satisfies $\alpha_0 = 0$, (1), (2) *and* (3). *It is the enumerating sequence of at least one synchronizing prefix code.*

It may be observed that when A is finite, i.e. when $\alpha_n = 0$ for all n larger than some finite value $\bar{n}$, Condition (2) is equivalent to $\sigma_{\bar{n}} = 0$. Indeed, from $\alpha_n = 0$, $(n > \bar{n})$, and $\sigma_{n+1} = \sigma_n k - \alpha_{n+1}$ we deduce $\sigma_{\bar{n}+p} = k^p \sigma_{\bar{n}}$. This implies $\sigma_{\bar{n}} = 0$ in view of $\sigma_{\bar{n}+p} \leqq \sigma_{\bar{n}} . (k^p - 1)$. Reciprocally, if $\sigma_{\bar{n}} = 0$, the hypothesis $0 \leqq \sigma_{n+1} = \sigma_n k - \alpha_{n+1}$ shows that $\alpha_n = \sigma_n = 0$ for all $n > \bar{n}$ and one has $\sigma_{n+\bar{n}} \leqq \sigma_n . (k^{\bar{n}} - 1)$ identically.

We also recall the known fact that $\alpha_0 = 0$ and Condition (1) suffice to insure that a sequence $\boldsymbol{\alpha}$ of non-negative integers is the enumerating sequence of at least one prefix code A. Indeed, let $A_0 = \emptyset$ and, inductively, let A_n be the union of A_{n-1} with an arbitrary set of $\alpha_n' = \boldsymbol{Min}\{\alpha_n , \boldsymbol{Card}\,(X^n \backslash A_{n-1}X^*)\}$ words from $X^n \backslash A_{n-1}X^*$. Each A_n and $A = \bigcup_{0 \leqq n} A_n$ is a prefix code. Suppose $\alpha_m' = \alpha_m$ and $\sigma_m = \boldsymbol{Card}\,(X^m \backslash A_m X^*)$ is already verified for $m < n$. We have $X^n \backslash A_{n-1}X^* = (X^{n-1} \backslash A_{n-1}X^*)X$ since $A_{n-1} \cap X^n = \emptyset$ and $\alpha_n \leqq \sigma_{n-1}k = \boldsymbol{Card}\,((X^{n-1} \backslash A_{n-1}X)X)$ since $0 \leqq \sigma_n = \sigma_{n-1}k - \alpha_n$. Thus $\alpha_n' = \alpha_n$ and $\sigma_n = \boldsymbol{Card}\,(X^n \backslash A_n X^*)$ and the observation is proved.

Finally, to simplify our later discussion, we establish the following remark in which x is any fixed letter of X.

Remark 1. Let $\boldsymbol{\alpha}$ satisfy $\alpha_0 = 0$, (1) and (2). It is the enumerating sequence of a prefix code A such that $S x^{2p} \cap S = \emptyset$. Thus the Property is true when, further, $\alpha_1 \geqq 1$.

Proof. Let $\bar{m}$ be any fixed integer and, for $n \geqq \bar{m}$, let the α_n words of $A_n \backslash A_{n-1}$ be successively chosen so that $fx^r \in A_n \backslash A_{n-1}$, $(f \in X^{n-r})$ only if every word of $X^n \backslash A_{n-1}X^*$ of the form $f'x^{r'}$, $(f' \in X^{n-r'}, r' > r)$ is already taken in A_n. Then to prove $sx^{2p} \notin S$ for each $s \in S \cap X^n$ it suffices to verify that Condition (2) implies $\sigma_n < \sum_{0<m \leqq 2p} \alpha_{n+m}$. Now, by definition

$$0 \leqq \sigma_{n+p} = \sigma_n k^p - \sum_{0 < m \leqq p} \alpha_{n+m} k^{p-m} \tag{4}$$

Hence, by (2),

$$\sigma_n \leqq \sum_{0<m \leqq p} \alpha_{n+m} k^{p-m}. \tag{5}$$

Replacing n by $n + p$ in (5) and using (4) we get

$$\sigma_n k^p - \sum_{0<m \leqq p} \alpha_{n+m} k^{p-m} = \sigma_{n+p} \leqq \sum_{0<m \leqq p} \alpha_{n+p+m} k^{p-m}$$

that is,

$$\sigma_n \leqq \sum_{0<m\leqq p} \alpha_{n+m}k^{-m} + \sum_{0<m\leqq p} \alpha_{n+p+m}k^{-m} \leqq \sum_{0<m\leqq 2p} \alpha_{n+m}\,,$$

and the first part of the Remark is proved. When $\alpha_1 = 1$, we can take $\bar{m} = 0$ and then, $x \in A$. Letting $\bar{a} = x^{2p}$ we have $S\bar{a} \subset A^*$. Hence $X^*\bar{a} \subset A^*$ because A is a prefix code and therefore every word of X^* has one and only one factorisation in the form as ($a \in A^*$, $s \in S$), i.e. because $X^* = A^*S$.

CONSTRUCTION OF THE PREFIX CODE A

We consider a fixed sequence $\boldsymbol{\alpha}$ satisfying $\alpha_0 = \alpha_1 = 0$, (1), (2), (3) and we let x and y be two distinct letters of X. We set the following:

$\bar{q}$ = the least member of N_α such that 1 is the g.c.d. of the elements of N_α, less or equal to $\bar{q}(2 < \bar{q} < \infty)$.

$\bar{n}$ = the supremum of the elements of $N_\alpha(\bar{q} \leqq \bar{n}$ and $\bar{n} = \infty$ iff $\sigma_n > 0$ for all $n \in \mathbf{N})$.

Define inductively a sequence $(\tau_n)_{n\in\mathbf{N}}$ by $\tau_0 = 0$ and $\tau_n = \boldsymbol{Max}\{0, 1 + \tau_{n-1} - \alpha_n\}$. We have $\sigma_n > \tau_n$ for all $n < \bar{n}$. Indeed, this is true for $n = 0$; for $n < \bar{n}$ it follows from $\sigma_n > 0$ and the induction hypothesis since $\sigma_n - \tau_n$ is equal to σ_n or to $\sigma_{n-1}k - 1 - \tau_{n-1} = (\sigma_{n-1} - \tau_{n-1}) + \sigma_{n-1}(k-1) - 1$, depending upon $\tau_n = 0$ or $= 1 + \tau_{n-1} - \alpha_n$.

Remark 2. Let $1 + \tau_{n-1} - \alpha_n \geqq 0$ for all $n \geqq \bar{q}$. The Property is true for $\boldsymbol{\alpha}$.

Proof. We first show that the hypothesis entails $k = 2$ and $\sigma_n = \alpha_n = 1$ for all $n \geqq \bar{q}$, hence $\bar{n} = \infty$. Indeed for $n \geqq \bar{q}$ we have

$$\begin{aligned}\sigma_n - \tau_n - 1 &= \sigma_{n-1}k - \alpha_n - 1 - \tau_{n-1} + \alpha_n - 1\\ &= (\sigma_{n-1} - \tau_{n-1} - 1)k + \tau_{n-1}(k-1) + k - 2.\end{aligned} \tag{6}$$

It follows that $\sigma_n - \tau_n - 1$ is identically zero because, otherwise, we would have for every $m \geqq 0$ the inequality $\sigma_{n+mp} - \tau_{n+mp} - 1 \geqq k^{mp}$ in contradiction with Condition (2) which imposes $\sigma_{n+mq} \leqq \sigma_n(k^q - 1)^m$. Thus, for $n \geqq \bar{q}$, we must have successively $k = 2$, $\tau_{n-1} = 0$, $\sigma_{n-1} = 1$ and $\alpha_n = 1$ which follow from $1 = \sigma_n = \sigma_{n-1}k - \alpha_n = 2 - \alpha_n$.

Using the construction described in Remark 1, we choose the words of the sets $A_n \backslash A_{n-1}$ in such a way that for $n \geqq \bar{q}$, $A_n \backslash A_{n-1} = \{x^{n-1}y\}$. Then S consists of words of lengths $<\bar{q}$ and of x^*. Let $\bar{a} = x^r y$ where $r \geqq 2\bar{q}$. If $s \in S$ has the form $x^{r'}$), we have $s\bar{a} = x^{r'+r}y \in A$; if not, s

has length $<\bar{q}$, sa does not belong to S and, accordingly, $sa = a'x'y$ where $a' \in A$ and $x'y \in A$. The Remark is verified.

Thus we can now define

$$q = \text{the least integer} \geqq \bar{q} \text{ such that } 1 + \tau_{q-1} - \alpha_q < 0.$$

Remark 3. Let α satisfy $\alpha_0 = \alpha_1 = 0$, (1), (2), (3) and $q < \infty$. It is the enumerating sequence of a prefix code A such that:

$$x^q \in A, \tag{7}$$

$$B = A \cap x^*yx^* \text{ consists of } q \text{ words } b_i = x^iyx^{\lambda_i - i - 1} \tag{8}$$

$(i = 0, 1, \cdots, q-1)$ where $\lambda_i \geqq i - 1$;

$$\lambda_i \leqq q \text{ identically with equality for } i \geqq q - \tau_{q-1} - 1; \tag{8.1}$$

$$1 \text{ is the g.c.d. of } \{\lambda_0, \lambda_1, \cdots, \lambda_{q-1}\}; \tag{8.2}$$

$$Sx^{rq} \cap S = \emptyset \text{ where } rq \geqq 2p. \tag{9}$$

Proof. We again use the construction of Remark 1. We can take $x^q \in A_q \backslash A_{q-1}$ since $\alpha_q \neq 0$ and $\sigma_n > 0$ for $n < q$ because $q \in N_\alpha$.

Let (for $n \leqq q$)

$Y_n = \{x^iyx^{n-1-i}, \quad i = 0, 1, \cdots, n-1\}$,

$B_0 = B_1 = \emptyset$ and, inductively,

$B_n =$ the union of B_{n-1} with the $\beta_n = \textbf{\textit{Min}}\{\alpha_n, \textbf{\textit{Card}}\,(Y_n \backslash B_{n-1}x^*)\}$ words $b_i = x^iyx^{n-1-i}$ of $Y_n \backslash B_{n-1}x^*$ for which i has its least values.

Setting $T_n = Y_n \backslash B_n x^* = (\{x^{n-1}y\} \cup T_{n-1}x) \backslash (B_n \backslash B_{n-1})$ and $\tau_n' = \textbf{\textit{Card}}\, T_n$, we have $\beta_n = \textbf{\textit{Min}}\{\alpha_n, 1 + \tau'_{n-1}\}$ and $\tau_n' = \textbf{\textit{Max}}\{0, 1 + \tau'_{n-1} - \beta_n\} = \textbf{\textit{Max}}\{0, 1 + \tau'_{n-1} - \alpha_n\}$. Thus, by induction, $\tau_n' = \tau_n$ and $\tau_q = 0$ follows from our choice of q. This proves (8.1), and (8.2) follows from $q \geqq \bar{q}$ and the fact that by construction $\beta_n > 0$ for each $n \in N_\alpha$ less or equal to q.

Finally, (9) results from the same reasons as in Remark 1.

It only remains to verify that A is synchronizing. In view of (7) and (9) and of $X^* = A^*S$ it suffices to show that the submonoid of A^* generated by $C = \{x^q\} \cup B$ contains at least one word $\bar{c}$ such that $x^m\bar{c} \in A^*$ for every m in the interval $I = \{0, 1, \cdots, q-1\}$. To do this we first verify the following Remark in which, for any $z \in \mathbf{Z}$, $[z]_{q'}$ denotes the least non-negative integer congruent of z modulo q' and for $d \in \mathbf{N}$, $I_d = \{q-1-d, q-d, q+1-d, \cdots, q-1\}$:

Remark 4. Let t be a positive integer less than q and define two maps u and v of I into itself by letting for each $i \in I$

$$\text{i.u} = [i + 1]_q \text{ and i.v} = [i - \lambda_i + 1]_q$$

where, identically, $1 + i \leqq \lambda_i \leqq q$ and $\lambda_i = q$ iff $i \in I_t$. If the g.c.d. of the numbers $\{\lambda_0, \lambda_1, \cdots, \lambda_{q-1}\}$ is 1, the monoid M generated by u and v contains an element sending I onto 0.

Proof. For $d \in \mathbf{N}$, let M_d denote the subsemigroup of M consisting of all $m \in M$ such that i.m $\in I_d$ for $i \in I$ and $i.m = i$ for $i \in I_d$. By definition $i.vu^{q-1} = q - (\lambda_i - i) =$ an element strictly greater than itself if $i \in I \backslash I_t$ and $=$ an element of I_t if $i \in I_t$. Thus some large enough power of vu^{q-1} belongs to M_t.

Let $d = \textbf{\textit{Min}} \{d' : M_{d'} \neq \emptyset\}$. If $d = 1$ and $m \in M_1$ the proof is complete because mu sends I onto 0. Thus from now on we can assume $d > 1$ and we verify the following statement: M_d consists of a single map m sending each $q - i \in I$ onto $q - [i]_d$.

Indeed, by the definition of M_d we have $(q - i) \cdot m = q - [i]_d$ for every $m \in M_d$ and $i \in I_d$. For the sake of contradiction, let $j > d$ be the least value for which $(q - j) \cdot m \neq q - [j]_d$, $(m \in M_d)$. Consider the map $u^{j-d-1}m$. It sends I onto I_d and its restriction to I_d is a permutation. Thus one of its positive powers, say m', belongs to M_d and $(q - d - 1) \cdot m' = q - d' \neq q - 1$ because of $(q - j) \cdot m \neq q - [j]_d$. It follows that we can assume $m = m'$, that is $j = d + 1$.

Under this supplementary hypothesis mu^{q-1} has the following properties:

(a) sends I onto the interval $\{q - 1 - d, q - d, q + 1 - d, \cdots, q - 2\}$,

(b) reduces to a permutation on $J' = \{q - 1 - d, q - d, \cdots, q - 1 - d'\}$,

(c) sends every $i \in I_d$, onto $i - 1$.

Thus one of its positive powers, say m'', sends I onto J' and reduces to the identity on J'. Multiplying m'' on the left and on the right by suitable powers of u, we obtain a map which belongs to $M_{d+1-d'}$ where $d + 1 - d' < d$ by construction. Since this contradicts the minimal character of d, the statement is verified.

Consider now $vu^{q-1}m$ where $\{m\} \in M_d$. Since vu^{q-1} reduces to the identity on I_t and $t \geqq d$, this map also belongs to M_d. However, $m = vu^{q-1}m$ is possible only if for each $i \in I$ one has $i \cdot vu^{q-1} = [i]_d$, that is, according to the definition of u and of v, only if all the numbers λ_i are

congruent to 0 modulo d. This shows $d = 1$ when the g.c.d. of the λ_i is 1 and it establishes the Remark.

To conclude, the proof to each $m \in M$ of the form $m = z_1 z_2 \cdots z_r$, where $z_i = u$ or v, we associate the word μm obtained by replacing in m every $z_i = u$ by x and every $z_i = v$ by yx^q, $(i = 1, 2, \cdots, r)$. By $x^i y x^{\lambda_i - i - 1} \in A$, $x^q \in A$ and our definition of the maps u and v, we have identically $i \cdot m = i'$ iff $x^i \mu m = a x^{i'}$ where $a \in A^*$. Thus $x^* \mu(mu) \subset A^*$ where $\{m\} = M_1 \neq \emptyset$ and the Property is entirely proved.

RECEIVED: JULY 25, 1967

REFERENCES

GILBERT, E. N. AND MOORE, E. F. (1959), Variable length binary encodings. *Bell System Tech. J.* **38,** 933–968.

GOLOMB, S. W. AND GORDON, B. (1965), Codes with bounded synchronization delay. *Inform. Control.* **8,** 355–372.

MANDELBROT, B. (1954), On recurrent noise limiting coding. *Proc. Symp. Inform. Networks.* pp. 146–148, New York, N. Y.

NEUMANN, P. G. (1962), Efficient error limiting variable length codes. *IRE Trans.* **IT-8,** 292–304.

WINOGRAD, S. (1964), Input error limiting automata. *Commun. Comp. Mach.* **11,** 338–351.

Année 1968

Bibliographie

[1] Marcel-Paul Schützenberger. A remark on acceptable sets of numbers. *J. Assoc. Comput. Mach.*, 15 :300–303, 1968.

[2] Marcel-Paul Schützenberger. On an enumeration problem. *J. Combinatorial Theory*, 4 :219–221, 1968.

[3] Marcel-Paul Schützenberger. Sur certains semi-groupes de matrices non négatives. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 9 :265–269, 1968.

[4] Noam Chomsky and Marcel-Paul Schützenberger. Théorie algébrique des langages "context-free". In Maurice Gross, editor, *Les modèles en linguistique*, volume 9 of *Langages*, pages 77–118. Didier/Larousse, mars 1968. Traduit par G. Fauconnier.

A Remark on Acceptable Sets of Numbers

MARCEL PAUL SCHÜTZENBERGER*

The RAND Corporation, Santa Monica, California

ABSTRACT. Two negative results concerning the so-called acceptable sets of numbers are extended to the case of arbitrary context-free languages with the help of conventional analytic techniques.

KEY WORDS AND PHRASES: acceptable sets, automata, context-free languages, regular sets, finite automata

CR CATEGORIES: 5.22, 5.23, 5.29

Introduction

In what follows, X^* denotes the free monoid with neutral element e that is generated by a fixed finite nonempty set X, $\mathbf{N}$ denotes the nonnegative integers, and $\mathbf{L}$ is the family of all context-free languages on X [4, 7]. We consider a fixed crossed homomorphism ρ of X^* into the ring $\mathbf{Z}$ of rational integers; ρ is defined by its restriction to X and by the identity

$$\rho ff' = \rho f \cdot \alpha f' + \rho f', \qquad f, f' \in X^*, \tag{1}$$

where α is a homomorphism of X^* into the multiplicative structure of $\mathbf{Z}$. Thus $\rho e = 0$ by definition. We make the assumption that $|\alpha x| > 1$ for all $x \in X$. This condition is satisfied when $X = \{0, 1\}$, $\alpha 0 = \alpha 1 = 2$, $\rho 0 = 0$, and $\rho 1 = 1$, in which case ρf is the number whose binary expansion is f.

The problem of showing that certain remarkable subsets of $\mathbf{Z}$ cannot have the form $\rho L = \{\rho f : f \in L\}$ for $L \in \mathbf{L}$, or for L in some given subfamily of $\mathbf{L}$, was first attacked by Elgot [6] using metamathematical methods. Recently, Minsky and Papert [8] have considerably generalized these results by a delicate analysis of the asymptotic properties of the function $\mathbf{Card}\{f \in L : |\rho f| < n\}$ of the nonnegative integer n. Being concerned with the subfamily of the so-called "regular sets," they indicated the possibility of extending their method to arbitrary languages $L \in \mathbf{L}$. (See also [2, 5, 10].) We show here two applications of the techniques of classical analysis to examples already discussed by other authors.

We rely on the following result [1]:

THEOREM [Bar-Hillel, Shamir, and Perles]. *Let $L \in \mathbf{L}$. Except for the members of a finite subset L_0 of L, every word $f \in L$ admits at least one factorization $f = g''h'g'hg$ such that $h' \neq e$ and that $H = \{h_n = g''h'^n g'h^n g : n \in \mathbf{N}\}$ is contained in L.*

This work was supported in part by contract with the US Air Force, AF 61(052)945. Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of the RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors.

* Present address: Faculté des Sciences de Paris, Paris, France

Journal of the Association for Computing Machinery, Vol. 15, No. 2, April 1968, pp. 300-303.

Without loss of generality we always assume $g = e$ when $h = e$. A straightforward computation gives

$$\rho h_n = b'' + b'(\alpha h)^n + b(\alpha h h')^n \tag{2}$$

where, setting $\beta f = \rho f(1 - \alpha f)^{-1}$ when $f \neq e$, and $\beta e = 0$, we have

$$b'' = \rho g + \beta h \cdot \alpha g;$$

$$b' = \beta h' \cdot \alpha g' g + \rho g' \cdot \alpha g - \beta h \cdot \alpha g;$$

$$b = \rho g'' \cdot \alpha g' g - \beta h' \cdot \alpha g' g.$$

In particular, $b'' = 0$ when $h = e$. Further, ρH is finite if and only if it reduces to $\{\rho h_0\} = \{\rho g'' g' g\}$.

First Example

Let $L \in \mathbf{L}$ and $k \in \mathbf{N}$ be such that no member of ρL has more than k different prime divisors. Then the set $\mathbf{Prm}(\rho L)$ of all prime divisors of the members of ρL is a finite set contained in $\mathbf{Prm}(\rho L_0 \cup \alpha X)$.

Let $f \in L \backslash L_0$ and assume that $\mathbf{Prm}(\rho f') \subseteq \mathbf{Prm}(\rho L_0 \cup \alpha X)$ is already verified for every $f' \in L$ strictly shorter than f. Since $f \notin L_0$, we can write $f = h_1 = g'' h' g' h g$ as indicated in the Introduction; and the result is still true for f if ρH is finite since then we know that $\rho f = \rho h_0$ where $h_0 = g'' g' g$ is strictly shorter than f. Thus we can assume that ρH is infinite. According to (2), ρh_n is the coefficient of t^n in the Taylor series expansion of the rational function

$$r(t) = b'' \cdot (1 - t)^{-1} + b' \cdot (1 - t \cdot \alpha h)^{-1} + b \cdot (1 - t \cdot \alpha h h')^{-1}$$

of the variable t. Noting that $r(t)$ has a zero for $t = \infty$, a well-known theorem of Polyá [9, p. 14, Satz II] indicates that $\mathbf{Prm}(\rho H)$ is infinite unless $r(t)$ has the form

$$\sum_{0 \leq i < m} c_i t^i \cdot (1 - c_i t^m)^{-1}$$

for some finite m. Now this condition is satisfied only if $b'' = b'b = 0$, and then ρH has the form

$$\{b' \cdot (\alpha h)^n : n \in \mathbf{N}\} \quad \text{or} \quad \{b \cdot (\alpha h h')^n : n \in \mathbf{N}\}.$$

Furthermore, $\rho h_0 = b'$ or b; and since α is a homomorphism, $\mathbf{Prm}(\alpha h)$ and $\mathbf{Prm}(\alpha h h')$ are contained in $\mathbf{Prm}(\alpha X)$. Thus $\mathbf{Prm}(\alpha H)$ is contained in $\mathbf{Prm}(\rho h_0) \cup \mathbf{Prm}(\alpha X)$ and the verification is concluded.

Second Example

Let $L \in \mathbf{L}$ and the polynomial π be such that **Card** $\rho L = \infty$ *and* $\rho L \subseteq \pi \mathbf{Z} (= \{\pi z : z \in \mathbf{Z}\}) \subseteq \mathbf{Z}$. *Then π is a trinomial, i.e., $\pi t = c(t + s)^d + c'(t + s)^{d'} + c''$ for some constant s.*

We can assume $\pi t = \sum_{0 \leq j \leq d} c_j t^{d-j}$ where the degree d of π is at least 3, since otherwise π is automatically a trinomial. Since ρL is infinite, L must contain a subset H of the type described in the introduction for which ρH is infinite. We set $a' = \alpha h$, $a = \alpha h h'$.

The hypothesis $\rho L \subseteq \pi \mathbf{Z}$ implies the existence of a map, denoted by ζ_n, of $\mathbf{N}$ into $\mathbf{Z}$ such that $\pi\zeta_n = \rho h_{nd} = ba^{nd} + b'(a')^{nd} + b''$ identically.

Let ζ_n' satisfy $c_0\zeta_n' = \rho h_{nd} - b'' = ba^{nd} + b'a'^{nd}$. We have

$$\zeta_n' = a^n(r_0 + \sum_{0<i} r_i(a'^{dn}/a^{dn})^1)$$

where $r_0 = (bc_0^{-1})^{1/d}$. Thus letting $\zeta_n = \zeta_n'(1 + \epsilon_n')$, it follows from $\zeta_n = \rho h_{nd}$ that

$$(1 + \epsilon_n')^d + \sum_{0<i\leq d} \zeta_n'^{-j}(1 + \epsilon_n')^{d-j} c_j c_0^{-1} = 1 + b''\zeta_n'^{-d}c_0^{-1},$$

showing that $\epsilon_n' = r'\zeta_n'^{-1} + \epsilon_n''\zeta_n'^{-2}$ where r' is a constant and ϵ_n'' has bounded modulus. Accordingly, if $|a'^d| \leq |a^{d-1}|$ we can write $\zeta_n = r_0a^n + r' + \epsilon_n$ where $|\epsilon_n|$ tends to zero at least as fast as $\max\{|a^{-n}|, |a'^{dn}a^{-dn+n}|\}$. If $|a'^d| > |a^{d-1}|$ there exists a finite integer k such that $|a'^{kd}/a^{kd-1}| > 1 \geq |a'^{kd+d}/a^{kd+d-1}|$, and then we can write $\zeta_n = r_0a^n + \sum_{0<i\leq k} r_ia'^{idn}a^{-idn+n} + r' + \epsilon_n$ where $|\epsilon_n|$ tends to zero at least as fast as $|a'^{(kd+d)n}a^{-(kd+d)n+n}|$.

In the first case, we have $\zeta_{n+1} - a\zeta_n = r'(a-1) + (\epsilon_{n+1} - a\epsilon_n)$. Since the left member of this relation is an integer and since $|\epsilon_{n+1} - a\epsilon_n|$ tends to zero for $n \to \infty$ we have in fact that, for all large enough $n \in \mathbf{N}$, $\epsilon_{n+1} - a\epsilon_n$ is equal to some fixed $r'' \in \mathbf{Z}$. Thus, for all large enough n, ζ_n satisfies a linear recurrence relation $\zeta_{n+1} - a\zeta_n = r'(a-1) + r''$; hence $\zeta_n = sa^n + s'$ where s and s' are constant rational numbers. Bringing this expression into the relation $\pi\zeta_n = \rho h_{nd}$ and identifying terms, we see instantly that π must have the form $c(t + s'')^d + c'(t + s'')^{d'} + c''$, and further that a' and d' must be such that $a'^d = a^{d'}$. This concludes the verification in this case.

If $|a'^d/a^{d-1}| > 1 \geq |a^{2d}/a^{2d-1}|$ (i.e., if $k = 1$), we have

$$\zeta_n = r_0a^n + r_1a'^{dn}a^{-dn+n} + r' + \epsilon_n.$$

Thus $a^{d-1}\zeta_{n+2} - (a^d + a'^d)\zeta_{n+1} + aa'^d\zeta_n$ is equal to a constant, plus a term whose modulus tends to zero when $n \to \infty$. As above we conclude that ζ_n satisfies a linear recurrence for all large enough n and, in fact, that $\zeta_n = sa^n + s'a'^{dn}a^{-dn+n} + s''$. More generally, for arbitrary $k > 1$, we replace the polynomial $\omega_1 = a^{d-1}t^2 - (a^d + a'^d)t + aa'^d$ used above by the polynomial ω_k of degree $k+1$ whose roots are $\{a, a'^da^{-d+1}, a'^{2d}a^{-2d+1}, \ldots, a'^{kd}a^{-kd+1}\}$ and whose coefficient of t^{k+1} is the product $a^{d-1}a^{2d-1}\ldots a^{kd-1}$. Substituting ζ_{n+i} for t^i in ω_k we obtain an expression which is equal to a constant plus a term whose modulus tends to zero for $n \to \infty$, and we conclude that in all cases ζ_n can be expressed as a finite sum

$$s_0a^n + \sum_{0<i\leq k} s_i(a'^{id}/a^{id-1})^n + s_{k+1}.$$

We now show that this is incompatible with the hypothesis $\pi\zeta_n = \rho h_{nd}$. Indeed, bringing the expression of ζ_n which has been obtained into the equation $\pi\zeta_n = \rho h_{nd}$, we can identify terms. Noting that $ba^{nd} + b'a'^{nd}$ is equal to the sum of the first two terms in the expansion of $c_0\zeta_n^d$, we find that all the other nonconstant terms of $\pi\zeta_n$ must cancel between themselves. Let j be the largest index less than d such that $c_j \neq 0$, and let i be the largest index less than $k+1$ such that $s_i \neq 0$. The

term $(a'^{id}/a^{id-1})^n\ s_{k+1}^{j-1}$ (or the term $(a'^{id}/a^{id-1})^{nj}$ if $s_{k+1} = 0$) in $\zeta_n{}^j$ cannot cancel with any other term. Thus the equation $\pi\zeta_n = \rho h_{nd}$ with integral ζ_n is impossible when $k \geq 1$, and the verification is concluded.

REFERENCES

1. Bar-Hillel, Y., Shamir, E., and Perles, M. On formal properties of simple phrase structure grammars. *Z. Phonetik, Sprachwiss. Kommunikationsforsch. 14* (1961), 143–172; in Bar-Hillel, Y., *Language and Information*, Addison-Wesley, Reading, Mass., 1965, pp. 116–150.
2. Buchi, J. R. Weak second order arithmetic and finite automata. *Z. math. Logik Grund. Math. 6* (1961), 66–92.
3. Cantor, D. G. On arithmetic properties of coefficients of rational functions. *Pacific J. Math. 15* (1965), 55–58.
4. Chomsky, N., and Miller, G. A. Finitary models of language users. In Luce, R. D., Bush, R. R., and Galanter, E. (Eds.), *Handbook of Mathematical Psychology, Vol. 2*, Wiley, New York, 1963, Ch. 13, pp. 419–491.
5. Cobham, A. Sets definable by finite automata. IBM Res. Notes #405, #458, #577 (1964, 1965, 1966).
6. Elgot, C. C. Decision problems of finite automata design and related arithmetics. *Trans. Amer. Math. Soc. 98* (1961), 21–51.
7. Ginsburg, S. *The Mathematical Theory of Context-Free Languages*. McGraw Hill, New York, 1966.
8. Minsky, M., and Papert, S. Unrecognizable sets of numbers. *J. ACM 13* (1966), 281–286.
9. Polyá, G. Arithmetisch Eigenschaften der Reihenentwicklung rationaler Funktionen. *J. reine angew. Math. 151* (1921), 1–31.
10. Ritchie, R. W. Finite automata and the set of squares. *J. ACM 10* (1963), 528–531.

RECEIVED SEPTEMBER, 1966; REVISED SEPTEMBER, 1967

Reprinted from JOURNAL OF COMBINATORIAL THEORY
All Rights Reserved by Academic Press, New York and London
Vol. 4, No. 3, April 1968
Printed in Belgium

On an Enumeration Problem*

M. P. SCHÜTZENBERGER

University of Paris and Department of Electrical Engineering, University of California, Berkeley, California

Communicated by Gian-Carlo Rota

ABSTRACT

We present an answer to a question raised by J. Riordan on the relationship between two families of maps of finite sets.

The following problem has been kindly communicated to me by Dr. J. Riordan.

Let $[n] = \{1, 2,..., n\}$ and define B_n as the set of all maps $\beta : [n] \to [n]$ such that there exists a permutation β^* of $[n]$ satisfying the condition:

For $j = 1, 2,..., n$, $\beta^* j$ is the least integer $\geqslant \beta j$ not already contained in $\{\beta^*1, \beta^*2,..., \beta^*(j-1)\}$.

For instance B_2 consists of the three maps $(\beta 1 = \beta 2 = 1)$, $(\beta 1 = 1; \beta 2 = 2)$, $(\beta 1 = 2; \beta 2 = 1)$, the associated β^* being the identity map for the first two and the inversion $(\beta^*1 = 2, \beta^*2 = 1)$ for the last one. More generally one finds that

$$\text{Card } B_n = (n+1)^{n-1}.$$

As it is well known $(n+1)^{n-1}$ is also the cardinality of the set A_n of all acyclic maps $\alpha: [n] \to [n]$ (i.e., of the $\alpha: [n] \to [n]$ such that $\alpha^{n-1} = \alpha^n$), and it is asked to exhibit a 1-1 correspondence $\beta \to \bar{\beta}$ between B_n and A_n. This we do by induction on n, starting with $n = 2$, where we associate, respectively, the three members of B_2 listed above with the following three maps of A_2 :

$$(\alpha 1 = \alpha 2 = 1), \qquad (\alpha 1 = \alpha 2 = 2), \qquad (\alpha 1 = 1; \alpha 2 = 2)$$

* This research was jointly sponsored under Air Force Office Scientific Research, Office of Aerospace Research, United States Air Force, AFOSR Grants AF-AFOSR-639-65 and AF-61(052)965.

For $n > 2$ we distinguish cases depending upon $\beta^* n = n$, $= 1$, or $=$ any other member of $[n]$.

CASE 1:

$$\beta^* n = n.$$

Assuming $\beta \in B_n$, the value of $\beta^* n$ is the only remaining member of $[n]$ once $\beta^* j$ has been constructed for $j \in 1, 2, \ldots, n-1$. Thus $\beta^* n = n$ implies $\beta j < n$ for every $j \in [n-1]$. Reciprocally, if this condition is met by some map $\beta\colon [n] \to [n]$ we can always define the permutation β^* and we shall have $\beta^* n = n$ whatever the value of βn. Thus our hypothesis amounts to the single requirement that the restriction β_1 of β to $[n-1]$ is a member of B_{n-1} and by the induction hypothesis we have a well-defined $\bar{\beta}_1 \in A_{n-1}$ associated with β_1.

SUBCASE 1.1:

$$\beta n = n.$$

We set

$$\bar{\beta} n = n;$$
$$\bar{\beta} j = n \quad \text{if} \quad j \in [n-1] \quad \text{and} \quad \bar{\beta}_1^{n-2} j = \bar{\beta}_1^{n-1} j;$$
$$\bar{\beta} j = \bar{\beta}_1 j \quad \text{otherwise.}$$

SUBCASE 1.2:

$$\beta n = m < n.$$

We set

$$\bar{\beta} n = m;$$
$$\bar{\beta} j = n \quad \text{if} \quad j \in [n-1] \quad \text{and} \quad \bar{\beta}_1^{n-2} j = \bar{\beta}_1^{n-1} j \neq \bar{\beta}_1^{n-1} m;$$
$$\bar{\beta} j = \bar{\beta}_1 j \quad \text{otherwise.}$$

It is clear that $\bar{\beta} \in A_n$ because, for every $j \in [n]$, $\bar{\beta}^{n-1} j = \bar{\beta}^n j = n$ in Subcase 1.1 and $\bar{\beta}^{n-1} j = \bar{\beta}^n j = \bar{\beta}^n m$ in Subcase 1.2.

Further, the correspondence $\beta \to \bar{\beta}$ is a 1-1 application of the maps $\beta \in B_n$ satisfying $\beta^* n = n$ onto the maps $\bar{\beta} \in A_n$ having a single fixed point.

CASE 2:

$$\beta^* n = 1.$$

This implies $\beta n = 1$ and $\beta j > 1$ for every $j \in [n-1]$. In fact a map $\beta\colon [n] \to [n]$ belongs to B_n and satisfies $\beta^* n = 1$ iff $\beta 1 = 1$ and there exists a map $\beta_2 \in B_{n-1}$ such that $\beta(j+1) = 1 + \beta_2 j$ for every $j \in [n-1]$. Then clearly $\beta^*(j+1) = 1 + \beta_2^* j$.

As above, we derive $\bar{\beta}$ from $\bar{\beta}_2$ by setting simply $\bar{\beta}n = n$ and $\bar{\beta}j = \bar{\beta}_2 j$ for $j \in [n-1]$. Thus $\bar{\beta} \in A_n$ because the restrictions of $\bar{\beta}$ to $[n-1]$ and to $\{n\}$ are two acyclic maps of these sets onto themselves and the correspondence $\beta \to \bar{\beta}$ is a 1-1 application of the maps $\beta \in B_n$ satisfying $\beta^*1 = n$ onto the maps $\bar{\beta} \in A_n$ such that $\bar{\beta}^{-1}n = \{n\}$.

CASE 3:

$$1 < \beta^* n = m < n.$$

We define:

$$I_1 = \{j \in [n-1] : \beta^* j < m\},$$
$$I_2 = \{j \in [n-1] : \beta^* j > m\}.$$

By hypothesis the restriction of β^* to $I_1 \cup I_2 = [n-1]$ is a bijection onto $[n]\backslash\{m\}$ and it implies $\beta j < m$ (resp. $> m$) for every $j \in I_1$ (resp. I_2). More accurately the present hypothesis is equivalent to the existence of th feollowing objects:

(i) a map $\beta_1 \in B_{m-1}$ and a non-decreasing surjection $\lambda_1 : [m-1] \to I_1$ such that $\beta_1 j = \beta\lambda_1 j$ for each $j \in [m-1]$ (then $\beta_1^* j = \beta^* \lambda_1 j$).

(ii) a map $\beta_2 \in B_p (p = n - m)$ and a non-decreasing surjection $\lambda_2 : [p] \to I_2$ such that $m + \beta_2 j = \beta\lambda_2 j$ for each $j \in [p]$ (then $m + \beta_2^* j = \beta^* \lambda_2 j$).

Reciprocally, if this is the case, we have $\beta \in B_n$ (with $\beta^* n = m$, automatically) iff $\beta n \in [m]$.

Thus letting $I_1' = I_1 \cup \{n\}$, $\lambda_1' j = \lambda_1 j$ or $= m$ depending upon $j \in [m-1]$ or $= m$ and $\beta_1' j = \beta_1 j$ or $= \beta m$ depending on the same condition, we have $\beta_1' \in B_m$ satisfying $\beta_1'^* m = m$ and we can combine the two constructions already introduced in the definition of $\bar{\beta} \in A_n$:

$$\bar{\beta}\lambda_1' j = \lambda_1' \bar{\beta}_1' j \qquad \text{for each} \quad j \in [m];$$

$$\bar{\beta}\lambda_2 j = \lambda_2 \bar{\beta}_2 j \qquad \text{for each} \quad j \in [p].$$

By construction the restriction of $\bar{\beta}$ to I_1' (resp. I_2) is a map of this set into itself and this map is acyclic by the induction hypothesis. Further by the discussion of Case 1, we know that this restriction has a single fixed point, hence that I_1' can be retrieved from $\bar{\beta}$ as being the set of all $j \in [n]$ for which $\bar{\beta}^n j = \bar{\beta}^n n$. This shows the 1-1 character of our application $\beta \to \bar{\beta}$ and it ends the verification of the validity of the construction.

PRINTED IN BRUGES, BELGIUM, BY THE ST. CATHERINE PRESS, LTD.

Z. Wahrscheinlichkeitstheorie verw. Geb. 9, 265—269 (1968)

Sur certains semi-groupes de matrices non negatives

Marcel Paul Schützenberger

Recu 1 Juillet 1966

Introduction

On se propose de vérifier l'énoncé suivant qui constitue l'une des généralisations possibles d'un théorème de Wolfowitz ([1], cf. [2]).

Propriété. *Soit A un semigroupe finiment engendré de matrices de dimension finie à éléments non négatifs satisfaisant les deux conditions suivantes:*

(I) *Il n'existe aucune paire d'indices telle que l'élément correspondant de toutes les matrices de A soit nul;*

(II) *Toutes les matrices $a \in A$ ont le mème nombre positif q de racines caractéristiques de module unité et satisfont* $\limsup \|a^n\| < \infty$.

On a alors $0 = \limsup_{m\to\infty} \left\{ \left\| a - \lim_{n\to\infty} a^{1+nq!} \right\| : a \in A^m \right\}$.

En raison de (II), l'existence des matrices limite $\lim_{n\to\infty} a^{1+nq!}$ résulte immédiatement du théorème de Perron et Frobenius qui établit que pour chaque $a \in A$ les q racines caractéristiques qui ne sont pas de module strictement inférieur à 1 sont de fait des racines $q!$-ièmes de l'unité.

Comme d'usage, on appelera «monoïde» tout semi groupe possédant un élément neutre (noté e) et, à ceci près, la terminologie sera celle de [3]. On utilisera le cas particulier suivant de théorèmes bien connus (cf. [3]).

Soit A^* un monoïde possédant des idéaux à droite minimaux R_i $(i \in I)$ et des idéaux à gauche minimaux L_j $(j \in J)$. On a $\bigcup \{R_i : i \in I\} = \bigcup \{L_j : j \in J\}$. *Les quasi idéaux minimaux $R_i \cap L_j = R_i A^* L_j = R_i L_j$ $(i \in I, j \in J)$ sont deux à deux disjoints et sont tous isomorphes à un mème group abstrait. Pour chaque $a \in A^*$, la translation $(R_i \cap L_j)\, a$ (resp. $a(R_i \cap L_j)$) est une bijection de $R_i \cap L_j$ sur un quasi-idéal minimal $R_i \cap L_{j'}$ (resp. $R_{i'} \cap L_j$).*

Il est commode de noter qu'un élément b d'un monoïde B^* appartient à des idéaux minimaux à gauche et à droite de ce dernier si et seulement si

$$b \in b\, b'\, B^* \cap B^* b'\, b$$

pour tout $b' \in B^*$. Cette condition est satisfaite si pour chaque $b' \in B^*$ il existe un entier naturel p tel que $b = (b\, b'\, b)^p$.

Vérification de la Propriété

Elle se réduit à celle des cinq remarques suivantes.

Remarque 1. *Soit* $\bar{A} = \left\{ \lim_{n\to\infty} a^{1+nq!} : a \in A \right\}$. *Le monoïde A^* engendré par $A \cup \bar{A}$ admet des idéaux minimaux à droite et à gauche dont l'union contient $\bar{A}$.*

Preuve. Par définition tout élément de A^* est égal à un produit $c = a_1' a_2' \cdots a_k'$ $(0 \leqq k < \infty)$ dont chacun des facteurs appartient à A ou à $\bar{A}$. Comme

$$\limsup_{n,n' \to \infty} \| a^{1+nq!} - a^{1+n'q!} \| = 0$$

pour tout $a \in A$, on peut écrire $c = \lim c^{(n)}$ où $c^{(n)}$ est le produit de facteurs a_i'' $(1 \leqq i \leqq k)$ de la forme a_i ou $a_i^{nq!+1}$ avec $a_i \in A$. Pour chaque valeur finie de n, $c^{(n)}$ appartient à A et possède donc q racines caractéristiques de module unité. On peut choisir les vecteurs propres associés à ces racines de telle facon qu'ils convergent quand n tend vers l'infini et par conséquent c possède au moins q racines caractéristiques de module unité.

Supposons maintenant que $c \in A^* \bar{A} A^*$, c'est à dire qu'au moins un des facteurs a_i'' a la forme $a_i^{nq!+1}$. L'espace nul du facteur correspondant $a_i' = \lim_{n \to \infty} a_i^{nq!+1}$ de c a codimension q et par conséquent l'espace nul de c a codimension $\leqq q$. Compte tenu de ce que c a au moins q racines caractéristiques de module unité, ceci établit que c a exactement q semblables racines et que q est aussi la codimension de son espace nul. Utilisant le théorème de Perron et Frobenius, on en conclut que $c = c^{1+q!}$ et $c^{q!} = c^{2q!}$ pour tout $c \in A^* \bar{A} A^*$. Maintenant, quelque soit $c' \in A^*$ le produit $cc'c$ appartient à $A^* \bar{A} A^*$ et satisfait donc $(cc'c)^{q!} = (cc'c)^{2q!}$. Les espaces nuls à droite et à gauche de $(cc'c)^{q!}$ contiennent les espaces nuls correspondant de $c^{q!}$ et plus précisément leur sont égaux puisqu'ils ont la mème codimension q. Comme $c^{q!}$ et $(cc'c)^{q!}$ sont idempotents, il en résulte que $c^{q!} = (cc'c)^{q!}$, donc comme on l'a rappelé dans l'Introduction que $c^{q!}$ appartient à des idéaux minimaux à droite et à gauche. Il en est de mème pour c puisque $c \in c^{q!} A^* \cap A^* c^{q!}$ en vertu de $c = c^{q!+1}$ et la vérification de la Remarque est achevée. On montrerait sans peine que $\bar{A}$ est exactement l'union de tous les idéaux minimaux de A^*.

Remarque 2. *Il existe un homomorphisme μ de A^* dans un monoïde fini qui est tel que sa restriction à chacun des quasiidéaux minimaux de A^* est injective et que tous les idemptotents de μA^*, sauf μe, sont contenu dans l'union de ses idéaux minimaux.*

Preuve. Utilisant les notations rappelées dans l'Introduction, on choisit un quasi-idéal minimal $R_1 \cap L_1$ et des bases fixes $R_1' \subset R_1$ et $L_1' \subset L_1$ des modules sur R engendrés respectivement par les matrices de R_1 et de L_1.

Pour $a, a' \in A^*$ on pose

$$[a, a'] = [a', a] = \operatorname{Sup} \{ \| bac - ba'c \| : b \in R_1', c \in L_1' \}.$$

La relation $[\ ,\ ] = 0$ sur $A^* \times A^*$ est une équivalence n'ayant qu'un nombre fini de classes. En effet, d'une part les ensembles R_1' et L_1' sont finis puisque la dimension commune des matrices de A^* est finie; d'autre part l'ensemble $R_1' A^* L_1'$ est fini puisqu'il est contenu dans $R_1 A^* L_1 = (R_1 A^*)(A^* L_1) = R_1 L_1 = R_1 \cap L_1$ et que ce dernier ensemble lui méme est fini en tant que groupe de matrices de dimension finie dont l'ordre des éléments est borné (par $q!$).

Cette mème relation est une congruence car $[a, a'] = 0$ entraine

$$\operatorname{Sup} \{ \| bac - ba'c \| : b \in R_1,\ c \in L_1 \} = 0$$

puisque R_1' et L_1' sont des bases de R_1 et de L_1 respectivement, donc, pour tout $d, d' \in A^*$, $\operatorname{Sup} \{ \| bdad'c - bda'd'c \| : b \in R_1, c \in L_1 \} = 0$ puisque R_1 et L_1

satisfont identiquement $R_1 d \subset R_1$ et $d' L_1 \subset L_1$ en tant qu'idéaux à droite et à gauche respectivment, donc enfin $[dad', da'd'] = 0$.

Soit μ l'homomorphisme naturel de A^* sur son monoïde quotient défini par la congruence $[\ ,\ ] = 0$. L'ensemble $\mu(R_1 \cap L_1)$ est contenu dans un quasi-idéal minimal de μA^* puisque $R_1 \cap L_1$ est un quasi idéal minimal de A^* et la restriction de μ à $R_1 \cap L_1$ est injective puisque par construction la restriction de $[\ ,\ ] = 0$ à cet ensemble se réduit à la relation d'identité. Maintenant, pour n'importe quel élément $d \in R_1 \cap L_1$ et chaque quasi-idéal $R_i \cap L_j$ $(i \in I,\ j \in J)$ l'application $R_i \cap L_j \to d(R_i \cap L_j)d$ est une bijection sur $R_1 \cap L_1$ et comme cette application commute avec μ on a vérifié que la restriction de μ à chacun des quasi-idéaux minimaux de A^* est injective.

Finalement si $a \in A^*$ est tel que $\mu a = \mu a^2$, on a $[a, a^2] = 0$, donc $[a, \bar{a}] = 0$ et $\mu a = \mu \bar{a}$ où $\bar{a} = \lim_{n \to \infty} a^{1+n q^1}$. Par conséquent si $a \neq e$ l'élément μa appartient à l'union des ideaux minimaux de μA^* puisqu'il est égal à $\mu \bar{a}$ où, comme on l'a vu dans la Remarque précedente, $\bar{a}$ appartient à l'union des idéaux minimaux de A^*. Ceci conclut la vérification de la Remarque.

Remarque 3. *Soit B^* (respectivement D) le monoïde (resp. l'idéal bilatére de B^*) formé de toutes les matrices b à éléments non négatifs de la forme*

$$b = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k \qquad (0 < k < \infty)$$

où les r_i sont des quantités réelles de somme 1 et les a_i des matrices de A^* (resp. de $A^* \bar{A} A^*$) ayant même image par μ. Le monoïde B^* admet des idéaux minimaux à droite et à gauche dont l'union est égale à D^2. De plus

$$\omega = \operatorname*{Sup}_{\text{def}} \{\| b \| : b \in B^*\} < \infty.$$

Preuve. Comme la restriction de μ à chacun des quasi-idéaux minimaux de A^* est injective, tout $b \in D$ a la forme $b = \sum_{ij} r_{ij} a_{ij}$ où chaque a_{ij} appartient à $R_i \cap L_j$ et où ij parcourt l'ensemble d'indices $I \times J$. On pose

$$p_i = \sum_j r_{ij}; \qquad q_j = \sum_i r_{ij}$$

et on note D' l'ensemble des $b \in D$ tels que $r_{ij} = p_i q_j$ pour tout $ij \in I \times J$.

Soient

$$b = \sum_{ij} r_{ij} a_{ij} \quad \text{et} \quad b' = \sum_{ij} r'_{ij} a'_{ij}$$

deux élements de D. Pour chaque paire $ij' \in I \times J$ tous les produits $a_{ij} a'_{i'j'}$ $(j \in J,\ i' \in I)$ sont contenus dans $R_i \cap L_{j'}$ et ont la même image par μ. En raison du caractère injectif de μ, ils sont donc tous égaux à un même élément $a''_{ij'} \in R_i \cap L_{j'}$ et on a $bb' = b'' = \sum_{ij'} p_i q'_{j'} a''_{ij'}$ ce qui montre d'abord que $D^2 \subset D'$, ensuite que si $b \in D'$ (resp. $b' \in D'$) les coefficients p''_i (resp. q''_j) de b'' sont les même que les coefficients correspondant de b (resp. de b') et qu'ils sont donc indépendants de l'autre facteur du produit.

Étendant de facon naturelle μ à un homomorphisme de B^* dans μA^*, on en conclut immédiatement que pour $b, b' \in D'$, l'ensemble $bD'b'$ est isomorphe au

19*

groupe $R_1 \cap L_1$ et qu'en particulier $bb''b = (bb''b)^{q!+1}$ quelques soient $b \in D'$ et $b'' \in D$, donc, quelque soit $b'' \in B^*$, puisque l'on peut écrire $bb''b = bb^{q!}b''b^{q!}b$ où $b^{q!}b''b^{q!} \in D$ et $b = bb^{q!}$. Ceci achève d'établir $D^2 = D'$ et le fait que D^2 est contenu dans l'union des idéaux minimaux de B^*.

Pour vérifier $\omega < \infty$, notons d'abord que la condition (I) sur A équivaut à l'existence d'une quantité positive telle que pour chaque paire d'indices une au moins des matrices de A ait son élément correspondant supérieur à cette quantité. Comme $\bar{A}$ est un idéal à droite et à gauche et que toutes les matrices de la forme $a^{q!}$ ($a \in \bar{A}$) ont trace q et une dimension finie, la même condition est satisfaite par $\bar{A}$. Comme pour chaque $b \in B^*$ et $a \in \bar{A}$ la matrice $aba \in D^2$ est d'ordre fini et que par conséquent aucun de ses éléments diagonaux ne peut être supérieur à 1, on en conclut que l'ensemble de tous les éléments des matrices $b \in B^*$ est borné supérieurement et la Remarque est entièrement vérifiée puisque les matrices de B^* sont de dimension finie.

Remarque 4. *L'application* π *de* B^* *dans l'intervalle* $[0, 1]$ *définie pour tout* $b \in B^*$ *par*

$$\pi b = \mathrm{Inf}\{s \in [0,1] : b = (1-s)b_1 + sb_2;\ b_1 \in D;\ b_2 \in B^*;\ \mu b_1 = \mu b_2\}$$

est submultiplicative et pour tout b, $b' \in B^*$ *on a*

$$\left\| bb' - \lim_{n\to\infty} (bb')^{1+nq!} \right\| \leqq 5\,\omega(\pi b + \pi b' - \pi b \cdot \pi b').$$

Preuve. Soient $b = (1-s)b_1 + sb_2$; $b' = (1-s')b_1' + s'b_2'$ où $s = \pi b$; $s' = \pi b'$; $b_1, b_1' \in D$; $b_2, b_2' \in B^*$; $\mu b_1 = \mu b_2$; $\mu b_1' = \mu b_2'$. On peut écrire $bb' = (1-ss')b_1'' + ss'b_2b_2'$ où la matrice b_1'' est égale à $(1-ss')^{-1}((1-s)b_1b_1' + (1-s)s'b_1b_2' + s(1-s')b_2b_1')$ et appartient à D puisque ses coefficients ont somme 1 et que les matrices b_1b_1', b_1b_2' et b_2b_1' appartiennent à D et ont la même image par μ. Ceci établit $\pi(bb') \leqq \pi b \cdot \pi b'$.

D'autre part on peut écrire $bb' = (1-t)d + td'$ où $t = \pi b + \pi b' - \pi b \cdot \pi b$; $d = b_1b_1' \in D^2$ et $d' \in B^*$. Si $c = \lim_{n\to\infty} (bb')^{nq!-1}$ on a $\mu dcd = \mu d$ car d'une part $\mu d = \mu(bb')$ par construction, et, d'autre part $\mu d = \mu d^{nq!+1}$ pour tous les entiers n puisque $d \in D^2$. Comme dcd et d appartiennent au même quasi-idéal minimal de B^* ainsi qu'on là vu dans la Remarque 3, on en conclut que de fait $dcd = d$. Tenant compte de cette égalité et substituant $(1-t)d + td'$ à bb' dans l'expression $bb' - bb'cbb'$ de $bb' - \lim_{n\to\infty} (bb')^{nq!+1}$, on trouve que cette différence est égale à $t(d' - (1-t)\,(dcd + dcd' + d'cd) - td'cd')$ ce qui livre l'inégalité cherchée.

Remarque 5. *A chaque* ε *positif il correspond un entier naturel* m*; tel des matrices de* $A^m \in A^*$ *soit égale à un produit* $a'a''$ *où* a', $a'' \in A^*$ *satisfont* $\pi a'$, $\pi a'' < \varepsilon$.

Preuve. L'hypothése que A est finiment engendré implique que

$$\bigcup \{A^{p'} : 0 < p' \leqq p\}$$

soit un ensemble fini pour tout entier naturel p et, en raison du caractère submultiplicatif de π, il suffit de vérifier l'existence d'un $p < \infty$ tel que $\pi a < 1$ pour tout $a \in A^p$.

Soit β l'homomorphisme de B^* dans le monoïde de relations binaires qui envoye chaque $b \in B^*$ sur l'ensemble des paires d'indices pour lesquelles l'élément correspondant de b est positif ([1]). βB^* est un monoïde fini. Il en est de même du produit direct $\mu B^* \times \beta B^*$ et on peut donc trouver un entier naturel p tel que chacune des matrices de A^p soit égale à un produit $a_1 a a_2$ où $a_1, a_2 \in A^*$ et où $a \in A A^*$ satisfait $\mu a = \mu a^2$ et $\beta a = \beta a^2$ (cf. [1]). Posant $\tilde{a} = \lim_{n\to\infty} a^{nq!+1}$, ces équations impliquent $\mu\tilde{a} = \mu a$ et $\beta\tilde{a} \subset \beta a$. Cette derniére relation entraine l'existence d'une quantité non négative $r < 1$ pour laquelle $r^{-1}(a - (1 - r)\tilde{a}) = a'$ est une matrice à éléments non nègatifs. On a $a' \in B^*$ puisque d'une part $r^{-1} - r^{-1}(1 - r) = 1$ et, d'autre part, $\mu\tilde{a} = \mu a$. Par conséquent $\pi a \leqq r < 1$ et la vérification de la Propriété est achevée.

Bibliographie

1. Wolfowitz, J.: Products of indecomposable, aperiodic stochastic matrices. Proc. Amer. math. Soc. **14**, 733—737 (1963).
2. Larisse, J., et M. P. Schützenberger: Sur certaines chaines de Markov non homogènes. Publ. Inst. Statist. Univ. Paris **13**, 57—66 (1964).
3. Clifford, A. H., and G. B. Preston: The algebraic theory of semi groups. Math. Survey **7**, Amer. Math. Soc. (1961).

Prof. M. P. Schützenberger
Faculté des Sciences
23, rue du Maroc
F 75 Paris 19^0 (France)

9 MARS 1968

LANGAGES

LES MODÈLES EN LINGUISTIQUE

DIDIER
4 et 6, rue de la Sorbonne
PARIS

LAROUSSE
13-21, rue du Montparnasse
PARIS

N. CHOMSKY ET M. P. SCHUTZENBERGER

THÉORIE ALGÉBRIQUE DES LANGAGES « CONTEXT-FREE » *

1. Motivation linguistique.

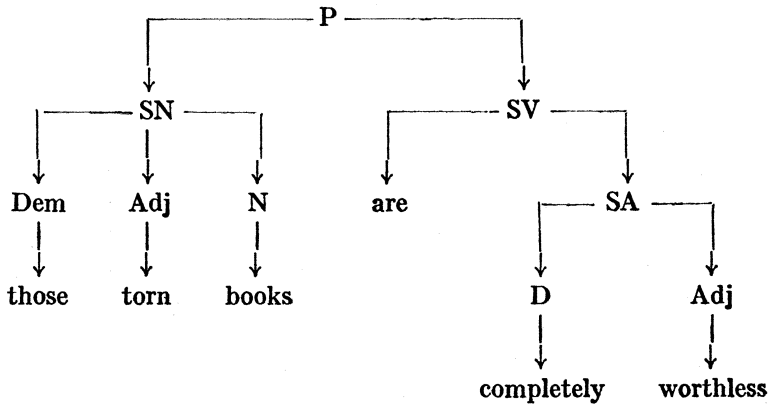
Nous nous intéresserons ici à plusieurs classes de processus générateurs de phrases qui sont liés de près, à beaucoup d'égards, aux grammaires des langues naturelles et de divers langages artificiels. Par *langage*, nous entendons simplement un ensemble de séquences sur un ensemble fini quelconque V de symboles, appelé *vocabulaire* du langage. Une *grammaire* sera un ensemble de règles énumérant récursivement les séquences appartenant au langage. Nous dirons que la grammaire *engendre* ces séquences. (En pensant aux langues naturelles nous appellerions les séquences engendrées, des *phrases;* en termes algébriques on les appellerait habituellement des *mots*, et le vocabulaire serait appelé un *alphabet;* en considérant la grammaire comme déterminant un langage de programmation, on appellerait les séquences des *programmes;* en général nous emploierons le terme neutre de *séquence.*)

Pour qu'une classe de grammaires soit linguistiquement intéressante, il doit exister un procédé qui fasse correspondre à n'importe quel couple (σ, G), où σ est une séquence et G une grammaire de cette classe, une *description structurale* satisfaisante de la séquence σ, par rapport à la grammaire G. En particulier la description structurale devrait indiquer, s'il en est ainsi, que la séquence σ est une phrase bien formée du langage $L(G)$ engendré par G. Dans ce cas, la description structurale doit contenir des renseignements grammaticaux servant de base à l'explication de la manière dont σ est interprétée par des « locuteurs » qui ont assimilé la grammaire G; sinon, il serait bon que la description structurale indique en quoi σ diffère d'une séquence bien formée.

Nous ne nous intéresserons ici qu'à un aspect de la description struc-

* Ce travail a été financé en partie par : U. S. Army Signal Corps, Air Force Office of Scientific Research, Office of Naval Research, et en partie par National Science Foundation et par un don du Commonwealth Fund. Il a été publié en anglais dans : *Computer Programming and Formal Systems*, P. Brafford et D. Hirschberg Eds, North Holland, Amsterdam, 1963.

turale d'une phrase, à savoir sa subdivision en syntagmes appartenant à différentes catégories. Ainsi, par exemple, une description structurale de la phrase anglaise « those torn books are completely worthless » devrait indiquer que *those* est un *Démonstratif*, *torn* et *worthless* des *Adjectifs*, *books* un *Nom*, *completely* un *Adverbe*, *those torn books* un *Syntagme Nominal*, *completely worthless* un *Syntagme Adjectival*, are *completely worthless* un *Syntagme Verbal*, que la séquence tout entière est une *Phrase*, ainsi que des détails supplémentaires quant à la sous-classification. Ces renseignements peuvent être représentés par un schéma du type (1) :



ou, d'une manière équivalente, par un parenthésage étiqueté de la séquence, comme dans (2) :

$$[_{P}[_{SN}[_{Dem}\text{those}][_{Adj}\text{torn}][_{N}\text{books}]][_{SV}\text{are}\ [_{SA}[_{D}\text{completely}][_{Adj}\text{worthless}]]]].$$

Une préoccupation essentielle de la théorie générale des langues naturelles est de définir la classe des séquences possibles (en fixant un alphabet phonétique universel); la classe des grammaires possibles; la classe des descriptions structurales possibles; un procédé permettant d'attribuer des descriptions structurales aux phrases, étant donnée une grammaire; et de faire tout ceci de telle façon que la description structurale attribuée à une phrase par la grammaire d'une langue naturelle soit une base pour expliquer comment une personne qui parle cette langue comprend cette phrase (en supposant l'absence de limitations dues à la mémoire, l'attention, etc.). Alors, la grammaire représentera certains aspects de la compétence linguistique de celui qui parle la langue.

Nous ne nous intéresserons pas ici à la question empirique de l'adéquation à la réalité des descriptions structurales ou des grammaires que nous étudierons. D'ailleurs les classes de grammaires que nous envisagerons et les genres de descriptions structurales qu'elles engendrent, sont sans aucun doute trop pauvres, pour être à la hauteur de la véritable

compétence linguistique de l'homme. Néanmoins, les systèmes que nous considérons (qui, effectivement, formalisent des notions traditionnelles de l'analyse logique et de l'analyse en constituants immédiats) sont à rapprocher des types de systèmes qui semblent empiriquement adéquats, et sont jusqu'à présent, trop complexes pour être soumis à une étude abstraite [1].

Dans la représentation (2), nous avons, en plus des parenthèses, deux sortes de symboles :

(i) des symboles de la séquence engendrée (i.e. les six symboles *those, torn, books, are, completely, worthless*) [2];

(ii) les symboles P, SA, $Dem.$, Adj, N, SV, SA, D, représentant des catégories syntaxiques. Nous appellerons les symboles du type (i) terminaux, ceux du type (ii) non terminaux.

Nous supposerons, ci-après, qu'il existe une collection déterminée de symboles terminaux et non terminaux à partir desquels les grammaires de toutes les langues sont construites. On peut considérer que l'ensemble des terminaux constitue un vocabulaire potentiel commun à toutes les langues. Par analogie avec le langage parlé, on peut considérer que l'ensemble des terminaux est défini par un alphabet phonétique universel (en supposant, comme il est naturel de le faire que la longueur des morphèmes est bornée supérieurement). En examinant de nouveau le langage naturel, on peut considérer l'ensemble fixe des non-terminaux comme un ensemble universel de catégories dans lequel on prend les divers types de syntagmes du langage. Une question traditionnelle importante de la linguistique générale touche à la possibilité de donner une interprétation concrète des non-terminaux à l'aide desquels sont construites les grammaires. Est-il possible, autrement dit, de trouver une définition générale, indépendante de toute langue particulière, de catégories telles que Nom, Verbe, etc..., en termes de contenu sémantique ou de propriétés formelles des grammaires? Le problème d'une interprétation concrète à donner à l'ensemble des terminaux et non-terminaux est évidemment le même que le problème qui consiste à rendre empiriquement adéquates certaines catégories des grammaires, un point capital dans la science du langage; mais il va au-delà de nos préoccupations immédiates.

Nous pouvons engendrer la phrase : « those torn books are completely worthless » avec la description structurale (2), au moyen de l'ensemble des *règles de réécriture* :

1. Pour une discussion plus poussée de ces questions, voir Chomsky [10].

2. Dans une grammaire linguistiquement adéquate, on n'engendrerait pas ces, symboles, mais plutôt une représentation plus abstraite, utilisant les symboles *the, démonstratif, pluriel, tear, participe, book, pluriel, be, pluriel, complete, by, worth, less*, dans cet ordre. La représentation au moyen de ces symboles (appelés morphèmes) serait transformée en une représentation phonétique par un ensemble de *règles phonologiques* auxquelles nous ne nous intéresserons pas ici. Voir Chomsky et Miller [15]. Nous n'utiliserons des phrases véritables comme (2) que pour des exemples descriptifs, et par conséquent nous laisserons de côté des raffinements de ce genre.

80

(3)

$$
\begin{aligned}
P &\to SN\ SV\\
SN &\to Det\ Adj\ N\\
Dem &\to \text{those}\\
Adj &\to \text{torn}\\
Adj &\to \text{worthless}\\
N &\to \text{books}\\
SV &\to \text{are}\ SA\\
SA &\to D\ Adj\\
D &\to \text{completely}
\end{aligned}
$$

par une *dérivation* construite de la manière suivante.

On écrit d'abord le *symbole initial* P comme première ligne de la dérivation. On forme la $(n+1)^e$ ligne de la dérivation en choisissant n'importe quelle occurrence d'un α non terminal dans la n^e ligne (où cette occurrence de α n'étiquette pas une parenthèse), et en la remplaçant par la séquence : $[\alpha\varphi]$, où $\alpha \to \varphi$ est une des règles de (3). On continue jusqu'à ce que les seuls non-terminaux qui apparaissent soient ceux qui étiquètent des parenthèses; la dérivation est alors *terminée*. En supprimant les parenthèses d'une dérivation terminée avec leurs étiquettes, on a une séquence qui ne contient que des terminaux. Appelons ceci une *séquence terminale*. Quatre séquences terminales différentes peuvent être engendrées par la grammaire (3). Il est possible de construire une grammaire qui engendre une infinité de séquences terminales, chacune avec une description structurale, en autorisant des récurrences, par exemple en ajoutant à (3) les règles :

(4)

$$
\begin{aligned}
SN &\to \text{that}\ P\\
SV &\to \text{is}\ SA\\
SA &\to \text{obvious}
\end{aligned}
$$

auquel cas on peut engendrer par exemple « that those torn books are completely worthless is obvious », etc. [3]. Chacune des phrases engendrées aura encore une description structurale du type voulu.

Des grammaires du type (3)-(4) seront appelées « context-free » (*(N. d. T.)* C-grammaires). Elles sont caractérisées par le fait qu'il apparaît exactement un symbole non terminal dans le membre gauche de chaque règle de réécriture.

Si cette restriction n'est pas exigée les systèmes obtenus ont alors des propriétés formelles entièrement différentes.

Il semble que les grammaires des langues naturelles doivent contenir

3. Dans ce cas, une infinité de phrases non anglaises seront également engendrées, par exemple « that those torn books is obvious are completely worthless », etc. Donc la grammaire ((3), (4)) est inacceptable. La difficulté qu'il y a à éviter de telles insuffisances empiriques peut être facilement sous-estimée. Soulignons à nouveau que c'est là le point déterminant, aussi bien pour la linguistique que pour la psychologie, bien qu'il ne soit pas abordé directement ici. Pour une discussion, voir Chomsky [13].

au moins quelques règles de réécriture de ce type plus général, et certaines règles qui ne sont pas du tout des règles de réécriture. Cf. Chomsky [8] [10] et [12], Chomsky et Miller [15] pour une discussion abstraite plus poussée de tels systèmes que nous n'examinerons pas plus en détail ici. Un ensemble de séquences terminales qui peut être engendré par une certaine C-grammaire sera appelé un *C-langage*.

Une C-grammaire peut engendrer une séquence terminale *(sans parenthèses)* φ avec plusieurs descriptions structurales différentes. Dans ce cas, si la grammaire est empiriquement adéquate, la séquence φ est structuralement ambiguë. Considérons par exemple la C-grammaire, ayant les règles :

(5)
$$\begin{aligned} P &\to SN\ SV \\ SN &\to \text{they};\ SN \to Adj\ N;\ SN \to N \\ SV &\to \text{are}\ SN;\ SV \to \text{Verbe}\ SN \\ Verbe &\to \text{are flying} \\ Adj &\to \text{flying} \\ N &\to \text{planes} \end{aligned}$$

Avec cette grammaire on peut engendrer aussi bien (6) que (7) :

(6) $[_P[_{SN}\text{they}]\ [_{SV}[_{Verbe}\text{are flying}]\ [_{SN}[_N\text{planes}]]]]$.

(7) $[_P[_{SN}\text{they}]\ [_{SV}\text{are}[_{SN}[_{Adj}\text{flying}]\ [_N\text{planes}]]]]$.

Corrélativement, la séquence terminale « they are flying planes » est structuralement ambiguë; elle peut vouloir dire : « my friends who are pilots are flying planes » : (mes amis, qui sont pilotes, sont en train de piloter des avions), ou : « those spots on the horizon are flying planes » (ces taches sur l'horizon sont des avions qui volent). L'étude de l'ambiguïté structurale est une des façons les plus instructives de déterminer si une grammaire est empiriquement adéquate ou non.

Nous verrons plus loin que l'ambiguïté de certains C-langages est inhérente, dans la mesure où toute C-grammaire qui les engendre attribue plusieurs descriptions structurales à certaines de leurs phrases.

De plus, nous verrons que le problème de savoir si une C-grammaire est ambiguë est récursivement indécidable [4], même pour des types de C-grammaires extrêmement simples.

Bien que les C-grammaires soient loin d'être suffisantes pour les langues naturelles, elles sont sans aucun doute satisfaisantes pour la description des langages artificiels usuels, et apparemment pour la description de certains (peut-être tous) langages de programmation. En particulier

4. En d'autres termes, il n'y a pas de procédure mécanique (d'algorithme) permettant de savoir si une C-grammaire quelconque attribue plus d'une description structurale à une séquence qu'elle engendre.

on peut donner une C-grammaire pour l'Algol [18] et chaque programme en Algol sera une des séquences terminales engendrées par cette grammaire.

Il est clair qu'un langage de programmation ne doit pas être ambigü. Par conséquent, il est important de pouvoir s'assurer qu'un langage de programmation particulier satisfait effectivement cette condition, ou encore que dans un certain ensemble infini de programmes, chacun d'eux est sans ambiguïté, certaines techniques utilisées pour les construire étant données (par exemple des techniques qu'on peut représenter comme des règles de construction de dérivations dans une C-grammaire). Comme on l'a signalé dans le précédent paragraphe, ces questions peuvent être assez difficiles.

Supposons que G_1 et G_2 soient des systèmes générateurs qui spécifient certaines techniques de construction de programmes de calculateurs; supposons, en fait, que G_1 et G_2 soient des grammaires engendrant les langages de programmation L_1 et L_2, consistant chacun en un nombre infini de séquences, chaque séquence étant un programme possible. Il est souvent intéressant d'étudier les puissances relatives des langages de programmation.

Nous verrons que si G_1 et G_2 sont des C-grammaires (comme par exemple pour l'Algol), la plupart des problèmes touchant aux rapports entre L_1 et L_2 sont récursivement indécidables, ceci est vrai en particulier pour le problème de savoir si L_1 et L_2 ont une intersection vide, ou infinie, ou si L_1 est contenu dans L_2 [2], ou s'il existe un transducteur fini (un compilateur) qui applique L_1 sur L_2 (Ginsburg et Rose, communication personnelle).

Par conséquent, il est possible que des questions générales sur les propriétés formelles des C-systèmes et de leurs relations formelles aient une interprétation concrète dans l'étude des systèmes de traitement de l'information aussi bien que dans celle des langues naturelles. Cette possibilité a été montrée en particulier par Ginsburg et Rice [18], Ginsburg et Rose [19].

Lorsqu'on considère une grammaire comme un processus générateur, on peut s'intéresser au langage (à l'ensemble des séquences terminales) qu'elle engendre, ou bien à l'ensemble des descriptions structurales qu'elle engendre (N. B. : chaque description structurale détermine une séquence terminale de manière unique, comme dans (2)). Cette dernière question est évidemment de loin la plus intéressante. De la même façon, dans l'étude de la capacité génératrice d'une classe de grammaires (ou de la capacité relative de plusieurs de ces classes, comme dans l'évaluation de théories linguistiques (soumises à un choix), on peut s'intéresser ou bien à l'ensemble des langages qu'on peut engendrer, ou bien à l'ensemble des systèmes de descriptions structurales qu'on peut engendrer. Ici encore, le dernier aspect est plus intéressant, mais beaucoup plus difficile. Ces questions ont toutes été abordées très récemment et on s'est limité presque

exclusivement à engendrer des langages plutôt que des systèmes de descriptions structurales.

Nous envisagerons la génération d'un point de vue intermédiaire entre les deux précédents. Nous considérerons une représentation d'un langage qui ne sera ni un ensemble de séquences ni non plus un ensemble de descriptions structurales, mais un ensemble de couples (σ, n), où σ est une séquence, et n son degré d'ambiguïté, c'est-à-dire le nombre des descriptions structurales différentes attribuées à σ par la grammaire G qui engendre le langage auquel σ appartient.

2. Les grammaires en tant que générateurs de séries formelles de puissances.

2.1. Supposons donné un vocabulaire fini V, où les ensembles V_T (= vocabulaire terminal) et V_N (= vocabulaire non terminal) forment une partition.

Considérons maintenant des langages sur le vocabulaire V_T, et des grammaires ayant leurs symboles non terminaux dans V_N. Soit $F(V_T)$ le monoïde libre engendré par V_T, i. e. l'ensemble de toutes les séquences sur le vocabulaire V_T. Un langage est alors un sous-ensemble de $F(V_T)$.

Considérons une application r qui fasse correspondre à chaque séquence $f \varepsilon F(V_T)$ un certain entier $< r, f >$. Une telle application peut être représentée par une *série formelle de puissances* (notée également r) sur les variables x non-commutatives de V_T. Ainsi :

$$(8) \qquad r = \sum_t < r, f_i > f_i = < r, f_1 > f_1 + < r, f_2 > f_2 + \ldots,$$

où $f_1, f_2, \ldots$ est une énumération de toutes les séquences de V_T. Le support de r (= *Supp.* (r)) est défini comme l'ensemble des séquences à coefficients non nuls dans r. Ainsi :

$$(9) \qquad \textit{Supp.}\ (r) = \{ f_i \varepsilon F(V_T) \mid < r, f_i > \neq 0 \}.$$

Il n'est pas exigé que les coefficients $< r, f_i >$ de la série formelle de puissance r soient positifs. S'ils le sont (pour tout i, $< r, f_i > \geqslant 0$), nous dirons que r est une série formelle de puissances POSITIVE. Si pour chaque $f_j \varepsilon F(V_T)$, le coefficient est 0 ou 1, nous dirons que r est la série formelle de puissances *caractéristique* de son support.

2.2. Si r est une série formelle de puissances et n un entier, le produit nr est par définition la série formelle de puissances de coefficients $< nr, f > = n < r, f, >$ où $< r, f >$ est le coefficient de f dans r. Si r et r' sont des séries formelles de puissances, $r + r'$ est par définition, la série formelle de puissances de coefficients : $< r + r', f > = < r, f > + < r', f >$ où $< r, f >$ et $< r', f >$ sont respectivement les coefficients de f dans r et r'. rr' sera définie comme la série formelle de puissances de

coefficients $< rr', f > = \sum_{i,j} < r, f_i > < r', f_j >$, avec $f_i f_j = f$. Ainsi l'ensemble des séries formelles de puissances est un anneau fermé pour les opérations : multiplication par un entier, addition, multiplication.

Remarquons que si r et r' sont des séries formelles de puissances le support de $r + r'$ est exactement la réunion des supports de r et r', et le support de rr' est exactement l'ensemble produit des supports de r et r' (i. e., l'ensemble de toutes les séquences $f_i f_j$ telles que f_i soit dans le support de r et f_i dans le support de r'). Nous discuterons ci-dessous l'interprétation d'autres opérations théoriques simples sur ces ensembles.

On dira que deux séries formelles de puissances r et r' sont équivalentes mod. degré n (i. e., $r \equiv r'$ (mod. *deg.* n)) si $< r, f > = < r', f >$ pour chaque séquence f de longueur (« degré ») $\leqslant n$. Supposons alors que nous ayons une suite infinie de séries formelles de puissances $r_1, r_2 \ldots$, telles que pour chaque n et chaque $n' > n$, $r_n \equiv r_{n'}$ (mod. *deg.* n). Dans ce cas la limite r de la suite $r_1, r_2, \ldots$, est bien définie comme étant :

$$r = \lim_{n \to \infty} \pi_n r_n$$

où, pour chaque n, $\pi_n r_n$ est le polynôme formé à partir de r_n en remplaçant tous les coefficients des séquences de longueur $> n$ par zéro. L'anneau des séries formelles de puissances devient donc ultramétrique, donc topologique.

Ces notions étant définies, abordons le problème du lien entre la représentation des langages en termes de série formelle de puissances et la représentation des langages par des processus générateurs tels que les C-grammaires.

2.3. Soit G un proccessus générateur engendrant le langage $L(G)$. A chaque séquence $f \varepsilon F(V_T)$, G associe un certain nombre $N(G, f)$ de descriptions structurales; $N(G, f) > 0$ seulement si $f \varepsilon L(G)$. $N(G, f)$ exprime le degré d'ambiguïté structurale de f par rapport à G. Il est naturel d'associer à G la série formelle de puissances $r(G)$ telles que $< r(G), f > = N(G, f)$, $< r(G), f >$ étant le coefficient de f dans $r(G)$. Ainsi $r(G)$ exprime l'ambiguïté de toutes les séquences terminales vis-à-vis de la grammaire G. Le coefficient $< r(G), f >$ n'est égal à *zéro* que si f n'est pas engendrée par G; il n'est égal à *1* que si f est engendrée sans ambiguïté (d'une manière et d'une seule) par G; il est égal à *2* s'il existe deux descriptions structurales différentes pour f, en termes de G; etc...

Un $r(G)$ associé à une grammaire G sera évidemment toujours positif; et son support *Supp.* $(r(G))$ sera exactement le langage $L(G)$ engendré par G. Nous pouvons considérer qu'une série formelle de puissances r qui a des coefficients positifs et négatifs est associée à *deux* processus générateurs G_1 et G_2. On peut prendre pour coefficient $< r, f >$ de f dans r la différence entre les nombres de fois où f est engendrée par G_1 et G_2; c'est-à-dire, dans ce cas,

$$< r, f > = N(G_1, f) - N(G_2, f).$$

Supposons que G soit une C-grammaire d'éléments non terminaux $\alpha_1, \alpha_2, \ldots \alpha_n$, où α_1 est le symbole initial désigné (i. e., $\alpha_1 = P$ dans l'exemple (1), ci-dessus).

Nous pouvons construire la série formelle de puissances $r(G)$ associée à G par une méthode d'itération directe. Pour cela nous procéderons de la façon suivante :

Remarquons d'abord que G peut s'écrire sous la forme d'un système d'équations par rapport aux variables $\alpha_1, \ldots, \alpha_n$. Soient $\varphi_{i,1} \ldots, \varphi_{i,m_i}$ les séquences telles que $\alpha_i \to \varphi_{i,j}$ $(1 \leqslant j \leqslant m_i)$ soient des règles de G. Associons alors à α_i l'expression polynômiale σ_i,

$$\sigma_i = \varphi_{i,1} + \varphi_{i,2} + \ldots + \varphi_{i,m_i}. \tag{11}$$

Associons maintenant à la grammaire G le système d'équations :

$$\alpha_1 = \sigma_1; \ldots \alpha_n = \sigma_n. \tag{12}$$

Supposons que la grammaire G ne contienne pas de règles de la forme :

$$\begin{aligned} &\alpha_i \to e \\ &\alpha_i \to \alpha_j. \end{aligned} \tag{13}$$

Il est clair que ces suppositions n'affectent en rien la capacité génératrice [2]. C'est-à-dire que pour chaque C-grammaire comportant de telles règles, il en existe une autre sans aucune règle de cette sorte et qui engendre le même langage. Nous exigerons explicitement encore, que si G est une C-grammaire, α un non-terminal de G, il existe des séquences terminales dérivables de α — i. e. si G' contient les règles de G et possède α comme symbole initial, le langage engendré par G' doit être non vide. Il est évident que cette exigeance n'affecte pas non plus la capacité génératrice.

Revenons maintenant au problème de la construction de la série de puissances associée à G_1 et qui représente le degré d'ambiguïté que G attribue à chaque séquence; remarquons que chaque équation $\alpha_i = \sigma_i$ de (12) peut être considérée comme définissant une application ψ_i qui applique un n-uple $(r_1, \ldots, r_n)$ de séries de puissances sur la série de puissances obtenue en remplaçant α_j par r_j dans σ_i. Ceci est légitime du fait des propriétés de clôture de l'anneau des séries de puissances, indiquées ci-dessus au § 2.2.

Ainsi l'ensemble d'équations (12) définit une application ψ,

$$\psi(r_1, \ldots, r_n) = (r'_1, \ldots, r'_n) \text{ où } r'_i = \psi_i(r_1, \ldots, r_n). \tag{14}$$

Considérons maintenant la suite infinie de n-uples de séries de puissances $\rho_0, \rho_1, \ldots$, où :

$$\begin{aligned} \rho_0 &= (r_{0,1}, \ldots, r_{0,n}) = (0, \ldots, 0) \\ \rho_1 &= (r_{1,1}, \ldots, r_{1,n}) \\ \rho_2 &= (r_{2,1}, \ldots, r_{2,n}) \end{aligned}$$

et où pour chaque i, j $(j > 0)$

(16) $$r_{j,i} = \psi_i (r_{j-1,1}, \ldots, r_{j-1,n}),$$

et où 0 est la série de puissances qui a tous ses coefficients nuls. Chaque $r_{j,i}$ de (15) n'a qu'un nombre fini de coefficients non nuls; autrement dit, c'est un polynôme. De plus, on peut montrer que pour tout i, j, j' tels que $j' > j > 0$, $1 \leqslant i \leqslant n$, on a bien :

(17) $$r_{j,i} \equiv r_{j',i} \text{ (mod. } deg.\ j).$$

Par la suite, comme on l'a vu au § 2.2, la limite $r_{\infty,i}$ de la suite infinie $r_{1,i}, r_{2,i}, \ldots$, est bien définie pour tout i (ce n'est évidemment pas en général un polynôme). Nous appellerons le n – uple $(r_{\infty,1}, \ldots, r_{,\infty n})$ ainsi défini, la *solution* du système d'équations (12). En effet, le n – uple $(r_{\infty'1}, \ldots, r_{\infty'n})$ est le seul n – uple à satisfaire, dans notre cadre, le système d'équations (12). Pour cette raison, nous dirons qu'une série de puissances est *algébrique* [42] si elle est un des termes d'une solution d'un système d'équations tels que (12), sans restriction sur le signe des coefficients numériques. Nous dirons qu'une série de puissances est « context-free » si les coefficients des équations de définitions sont tous positifs.

En particulier $r_{\infty,1}$, que nous appellerons désormais, la *série de puissances engendrée* par la grammaire G de (12) de symbole initial α_1, est la série de puissances associée à G, de la manière décrite au début du § 2.3. Son support est le langage $L(G)$ engendré par G, et le coefficient $< r_{\infty,1}, f >$ d'une séquence $f \varepsilon F(V_T)$ détermine l'ambiguïté de ce f par rapport à G, de la manière décrite ci-dessus.

Remarquons que si une série algébrique de puissances est « context-free », elle est positive, mais la réciproque n'est pas nécessairement vraie. C'est ainsi qu'une série de puissances pourra être un terme d'une solution d'un système d'équations, et n'avoir que des coefficients positifs, mais ne pas être un terme d'une solution de n'importe quel système d'équations à coefficients tous positifs[5].

2.4. Comme exemple du procédé ci-dessus, considérons les deux grammaires (18) et (19) :

(18) $$P \to bPP;\ P \to a$$

(19) $$P \to PbP;\ P \to a.$$

Chacune de ces grammaires n'a qu'un non-terminal, donc le système d'équations correspondant, consistera, dans les deux cas, en une équation unique. A (18) correspond (20) et à (19), (21) :

(20) $$P = bPP + a$$

5. Par exemple, en utilisant les notions qui seront définies plus bas § 3.1, le carré d'Hadamard $s \odot s$, pour $s \varepsilon \lambda_0$ n'a que des coefficients positifs (et a le même support que s), mais en général, n'est pas engendré par un ensemble d'équations à coefficients seulement positifs.

(21) $$P = PbP + a.$$

Les équations (19) et (20) correspondent à (12) ci-dessus, avec $n = 1$. Elles remplissent toutes deux la condition (13).

Envisageons d'abord la grammaire (18) représentée sous la forme (20). En procédant comme dans l'alinéa précédent, on considère que (20) définit une application ψ telle que $\psi(r) = a + brr$, où r est une série de puissances.

On forme alors (comme en (15)) la suite infinie $\rho_0, \rho_1, \rho_2, \ldots$, de la façon suivante :

(22)
$$\begin{aligned}
&\rho_0 = r_0 = 0\\
&\rho_1 = r_1 = a + br_0r_0 = a + b00 = a\\
&\rho_2 = r_2 = a + br_1r_1 = a + baa\\
&\rho_3 = r_3 = a + br_2r_2 = a + b(a + baa)\,(a + baa)\\
&\qquad\qquad = a + baa + babaa + bbaaa + bbaabaa\\
&\rho_4 = r_4 = a + br_3r_3\\
&\ldots\quad\ldots\\
&\ldots\quad\ldots
\end{aligned}$$

Il est clair que pour tout j, j', tels que $j' > j > 0$, on a $r_j \equiv r_{j'}$ (mod. *deg. j*). Par suite la limite r_∞ est bien définie. Cette série de puissances est la solution de l'équation (20), et son support est le langage engendré par la C-grammaire (18). Remarquons que la série de puissances r_∞ est, dans ce cas, caractéristique, et que son support, est l'ensemble des *formules bien formées* du « *calcul des implications* » à une variable, dans la notation sans parenthèses (notation polonaise) (le symbole a jouant le rôle de variable propositionnelle et b le rôle de l'opérateur « conditionnel »).

Considérons maintenant la grammaire (19) représentée sous la forme (21). Nous regarderons (21), comme définissant une application ψ telle que $\psi(r) = a + rbr$, où r est une série de puissances. Formons la suite infinie $\rho_0, \rho_1, \rho_2 \ldots$:

(23)
$$\begin{aligned}
&\rho = r_0 = 0\\
&\rho = r_1 = a + r_0br_0 = a + 0b0 = a\\
&\rho = r_2 = a + r_1br_1 = a + aba\\
&\rho = r_3 = a + r_2br_2 = a + (a + aba)b(a + aba)\\
&\qquad\qquad = a + aba + 2ababa + abababa\\
&\rho = r_4 = a + r_3br_3\\
&\qquad = a + aba + 2(ab)^2\,a + 5(ab)^3\,a + 6(ab)^4\,a + 6(ab)^5\,a +\\
&\qquad\quad 4(ab)^6\,a + (ab)^7\,a\\
&\ldots\quad\ldots
\end{aligned}$$

Ici encore pour tout j, j' tels que $j' > j > 0$, on a $r_j \equiv r_{j'}$ (mod. deg j) et la limite r_∞ est définie comme étant la série des puissances :

88

$$(24)\quad r_\infty = \sum_n \begin{bmatrix} 2n \\ n \end{bmatrix} \frac{1}{n+1} (ab)^n a = a + aba + 2(ab)^2 a + 5(ab)^3 a + 14(ab)^4 a + 42(ab)^5 a + \ldots\ldots$$

où $$\begin{bmatrix} 2n \\ n \end{bmatrix} = \frac{2n \times 2n - 1 \times \ldots \times n + 1}{1 \times 2 \times \ldots \times n}.$$

La série de puissances r_∞ de (24) est la solution de l'équation (21) et son support est le langage engendré par la grammaire (19). Ce n'est pas, dans ce cas, une série de puissances caractéristique. En prenant encore le symbole a comme variable propositionnelle et b comme signe pour « conditionnel », la grammaire (19) est l'ensemble de règles qui engendre les *formules bien formées* du *calcul des implications* à une variable, en notations ordinaires mais sans parenthèses. Les descriptions structurales engendrées par (19), de la manière décrite dans le premier alinéa (cf. (3)) sont évidemment sans ambiguïté, puisqu'on conserve les parenthèses, mais les séquences terminales formées en supprimant les parenthèses sont ambiguës et le degré d'ambiguïté de chaque séquence terminale engendrée est exactement son coefficient dans r_∞; ainsi on peut interpréter $ababa$ de deux façons, soit comme $(ab(aba))$, soit comme $((aba)ba)$, etc. Un cas plus général a été traité par Raney [38] au moyen de la formule d'inversion de Lagrange.

Dans (20) et (21) tous les coefficients sont positifs et la solution est donc une série de puissances positive. Considérons, toutefois, le système d'équations constitué par l'équation unique :

$$(25)\qquad S = a - SbS.$$

Nous avons alors la suite :

$$(26)\quad \begin{aligned} \rho_0 &= r_0 = 0 \\ \rho_1 &= r_1 = a - r_0 b r_0 = a - 0b0 = a \\ \rho_2 &= r_2 = a - r_1 b r_1 = a - aba \\ \rho_3 &= r_3 = a - r_2 b r_2 = a - (a - aba)\, b(a - aba) \\ &\qquad = a - aba + 2\,ababa - abababa. \end{aligned}$$

Les coefficients de ρ_i dans (26) sont précisément les mêmes que ceux de ρ_i dans (23) sauf pour le signe —, le coefficient de f dans ρ_i de (26) n'est positif que si f comporte un nombre pair de b.

La série de puissances r_∞, solution de (25), n'est pas positive et donc n'est pas « context-free » (bien qu'il se trouve que son support soit ici un langage « context-free »; c'est d'ailleurs un langage dont (19) est une grammaire). Nous pouvons cependant considérer r_∞ comme la différence entre les deux séries de puissances « context-free » r^+ et r_∞^-; et corrélativement nous pouvons considérer que son support est l'ensemble des séquences qui ne sont pas engendrées le même nombre de

fois par un couple de C-grammaires $G+$ et $G-$ qui engendrent $r_\infty+$ et $r_\infty-$ respectivement. Posons $S = S+ - S-$ de telle façon que (25) devienne :

$$(27)\quad \begin{aligned} S+ - S- &= a - (S+ - S-)\, b\, (S+ - S-) \\ &= a - (S+bS+ - S+bS- - S-bS+ + S-bS-) \\ &= a + S+bS+ + S-bS+ - (S+bS+ + S-bS-). \end{aligned}$$

Considérons alors l'ensemble des équations :

$$(28)\quad \begin{aligned} &(i) && S+ = a + S+bS- + S-bS+ \\ &(ii) && S- = S+bS+ + S-bS-. \end{aligned}$$

C'est un ensemble d'équations positives à deux variables $S+$ et $S-$ admettant comme solution $(r_\infty+, r_\infty-)$, où $r_\infty+$ est la limite de la suite $r_0+, r_1- \ldots$, et $r_\infty-$ la limite de la suite $r_0+, r_1-, \ldots$ de (29) :

$$(29)\quad \begin{aligned} \rho_0 &= (r_0+, r_0-) = (0, 0) \\ \rho_1 &= (r_1+, r_1-) = (a, 0) \\ \rho_2 &= (r_2+, r_2-) = (a, aba). \end{aligned}$$

Il est clair que lorsque r_∞ est la solution de (25), $r_\infty = r_\infty{}^+ - r_\infty{}^-$. Mais de plus, $r_\infty{}^+$ est la série de puissances engendrée par la C-grammaire G^+ de symbole initial S^+ et de grammaire (28 i) et $r_\infty{}^-$ est la série de puissances engendrée par la C-grammaire G^- de symbole initial S^- et de grammaire (28 ii).

D'une manière analogue toute série algébrique de puissances peut être représentée (d'une infinité de façons différentes) par la différence de deux séries de puissances « context-free », et son support peut donc être considéré comme l'ensemble des séquences qui ne sont pas engendrées le même nombre de fois par deux C-grammaires. C'est ce que nous pouvons donner de plus concret comme interprétation d'une série algébrique de puissances.

Plus généralement, la même construction pourrait se faire pour un anneau quelconque de coefficients, au lieu de l'anneau des nombres naturels utilisés ci-dessus. Ce domaine reste inexploré. Par exemple si les coefficients sont pris modulo un nombre premier (i. e. si on considère comme « non produites » les séquences produites un nombre de fois égal à un multiple de p), la série formelle de puissances $\Sigma n > o z^{p^n}$ à un seul terminal z est algébrique [27] alors que son support ne peut être aucune des séries de puissances introduites plus haut.

3. Autres opérations sur les séries formelles de puissances.

3.1. Au § 2.2 nous avons vu qu'un ensemble de séries de puissances est fermé pour les opérations d'addition, produit, et multiplication par un entier. Nous avons signalé que le support de $r + r'$ est la réunion des

supports de r et r' et que le support de rr' est l'ensemble produit des supports de r et r', pourvu que les coefficients ne soient pas négatifs.

Considérons maintenant deux autres opérations pour lesquelles l'ensemble des séries de puissances est fermé, et considérons l'interprétation correspondante en théorie des ensembles pour leurs supports.

Il est classique de dire que r est quasi régulier si $< r, e > = 0$. Alors $r^{n'} \not\equiv 0 \pmod{\deg n}$ pour $0 < n < n'$ et l'élément $r^* = \lim_{n\to\infty} \Sigma_{0<n'<n} r^{n'}$ est bien défini. De plus r^* vérifie l'identité

$$r + r^*r = r + rr^* = r^* \tag{30}$$

qui le détermine de façon unique. C'est pourquoi on appelle habituellement r^* le quasi-inverse de r. Cette notion est en rapport direct avec la notion plus familière d'inverse grâce à la remarque suivante : si $r' = e - r$ et $r'' = e + r^*$, $r'r'' = (e - r)(e + r^*) = e - r + r^* - rr^* = e = r''r'$, c'est-à-dire $r'' = r'^{-1}$.
Inversement, étant donné r' tel que $< r', e > = 1$, on peut l'écrire : $r' = e - r$, où r est quasi régulier, si bien que $e + r^*$ est l'inverse de r''.

Remarquons que, par définition même de r^*, cette série de puissances n'a que des coefficients non négatifs si c'est le cas pour r, et que *supp.* $r^* = (supp.\ r)^*$ où au deuxième membre, l'étoile représente l'opération étoile de Kleene [21].

En particulier, si V est un ensemble arbitraire de lettres et si la série de puissances ν est définie par $<\nu, x> = 1$ si $x \in V$, $<\nu, x> = 0$ si $x \notin V$ (i. e. si ν est la fonction caractéristique de V), $e + V^*$ (au sens de Kleene) est l'ensemble de tous les mots engendrés par les lettres de V et $e + \nu^* = (e - \nu)^{-1}$ est la fonction caractéristique de cet ensemble. Ceci résulte du fait que tout mot $f \in V^*$ apparaît une fois et une seule dans la somme infinie $\Sigma_{n>0} V^n$. Par la suite, quand on connaît la fonction caractéristique r d'un ensemble de séquences, on peut aussi écrire la fonction caractéristique $(1 - V_T)^{-1} - r$ de son complément.

Il est inutile de remarquer que dans ce cas, cette dernière a des coefficients non négatifs et, bien qu'algébrique au sens défini plus haut, elle n'est pas pour autant obligatoirement « context-free ».

La deuxième opération que nous définissons est le produit d'Hadamard, ce qui généralise de l'une des manières possibles, la notion habituelle de l'analyse classique. La définition que nous donnons diffère des extensions diverses au cas de plusieurs variables que l'on trouve dans la littérature, mais paraît être l'extension la plus naturelle pour les séries de puissances non commutatives.

Si r et r' sont deux séries de puissances, leur produit d'Hadamard $r \odot r'$ sera la série de puissances dont les coefficients sont :

$$<r \odot r', f> = <r, f> <r', f> \tag{31}$$

identiquement pour toutes les séquences f.

D'où *supp.* $(r \odot r') = (supp.\ r) \cap (supp.\ r')$ et $r \odot r'$ est une fonction caractéristique si r et r' le sont.

Enfin, nous introduisons la notation suivante : étant donnée une séquence $x_{i_1} x_{i_2} \ldots x_{i_{n-1}} x_{i_n} = f(x_{i_j} \varepsilon V)$ nous définissons $\tilde{f}$ (l'image miroir de f) comme la séquence :

$$\tilde{f} = x_{i_n} x_{i_{n-1}} \ldots\ldots\ldots x_{i_2} x_{i_1}. \tag{32}$$

Il est clair que $\tilde{\tilde{f}} = f$ et la relation $ff' = f''$ implique $\tilde{f}'' = \tilde{f}'\tilde{f}$. Formellement, cette application est un *antiautomorphisme involutif* de l'anneau des séries de puissances, et on peut démontrer qu'il est caractérisé de façon unique par cette propriété (à une permutation près des éléments de V).

3.2. La notation qui vient d'être introduite sera utilisée plus loin pour simplifier la description des grammaires de la manière suivante. Supposons que la grammaire G contienne les règles :

$$\begin{aligned} \alpha_1 &= \pi_1\alpha_2\pi_2 + \pi_1\pi_2 + \pi_3 \\ \alpha_2 &= \alpha_2\pi_4 + \pi_4 \end{aligned} \tag{33}$$

où les π_j sont des expressions polynômiales sur $V - \{\alpha_1\}$. Alors la seconde règle entraîne :

$$\alpha_2 = \left(\sum_{n>0} \pi_4^n\right) \tag{34}$$

et on peut remplacer les règles (33) par la règle plus simple :

$$\alpha_1 = \pi_1(1 - \pi_4)^{-1}\pi_2 + \pi_3. \tag{35}$$

On peut, d'ailleurs, donner une interprétation linguistique de cette forme simplifiée de description. Ainsi, par exemple, un couple de règles de la forme $\alpha_1 \to f_1\alpha_2 f_2$, $\alpha_2 \to \alpha_2\alpha_2$ c'est-à-dire un couple que l'on peut désormais écrire : $\alpha_1 \to f_1(1 - \alpha_2)^{-1} f_2$ peut être considéré comme constituant en fait un schéma de règle : $\alpha_1 \to f_1\alpha_2^n f_2 (n = (1, 2, \ldots))$. Avec cette nouvelle interprétation, la grammaire, bien qu'encore déterminée par un nombre fini de schémas de règle, contient une infinité de règles. Rappelons alors la façon dont une description structurale (un parenthésage étiqueté) est attribuée à une séquence terminale engendrée par une C-grammaire (voir ci-dessus, § 1). Une grammaire déterminée par le schéma de règle ci-dessus peut engendrer une description structurale de la forme :

$$\ldots [_{\alpha_1} f_1 [_{\alpha_2} p_1] [_{\alpha_2} p_2] \ldots [_{\alpha_2} p_n] f_2] \ldots \tag{36}$$

pour chaque n, où chaque p_k est dérivé de α_2. Dans la phrase (séquence terminale) ayant cette description, chaque $\bar{p}_k$ est un syntagme du type α_2, où $\bar{p}_k$ est formé par « déparenthésage » de p_k. Les syntagmes successifs $\bar{p}_1, \ldots, \bar{p}_n$, constituent une « coordination », qui, prise avec les séquences

finales provenant de f_1 et f_2, est une construction de type α_1. Ceci est la manière naturelle d'étendre les C-grammaires pour rendre compte de la véritable coordination, comme par exemple lorsqu'une séquence d'adjectifs de longueur arbitraire et sans structure interne peut apparaître en position d'attribut. Cf. Chomsky [10].

3.3. Essayons de rattacher ce qui a été fait jusqu'à présent, à l'analyse classique en écrivant $\varphi f = \varphi f'$, pour deux séquences quelconques f et f', si elles contiennent exactement le même nombre de chacune des lettres (qu'elles soient terminales ou non).

Il est clair que φ se prolonge en une application de nos séries de puissances non commutatives sur l'anneau des séries *formelles* de puissances ordinaires (commutatives) à coefficients entiers et il est facile de voir que φ est un homomorphisme. Par exemple, si $\alpha = a + b\alpha\alpha$, on a : $\varphi\alpha = \varphi a + \varphi b\varphi\alpha\varphi\alpha$, et $\varphi\alpha$ est la série de puissances ordinaire

$$\varphi\alpha = \sum_n (\varphi a)^{n+1} (\varphi b)^n \begin{bmatrix} 2n \\ n \end{bmatrix} \frac{1}{n+1} \tag{37}$$

par rapport aux variables ordinaires φa, φb. (Ici, avec $\alpha' = a + \alpha' b\alpha'$, on aurait aussi $\varphi\alpha' = \varphi\alpha$.)

De plus, on peut montrer directement, à partir de la façon dont on obtient nos séries de puissances que les coefficients n'augmentent pas plus vite qu'une fonction exponentielle du degré (longueur) des séquences. Ainsi l'image φ de n'importe laquelle de nos séries de puissances est en fait une série de Taylor convergente ordinaire, développement d'une fonction algébrique.

Réciproquement, si on se donne des variables (ordinaires) $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$, une fonction algébrique (ordinaire) de cette quantité $\bar{y}$ est définie par un polynôme en $\bar{y}$ et les $\bar{x}$; et si $\bar{y}$ admet un développement en série de Taylor (à coefficients entiers) au voisinage de zéro, par rapport aux $\bar{x}_i$, on peut lui associer une infinité de séries formelles de puissances β telles que $\varphi\beta = \bar{y}$ et β est définie par des équations formelles. Par exemple en partant de la fonction algébrique $\bar{y}$ de $\bar{a}$ et $\bar{b}$ définie par $\bar{y}^2\bar{b} - \bar{y} + \bar{a} = 0$ on obtient les deux exemples donnés plus haut, ainsi que la série formelle de puissances :

$$\alpha = a + b\alpha\alpha + \pi\alpha - \alpha\pi \tag{38}$$

où π est un polynôme quelconque en a et b. Ainsi par exemple, pour $\pi = b$:

$$\begin{aligned} &\alpha_0 = a \\ &\alpha_1 = a + baa + ba - ab \\ &\ldots\ldots\ldots \\ &\text{etc.} \end{aligned} \tag{39}$$

3.4. Concluons en donnant quelques liens entre nos réflexions et la théorie de Lyndon des équations dans un groupe libre (Lyndon, 1960).

Soit $\{ x_i \}$ $(1 \leqslant i \leqslant n)$ un vocabulaire terminal, ξ une lettre non terminale, et w un produit de termes de la forme $1 - x_i, (1 - x_i)^{-1}, 1 - \xi, (1 - \xi)^{-1}$. On définit $deg\ (w) = d^+ - d^-$ où d^+ et d^- sont les nombres de facteurs $1 - \xi$ et $(1 - \xi)^{-1}$ dans w. Ainsi par exemple pour $w = (1 - x_2)(1 - x_1)(1 - \xi)(1 - x_i)^{-1}(1 - \xi\xi_i)^{-1}(1 - x_2)^{-1}$, on a $deg(w) = 1 - 1 = 0$.

Il est bien connu que les éléments $1 - x_i$ engendrent (par multiplication) un groupe libre G. La relation $w = 1$ peut être considérée comme une équation d'inconnue ξ. Avec notre terminologie, une solution de $w = 1$ serait une série de puissances ξ_0 en les x_i telle que $w = 1$ identiquement, quand ξ_0 est substituée à ξ dans w; ξ_0 sera une solution de groupe si de plus, $1 - \xi_0 \in G$; i. e., si $1 - \xi_0$ est exprimable comme produit de termes $(i - x_i)^{\pm 1}$. R. C. Lyndon a démontré le résultat très remarquable, que l'on peut obtenir par algorithme la *totalité* des *solutions de groupes*.

Rattachons une partie de cette question à nos remarques du § 2.3. Pour cela introduisons les nouveaux symboles ξ_i $(1 \leqslant i \leqslant n)$, et les équations :

$$\xi_i = x_i + \xi_i x_i \ ; \ \mu = \xi^2 + \xi\mu \tag{1}$$

de telle façon que $(1 - x_1)^{-1} = 1 + \xi_i$ et $(1 - \xi)^{-1} = 1 + \xi + \xi^2 + \xi\mu$

En substituant ces expressions dans $w = 1$, et après simplification, on obtient une relation :

$$(deg(w))\xi = \rho \tag{2}$$

où ρ est un polynôme en les variables x_i, ξ_i, μ, sans terme de degré inférieur à 2.

Par suite si $deg(w) \neq 0$ le système (1), (2) a une solution et une seule en série de puissances (le fait que les coefficients puissent être éventuellement rationnels plutôt qu'entiers ne change rien à la démonstration du § 2.3) et puisque les solutions de groupe forment un sous-ensemble des séries de puissances solutions, nous avons vérifié directement que si $deg(w) \neq 0$ l'équation de groupe libre $w = 1$ a au plus une solution.

Au contraire, si $deg(w) = 0$ (comme par exemple pour l'équation $w = (1 - \xi)(1 - x_i)(1 - \xi)^{-1}(1 - x^i)^{-1} = 1$ notre méthode n'opère plus du tout et ne dit même rien quant aux solutions quelconques (sans restriction) de $w = 1$.

Par exemple $(1 - x_i)(1 - \xi)(1 - x_i)^{\varepsilon}(1 - \xi)^{-1} = 1$ n'a pas de solution pour $\varepsilon \neq -1$ et a une infinité de solutions de *groupe* si $\varepsilon = -1$, viz. $1 - \xi = (1 - x_i)^{\pm n}$ $(n > 0)$. En effet, l'équation peut alors aussi bien s'écrire : $\xi x_1 = x_1 \xi$ (qui a comme solutions, dans notre théorie, toutes les séries de puissance en x_1).

Évidemment, le cas $deg(w) = 0$ est justement celui dans lequel l'inconnue $1 - \xi$ disparaît, quand on prend l'image commutative comme au § 3.3 et c'est le cas non trivial du point de vue de la théorie des groupes.

4. Types de C-grammaires et leurs propriétés générales.

4.1. En termes de conditions sur les règles qui les constituent, on peut définir plusieurs catégories de C-grammaires particulièrement intéressantes. Dans la suite α,β ... seront des symboles non terminaux; f, g, ... des séquences terminales (pouvant être nulles); et φ, ψ des séquences quelconques. Rappelons que nous avons exclu la possibilité des règles de la forme $\alpha \to e$ ou $\alpha \to \beta$ en remarquant que cette restriction ne modifie pas la capacité génératrice. Nous décrirons les C-grammaires en termes de règles ou d'équations, selon ce qui sera le plus commode.

Si la grammaire G ne contient pas de non-terminal α duquel on peut dériver à la fois une séquence f' et une séquence $f\alpha g$, le langage terminal $L(G)$ engendré par G sera fini. Dans ce cas G sera appelée une *grammaire polynômiale.*

Considérons maintenant des règles grammaticales des types suivants :

(40) (i) $\alpha \to f\beta$ (linéaire à droite)
(ii) $\alpha \to \beta f$ (linéaire à gauche)
(iii) $\alpha \to f\beta g$ (linéaire)
(iv) $\alpha \to fg$ (terminantes)

Une grammaire ne contenant que des règles linéaires à droite et terminantes ou des règles linéaires à gauche et terminantes sera appelée une grammaire *linéaire unilatère.*

Une grammaire ne contenant que des règles du type (40) sera dite *linéaire.* Supposons que G ne contienne que des règles du type (40) et du type $\alpha_1 \to \varphi$ où α_1 est le symbole initial de G; et que, de plus, elle ne contienne aucune règle $\beta \to \varphi\alpha_1\psi$. Ainsi, l'équation de définition de α_1 sera $\alpha_1 = \pi_1$ où π_1 est un polynôme qui ne fait pas intervenir α_1. Une telle grammaire sera dite *méta-linéaire.*

Étant donnée une grammaire G (i. e. un ensemble d'équations positives) polynômiale, linéaire unilatère, linéaire, méta-linéaire ou « context-free », on dira que la série de puissances r, terme principal de sa solution (i. e. qu'elle *engendre*, au sens du § 2.3) et le langage *Supp.* (r) qu'elle engendre, sont respectivement polynômiaux, linéaires unilatères, linéaires, méta-linéaires, ou « context-free ». Ces familles de séries de puissances seront désignées respectivement par $P+, L_o^+, L+, L_m^+, C+$; et pour chaque famille F la famille des supports de F sera notée *Supp.* (F).

Remarquons que *Supp.* ($P+$) est simplement la famille des ensembles finis, et que *Supp.* (L_o+) est la famille des événements réguliers, au sens de Kleene [21] (cf. Chomsky [7]. Remarquons que la classe des événements réguliers est fermée par réflexion).

Considérons maintenant quelques propriétés élémentaires de ces familles de langages.

Il est d'abord immédiat que l'on a les relations d'inclusion suivantes pour ces familles :

(41) $Supp.(P^+) \subset Supp.(L_0{}^+) \subset Supp.(L^+) \subset Supp.(L_m{}^+) \subset Supp.(C^+)$. De plus, dans chacun de ces cas l'inclusion est stricte. D'où :

PROPRIÉTÉ 1.

$$Supp.(P^+) \subsetneq Supp.(L_0{}^+) \subsetneq Supp.(L^+) \subsetneq Supp.(L_m{}^+) \subsetneq Supp.(C^+).$$

L'exemple le plus simple d'un langage de $Supp.(L^+)$ mais non de $Supp.(L_0{}^+)$ est l'ensemble de toutes les séquences $\{a^n b a^n\}$ $(a,b \in V_T)$. Il est engendré par la grammaire : $\alpha = a\alpha a + b$, et il est facile de montrer que ce n'est pas un événement régulier. Le produit des langages dans $Supp.(L^+)$ est toujours dans $Supp.(L_m{}^+)$, mais n'est généralement pas dans $Supp.(L^+)$. Le langage L_{IC} de notre exemple (18) ci-dessus, avec la grammaire

$$\alpha = a + b\alpha\alpha \tag{42}$$

qui est formé des formules du calcul des implications à une variable libre en notation polonaise, est dans $Supp.(C^+)$ mais non dans $Supp.(L_m{}^+)$. Ceci résulte du fait que L_{IC} contient toutes les séquences de la forme :

$$b^{m_1} a^{m_1} b^{m_2} a^{m_2} \ldots b^{m_k} a^{m_k} a, \tag{43}$$

pour tout $k \geqslant 1$, $m_i \geqslant 1$. Mais chaque séquence de L_{IC} contient n occurrences de b et $n+1$ occurrences de a, pour un $n \geqslant 1$. Par suite un entier k étant fixé pour engendrer toutes les séquences de la forme (43), on doit pouvoir dériver du symbole initial de la grammaire de L_{IC} une séquence φ contenant k occurrences de non-terminaux. Par suite cette grammaire ne peut être métalinéaire.

Dans une interprétation empirique des C-grammaires, la relation entre $Supp.(C^+)$ et $Supp.(L_0{}^+)$ est particulièrement importante, du fait qu'un procédé fini, où sont incorporées les instructions d'une C-grammaire G engendrant $L(G)$ comme représentation de sa compétence intrinsèque, ne pourra interpréter que les phrases d'un sous-ensemble fixe $R \in Supp.(L_0{}^+)$ de $L(G) \in Supp.(C^+)$ au moyen de mécanismes supplémentaires fixés). Cette relation peut justement se décrire grâce à certains traits formels des descriptions structurales (parenthésages étiquetés) engendrées par les C-grammaires. Cf. § 1.

Disons que G est une grammaire *auto-imbriquée* si elle engendre une description structurale de la forme :

$$[\alpha\varphi[\alpha\,\psi]\varkappa]\ldots, \tag{44}$$

où φ et $\varkappa$ contiennent des terminaux non nuls et où ψ est une expression bien parenthésée. Nous avons le résultat suivant :

THÉORÈME 1*a*.

$L \not\in L_0^+$ *si et seulement si toute C-grammaire engendrant* L *est auto-imbriquée.* Chomsky [9].

Ce résultat peut s'étendre de la manière suivante. Définissons le *degré d'auto-imbrication* d'une description structurale D comme le plus grand N telle que D contienne une sous-configuration :

$$[\alpha\varphi_1[\alpha\varphi_2[\cdots[\alpha\varphi_{N+1}]\varphi_{N+2}]\cdots]\varphi_{2N+1}]$$

où chaque φ contient des terminaux non-nuls. Alors il existe une bijection effective Φ de $\{(G, n);\ G$ est une C-grammaire, $n \geqslant 1\}$ dans l'ensemble des grammaires linéaires unilatères et une bijection effective Ψ de l'ensemble Δ des descriptions structurales dans Δ telles que :

THÉORÈME 1*b*.

Pour tout $L \in$ *Supp.* (C^+), *il y a une C-grammaire qui engendre* L, *telle que pour chaque* N, $\Phi(G, N)$ *engendre* f *avec la description structurale* D *si et seulement si* G *engendre la séquence terminale* f *avec la description structurale* (ΨD) *où* (ΨD) *a un degré d'auto-imbrication* $\leqslant N$. Chomsky [8].

Ainsi, intuitivement, on peut, étant donnée G, construire un procédé fini $\Phi(G, N)$ qui reconnaisse la structure d'une séquence f engendrée par G pourvu que le degré d'auto-imbrication d'une description structurale particulière de f ne dépasse pas N. Ceci suggère plusieurs conséquences d'ordre empirique. Pour une discussion, cf. Chomsky [10], Miller et Chomsky [29].

4.2. Considérons maintenant diverses propriétés de clôture de ces familles de langages.

On peut caractériser algébriquement les familles de séries de puissances ci-dessus de la manière suivante : P^+ est un demi-anneau [6], L_o^+ est le plus petit demi-anneau contenant P^+ et fermé par quasi-inversion des éléments quasi-réguliers.

L^+ est un module, et L_m^+ est le plus petit demi-anneau le contenant. L'ensemble C^+ est un demi-anneau fermé par quasi-inversion des éléments quasi-réguliers.

Corrélativement, on a les propriétés suivantes des supports : *Supp.* (P) est fermé pour la réunion ensembliste, et le produit ensembliste; *Supp.* (L_o^+) est le plus petit ensemble contenant les ensembles finis et fermé pour les opérations : union ensembliste, produit ensembliste, et l'opération étoile décrite au § 3.1 [21]; *Supp.* (L^+) est fermé pour l'union ensembliste, mais non pour le produit ensembliste, *Supp.* (L_m^+) est le

6. La notion de demi-anneau généralise celle d'anneau par le fait que la structure d'addition n'est qu'une structure de monoïde (et non nécessairement de groupe). Un demi-anneau typique, est « l'anneau Booléen » à deux éléments *0* et *1* et avec les règles $(0 = 0 + 0 = 00 = 01 = 10;\ 1 = 0 + 1 = 1 + 0 = 1 + 1 = 11)$.

plus petit ensemble contenant les ensembles de *Supp.* (L^+) et fermé pour le produit ensembliste (c'est évidemment la raison de la construction de $L_m{}^+$); l'ensemble *Supp.* (C^+) est fermé pour l'union, le produit, et l'opération étoile.

Ces propriétés sont immédiates et il est naturel d'examiner la clôture par rapport aux autres opérations ensemblistes élémentaires, à savoir l'intersection et la complémentation.

Il est évident que *Supp.* (P^+) est fermé pour l'intersection, et il est bien connu que la classe *Supp.* $(L_0{}^+)$ des événements réguliers est fermée pour l'intersection et la complémentation.

Pour les autres familles, on a les résultats suivants : la famille *Supp.* (C^+) de tous les C-langages n'est pas fermée pour l'intersection et donc (puisqu'elle est fermée pour la réunion) n'est pas fermée pour la complémentation [40], [2]. L'exemple donné dans chacune de ces références est un couple de langages métalinéaires dont l'intersection n'est pas « context-free ». Il s'ensuit donc que *Supp.* $(L_m{}^+)$ n'est pas non plus fermé pour l'intersection, donc pour la complémentation. On peut obtenir un résultat plus fort qui couvre les grammaires linéaires, et d'ailleurs (pour l'intersection) même les grammaires linéaires à un seul non-terminal.

Pour cela, considérons les grammaires G_1 et G_2 définies respectivement par (45) et (46) :

$$\alpha = aa\alpha c + b\alpha c + bc \tag{45}$$

$$\alpha = a\alpha cc + a\alpha b + ab. \tag{46}$$

G_1 et G_2 sont chacune linéaires à un seul non-terminal, mais l'intersection des langages qu'elles engendrent est l'ensemble des séquences $\{a^{2n}b^na^{2n}\}$ qui n'est pas « context-free ». Cet exemple (plus le fait que ces familles, sont fermées pour la réunion) établit la /

PROPRIÉTÉ 2.

Les familles *Supp.* (L^+), *Supp.* $(L_m{}^+)$, *Supp.* (C^+) ne sont fermées ni pour l'intersection, ni pour la complémentation; l'intersection de deux ensembles dans une de ces familles peut n'être même pas dans *Supp.* (C^+), même quand les ensembles en question sont engendrés par des grammaires à un seul non-terminal.

On peut penser que le complément d'un langage de *Supp.* (L^+) ou de *Supp.* $(L_m{}^+)$ n'est pas un C-langage (i. e. n'est pas un élément de *Supp.* $(\bar{C}^+)$). Cependant, nous n'avons pas d'exemple qui indique ceci.

Donc, parmi les classes de langages considérés ci-dessus, seuls les événements réguliers (et les ensemble finis) sont fermés par formation d'intersections. Cependant, l'intersection d'un événement régulier et d'un C-langage est encore un C-langage. Nous avons en fait le résultat suivant plus fort et qui étend un théorème d'analyse classique dû à R. Jungen [20].

THÉORÈME 2.

Supposons que $r_1 \varepsilon \lambda_0{}^+$. Soit U^+ une des familles P^+, $\lambda_0{}^+$, λ^+, $\lambda_m{}^+$, C^+. Soit $r_1 \odot r_2$ le produit d'Hadamard de r_1, r_2 (cf. § 3.1). Alors $r_1 \odot r_2 \varepsilon U^+$, pour tout $r_2 \varepsilon U^+$. De plus si $r_2, r_3 \varepsilon \lambda_0{}^+$, alors $r_2 \odot r_3 \varepsilon \lambda_0{}^+$.

Cf. Schützenberger [46]. Il s'ensuit que l'intersection d'un langage de *Supp.* (U^+) avec un événement régulier est dans *Supp.* (U^+) pour tout U^+. La démonstration de ce résultat, lié à un résultat analogue sur la clôture par transduction, sera esquissée au § 8, ci-dessous.

4.3. La catégorie des grammaires linéaires est particulièrement intéressante, comme nous le verrons directement, et nous allons maintenant faire quelques observations préliminaires à son sujet.

Remarquons que si L est un langage engendré par une grammaire linéaire, on peut trouver un vocabulaire V', disjoint de V_T, deux homomorphismes α, α' de $F(V')$ dans $F(V_T)$, un événement régulier R dans V' et un ensemble fini $C \subset F(V_T)$ tel que L se compose exactement des séquences $f = \alpha(g)c\alpha'(\overset{\leftarrow}{g})$, où $g \varepsilon R$, $\overset{\leftarrow}{g}$ est la réflexion de g et $c \varepsilon C$. Ainsi un processus fini appliqué à une collection de couples de séquences ou un couple de processus finis coordonnés peut, en général, être rattaché à une grammaire linéaire et étudié de cette façon.

D'une manière équivalente, on peut caractériser un langage linéaire de la façon suivante légèrement différente. Soit $V' = V^+ \cup V^- - (V^+ = \{ \nu_i : 0 \leqslant i \leqslant n \}; V^- = \{ \nu_i : -n \leqslant i \leqslant -1 \}$. Si $f \varepsilon F(V^+)$, définissons f comme le résultat de la substitution de ν_{-i} à ν_i dans f, partout. Alors un langage linéaire L est déterminé par le choix d'un homomorphisme β de $F(V')$ dans $F(V_T)$, un événement régulier R dans V^+, et un ensemble fini $C \subset F(V_T)$. L est maintenant l'ensemble de séquences $\beta(f)c\beta(f)$, où $f \varepsilon R$ et $c \varepsilon C$. Nous utiliserons cette deuxième caractérisation ci-dessous.

Nous pouvons maintenant déterminer des classes spéciales de langages linéaires en imposant des conditions supplémentaires à l'événement régulier R correspondant, aux applications α, α', et à la classe C. En particulier dans les applications ci-dessous nous nous intéresserons au cas où R, est simplement un monoïde libre (un événement régulier défini par un automate à un seul état) et où C contient seulement $c \varepsilon V_T$, où $\alpha(f) \neq \varphi c \psi \neq \alpha'(f)$. Nous appellerons les grammaires définies par cette condition des *grammaires linéaires minimales.*

Une grammaire linéaire minimale contient un seul symbole non terminal S et une seule règle terminale $S \to c$, et aucune règle non terminale $S \to \varphi c \psi$. Ainsi toute séquence du langage qu'elle engendre a le « marqueur central » désigné c. Ceci est l'ensemble de langages le plus simple de notre cadre, après les événements réguliers et nous verrons qu'ils diffèrent nettement des événements réguliers par beaucoup de propriétés formelles.

Donnons tout de suite un résultat sur les grammaires linéaires mini-

males qui sera utilisé par la suite. Prenons V', $V_T = W \cup \{ c \}$ $(c \notin W)$, α et α' comme ci-dessus. Soit G la grammaire linéaire minimale définie par α, α' et engendrant $L(G)$. Ainsi G a l'équation de définition :

$$\beta = c + \Sigma \{ \alpha(\nu)\beta\alpha'(\nu) : \nu \in V' \} \tag{47}$$

où α, α' sont des applications de $F(V')$ dans $F(W)$. Alors on a :

THÉORÈME 3.

Si α est un monomorphisme (isomorphisme dans), le complémentaire $F(V_T) \setminus L(G)$ *de* $L(G)$ *par rapport à* $F(V_T)$ *est engendré par une grammaire linéaire non-ambiguë.*

Démonstration : Soit $A = \alpha(V')$, $F(A) = \alpha F(V')$, et pour tout ensemble $F \subset F(W)$ soit $F^+ = \{ f \in F : f \neq e \}$.

Il est clair qu'il y a une partition : $F(V_T) \setminus L(G) = L \cup L'$, telle que

$$L = fcf' : f \in F^+(A),\ f' \in F(W),\ fcf' \notin L(G); \tag{48}$$

$L' = F(W) \cup cF(W) \cup ((F(W) \setminus F(A))cf(W) \cup F(V_T)cF(V_T)cF(V_T)$. Mais L' est un événement régulier. Il suffit donc de montrer que L est engendré par une grammaire linéaire non ambiguë.

Puisque α est un monomorphisme, il existe un isomorphisme $\bar{\alpha}$: $F(A) \to F(V')$. On étend α' à $F^+(A)$ en définissant $\alpha' a = \alpha'(\bar{\alpha}\, a)$, pour $a \in F^+(A)$.

Supposons que $acf' \in L$. Ainsi $a \in F^+(A)$, $f' \in F(W)$ et $f' \neq \alpha' a$. Par définition il n'y a que trois possibilités pour acf' et elles s'excluent mutuellement.

(49) (i) $f' \in F^+(W)\alpha' a$
(ii) $\alpha' a \in F^+(W)f'$
(iii) $a = a_1 a_2 a_3$ et $f' = hwg\alpha' a_1$ (où $a_1, a_3 \in F(A)$; $a_2 \in A$; $w \in W$; $h, g \in F(W)$; $\alpha' a_2 \in F^+(W)g$; $\alpha' a_3 \in F(W)wg$).

(49i) est le cas où f' a $\alpha' a$ comme facteur propre à droite.

(49ii) est le cas où $\alpha' a$ a f' comme facteur propre à droite.

(49iii) est le cas où $\alpha' a$ et f' ont le même facteur maximal à droite la séquence $g\alpha' a_1$, qui est une sous-séquence propre de $\alpha' a$ et f' à la fois.

Les trois cas s'excluent donc deux à deux et sont exhaustifs; on a une partition de L en trois sous-ensembles L_1, L_2, L_3, constitués respectivement des séquences qui vérifient (i), (ii), (iii). Ce qu'il nous reste à montrer, c'est que chacun des langages L_1, L_2, L_3 est engendré par une grammaire linéaire non ambiguë.

Pour L_1 et L_2 c'est évident. Soit $\overline{A} = \Sigma \{ a : a \in A \}$ et $\overline{W} = \Sigma \{ w :$

$w \varepsilon W \}$. Alors L_1 est engendré par la grammaire (50) et L_2 par la grammaire (51) (cf. § 3.2).

$$\beta = \Sigma \{ a\beta\alpha' a : a \varepsilon A \} + c(1 - \overline{W})^{-1} \tag{50}$$

$$\beta = \Sigma \{ a\beta\alpha' a : a \varepsilon A \} + (1 - \overline{A})^{-1} c. \tag{51}$$

Envisageons maintenant le cas de L_3. Pour tout $a \varepsilon A$, soit $B(a)$ l'ensemble de toutes les séquences wg ($w \varepsilon W$, $g \varepsilon F(W)$) telles que $\alpha' a \varepsilon F^+(W)\, g$ et $\alpha' a \notin (W)\, wg$. Il est clair que $B(a)$ est toujours un ensemble fini, puisque g est plus court que $\alpha' a$. On peut alors engendrer L_3 par grammaire linéaire non-ambiguë d'équations :

$$\beta_1 = \Sigma \{ a\beta_1\alpha' a : a \varepsilon A \} + \Sigma \{ a\beta_2 b : a \varepsilon A, b \varepsilon B(a) \} \tag{52}$$

$$\beta_2 = c + c(1 - \overline{W})^{-1} + (1 - \overline{A})^{-1} c + \Sigma \{ a\beta_2 w : a \varepsilon A, w \varepsilon W \}.$$

La vérification est sans problème. Mais alors $F(V_T) \setminus L(G)$ se trouve être exprimé comme la réunion de quatre ensembles disjoints L_1, L_2, L_3, L', qui ont chacun une grammaire linéaire non-ambiguë. Il en résulte que $F(V_T) \setminus L(G)$ a lui-même une grammaire linéaire non ambiguë, ce qu'on voulait démontrer.

Remarquons que si on avait pris pour α au départ « une transduction sans perte d'information » [43] au lieu d'un monomorphisme, on aurait pu démontrer un résultat où la seule différence avec le théorème 3 serait que la grammaire linéaire construite aurait une ambiguïté bornée au lieu d'être non ambiguë.

4.4. Nous avons considéré plusieurs sous-familles de la classe des C-grammaires, en les classant d'après les propriétés structurales des règles de définition. On peut envisager d'autres principes de classification. Ainsi par exemple, il serait peut-être utile d'isoler la classe de grammaires (langages) étoile caractérisée de la façon suivante : G est une grammaire étoile si à chaque non-terminal α_i de G sont associés un ensemble Σ_i de non-terminaux et trois séquences terminales f_i, f'_i, f''_i, et G contient toutes les règles suivantes à l'exclusion de toute autre : $\alpha_i \to f''_i$, $\alpha_i \to f_i \alpha_j f'_i$ ($\alpha_j \varepsilon \Sigma_i$), $\alpha_j \to \alpha_k \alpha_l (\alpha_j, \alpha_k, \alpha_l \varepsilon \Sigma_i)$. Ce sont, en un sens, les C-grammaires les « moins structurées ». L'intérêt de ces langages vient du fait que les équations définissant les séries de puissances associées sont exprimables en n'utilisant de manière essentielle, que le quasi-inverse et l'addition, comme nous l'avons remarqué au § 3.2. Remarquons en particulier, que le langage non-métalinéaire L_{IC} défini par (42) est un langage étoile. Nous avons suggéré une interprétation linguistique de la notion de langage étoile au § 3.2.

Un autre principe de classification pourrait résider dans le nombre des non-terminaux de la grammaire définissante minimale d'une certaine série de puissances. Cependant, il ne paraît pas probable que les propriétés intéressantes du langage puissent être reliées à une mesure aussi peu sensible aux traits structuraux des grammaires (sauf dans le cas particu-

lier des langages définis par des grammaires à un seul non-terminal), car pour les monoïdes différents des groupes, il n'y a pas de relation intéressante entre les paramètres numériques grossiers, et la structure fine. Remarquons, d'ailleurs, que pour tout N fini, on peut construire un événement régulier qui ne peut être engendré par une C-grammaire à moins de N symboles non-terminaux.

La considération des inter-dépendances entre les différentes parties d'une grammaire suggère un autre principe de classification. Disons qu'une C-grammaire est *irréductible*, si aucun sous-ensemble propre de l'ensemble des équations de définition ne constitue une C-grammaire (rappelons que des séquences terminales doivent être dérivables de chaque symbole non terminal non-initial d'une C-grammaire); dans le cas contraire la grammaire sera dite *réductible*. Si une C-grammaire est réductible dans ce sens, il doit y avoir des sous-ensembles propres Σ_1 de ses règles et Σ_2 de ses non-terminaux, tels que seules des règles de Σ_1 interviennent dans la transformation des dérivations en dérivations terminales aux points où des symboles de Σ_2 apparaissent dans les lignes de dérivations.

Un cas extrêmement particulier de la réductibilité a été étudié par Ginsburg et Rice [18]. Comme eux, disons qu'une C-grammaire G est séquentielle si ses non-terminaux peuvent être ordonnés en une suite $\alpha_1, \ldots, \alpha_n$ (où α_1 est le symbole initial) de telle façon qu'il n'y ait aucune règle $\alpha_i \to \varphi\alpha_j\psi$ pour $j < i$. La solution d'une grammaire séquentielle est particulièrement facile à déterminer par le processus itératif décrit au § 2.3, par élimination successive des variables.

Pour la famille S^+ des grammaires séquentielles et pour la famille *Supp.* (S^+) de leurs supports, Ginsburg et Rice établissent les résultats suivants, analogues aux précédents. D'abord il est clair que S^+, comme C^+ est un demi-anneau fermé par quasi-inversion d'éléments quasi-réguliers. Corrélativement *Supp.* (S^+) est fermé par réunion, produit et opération étoile. De ce fait, et du fait que $P^+ \subset S^+$ il résulte que *Supp.* $(L_o{}^+) \subset$ *Supp.* (S^+). De plus, l'inclusion est stricte, comme le montre la grammaire (42) qui, puisqu'elle ne contient qu'un seul terminal, est séquentielle. On a donc :

$$\text{(53)} \qquad \textit{Supp.}\ (L_o{}^+) \subsetneq \textit{Supp.}\ (S^+) \subsetneq \textit{Supp.}\ (C^+).$$

Ginsburg et Rice montrent qu'il n'y a pas de grammaire séquentielle pour le langage de vocabulaire $\{a, b, c, d\}$, et qui contient les séquences :

$$\text{(54)} \qquad a^{n_{2k-1}} d \ldots d b^{n_2} d a^{n_1} d b^{n_2} d \ldots b^{n_{2k-2}} d a^{n_{2k-1}}$$

(qui est symétrique par rapport à c) pour toute suite $(k, n_1, \ldots, n_{2k-1})$ d'entiers positifs, bien que ce langage soit engendré par la grammaire

$$\text{(55)} \qquad \begin{aligned} \alpha &= ad\beta da + a\alpha a + aca \\ \beta &= b\beta b + bd\alpha db. \end{aligned}$$

Il n'existe cependant pas de relation plus forte que (53) entre *Supp.* (S^+) et les familles de *Propriété 1*, § *4.1.* La grammaire (55) est en fait linéaire, mais non séquentielle, si bien que *Supp.* $(L^+) \not\subset$ *Supp.* (S^+); et la grammaire (42) est séquentielle mais non méta-linéaire, si bien que *Supp.* $(S^+) \not\subset$ *Supp.* $(L_m{}^+)$.

Les grammaires (45) et (46) étant séquentielles, on voit que la *Propriété 2* (mais non le *théorème 2*) peut se généraliser à *Supp.* (S^+). Pour d'autres résultats sur les langages séquentiels, voir Ginsburg and Rose [19], Shamir [51].

5. Une autre caractérisation des familles de C-langages.

Dans cette section, nous aborderons d'une façon assez différente la définition des familles de langages et nous montrerons en quoi elle se rattache à la classification présentée ci-dessus. Nous nous appuierons ici sur deux notions fondamentales : celles d'*événement régulier standard* et de *langage de Dyck*, que nous définissons maintenant.

Un *événement régulier standard* A est donné par un alphabet fini X, deux sous-ensembles J_1 et J_2 de (X, X) et la règle que $f \varepsilon A$ si et seulement si

(56) (i) $f \varepsilon xF(X) \cap F(X)x'$, où $(x, x') \varepsilon J_1$

(ii) $f \notin F(X)xx'F(X)$, où $(x, x') \varepsilon J_2$.

A est ainsi l'ensemble de toutes les séquences qui commencent et finissent par des lettres imposées et qui ne contiennent aucun couple de lettres consécutives appartenant à J_2. C'est, plus techniquement, l'intersection du quasi-idéal déterminé par J_1 avec le complémentaire de l'idéal bilatère engendré par tous les produits xx' $((x, x') \varepsilon J_2)$. A est en particulier ce qu'on appelle parfois un *événement 1-défini* [21] [35].

Le langage de Dyck D_{2n} est défini sur les $2n$ lettres $x_{\pm i}$ $(1 \leqslant i \leqslant n)$ comme l'ensemble de toutes les séquences f qui se réduisent à la suite vide par la suppression réitérée de couples de lettres consécutives $x_j x_{-j}$ $(-n \leqslant j \leqslant n)$. Le langage de Dyck est un objet mathématique très connu : si φ est l'homomorphisme du monoïde libre engendré par $\{x_{\pm i}\}$ sur le groupe libre engendré par le sous-ensemble $\{x_i\} : i > 0$ qui satisfait identiquement $(\varphi x_i)^{-1} = \varphi x_{-i}$, D_{2n} est le noyau de φ, c'est-à-dire l'ensemble de séquences f telles que $\varphi f = 1$.

En ce qui concerne ces notions, nous avons les résultats suivants.

Proposition 1.

Pour tout événement régulier $BC \subset (Z)$, on peut trouver un événement régulier standard A et un homomorphisme $\alpha : F(X) \to F(Z)$, tels que $B = \alpha A$.

Il est bon de remarquer qu'on peut choisir cette représentation de telle façon que non seulement $B = \alpha A$ mais encore que chaque séquence

$f \varepsilon A$ ait le même degré d'ambiguïté que la séquence correspondante $\alpha f \varepsilon B$. C'est-à-dire que si $B = Supp.\ (\beta)$ on peut trouver γ tel que $A = Supp.\ (\gamma)$ et pour tout f, $< , \alpha f > = < \beta, \alpha f >$.

On peut généraliser la *Proposition 1* aux C-langages, en utilisant la propriété suivante de D_{2n}.

PROPRIÉTÉ 1.

D_{2n} *est engendré par une C-grammaire non-ambiguë.*

Pour obtenir une grammaire non-ambiguë de D_{2n}, on introduit $2n + 1$ non-terminaux : $\alpha_{\pm i} (1 \leqslant i \leqslant n)$ et β. Considérons maintenant les $2n + 1$ équations

$$(57)\quad (i) \qquad \alpha_i = x_i \Big(1 - \sum_{j \neq -i} \alpha_j\Big)^{-1} x_{-i}$$

$$\qquad (ii) \qquad \beta = (1 - \Sigma \alpha_i)^{-1}$$

(Cf. § 3.2, pour les notations.)

Intuitivement, on peut interpréter β comme la somme de toutes les séquences qui peuvent se réduire à la séquence vide par suppression de deux lettres consécutives $x_i x_{-i}$ Chaque α_i est la somme de tous les mots de *Supp.* (β) qui commencent par x_i et qui n'ont pas de facteur propre à gauche (ou à droite) dans *Supp.* (β). L'équation (57i) implique que tout $f \varepsilon$ *Supp.* (α_i) admet une factorisation et une seule

$$(58) \qquad f = x_i f_1 f_2 \ldots f_m x_{-i}$$

où chaque f_j appartient à un ensemble bien défini *Supp.* (α_i) (où j n'est pas $-i$, car nous voulons que la lettre initiale x_i ne s'annule qu'avec la lettre finale x_{-i}). De la même manière, chaque $f \varepsilon$ *Supp.* (β) admet une factorisation et une seule $f = f_1 \ldots f_m$, où les f_j appartiennent à $\cap$ *Supp.* (α_i).

Nous avons maintenant le résultat suivant, analogue à la *proposition 1.*

PROPOSITION 2.

Tout C-langage $L \subset F(Z)$ *est donné par un entier n, un événement régulier standard* A *sur* $X_{2n} = \{ x_{\pm i};\ 1 \leqslant i \leqslant n \}$, *un homomorphisme* φ : $F(X_{2n}) \to F(Z)$ et la règle $L = \varphi (A \cap D_{2n})$. [48] [49] [11] [12].

De nouveau, comme ci-dessus, l'énoncé implique que les séquences sont produites avec l'ambiguïté convenable. D'autre part, il est possible de choisir J_1 tel que $(x, x') \varepsilon J_1$ si x appartient à un certain sous-ensemble de X (cf. [48]).

On peut définir des familles particulières de langages comme celles qui viennent d'être envisagées, en imposant des conditions à l'événement régulier standard A et à l'homomorphisme φ. Ainsi, supposons qu'on

prenne l'événement régulier standard A sur l'alphabet $X \cup Y$ (où $X = \{ x_{\pm i};\ 1 \leqslant i \leqslant n \}$, $Y = \{ y_{\pm i};\ 1 \leqslant i \leqslant m \}$), défini par les conditions suivantes sur J_1 et J_2 :

(59) $J_1 = \{ (x_j, x_i) : i > 0 \}$
$J_2 = \{ (x_j, x_i) : \text{signe}(i) \neq \text{signe}(j) \} \cup \{ (y_i, y_j) : i < 0 \text{ ou } j > 0 \} \cup \{ (x_i, y_j) : i < 0 \text{ ou } j < 0 \} \cup \{ (y_i, x_j) : i > 0 \text{ ou } j > 0 \}$.

Ainsi chaque séquence a la forme $fgg'f'$, où $f, f' \in F(X)$; $g, g' \in F(Y)$; f, g (respectivement f', g') ne contiennent que des lettres d'indices positifs (respectivement négatifs). Si on désigne par X^+ et X^- les sous-ensembles de X constitués de lettres à indices positifs et négatifs, respectivement (de même Y^+ et Y^-) on peut représenter les transitions permises et exclues, par la matrice (60), où l'entrée 1 (0) indique que la transition de l'élément en tête d'une rangée à celui en tête d'une colonne est (n'est pas) permise et où U est une matrice de 1 et O une matrice de zéros.

(60)

	Y^+	Y^-	X^+	X^-
Y^+	U	U	O	O
Y^-	O	U	O	U
X^+	U	O	U	O
X^-	O	O	O	U

Mais considérons alors l'ensemble $A \cap D_{XY}$ (où D_{XY} est le langage de Dyck sur l'alphabet $X \cup Y$). Si $fg \in A$ (où $f \in F(X^+ \cup Y^+)$, $g \in F(X^- \cup Y^-)$), remplit la condition supplémentaire $fg \in D_{XY}$, g doit être l'image miroir de f (au changement près du signe des indices). C'est-à-dire, avec les notations du deuxième paragraphe de 4.3, $g = f$. Il est clair que si α est un homomorphisme de $F(X \cup Y)$ dans $F(V_T)$, $\alpha(A \cap D_{XY})$ est un langage linéaire. De plus, si on ajoute la condition $y_i = e$ pour $i < 0$ et $y_i = c$ pour tout $i > 0$, où $\alpha x_i \notin F(V_T) c F(V_T)$ pour tout i, alors $L = \alpha(A \cap D_{XY})$ est un langage linéaire minimal avec c comme symbole central désigné, et tout langage linéaire minimal est obtenu par un tel choix de α. Ceci donne une caractérisation indépendante des langages linéaires minimaux.

De plus, en ajoutant des couples supplémentaires à J_2, on peut délimiter le langage canonique A défini de telle façon que $\{ f : f \in F(X^+)$ et il existe g tel que $fg \in A$ et $g \in F(Y)F(X) \}$ soit un événement régulier quelconque (et non plus simplement le monoïde libre sur X^+, comme auparavant), si bien que $L = \alpha(A \cap D_{XY})$ sera un langage linéaire quelconque. On a ainsi une définition indépendante de la notion de « langage linéaire ». (Remarquons que ces restrictions supplémentaires sur J_2, ne jouent que sur les transitions permises dans les matrices de la diagonale principale de (60).)

D'une façon tout à fait semblable, on peut donner une définition générale d'un « langage métalinéaire ». Ainsi, par exemple, considérons le langage métalinéaire particulier engendré par la grammaire d'équations :

(61)
$$\begin{aligned} \xi_i &= \xi_1 \xi_2 \\ \xi_1 &= e + \Sigma \{ a\xi_1 b : a, b \in V_T \} \\ \xi_2 &= e + \Sigma \{ a\xi_2 b : a, b \in V_T \}. \end{aligned}$$

Dans ce cas la matrice de l'événement régulier standard sous-jacent serait :

(62)

	X_1^+	X_1^-	X_2^+	X_2^-
X_1^+	U	U	0	0
X_1^-	0	U	U	0
X_2^+	0	0	U	U
X_2^-	0	0	0	U

Tous les langages métalinéaires et ceux-là seulement, seront basés sur un événement standard avec une matrice essentiellement de ce type (avec, peut-être, des restrictions supplémentaires sur la diagonale principale).

Les *propositions* 1 et 2 fournissent ainsi la possibilité de définir très naturellement la classe entière des C-langages, ainsi que différentes sous-familles de cette classe, indépendamment de la démarche adoptée dans les sections précédentes.

6. Indécidabilité.

6.1. Il est démontré dans Post [36] que le problème suivant, connu sous le nom de *problème de correspondance*, est récursivement insoluble. Si $\Sigma = (f_1, g_1), \ldots (f_n, g_n)$ est une suite de couples de séquences, nous dirons qu'une suite $I = (i_1, \ldots, i_m)$ d'entiers $(1 \leqslant i_j \leqslant n)$ satisfait Σ si :

(63)
$$f_{i_1} \cdots f_{i_m} = g_{i_1} \cdots g_{i_m}.$$

Le problème de correspondance consiste à demander si, étant donnée la condition Σ, il existe une suite d'indices qui y satisfasse. Remarquons qu'ou bien Σ n'est satisfaite par aucune suite d'indices, ou bien par une infinité, puisque si $(i_1, \ldots, i_m)$ satisfait Σ, c'est encore le cas pour $(i_1, \ldots, i_m, i_1, \ldots, i_m)$. Post a montré qu'il n'existe pas d'algorithme qui détermine, pour Σ quelconque s'il n'y a pas de suite d'indices satisfaisant Σ, ou s'il y en a une infinité, ce qui constitue les deux seules possibilités.

On peut reformuler directement le problème de correspondance en termes de grammaires linéaires minimales. Étant donnée $\Sigma = \{ (f_1, g_1), \ldots,$

$(f_n, g_n)\}$, formons $G(\Sigma)$ avec l'unique non-terminal S et l'équation de définition :

$$S = a + f_1 S \tilde{g}_1 + \ldots + f_n S \tilde{g}_n \tag{64}$$

où a est un symbole qui ne figure dans aucun des f_i ou des g_i. Il est clair qu'il n'y a une suite d'indices satisfaisant Σ que si $G(\Sigma)$ engendre une séquence $fa\tilde{f}$. Ou, en d'autres termes, soit L_m le langage « image-miroir » constitué de toutes les séquences $fa\tilde{f}$, $f \in F(V_T)$ et soit $L(G(\Sigma))$ le langage engendré par G. Alors, ou bien il n'y a aucune suite d'indices qui satisfasse Σ auquel cas $L_m \cap L(G(\Sigma))$ est vide; ou bien il y en a une infinité, auquel cas $L_m \cap L(G(\Sigma))$ est infini. Du fait que le problème de correspondance est indécidable et que L_m est engendré par une grammaire linéaire à un seul non-terminal, on tire aussitôt que :

THÉORÈME D'INDÉCIDABILITÉ 1.

Étant données deux grammaires G_1 *et* G_2 *engendrant respectivement* L_1 *et* L_2 *il n'existe pas d'algorithme qui détermine si* $L_1 \cap L_2$ *est vide ou infini. Ceci est vrai, même si* G_1 *et* G_2 *sont des grammaires linéaires minimales et si* G_1 *est une grammaire particulière fixée de* L_m.

On voit facilement que le problème de savoir si l'intersection est vide ou finie est décidable pour les grammaires linéaires unilatères, mais dans notre cadre, pour les grammaires les plus simples, dont la capacité génératrice dépasse celle des événements réguliers, ces problèmes ne sont plus décidables.

Cette remarque est généralisée dans Bar-Hillel, Perles, Shamir [2], où l'on montre que beaucoup de problèmes relatifs aux C-grammaires sont récursivement indécidables. Leur méthode est en gros la suivante : limitons V_T à l'ensemble $\{a, 0, 1\}$. Si $\Sigma = \{(f_1, g_1), \ldots, (f_n, g_n)\}$ est un ensemble de couples de séquences dans le vocabulaire $\{0, 1\}$ (i. e., $f_i, g_i \in F\{0, 1\}$), soit $L(\Sigma)$ l'ensemble de toutes les séquences :

$$10^{i_k} \ldots 10^{i_1} a f^{i_1} \ldots f_{i_k} a \tilde{g}_{j_l} \ldots g_{j_1} a 0^{j_1} 1 \ldots 0^{j_l} 1, \tag{65}$$

où $1 \leqslant i_{i_1}, \ldots, i_k, j_1, \ldots, j_l \leqslant n$.

Pour plus de clarté, utilisons $\bar{i} = 01^i$ pour coder le nombre i. Une séquence de $L(\Sigma)$ est alors formée en choisissant des suites d'indices $I = (i_1, \ldots, i_k)$ et $J = (j_1, \ldots, j_l)$, et en formant :

$$\bar{i}_k \ldots \bar{i}_1 a f_{i_1} \ldots f_{i_k} a \tilde{g}_{j_l} \ldots \tilde{g}_{j_1} a \bar{j}_1 \ldots \bar{j}_l. \tag{66}$$

$L(\Sigma)$ joue a ors le même rôle que le langage engendré par (64) dans la démonstration précédente du *Théorème d'indécidabilité 1.* C'est évidemment un C-langage (engendré, d'ailleurs, par une grammaire méta-linéaire qui est une variante évidente de (64)). Mais le Théorème 3, § 4.3 ci-dessus

entraîne aussitôt que le complémentaire $F(V_T) \setminus L(\Sigma)$ de $L(\Sigma)$ par rapport au vocabulaire V_T est un C-langage et qu'on peut construire sa grammaire à partir de la grammaire de $L(\Sigma)$. (Remarquons, en fait, qu'on aurait pu utiliser n'importe quel code au lieu du choix particulier $\bar{i} = 01^i$, pour définir $L(\Sigma)$.)

Au lieu du langage image-miroir L_m utilisé dans la démonstration du *Théorème d'indécidabilité 1*, considérons le langage L_{dm} « double image miroir » constitué par toutes les séquences :

(67) $x_1 a x_2 a \tilde{x}_2 a \tilde{x}_1$, où x_1 et x_2 sont des séquences de $\{ 0, 1 \}$.

Il n'est pas difficile de montrer que L_{dm} et son complémentaire par rapport à V_T sont tous deux des C-langages. Remarquons que

(68) $L(\Sigma) \cap L_{dm} = \{ \bar{i}_k \ldots \bar{i}_1 a f_{i1} \ldots f_{ik} a \tilde{g}_{ik} \ldots \tilde{g}_{i1} a \bar{i}_1 \ldots \bar{i}_k \}$
où $(i_1, \ldots, i_k)$ satisfait Σ (c'est-à-dire où $f_{i1} \ldots f_{ik} = g_{i1} \ldots g_{ik}$).

Remarquons aussi qu'un ensemble infini de séquences de la forme (68) ne peut constituer un C-langage (ni, a fortiori, un événement régulier).

Supposons maintenant qu'il existe une solution positive au problème de correspondance pour Σ; c'est-à-dire qu'il y ait une suite d'indices satisfaisant Σ. Alors, comme nous l'avons signalé, il existe une infinité de telles séquences. Par suite $L(\Sigma) \cap L_{dm}$ est infini. Ce n'est donc ni un événement régulier ni un C-langage.

Supposons au contraire, qu'il n'y ait pas de suite d'indices satisfaisant Σ. Alors $L(\Sigma) \cap L_{dm}$ est vide; c'est donc à la fois un événement régulier et un C-langage; et, Σ étant fixée, on peut construire leurs C-grammaires $G(\Sigma)$ et G_{dm} (qui sont, en fait, métalinéaires). Ainsi, s'il y avait un algorithme permettant de déterminer si l'intersection de langages engendrés par deux C-grammaires G_1 et G_2 est vide, finie, ou est un événement régulier, ou un C-langage, cet algorithme fournirait aussi une solution du problème général de correspondance. Nous en concluons :

THÉORÈME D'INDÉCIDABILITÉ 2.

Étant données des C-grammaires G_1 *et* G_2, *il n'y a pas d'algorithme qui détermine si l'intersection des langages qu'elles engendrent est vide, finie, un événement régulier, où un C-langage. Ceci reste vrai, en particulier, quand toutes deux sont métalinéaires et quand* G_2 *est une grammaire fixée de* L_{dm}.

Soit $\bar{G}_{dm}$ la C-grammaire qui entendre le complémentaire $\bar{L}_{dm}$ (tous les complémentaires sont désormais pris par rapport à V_T) de L_{dm}. Et, étant donnée Σ soit $\bar{G}(\Sigma)$ la C-grammaire qui entendre le complémentaire $\overline{L(\Sigma)}$ de $L(\Sigma)$, et dont l'existence est garantie par le théorème 3, § 4.3. Considérons maintenant la grammaire G qui engendre le langage $L(G) = \bar{L}_{dm} \cup \overline{L(\Sigma)}$. Il est clair que G est une C-grammaire et peut se construire à partir de G_{dm} et $G(\Sigma)$. Mais le complémentaire $\overline{L(G)}$ de $L(G)$ est l'ensemble $L_{dm} \cup L(\Sigma) = L_{dm} \cap L(\Sigma)$ et l'on sait d'après le *Théorème*

d'indécidabilité 2 qu'il n'y a pas d'algorithme qui détermine, quand Σ est donnée, si cet ensemble est vide, fini, un événement régulier ou un C-langage. Mais, étant donnée Σ, G est déterminée comme étant une C-grammaire. On a donc :

THÉORÈME D'INDÉCIDABILITÉ 3.

Il n'y a pas d'algorithme qui détermine sur la donnée d'une C-grammaire G, si le complément du langage engendré par G *est vide, fini, un événement régulier ou un C-langage.*

Il n'existe pas, en particulier, de procédé général pour déterminer si la C-grammaire G engendre le langage universel $F(V_T)$ ou si G engendre un événement régulier (puisque le complémentaire d'un événement régulier est un événement régulier).

Par suite, il n'y a pas d'algorithme qui détermine, sur la donnée de C-langages L_1 et L_2, s'il existe ou non un transducteur appliquant L_1 sur L_2, puisque tous les langages réguliers, et eux seuls, peuvent s'obtenir par transduction à partir du C-langage $F(V_T)$. (Ginsburg et Rose, communication personnelle).

Il n'y a, d'autre part, aucune méthode générale qui permette de savoir si deux C-grammaires sont équivalentes, c'est-à-dire si elles engendrent le même langage, puisqu'une telle méthode pourrait servir à décider si une C-grammaire G est équivalente à la grammaire G_U qui engendre $F(V_T)$. Il s'ensuit aussi immédiatement qu'étant données deux C-grammaires, il n'y a pas d'algorithme permettant de décider si le langage engendré par l'une contient le langage engendré par l'autre, puisque ceci fournirait une solution du problème d'équivalence.

Ces résultats ont été esquissés pour des langages construits à partir d'un vocabulaire V_T à trois éléments, mais il est clair qu'avec un recodage convenable ils s'appliquent encore aux langages sur un vocabulaire de deux lettres ou plus. Ceci est explicité en détail dans Bar-Hillel, Perles, Shamir [2].

6.2. Nous avons observé au § 4 que les processus finis faisant intervenir des couples de séquences pouvaient être formulés d'une façon naturelle, en termes de grammaires linéaires. En particulier, comme on vient de le voir, le problème de correspondance peut se décrire directement comme problème de grammaires linéaires minimales. Il en est de même pour un second problème combinatoire, également dû à Post appelé le problème de l'étiquette (« Tag problem »).

On peut énoncer une forme générale de ce problème de la manière suivante. Soit W l'ensemble des séquences (monoïde libre) sur un vocabulaire fini quelconque, et P un sous-ensemble fini de séquences non nulles de W remplissant la condition qu'aucune séquence de W n'a plus d'un facteur à gauche dans P. C'est-à-dire qu'il n'existe pas de séquences p_1, p_2, w_1, w_2, w_3 ($p_i \varepsilon P$, $w_i \varepsilon W$) telles que $p_1 \neq p_2$ et $w_1 = p_1 w_2 = p_2 w_3$.

Soit V l'ensemble des séquences de W sans facteur à gauche dans P. C'est-à-dire, $v \varepsilon V$ si et seulement s'il n'existe aucun $p \varepsilon P$ tel que $v = pw$, pour $w \varepsilon W$. V est manifestement un ensemble récursif, d'ailleurs régulier. Soit α une application de P dans W(α définit donc un ensemble de couples de séquences (p, w), où $w = \alpha p$, $p \varepsilon P$, $w \varepsilon W$). Définissons une application T sur W, où :

(69)
$$Tf = f'\alpha p \text{ si } f = pf'$$
$$Tf = H \quad \text{si } f \varepsilon V \ (H \varepsilon W).$$

Considérons le problème :

(70) étant donnée une séquence f, existe-t-il un entier n tel que $T^n f = H$?

En considérant que T définit le calcul d'une machine de Turing, (70) est le *problème de l'arrêt* pour cette machine.

Minsky [30] a montré que (70) est un problème récursivement indécidable.

Le problème de l'étiquette, tel qu'il est formulé par Post, est un cas particulier de (70), ci-dessus, où T remplit les conditions supplémentaires suivantes : P est l'ensemble de toutes les séquences de longueur k, pour $k \geqslant 2$, fixé quelconque; αp ne dépend que du symbole le plus à gauche de p. Même avec cette restriction, le problème (70) est insoluble, comme l'a montré Minsky. Ce résultat est assez surprenant du fait du caractère déterministique *(monogène)* du processus générateur T.

Un pas dans la direction d'une reformulation du problème de l'étiquette généralisé en termes de grammaires linéaires minimales, est de l'énoncer de la manière suivante. W, P, V, α, T étant donnés comme ci-dessus, la question (70) ne peut recevoir de réponse affirmative que si

(71) il y a des séquences $p_1 \ldots p_n \varepsilon P$ et $v \varepsilon V$ telles que
$$p_1 \ldots p_n v = f\alpha p_1 \ldots \alpha p_n.$$

On peut alors réénoncer le problème de l'étiquette généralisé, sous la forme du problème suivant relatif aux grammaires linéaires. Étant donnés W, P, V, α, T, définissons la grammaire G engendrant $L(G)$ par la seule équation

(72)
$$S = \Sigma_i \nu_i c + \Sigma_i (p_i \tilde{S} \alpha p_i)$$

où $\nu_i \varepsilon V$, $p \varepsilon P$, et $c \notin W$ est le marqueur central distingué. Définissons le langage $M(f) = \{ fgc\tilde{g} \}$ (ainsi $M(f) = fL_m$; où L_m est le langage « image miroir » défini plus haut). Alors la réponse à (71) (ou, ce qui revient au même, à (70)) est affirmative si et seulement si l'intersection de $L(G)$ et $M(f)$ est non vide. On voit ainsi qu'il n'existe pas d'algorithme pour déterminer, pour f fixé, si le langage $M(f)$ a ou non une intersection non vide avec un langage, dont la grammaire correspond à (72) (même dans le cas

particulier où P est l'ensemble de toutes les séquences de longueur k, k fixé $\geqslant 2$, et où αp ne dépend que de la lettre de P la plus à gauche).

Remarquons que le *Théorème d'Indécidabilité 1*, ci-dessus, résulte aussi directement de l'insolubilité du problème de l'étiquette. En effet le problème de correspondance et celui de l'étiquette sont tous deux relatifs à la cardinalité de l'intersection d'un langage linéaire minimal L avec les langages $M(f)$, où $f = e$ et L quelconque, dans le cas du problème de correspondance, tandis que f est quelconque et L remplit la condition (72), ci-dessus, pour le problème de l'étiquette.

7. Ambiguïté.

7.1. Nous avons défini une série de puissances caractéristiques r, comme ayant chaque coefficient $< r, f >$ égal à zéro ou un. Nous dirons qu'une C-grammaire est *non ambiguë*, si le terme principal de sa solution est une série de puissances caractéristiques. Dans ce cas, chaque phrase engendrée, l'est avec une seule description structurale et le « déparenthésage » n'apporte aucune ambiguïté. Disons qu'un C-langage est *intrinsèquement ambigu*, si toutes ses C-grammaires sont ambiguës.

Il est bien connu qu'aucun événement régulier n'est intrinsèquement ambigu : tout événement régulier est le support d'une série de puissances caractéristiques qui est le terme principal de la solution d'une grammaire linéaire unilatère [14], [37]. Cependant, cette remarque ne s'étend pas à la classe entière des C-grammaires. Parikh [34] a montré qu'il existe des C-langages inhéremment ambigus. Un exemple de langage inhéremment ambigu est l'ensemble :

$$\{ a^n b^m c^p : n = m \text{ ou } m = p \}. \tag{73}$$

Dans ce cas les séquences de la forme $a^n b^n c^n$ doivent avoir une ambiguïté au moins égale à 2 dans toute C-grammaire engendrant (73) (et il existe une C-grammaire engendrant (73) dans laquelle leur ambiguïté est exactement égale à 2).

Nous n'avons pas d'exemples qui montrent l'étendue de l'ambiguïté inhérente dans les C-langages, ou des types particulier de C-langages.

Remarquons qu'une conséquence immédiate du *Théorème d'Indécidabilité 1* du § 6, est qu'il ne peut exister d'algorithme déterminant si une C-grammaire, ou même une grammaire linéaire est ou non ambiguë. Supposons d'ailleurs, comme plus haut, que $\Sigma = \{ (f_1, g_1), \ldots (f_n, g_n) \}$ est une suite de couples de séquences. Choisissons $n + 1$ symboles nouveaux, $x_o, \ldots, x_n$ et construisons les grammaires G_f de règles :

$$S_f \to x_o,\ S_f \to x_i S_f \overset{\leftarrow}{f_i}\ (1 \leqslant i \leqslant n)$$

et G_g de règles :

$$S_g \to x_o,\ S_g \to x_i S_g g_i\ (1 \leqslant i \leqslant n).$$

Il est clair que G et G_g sont non-ambiguës et le problème de correspondance pour Σ a une solution affirmative, si et seulement s'il existe une séquence engendrée à la fois par G_f et G_g c'est-à-dire si et seulement si la grammaire G_{fg} est ambiguë, G_g contenant les règles de G_f, de G_g et les règles $S \to S_f$, $S \to S_g$, où S est le symbole initial de G_{fg}. Donc il ne peut y avoir aucune procédure pour décider si, étant donné Σ quelconque, la grammaire G_{fg} associée ainsi à Σ est non ambiguë.

La grammaire G_{fg} est linéaire, elle a trois non-terminaux et un marqueur central, et l'on voit que pour cette classe de grammaires, le problème de l'ambiguïté est indécidable.

On peut penser que cette remarque s'étend aux grammaires à deux non-terminaux. En revanche, la question intéressante de savoir si le problème de l'ambiguïté est encore indécidable pour les grammaires linéaires minimales reste ouverte. Résumons la question de l'ambiguïté telle qu'elle se présente à l'heure actuelle, par les résultats suivants.

THÉORÈME D'AMBIGUÏTÉ 1.

Il existe des C-langages inhéremment ambigus.

THÉORÈME D'AMBIGUÏTÉ 2.

Il n'existe pas d'algorithme permettant de savoir si une C-grammaire (même linéaire, à marqueur central désigné), est, ou non, ambiguë.

8. Transduction finie.

Nous voulons décrire une famille particulièrement simple de transformations d'un langage en un autre. La première, et aussi la plus importante, est l'*homomorphisme.*

Soit L un langage quelconque sur un vocabulaire terminal Z et supposons que pour tout $z \varepsilon Z$, on se donne un langage L sur un deuxième vocabulaire X. Notons par ΘL l'ensemble de toutes les séquences (sur X) qu'on obtient en prenant un mot $g = z_{i_1} z_{i_2} \ldots z_{i_m} \varepsilon L$ et en remplaçant chaque z_{i_j} par un mot arbitraire de $L_{z_{i_j}}$. Le nom d' « homomorphisme » explique en soi la transformation. En effet, si on considère les anneaux $A(Z)$ et $A(X)$ des séries formelles de puissances par rapport aux variables $z \varepsilon Z$ et $x \varepsilon X$, et si on note par Θ, l'homomorphisme de $A(Z)$ dans $A(X)$ induit par l'application $\Theta z =$ la série formelle de puissances associées à L_z, alors ΘL est le support de l'image par Θ de la série formelle de puissance associée à L.

Une interprétation en rapport avec notre démarche présente peut être donnée si les L_z sont des C-langages. Dans ce cas, supposons que L est produit par la C-grammaire G_z(de vocabulaire non-terminal Y), et que chaque L_z est produit par la C-grammaire G_z (avec l'ensemble des non-terminaux Y_z et la lettre initiale $y_{z,0}$). Supposons que les ensembles Y

soient disjoints et considérons une C-grammaire $\bar{G}$ de non-terminaux $Y \cup Z \cup \bigcup_{z \in Z} Y_z$ constituée des règles de G, des G_z, et des règles $z \to y_{z,o}$ $(z \in Z)$. (Plus simplement, nous identifions chaque z à $y_{z,o}$). Il est clair que G produit exactement ΘL.

Généralisons maintenant cette construction au type suivant de relation contextuelle : soient $R_i (i \in I)$ et $R_{i'}(i' \in I')$ deux familles finies d'événements réguliers telles que chaque $g \in F(Z)$ appartient à un élément et un seul de chaque famille. Supposons aussi que pour chaque triplet $(z \in Z, i \in I, i' \in I')$, on ait un langage $L_{z,i,i'}$ dans le vocabulaire X.

Alors pour tout $y = z_{j_1} z_{j_2} \ldots z_{j_k}$ on remplace chaque z_{j_i} par une séquence arbitraire du langage $L(z_k, i, i')$ où i et i' sont déterminés par la condition que la séquence $z_{j_1} z_{j_2} \ldots z_{j_{k-1}}$ est dans R_i et que la séquence $z_{j_1} \ldots z_{j_k}$ est dans $R_{i'}$. Il est facile de voir qu'on peut, sans diminuer la généralité, supposer que pour toute séquence g appartenant à un ensemble quelconque R_{i_1} et pour $z \in Z$, l'ensemble R_{i_z} contenant gz ne dépend que de l'indice i_1, et de la lettre z. Autrement dit, on peut supposer donnés un ensemble d'états I, une application de transition $I \times Z \to I$ et un état initial $i_o \in I$, tels que $z_{j_1} \ldots z_{j_{k-1}} \in R_i$ si et seulement si i est l'état atteint à partir de i_o et après lecture de $z_{j_1} z_{j_2} \ldots z_{j_{k-1}}$.

Une construction analogue s'applique à R_i et pour des raisons de clarté, on écrira l'application correspondante sous la forme d'une multiplication à gauche. Étant données les deux applications $I \times Z \to I$ et $Z \times I' \to I'$, on notera σg, pour tout $g = z_{j_1} z_{j_2} \ldots z_{j_m} \in F(Z)$, la séquence de triplets :

$$(74) \quad (i_1, z_{j_1}, i'_m)\,(i_2, z_{j_2}, i'_{m-1}) \ldots (i_k, z_{j_k}, i'_{m-k+1}) \ldots (i_m, z_{j_m}, i'_1)$$

où, par récurrence :

$$(75) \quad i'_2 \; i_2 = i_1 z_{j_1}, i_3 = i_2 z_{j_2}, \ldots, i_m = i_{m-1} z_{j_m}, \; i_k = i_{k-1} z_{j_{k-1}} \text{ et } = z_{j_m} i'_1, \; i'_3 = z_{j_{m-1}} i'_2, \ldots, i'_m = z_{j_2} i'_{m-1}.$$

Avec ces notations on peut considérer les transformations décrites comme se déroulant en deux étapes :

(76) (i) remplacement de chaque $g \in L$ par la séquence $\sigma g = (i, z_{j_1}, i_m) \ldots (i_m, z_{j_m}, i')$ dans un alphabet U consistant en des triplets (i, z, i');
(ii) remplacement dans σg de chaque triplet $(i_k, z_{j_k}, i'_{m-k+1})$ par une séquence quelconque du langage $L(z_{jk}, i_k, i'_{m-k+1})$.

Puisque la deuxième étape n'est qu'un homomorphisme, il suffit de discuter la première. Pour cela, soit U l'ensemble de tous les triplets (i, z, i') et considérons le langage L' obtenu à partir de L en ajoutant à sa grammaire toutes les règles $z_j \to (i, z_j, i')$ (avec $i \in I$, $i' \in I'$, quelconques).

Il est clair qu'une séquence de L' appartient à l'ensemble $\{\sigma g : g \in L\}$ si et seulement si elle satisfait la condition (75) ci-dessus, ou encore si elle appartient à l'événement régulier $\overline{R}$ défini par la condition (75) sur l'ensemble $F(U)$ de toutes les séquences dans l'alphabet U.

La première étape consiste donc seulement en un homomorphisme de L dans l'ensemble de toutes les séquences sur U (ce qui donne L') suivi de l'intersection de L' avec un événement régulier.

Donnons maintenant une dernière interprétation de ce que nous avons fait : pour tout $z \in Z$, soit μz la matrice dont les lignes et les colonnes sont indexées par des couples $(i \notin I,\ i' \notin I')$, et dont les entrées sont les suivantes :

(77) $\mu z_{(i,i')\,(i'',i''')} =$ le triplet (i, z, i''') si $i'' = iz$ et $i' = z\,i''' = o$ autrement.

Si on calcule alors :
$\mu z_j\, \mu z_{j_2} \ldots \mu z_{j_n} = \mu g$, il est facile de vérifier que l'entrée (i, i'_m) (i_m, i'_1) de μg est justement σg. De là il s'ensuit que $\{\sigma g : g \in\} L = L' \cap \overline{R}$ est aussi un C-langage. μ est effectivement un homomorphisme, on remplace chaque non-terminal y par une matrice μy dont les entrées sont de nouveaux non-terminaux et on vérifie que μ commute avec les substitutions utilisées pour définir le langage comme solution d'un système d'équations. Par ailleurs l'identification des entrées dans l'image μ de nos équations donne un nouveau système d'équations du type habituel qui définit exactement $L' \cap \overline{R}$ [46]. Plus simplement encore, on peut définir μ' comme plus haut à ceci près que pour chaque entrée non-nulle on prend la série formelle de puissances $L(z_j, i, i')$ au lieu du triplet (i_1, z_j, i'). Les deux étapes de la construction sont alors télescopées en une seule, et la série de puissances associée au langage (sur X) obtenue par notre transformation est simplement une entrée de

(78) $$\Sigma \{\mu' g : g \in L\}.$$

Ceci est le fondement de la démonstration du Théorème 2, § 4, plus haut.

9. Rapports avec la théorie des automates.

Jusqu'à présent, nous avons étudié des processus générateurs, les langages et les systèmes de descriptions structurales qu'ils définissent, et certaines applications finies sur ces langages, d'un point de vue entièrement abstrait. Pour relier ces remarques à la théorie des automates, il est commode d'introduire une assymétrie temporelle dans nos considérations.

Un automate M peut être considéré comme un dispositif consistant en un ensemble d'états Σ (mémoire de M) qui accepte (ou ce qui revient

au même produit) une suite de symboles d'un vocabulaire (alphabet) V, selon des instructions fixées, énonçables de manière finie (qu'on peut donner en associant à chaque $v \varepsilon V$ une application φ_v de Σ dans lui-même (ou dans l'ensemble des parties de Σ, dans le cas d'un automate « non déterministique »). Si on prend un état initial et un ensemble d'états final, on définit un langage $M(L)$ constitué de séquences pouvant être acceptées par M, quand il fonctionne selon ses instructions de l'état initial à l'état final, allant de $S \varepsilon \Sigma$ à $S' \varepsilon \Sigma$, en acceptant v, seulement si $\varphi_v(S) = S'$ (ou $S' \varepsilon \varphi_v(S)$, dans le cas non déterministique).

La taille de la mémoire de M, ou sa vitesse de croissance au cours du calcul, fournit un certain indice de richesse de langage $L(M)$, au moyen duquel on peut comparer diverses familles de langages du type qui vient d'être envisagé.

Étant donné un ensemble de séquences L, écrivons $f \sim f'$, si pour tout g, $fg \varepsilon L$ si et seulement si $f'g \varepsilon L$. Il est clair que $\sim$ est une équivalence. De plus on peut manifestement prendre les classes d'équivalence définies par $\sim$ comme états d'un automate $M(L)$ qui accepte L, puisque toute l'information sur f servant à la poursuite du calcul de $M(L)$, f étant lue, est donnée par la classe d'équivalence de f.

Remarquons que L est la réunion de certaines de ces classes d'équivalence, et que $f \sim f'$ implique que $fg \sim f'g$ pour tout g.

En second lieu, étant donné L, écrivons $f \equiv f'$ si et seulement si pour tout g, $gf \sim gf'$ il est clair que $f \equiv f'$ si et seulement si pour tout g, g', $gfg' \varepsilon L$ si et seulement si $gf'g' \varepsilon L$. Ainsi $\equiv$ est symétrique et il est facile de montrer que $f_1 \equiv f_2$ et $f_3 \equiv f_4 \equiv$ est donc une relation de congruence et les $\equiv$ — classes de l'ensemble $F(V)$ peuvent être multipliées entre elles ce qui donne un monoïde quotient de $F(V)$. Ce monoïde quotient $F'(V) = \varphi F(V)$ est tel que $L = \varphi^{-1}\varphi L$ et il est associé canoniquement à L_o [41].

Cette remarque rattache la théorie présentée ici à celle des monoïdes. L'intérêt est que dans certains cas les $\sim$ -classes (et le monoïde quotient) ont une interprétation simple traduisible en langage d'automates, et inversement que certaines notions algébriques (en particulier, celle d'*extension*), reçoivent une interprétation simple.

Revenons maintenant au problème de la caractérisation des familles de langages en termes d'automates; il est bien connu que la sous-famille *Supp.* (L_o^+) des C-langages est caractérisée de façon unique par le fait que pour chaque langage $L \varepsilon$ *Supp.* (L_o^+), il existe un automate $M(L)$ à mémoire bornée, qui accepte L.

Considérons maintenant la famille *Supp.* (L_o), c'est-à-dire l'ensemble des supports des séries de puissance qui sont solutions de systèmes d'équations « linéaires unilatères » à coefficients entiers positifs ou négatifs.

Comme nous l'avons vu $L \varepsilon$ *Supp.* (L_o), si et seulement si $L =$ *Supp.* $(r_1 - r_2)$ où $r_1, r_2 \notin (L_o^+)$. On peut alors montrer que les énoncés suivants sont équivalents.

(79) (i) $L \varepsilon Supp.(L_o{}^+)$;
(ii) il existe une correspondance biunivoque entre les $\sim$-classes pour L et un espace de dimension finie de vecteurs entiers $\nu(f)$ tels que pour tout $x \varepsilon V$, $\nu(fx) = \nu(f)\mu x$, où μx est une matrice;
(iii) $F/\equiv$ est isomorphe à un monoïde de matrices entières de dimension finie (les matrices μ de (ii);
(iv) L est accepté par un automate $M(L)$, dont la mémoire est un espace de dimension finie de vecteurs à coordonnées entières, et les transitions sont comme dans (ii), ci-dessus.

(Schützenberger, [44], la classe d'automates A étant celle qui est définie par (79 iv).)

Considérons maintenant les deux restrictions suivantes sur la classe d'automates A,

(80) (i) il existe un N tel que pour tout $f \varepsilon F(V)$, $|| \nu(f) || < N$;
(ii) pour tout $f, f', f'' \varepsilon F(V)$ et $\varepsilon > O$, $\lim_{n\to\infty} e^{-\varepsilon n} || \nu(f'f^n f'') || = O$

où $|| \nu ||$ est la longueur du vecteur ν au sens habituel.

Il est clair que (80 i) entraîne (80 ii). De plus L est manifestement un événement régulier ($L \varepsilon Supp.(L_o{}^+)$ seulement si (80 i) est remplie par un automate de la classe A qui accepte L. Un automate de la classe A qui remplit la condition (80 ii) est appelé un automate fini à compteur dans Schützenberger [47] où de tels dispositifs sont étudiés. On peut montrer qu'en gros (80 ii) signifie que la quantité d'information (en bits) enregistrée dans la mémoire ne croît pas plus vite qu'une fonction linéaire du logarithme de la longueur d'un mot d'entrée.

Il est intéressant de remarquer que (comme dans le cas de la classe totale des C-grammaires), il n'y a pas d'algorithme qui permette de décider, étant donné $M \varepsilon A$, s'il y a ou non un f accepté par M [28]. De plus, on peut facilement montrer que le même problème pour les automates finis à compteur est indécidable, si le dixième problème de Hilbert (existence d'une solution entière pour une équation diophantienne quelconque) est indécidable [47].

Considérons maintenant un automate M qui présente une structure du type suivant : les états de M (les $\sim$-classes dans le langage d'entrée de M) sont identifiés aux séquences dans un certain alphabet nouveau (« interne ») et pour tout $\nu \varepsilon V$, « l'instruction de calcul » φ_ν, application : [$\sim$-classe de f]$\to$[$\sim$-classe de $f\nu$] consiste en l'addition ou la suppression de lettres à l'extrémité droite de la séquence interne associée à [$\sim$-classe de f]. Nous appellerons un tel automate (en accord avec la terminologie habituelle), un automate à pile. Les automates à pile forment une sous-classe restreinte de la classe des automates linéaires bornés étudiés par Myhill [31], Ritchie [39].

Si M est un automate à pile, le langage L qu'il accepte est un

C-langage et tout C-langage peut s'obtenir par un homomorphisme à partir d'un langage accepté par un automate à pile [48], [49]. En particulier si D est un langage de Dyck et A un événement régulier standard (cf. § 5) $D \cap A$ est accepté par un automate à pile.

Un automate à pile non déterministique est un automate du type ci-dessus, à ceci près que φ_v applique un état dans un ensemble d'états. Nous pouvons maintenant démontrer directement que les C-langages (les langages de la classe *Supp.* (C^+)) sont ceux qu'accepte un automate à pile non déterministique [11] [12].

Traduit par G. Fauconnier.

BIBLIOGRAPHIE

[1] Ajdukiewicz, K. Die Syntaktische Konnexität. *Studia Philosophica*, 1 (1935), 1-27.

[2] Bar-Hillel, Y., Perles, M. and Shamir, E. On formal properties of simple phrase structure grammars. *Tech. Report*, 4, July 1960.

[3] — Applied Logic Branch. The Hebrew University of Jerusalem. In *Zeit. für Phonetik, Sprachwissenschaft und Kommunikationsforschung*, Band 14, Heft 2 (1961), 143-172.

[4] — Finite state languages. *Bull. Research Council Israel*, 8F (1960), 155-166.

[5] Birkeland, R. Sur la convergence de développements qui expriment les racines de l'équation algébrique générale. *C. R. Acad. Sciences*, 171 (1920), 1370-1372; 172 (1921), 309-311.

[6] Čulik, K. Some notes on finite state languages. *Časopis pro pěstovani Mat.* (1961), 86, 43-55.

[7] Chomsky, N. Three models for the description of language. *I. R. E. Trans. PGIT*, 2 (1956), 113-124.

[8] — On certain formal properties of grammars. *Information and Control*, 2 (1959), 137-167.

[9] — A note on phrase structure grammars. *Information and Control*, 2 (1959), 393-395.

[10] — On the notion « Rule of Grammar ». *Proc. Symp. Applied Math.*, 12, Am. Math. Soc. (1961).

[11] — Context-free grammars and pushdown storage. *Quarterly Progress Reports*, nº 65, Research Laboratory of Electronics, M. I. T. (1962).

[12] — Formal properties of grammars, in Bush, Galanter, Luce (eds.) *Handbook of Mathematical Psychology*, vol. 2, Wiley (1963).

[13] — The logical basis for linguistic theory. *Proc IXth Int. Cong. Linguists*. Cambridge, Mass. (1962).

[14] Chomsky, N. and Miller, G. A. Finite state languages. *Information and Control*, 1 (1958), 91-112.

[15] — Introduction to the formal analysis of natural languages, in Bush, Galanter, Luce (eds.), *Handbook of Mathematical Psychology*, vol. 2, Wiley (1963).

[16] Davis, M. *Computability and Unsolvability.* New York, McGraw-Hill (1958).

[17] Elgot, C. C. Decision problems of finite automata design and related arithmetics. *Trans. Am. Math. Soc.*, 98 (1961), 21-51.

[18] Ginsburg, S. and Rice, H. G. Two families of languages related to Algol. *Technical Memorandum. Systems Development Corporation.* Santa Monica, California (1961).

[19] Ginsburg, S. and Rose, G. F. Operations which preserve definability in languages. *Technical Memorandum. Systems Development Corporation.* Santa Monica, California (1961).

[20] Jungen, R. Sur les séries de Taylor n'ayant que des singularités algebrico-logarithmiques sur leur cercle de convergence. *Comm. Math. Helvetici*, 3 (1931), 286-306.

[21] Kleene, S. C. Representation of events in nerve nets, and finite automata. *Automata Studies*, Princeton University Press (1956), 3-41.

[22] Kulagina, O. Ob odnom sposobe apredelenija grammatičeskix ponjatij. *Problemy Kivernetiki*, 1. Moscou (1958).

[23] Lambek, J. The mathematics of sentence structure. *Am. J. Math.*, 65 (1958), 153-170.

[24] — On the calculus of syntactic types. *Proc. Symposium Applied Math.*, 12, Am.

[25] Lyndon, R. C. Equations in free groups. *Trans. Am. Math. Soc.*, 96 (1960), 445-457.

[26] McNaughton, R. The theory of automata, in *Advances in Computers*, vol II (Academic Press).

[27] Mahler, K. On a theorem of Liouville in fields of positive characteristic. *Canadian J. of Math.*, 1 (1949), 397-400.

[28] Markov, A. A. ob odnoi nevazrešimoi probleme, *Doklady Akad. Nauk*, n. s. 78 (1951), 1089-1092.

[29] Miller, G. A. and Chomsky, N. Finitary models of language users, in Bush, Galanter, Luce (eds.). *Handbook of Mathematical Psychology*, vol. 2, Wiley (1963).

[30] Minsky, M. L. Recursive unsolvability of Post's problem of Tag. *Ann. of Math.*, 74 (1961), 437-455.

[31] Myhill, J. Linear bounded automata. Wadd *Tech. Note* 60-165. Wright Air Dvpt. Division. Wright Patterson Air Force Base Ohio (1960).

[32] Newell, A. and Shaw, J. C. Programming the logic theory machine. *Proc. Western Joint Computer Conference* (1957), 230.

[33] Œttinger, A. G. Automatic syntactic analysis and the pushdown store. *Proc. of Symposia in Applied Math.*, 12, Am. Math. Soc. (1961).

[34] Parikh, R. J. Language generating devices. *Quarterly Progress Report* nº 60, Research Laboratory of Electronics, M. I. T. January (1961), 199-212.

[35] Perles, M. Rabin, M. O. and Shamir, E. The theory of definite automata. *Tech. Report*, nº 6, O. N. R. (1961).

[36] Post, E. A variant of a recursively unsolvable problem. *Bull. Amer. Math. Soc.*, 52 (1946), 264-268.

[37] Rabin, M. O. and Scott, D. Finite automata and their decision problems. I. B. M. *Journal of Research*, 3 (1959), 115-125.

[38] Raney, G. N. Functional composition patterns and power-series reversion, *Trans. Am. Math. Soc.*, 94 (1960), 441-451.

[39] Ritchie R. W. *Classes of recursive functions of predictable complexity.* Thèse, Dept. of Math, Princeton Univ. (1960).

[40] Scheinberg, S. Note on the Boolean properties of context-free languages. *Information and Control*, 3 (1960), 372-375.

[41] Schützenberger, M. P. On an application of semi-group methods. *I. R. E. Trans.*, IT2 (1956), 47-60.

[42] — Un problème de la théorie des automates. *Séminaire Dubreuil-Pisot.* Paris, déc. (1959).

[43] — A remark on finite transducers. *Information and Control*, 4 (1961), 185-196.

[44] — On the definition of a family of automata. *Information and Control*, 4 (1961), 245-270.

[45] — Some remarks on Chomsky's context-free languages. *Quarterly Progress Report*, n° 68, Research Laboratory of Electronics, M. I. T., oct. (1961).

[46] — On a theorem of R. Jungen. *Proc. Am. Math. Soc.*, 13 (1962), 885-890.

[47] — Finite counting automata. *Information and Control*, 5 (1962), 91-107.

[48] — On Context-free languages and pushdown storage. *Information and Control*, 6 (1963), 246-264.

[49] — Certain elementary families of automata. *Symp. on mathematical theory of automata*, Polytechnic Institute of Brooklyn, 1962.

[50] Shepherdson, J. C., The reduction of two-way automata to one-way automata. I. B. M. *Journal of Research* (1959), 198-200.

[51] Shamir, E. On sequential languages. *Tech. Report*, n° 7, O. N. R. (1961).

[52] Yamada, A. *Counting by a class of growing automata.* Thèse Univ. of Penna., Philadelphia (1960).

Table des matières

Tome VI

Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par Jean Berstel, Alain Lascoux et Dominique Perrin

Les treize tomes de cette édition contiennent l'ensemble des œuvres de Marcel-Paul Schützenberger qui ont fait l'objet d'une publication dans une revue scientifique ou un livre. Ses travaux couvrent une période de plus de 50 ans, depuis sa première note aux Comptes Rendus en 1943 jusqu'à son dernier article, paru en 1997.
Les publications sont présentées dans l'ordre chronologique. Chaque tome est précédé d'une courte introduction qui essaie d'éclairer certains des travaux, tant pour leur intérêt scientifique intrinsèque que pour l'écho qu'ils ont rencontré et les développements qu'ils ont suscités.

Tome 6 : 1964 – 1968

Le plus connu et le plus cité des articles de cette période est « On finite monoids having only trivial subgroups », où Schützenberger caractérise les langages rationnels dont le monoïde syntactique est apériodique, c'est-à-dire n'a pas de groupe non trivial. C'est le résultat pionnier dans ce qui deviendra la théorie des variétés de langages reconnaissables. Eilenberg, dans le volume B de son traité écrit : « Next to Kleenes's Theorem, Schützenberger's Theorem is probably the most important result dealing with recognizable sets. ».
Cette période est aussi celle d'autres articles importants en théorie des codes comme « Codes à longueur variables », un texte qui a été d'une importance fondamentale pour ses élèves et disciples et est resté non publié. Ce sont les notes d'un cours sur la théorie des codes, écrites pour l'école d'été de Royan. D'autres articles sont « On the synchronizing properties of certain prefix codes », qui contient la théorie des codes sémaphores, ou « On a question concerning certain free submonoids » qui contient la solution d'une conjecture proposée par Gilbert et Moore en 1959.
Dans le bref article intitulé « Classification of Chomsky Languages », Schützenberger propose une présentation particulière des langages algébriques : ceux-ci sont vus essentiellement comme des images, par des transductions rationnelles de langages de Dyck.