COMPLEXITE DES DEMI - GROUPES DE MATRICES .

G. Jacob

Université Lille I

et

Laboratoire d'Informatique Théorique et Programmation

(C.N.R.S., laboratoire associé 248)

Abstract. Let us call measure of complexity over a class $\mathcal{H}$ of semigroups any function β from $\mathbb{N}$ into $\mathbb{N}$ such that any semigroup H in $\mathcal{H}$ generated by at most n elements has its cardinality less than $\beta(n)$. If β is a measure of complexity over the class of all subgroups of a finite matrix semigroup H, then we can compute an integer $T(\beta)$ which is greater than the cardinality of H. We give here equations computing effectively such an integer $T(\beta)$ for some classes of matrix semigroups, or of quotients semigroups of matrix semigroups.

As a consequence we prove, using a theorem of A.I. Kostrikin, that there exist an effective decision procedure for the finiteness of matrix semigroups over skewfields, under the condition that each of its elements admits a given prime integer p as period.

Introduction.

Il est classique de souligner les liens entre la structure d'un demi-groupe fini et la structure de ses classes d'idéaux, reflétées essentiellement par les propriétés des relations de Green (cf. Clifford et Preston [3]). C'est plus tard que fut mis en évidence le lien entre certaines classes de demi-groupes et les propriétés de la classe de leurs sous-groupes. (cf. Eilenberg [4]), ainsi qu'avec les langages dont les demi-groupes syntactiques appartiennent à ces classes.

Il revient à M.P. Schützenberger [16] d'avoir montré que les langages qui ont pour demi-groupes syntactiques des demi-groupes apériodiques, sont exactement les langages obtenus par opérations booléennes et concaténations en partant des langages finis. Dans le même ordre d'idées, on notera le lien entre la théorie des codes et celle des sous-groupes de leurs demi-groupes syntactiques (cf. D. Perrin [14]), et plus généralement le rôle joué par les sous-groupes dans l'étude des monoïdes syntactiques des langages algébriques. (cf. J.F. Perrot [15]).

Cependant, notre objet ne sera pas ici le lien entre les demi-groupes et les langages, mais l'étude d'une notion de complexité que l'on peut définir sur la classe des sous-groupes d'un demi-groupe "abstrait", notion de complexité qui permet de mesurer le cardinal de ses sous-groupes. Plus précisément, nous appelons mesure de complexité sur la classe des sous-groupes d'un demi-groupe H toute fonction β qui majore le cardinal de chacun des sous-groupes finis de H en fonction du nombre minimum de ses générateurs.

Une telle mesure de complexité existe naturellement sur la classe des sous groupes des demi-groupes finis. Or on sait que tout demi-groupe fini peut être représenté fidèlement comme demi-groupe de matrices à coefficients 0 ou 1. Il est assez naturel de chercher à généraliser cette étude aux demi-groupes de matrices à coefficients dans un corps quelconque.

Nous avons montré dans [7] que la donnée d'une mesure de complexité β sur la classe des sous-groupes d'un demi-groupe fini de matrices H permet de calculer a priori un entier $T\beta$ qui en majore le cardinal, et qui ne dépend que de la dimension des matrices de H, de β, et du nombre minimum des générateurs de H.

L'existence de l'algorithme calculant $T\beta$ nous a déjà permis [7,9] de retrouver en corollaires tous les résultats établis par Zalcstein [18], et par McNaughton et Zalcstein [13] sur les demi-groupes de matrices. Nous avons déjà montré aussi que l'on peut décider par un algorithme effectif (voir [6]) si un demi-groupe de matrices sur un corps commutatif est fini. Nous ajoutons ici un autre résultat, qui s'appuie sur un théorème de A.I. Kostrikin [11] : nous montrons qu'il existe un algorithme effectif permettant de décider si un demi-groupe de matrices sur un corps gauche, dont tous les éléments admettent comme période un nombre premier p fixé, est un demi-groupe fini.

La construction de l'entier $T\beta$ peut aussi être interprétée comme suit : tous les demi-groupes finis de matrices de rang au plus égal à un entier m et admettant une même mesure de complexité β sur la classe de leurs sous-groupes forme une classe $D\beta_m$ de demi-groupes, sur laquelle on peut construire une mesure de complexité $T\beta_m$.

Nous donnons alors plusieurs algorithmes qui permettent de calculer de telles mesures de complexités sur des classes plus ou moins restreintes de demi-groupes. Nous précisons leur domaine de validité, et en donnons les équations sous une forme qui permet d'en calculer et comparer aisément les performances.

Toute cette étude peut se faire pour des demi-groupes infinis de matrices, mais dans ce cas il ne suffira plus de prendre en considération les seuls sous-groupes (de type fini) de H. Il nous faut alors définir la classe un peu plus large des "groupes caractéristiques" de H. Il s'agit d'une classe de groupes de type fini s'identifiant à celle des sous-groupes de H quand H est fini.

Tous les résultats que nous obtenons ici reposent sur les techniques combinatoires de [5,7], qui nous ont déjà permis de montrer que le rang d'un espace vectoriel peut jouer le même rôle, pour l'étude des demi-groupes de matrices, que celui joué par le cardinal d'une partie de l'ensemble des états d'un automate fini.

Cette dernière remarque nous amène à faire retour sur les langages définis par les automates finis, et plus généralement sur les séries formelles rationnelles, qui sont définies par des demi-groupes de matrices. Ceci pour noter que les résultats que nous établissons dans cette note peuvent s'interpréter en termes de décidabilité pour les séries formelles, suivant la démarche que nous avons indiquée dans [8,9].

En introduisant ainsi une nouvelle notion de complexité des demi-groupes, nous ne pouvons manquer de situer cette notion par rapport à la théorie aujourd'hui classique de la complexité des demi-groupes issue du théorème de décomposition de Krohn et Rhodes. Cette théorie classique évalue la complexité en structure des demi-groupes. Elle cherche à calculer la distance entre un demi-groupe donné S et une classe de demi-groupes de structure très simple (ex. groupes, demi-groupes apériodiques), en calculant le nombre d'étapes de "décomposition" nécessaires pour obtenir ce demi-groupe S. Sur ce sujet, nous renvoyons le lecteur aux nombreuses publications parues, mais surtout en dernier lieu aux deux chapitres écrits par Bret Tilson dans le récent livre de S. Eilenberg ([4] ,vol B). On y trouvera le dernier état de la question, ainsi qu'une abondante bibliographie, que nous ne reproduisons pas.

La notion de complexité que nous proposons ici n'est pas liée à la structure algébrique: elle cherche à "mesurer" le cardinal des demi-groupes de certaines classes, avec l'idée que la croissance de ces mesures de complexité déterminent si la classe de demi-groupes que l'on étudie peut être effectivement et entièrement calculée. C'est donc de mesurer la finitude qu'il s'agit, cela permet de poser les questions de décidabilité théorique, et de décidabilité concrète de la finitude.

Nous terminons cette introduction par le plan de l'article.

1. Rappels et définitions.
   - a) Type et largeur d'un demi-groupe.
   - b) Demi-groupes de matrices.
2. Classes de demi-groupes et mesures de complexité.
3. Mesures concrètes de la finitude, comparaison de quelques algorithmes.
   - a) Mesures concrètes de finitude.
   - b) Complexité des demi-groupes de matrices.
   - c) Complexité des quotients des demi-groupes de matrices.
   - d) Mesures de complexité et variétés de demi-groupes.

Conclusion.

1. Rappels et définitions.

a) Type et largeur d'un demi-groupe (cf. [7])

Le type d'un demi-groupe H est le plus petit cardinal d'un ensemble de générateurs de H.

Soit S un ensemble de générateurs de H. Nous appelons S-largeur de H le plus petit entier $j = \text{larg}_S(H)$, s'il existe, vérifiant :

$$S^j \subset S \cup S^2 \cup \ldots \cup S^{j-1}$$

Si un tel entier j n'existe pas, la S-largeur de H est infinie.

La largeur de H est la borne supérieure, notée larg(H), des S-largeurs de H pour tous les systèmes de générateurs S de H.

Lemme 1.1 Pour un demi-groupe H, les énoncés suivants sont équivalents:

(i) H est fini.

(ii) $\text{larg}_S(H)$ est fini pour un système fini S de générateurs.

(iii) H est de type fini et de largeur finie.

Preuve. Immédiate. On notera que l'on a:

$$\text{larg}(H) \leqslant \text{Card } H$$

et que si S est un système fini de générateurs de H, et s le cardinal de S, on a:

$$\text{Card } H \leqslant s + s^2 + \ldots + s^{\text{larg}(H)-1}$$

b) Demi-groupes de matrices.

Soit H un demi-groupe multiplicatif de matrices à coefficients dans un corps gauche K. Nous le considérons comme représentant un demi-groupe d'endomorphismes d'un K-espace vectoriel à droite de dimension finie. On considère donc les matrices comme opérant à droite sur des vecteurs lignes (le choix dual serait aussi possible).

Définition 1.1 Nous appelons Im-noyau de H tout sous-demi-groupe de H de type fini dont toutes les matrices ont le même espace vectoriel image.

Nous appelons groupe caractéristique d'un Im-noyau $\mathcal{N}$ de H le groupe de matrices engendré par les automorphismes qu'induisent les matrices de $\mathcal{N}$ sur leur image commune.

En d'autres termes, un sous-demi-groupe $\mathcal{N}$ de H est un Im-noyau si et seulement si toutes ses matrices peuvent s'écrire, pour le même changement de base et la même décomposition par blocs, sous la forme:

$$A_i \qquad \text{ou} \qquad \begin{pmatrix} A_i & 0 \\ B_i & 0 \end{pmatrix}$$

où les matrices A_i sont carrées inversibles.

Le groupe caractéristique $G(\mathcal{N})$ est alors isomorphe au groupe engendré par les matrices A_i.

Dans notre théorie, le rôle essentiel est joué par les groupes caractéristiques. Le lemme suivant montre que les groupes caractéristiques jouent le même rôle, pour les demi-groupes infinis de matrices, que les sous-groupes dans les demi-groupes finis.

Lemme 1.2 Un Im-noyau $\mathcal{N}$ de H est fini si et seulement si son groupe caractéristique $G(\mathcal{N})$ est fini.

Tout Im-noyau fini $\mathcal{N}$ de H contient un sous-groupe isomorphe à son groupe caractéristique $G(\mathcal{N})$.

Preuve. Voir [6].

Corollaire 1.1 Si H est un demi-groupe de matrices périodiques (i.e. vérifiant une équation de la forme $m^{s+t} = m^s$ pour des entiers s et t strictement positifs) sur un corps gauche, les groupes caractéristiques de H s'identifient, à isomorphisme près, aux sous-groupes de type fini de H.

2. Classes de demi-groupes et mesures de complexité.

Définition 2.1 Soient $\mathcal{H}$ une classe de demi-groupes et β une fonction de $\mathbb{N}$ dans $\mathbb{N}$. Nous dirons que β est une mesure de complexité sur $\mathcal{H}$, ou encore que $\mathcal{H}$ est β-complexe, si tout demi-groupe fini de $\mathcal{H}$ vérifie l'inégalité:

$$\text{Card } H \leqslant \beta(\text{type } H)$$

Considérons à présent un demi-groupe H de matrices à coefficients dans un corps (qui peut être un corps gauche), et β une fonction de $\mathbb{N}$ dans $\mathbb{N}$. Notons $\mathcal{R}$ une congruence de demi-groupes sur H.

Définition 2.2 Nous dirons que β est une mesure de finitude sur H, ou encore que H est β-fini, si la fonction β est une mesure de complexité sur la classe des groupes caractéristiques de H.

Plus généralement, nous dirons que β est une mesure de finitude modulo $\mathcal{R}$ sur H, ou que $\mathcal{R}$ est une congruence β-finie sur H, si β est une mesure de complexité sur la classe des quotients par $\mathcal{R}$ des groupes caractéristiques de H.

Si β est une fonction de $\mathbb{N}$ dans $\mathbb{N}$ et m un entier strictement positif, nous notons $D\beta_m$ la classe des demi-groupes de matrices β-finis de dimension au plus m. Nous notons $R\beta_m$ la classe des demi-groupes qui sont quotients d'un demi-groupe de matrices de dimension au plus m par une congruence β-finie.

La définition 2.2 est justifiée par le théorème suivant:

Théorème 1. (Procédure LARGEVAL, [6]).

Il existe un algorithme calculant une fonction $T\beta_m$ de $\mathbb{N}$ dans $\mathbb{N}$ qui est une mesure de complexité sur $D\beta_m$, et aussi plus généralement sur $R\beta_m$. Une telle fonction $T\beta_m$ peut être calculée par les équations suivantes:

$$T\beta_m(t) = \underbrace{\psi \circ \psi \circ \ldots \circ \psi}_{m \text{ fois}}(1)$$

$$\psi(z) = z.\ \underbrace{(\chi_z \circ \chi_z \circ \ldots \circ \chi_z)}_{t^z \text{ fois}}(1)$$

$$\chi_z(x) = x.(1 + (\beta \circ \tau)(z.(2x-1)))$$

$$\tau(u) = t + t^2 + \ldots + t^u$$

Preuve. La preuve est donnée par la justification de la procédure LARGEVAL, que nous avons donnée dans [6]. Nous donnons ces équations sous une forme qui met en évidence la croissance de $T\beta_m$ en fonction de m et de l'argument t.

Nous présentons à présent deux exemples de mesures de complexité non triviales. Le premier est donné par la solution du problème de Burnside pour les groupes G d'exposant un entier premier fixé p, c'est-à-dire vérifiant:

$$\forall x \in G \quad , x^p = 1$$

Théorème 2 (Théorème de Kostrikin [11]).

Il existe une mesure de complexité sur la classe des groupes ayant pour exposant un nombre premier fixé p.

Le second exemple concerne les demi-groupes de matrices sur un corps commutatif.

Théorème 3.

Soit K un corps commutatif engendré par un nombre fini d'éléments, et soit m un entier strictement positif. Il existe sur la classe des groupes de matrices de dimension au plus m à coefficients dans K une mesure de complexité.

Preuve. Une preuve d'existence d'un algorithme a été donnée par Kopytov[10]. Nous avons construit un tel algorithme, et l'avons justifié dans [6], sous forme d'une procedure BETA, en langage de style algol. Nous en donnerons plus loin les équations.

3. Mesures concrètes de finitude, comparaison de quelques algorithmes.

Les théorèmes 1 et 3 montrent l'existence de classes de demi-groupes pour lesquelles on ne peut définir de mesure de complexité qu'en se limitant aux demi-groupes de cette classe qui sont de rang borné par un entier fixé. Cela nous conduit naturellement à la notion de mesure concrète de complexité, que nous allons proposer ci-dessous.

Il en résultera une notion de mesure concrète de finitude, à laquelle nous devrons la possibilité de construire des algorithmes plus fins, améliorant par exemple l'algorithme LARGEVAL .

a) Mesures concrètes de finitude.

Définition 3.1 Nous appelons mesure concrète de complexité sur une classe $\mathcal{H}$ de quotients de demi-groupes de matrices , la donnée d'une suite $\beta = (\beta_j)_{j \in \mathbb{N}}$, où pour tout entier j, β_j est une mesure de complexité sur la classe des demi-groupes de $\mathcal{H}$ qui sont quotients de demi-groupes de matrices de rang au plus j.

Définition 3.2 Soit H un demi-groupe de matrices, et soit $\beta = (\beta_j)_{j \in \mathbb{N}}$ une suite de fonctions de $\mathbb{N}$ dans $\mathbb{N}$. Nous dirons que β est une mesure concrète de finitude sur H, ou que H est β-fini, si β est une mesure concrète de complexité sur la classe des groupes caractéristiques de H.

Plus généralement, nous dirons que β est une mesure concrète de finitude modulo $\mathcal{R}$ sur H, ou que $\mathcal{R}$ est une congruence β-finie sur H, si pour tout entier j, β_j est une mesure de complexité sur la classe des groupes qui sont images des groupes caractéristiques de H de rang au plus j par la congruence induite par $\mathcal{R}$.

Soit $\beta = (\beta_j)_{j \in \mathbb{N}}$ une suite de fonctions de $\mathbb{N}$ dans $\mathbb{N}$. Notons $D\beta$ (resp. $R\beta$) la classe des demi-groupes β-finis de matrices (resp. la classe des quotients β-finis des demi-groupes de matrices). Le théorème 1 peut être généralisé comme suit:

Théorème 1(bis)

Pour toute suite $\beta = (\beta_j)_{j \in \mathbb{N}}$ de fonctions de $\mathbb{N}$ dans $\mathbb{N}$, il existe un algorithme calculant une mesure concrète de complexité $T\beta$ sur la classe $D\beta$, qui est aussi une mesure de complexité sur la classe $R\beta$.

On peut calculer une telle mesure concrète de complexité par les équations:

$$T\beta_j(t) = (\psi_1 \circ \psi_2 \circ \ldots \circ \psi_j) \quad (1)$$

$$\psi_j(z) = z.\underbrace{(\chi_{j,z} \circ \chi_{j,z} \circ \ldots \circ \chi_{j,z})}_{t^z \text{ fois}} \quad (1)$$

$$\chi_{j,z}(x) = x.(1+(\beta_j \circ \tau_t)(z.(2x-1))$$

$$\tau_t(u) = t + t^2 + \ldots + t^u$$

Preuve. Ces équations décrivent l'algorithme LARGEVAL, que nous avons présenté et justifié dans [6].

Théorème 3(bis)

Soit K un corps commutatif engendré par un nombre fini d'éléments.

On peut calculer sur tout demi-groupe H de de matrices à coefficients dans K une mesure concrète de finitude γ_K. Cette mesure concrète de finitude ne dépend que du corps K. En particulier, si K est de caractéristique nulle, les fonctions γ_{Kj} sont des fonctions constantes.

Preuve. Elle est donnée dans [6]. Nous rappelons ici les équations permettant le calcul de γ_K, et qui décrivent l'algorithme BETA de l'article cité.

On note m la dimension de H, et t son type. On note deg le degré d'algébricité de K sur son sous-corps premier.

En caractéristique nulle, les équations de γ_K sont:

$$\gamma_{Kj}(t) = (W_m)^{j^3}$$

$$W_m = u.(u+1)/2$$

$$u = m.deg.(1 + \theta(m.deg))$$

où $\theta(x)$ est l'unique entier vérifiant:

$$\theta(x)! \leqslant x < (1+\theta(x))!$$

En caractéristique p non nulle, les équations de γ_K sont :

$$\gamma_{Kj}(t) = \underbrace{(\psi_t \circ \psi_t \circ \ldots \circ \psi_t)}_{(j-1) \text{ fois}} (W_m)$$

$$\psi_t(x) = (2t + W_m.x).p^{(2t + W_m.x)}$$

$$W_m = u.(u+1)/2$$

$$u = p^{m.deg} - 1$$

b) Complexité des demi-groupes de matrices.

Nous présentons ici deux algorithmes qui calculent des mesures concrètes de complexité sur les demi-groupes de matrices, qui s'inspirent de l'algorithme donné par Mandel et Simon pour les matrices à coefficients dans Q [10].

Ces algorithmes convergent plus vite que l'algorithme LARGEVAL, et calculent donc des mesures de complexité plus petites. On verra cependant au c) qu'ils sont de portée moins générale.

On les obtient en calculant par récurrence une suite A_j d'entiers positifs, tels que toute matrice de H de rang j puisse s'écrire comme produit de moins de A_j éléments de l'ensemble S des générateurs du demi-groupe étudié.

Proposition 1 (Mesures de finitude bornées).

Soit $g = (g_j)_{j \in \mathbb{N}}$ une suite d'entiers positifs. Notons Dg la classe des demi-groupes g-finis de matrices sur un corps gauche.

On peut calculer une mesure concrète de complexité Sg sur la classe Dg par les équations suivantes:

$$Sg_j(t) = (\psi_1 \circ \psi_2 \circ \ldots \circ \psi_{j-1})\ (1+g_j+g_j g_{j-1})$$

$$\psi_i(x) = x + 1 + g_i . \tau_t(x)$$

$$\tau_t(u) = t + t^2 + \ldots + t^u$$

Preuve. Ces équations sont celles de l'algorithme de Mandel et Simon [12], que nous avons raffinées en utilisant la donnée d'une mesure concrète de la finitude. Les équations de Mandel et Simon seront retrouvées en effaçant les indices i et j des équations ci-dessus.

En utilisant la même méthode de récurrence descendante sur le rang, on obtient le résultat suivant:

Proposition 2 (Mesures de finitude non bornées).

Soit $\beta = (\beta_j)_{j \in \mathbb{N}}$ une suite de fonctions de $\mathbb{N}$ dans $\mathbb{N}$, et soit Dβ la classe des demi-groupes de matrices sur un corps gauche qui sont β-finis.

On peut calculer une mesure concrète de complexité Jβ sur la classe Dβ par les équations suivantes:

$$J\beta_j(t) = (\tau_t \circ \psi_1 \circ \psi_2 \circ \ldots \circ \psi_{j-1})\ (\beta_j(t) + \theta_1(\beta_j(t)))$$

$$\psi_i(x) = x + \theta_i(\tau_t(x))$$

$$\theta_i(z) = \underbrace{(\eta_j \circ \eta_j \circ \ldots \circ \eta_j)}_{z \text{ fois}}\ (1)$$

$$\eta_i(u) = u.\beta_{j-i}(2u-1)$$

$$\tau_t(v) = t + t^2 + \ldots + t^v$$

Preuve. Elle se fait par la même méthode de récurrence descendante sur le rang que la proposition 1. Mais l'argument de Mandel et Simon pour établir le pas de la récurrence n'est plus valable. Nous l'établissons en utilisant le "lemme de Brown" [1] pour lequel nous avons fourni un algorithme dans [6].

Corollaire 3.1 Soit ε la suite d'entiers constamment égale à 1. Alors la suite $S\varepsilon = (S\varepsilon_j)_{j\in\mathbb{N}}$ définie par la proposition 1 est une mesure concrète de complexité sur la classe des demi-groupes de matrices qui n'ont que des groupes caractéristiques triviaux.

En particulier, $S\varepsilon$ est une mesure concrète de complexité sur la classe des demi-groupes apériodiques de matrices périodiques sur un corps gauche.

(Rappelons qu'un demi-groupe est dit apériodique si tous ses sous-groupes sont triviaux)

Corollaire 3.2 Soit K un corps commutatif engendré par un nombre fini d'éléments, et soit $\gamma_K = (\gamma_{Kj})_{j\in\mathbb{N}}$ la suite de fonctions définie par le théorème 3bis.

Si K est de caractéristique nulle (resp. non nulle), la suite $S\gamma_K$ (resp. $J\gamma_K$) est une mesure concrète de complexité sur la classe des demi-groupes de matrices à coefficients dans K.

Les algorithmes donnés par les propositions 1 et 2 ne sont plus valables pour les demi-groupes qui sont quotients d'un demi-groupe de matrices. De même nous ne connaissons pas d'équivalent du théorème 3 et du corollaire 3.2 pour les quotients des demi-groupes de matrices sur un corps commutatif. Cependant l'algorithme LARGEVAL permet d'obtenir des résultats appréciables, dont l'un au moins (corollaire 3.3) fournit des fonctions assez petites pour qu'on puisse espérer les programmer effectivement.

c) Complexité des quotients des demi-groupes de matrices.

Nous donnons d'abord deux exemples d'utilisation de l'algorithme défini par le théorème 1 (bis), et calculant la mesure concrète de complexité $T\beta$.

Corollaire 3.3 Soit ε la suite d'entiers constamment égale à 1. Alors $T\varepsilon$ est est une mesure concrète de complexité pour la classe des demi-groupes $H/\mathcal{R}$ où H est un demi-groupe de matrices sur un corps gauche dont tous les groupes caractéristiques sont triviaux modulo $\mathcal{R}$.

En particulier, T est une mesure concrète de complexité sur la classe des demi-groupes finis apériodiques qui sont quotients d'un demi-groupe de matrices sur un corps gauche.

Preuve. Si $H/\mathcal{R}$ est fini, les quotients des groupes caractéristiques de H par la congruence induite par $\mathcal{R}$ sont isomorphes à des sous-groupes de $H/\mathcal{R}$ et sont donc triviaux, puisque $H/\mathcal{R}$ est supposé être apériodique.

Un autre exemple nous est fourni par le théorème de Kostrikin. Appelons exposant d'un demi-groupe H le plus petit entier m positif non nul, s'il existe, tel que tout élément h de H vérifie l'équation:

$$h^{s+m} = h^{s} \quad , \text{ où s est un entier positif.}$$

En d'autre termes, m est la plus petite période commune à tous les éléments de H.

Théorème 4

Soit p un nombre premier.

Il existe une mesure concrète de complexité sur la classe des demi-groupes d'exposant p de la forme $H/\mathcal{R}$, où H est un demi-groupe de matrices sur un corps gauche.

Preuve. Si $H/\mathcal{R}$ est d'exposant p, les quotients des groupes caractéristiques de H par la congruence induite par $\mathcal{R}$ sont des groupes d'exposant p. D'où le résultat, par le théorème de Kostrikin (théorème 2) et le théorème 1 (bis).

Corollaire 3.4 On peut décider si un demi-groupe d'exposant p premier, quotient d'un demi-groupe de matrices sur un corps gauche, est un demi-groupe fini.

d) Mesures de complexité et variétés de demi-groupes.

Rappelons qu'une variété de demi-groupes, au sens d'Eilenberg (voir [4]) est une classe de demi-groupes qui est fermée par sous-objet, passage au quotient, et produit direct fini.

Soit $\beta = (\beta_j)_{j \in \mathbb{N}}$ une suite de fonctions de $\mathbb{N}$ dans $\mathbb{N}$. Nous dirons qu'elle est de croissance au moins exponentielle si et seulement si pour tout entier t, on a les inégalités:

$$\forall j,k \in \mathbb{N} \quad , \beta_{j+k}(t) \geqslant \beta_j(t).\beta_k(t)$$

Rappelons que si β est une suite de fonctions de $\mathbb{N}$ dans $\mathbb{N}$, nous notons $R\beta$ la classe des demi-groupes qui sont quotients d'un demi-groupe de matrices sur un corps gauche par une congruence β-finie.

Si $\mathcal{R}$ est une congruence sur un demi-groupe de matrices H, nous dirons que $\mathcal{R}$ est une congruence β-**complexe** sur H si l'on a l'inégalité:

$$\text{Card}(H/\mathcal{R}) \leqslant \beta_j(\text{type } H) \quad , \text{ où } j \text{ est la dimension de } H.$$

On dira aussi, dans ce cas, que $H/\mathcal{R}$ est β-complexe.

Lemme 3.1 Soit β une suite **de croissance** aumoins exponentielle de fonctions de $\mathbb{N}$ dans $\mathbb{N}$.

La classe des quotients des demi-groupes de matrices sur un corps gauche par des congruences β-complexes est une variété de demi-groupes Vβ.

En particulier, la variété de demi-groupes engendrée par la classe des demi-groupes de matrices β-complexes est une variété de demi-groupes β-complexes.

Preuve. Puisque β est une suite de croissance au moins exponentielle, le produit de deux demi-groupes quotient d'un demi-groupe de matrices par une congruence β-complexe est le quotient du produit des deux demi-groupes de matrices par une congruence β-complexe,le reste de la preuve est immédiat.

Théorème 5.

Soit β une suite de croissance au moins exponentielle de fonctions de $\mathbb{N}$ dans dans $\mathbb{N}$.

La classe des demi-groupes qui sont quotient d'un demi-groupe de matrices sur un corps gauche par une congruence β-finie est une variété de demi-groupes.

En particulier, la variété de demi-groupes engendrée par les demi-groupes de matrices β-finis est une variété de demi-groupes quotients de demi-groupes de matrices par des congruences β-finies.

Les deux variétés ainsi définies admettent la suite de fonctions Tβ comme mesure concrète de complexité.

Conclusion.

Les résultats que nous avons présentés restent valables, plus généralement, pour les demi-groupes de matrices munis d'une "image à droite" et de rang borné, en suivant les résultats et la méthode indiquées dans [7].

Il faut aussi noter que les algorithmes ici présentés ne sont pas nécessairement les meilleurs possibles. On aimerait la mesure de complexité minimale sur chaque classe de demi-groupes.

Enfin, la présente étude suggère l'étude systématique des classes de demi-groupes qui sont β-finis pour une suite donnée $\beta = (\beta_j)_{j \in \mathbb{N}}$ de fonctions de $\mathbb{N}$ dans $\mathbb{N}$.

Bibliographie.

1 T.C. BROWN, On van der Waerden's theorem on arithmetic progressions ; Notices Amer. Math. Soc., 16 (1969) 245.

2 J.A. BRZOZOWSKI and I. SIMON, Characterizations of locally testable events ; Discrete Math., 4 (1973) 243-271.

3 A.H. CLIFFORD and G.B. PRESTON, The algebraic theory of semigroups ; Amer. Math. Soc., Providence, R.I., vol.I, 1961.

4 S. EILENBERG, Automata, languages and machines ; vol. A and B, Academic Press, New-York, 1975, 1976.

5 G. JACOB, Un théorème de factorisation des produits d'endomorphismes de K^N ; Journal of Algebra, to appear.

6 G. JACOB, Un algorithme calculant le cardinal, fini ou infini, des demi-groupes de matrices ; Theoretical Computer Science, to appear.

7 G. JACOB, La finitude des représentations linéaires des demi-groupes est décidable (sur un corps commutatif) ; submitted to Journal of Algebra.

8 G. JACOB, Décidabilité de la finitude des demi-groupes de matrices ; 3rd G.I. Conference on Theoretical Computer Science, Darmstadt (march 1977) to appear, Lecture Notes, Springer Verlag.

9 G. JACOB, Demi-groupes de matrices localement testables, caractérisation et décidabilité ; Publication n° 82 du Laboratoire de Calcul de l'Université LILLE I, 59650, Villeneuve d'Ascq.

10 V.M. KOPYTOV, Solvability of the problem of occurence in finitely generated soluble groups of matrices over the field of algebraic numbers ; Algebra and Logic, 7 (1968) 388-393. Translated from Russian.

11 A.I. KOSTRIKIN, The Burnside Problem ; Izv. Akad. Nauk. SSSR, 23 (1959) 3-34. (english transcription : Amer. Math. Soc. Translations 36 (1964) 63-99).

12 A. MANDEL and I. SIMON, On finite semigroups of matrices ; Instituto de Matematica e Estatistica, Universidade de Sao Paulo, Brasil.

13 R. McNAUGHTON and Y. ZALCSTEIN, The Burnside theorem for semigroups ; Journal of Algebra, 34 (1975) 292-299.

14 D. PERRIN, Codes bipréfixes et groupes de permutations ; Thèse, Paris (1975).

15 J.F. PERROT, Contribution à l'étude des monoïdes syntactiques de de certains groupes associée aux automates finis ; Thèse, Paris (1972).

16 M.P. SCHUTZENBERGER, On finite monoids having only trivial subgroups ; Inf. and Control, 8 (1965) 190-194.

17 D. SUPRUNENKO, Matrix groups ; Transl. of Math. Monographies, vol. 45 (1976) Amer. Math. Soc., Providence, Rhode-Island.

18 Y. ZALCSTEIN, Finiteness conditions for matrix semigroups ; Proc. Amer. Math. Soc., 38 (1973) 247-249.