Le théorème de Cobham, automates et logique

Raphaël Beuzart-Plessis

9 février 2007

Introduction : Il s'agit ici d'exposer les liens entre arithmétique et automates à travers le théorème de Cobham qui jouera le rôle de pierre angulaire tout au long de l'exposé. Dans un premier temps on introduira la notion d'ensemble k-reconnaisable et l'on y dégagera quelques résultats qui permettent de mieux cerner le concept. On introduira en premier lieu la notion de k-reconnaissabilité et on l'étudiera sur quelques exemples. Cependant plusieurs points de vue prévalent en ce qui concerne les ensembles k-reconnaissables et une partie du travail consistera à démontrer l'équivalence des différentes notions et comprendre leur complémentarité. Enfin on verra comment généraliser les résultats des parties précédentes à des systèmes de numération non standards.

Chapitre 1

Les ensembles k-reconnaissables, premiers exemples, énoncé du théorème de Cobham

On présente d'abord ici la notion de sous ensemble de $\mathbb{N}$ k-reconnaissable et on étudie quelques exemples. On sera alors en mesure d'énoncer le théorème de Cobham.

1.1 Premières définitions

Posons ici des notations qui seront utilisées tout au long du mémoire : on notera $\Sigma_k = \{0, \dots, k-1\}$ l'alphabet constitué des k premiers entiers ($k > 1$). Si $n \in \mathbb{N}$ on sait que l'on peut décomposer de façon unique n sous la forme $n = d_l k^l + \cdots + d_0$ où pour tout $i \in \{0, \dots, l\}$ on a $d_i \in \Sigma_k$ et $d_l > 0$ (c'est la décomposition de n en base k), on associe alors à n le mot $[n]_k$ de Σ_k^* : $[n]_k = d_l \dots d_0$ (c'est l'écriture en base k de n). On note de plus σ_k l'application $\mathbb{N} \to \Sigma_k^*$ qui à l'entier n associe $[n]_k$. De façon inverse à tout mot de Σ_k^* noté $u = d_0 \dots d_n$ on associe l'entier $d_0 k^n + \cdots + d_n$ et on note ν_k cette application. Clairement ν_k est une application surjective mais non injective et on a $\nu_k \circ \sigma_k = Id$.

<u>Définition-Théorème $I.1$</u> : Soit $A \subseteq \mathbb{N}$ les propositions suivantes sont alors équivalentes :

1. (i) Le langage $\sigma_k(A)$ est un langage rationnel.
2. (ii) Le langage $\nu_k^{-1}(A)$ est un langage rationnel.
3. (iii) Il existe un langage rationnel L tel que $\nu_k(L) = A$.

Si l'une des propositions est vérifiées on dit alors que A est k-reconnaissable.

démonstration : Puisque $\nu_k^{-1}(A) = 0^*\sigma_k(A)$ et $\sigma_k(A) = \nu_k^{-1}(A) \cap (\Sigma_k^* - 0\Sigma_k^*)$ on a clairement $(i) \Leftrightarrow (ii)$. De plus il est évident que $(ii) \Rightarrow (iii)$. Enfin pour prouver que $(iii) \Rightarrow (ii)$ il suffit de voir que $\nu_k^{-1}(A) = 0^*[0^{*-1}L]$.

Exemples :

- Si A=$\{k^n | n \in \mathbb{N}\}$ alors $\sigma_k(A) = 10^*$ donc A est k-reconnaissable.
- On verra plus loin que l'ensemble des termes d'une suite arithmétique est k-reconnaissable pour tout $k > 1$.
- Comme va le montrer la proposition suivante $A = \{n^2 | n \in \mathbb{N}\}$ n'est pas k-reconnaissable pour tout $k > 1$ (en fait on verra que c'est plus généralement le cas pour $\{n^b | n \in \mathbb{N}\}$).

Proposition $I.2$:L'ensemble $\{n^2 | n \in \mathbb{N}\}$ n'est pas k-reconnaissable pour tout $k > 1$.

démonstration : Soit $k > 1$ et supposons que le langage $L = \{\sigma_k(n^2) | n \in \mathbb{N}\}$ soit rationnel. Remarquons que $\forall n \in \mathbb{N}, (k-1)^n(k-2)0^n1 \in L$ en effet : $\nu_k((k-1)^n(k-2)0^n1) = (k^{n+1}-1)^2$. Par le lemme de l'étoile $\exists n, p \in \mathbb{N}^*$ tels que $\forall l \in \mathbb{N}, (k-1)^{n+lp}(k-2)0^n1 \in L$ alors que pour $l > 0$ pair c'est à dire $l = 2m$ avec $m > 0$ on a : $\nu_k((k-1)^{n+lp}(k-2)0^n1) = 1 - 2k^{n+1} + k^{2(n+mp+1)}$ et $(k^{n+mp+1} - 1)^2 < 1 - 2k^{n+1} + k^{2(n+mp+1)} < (k^{n+mp+1})^2$ on aboutit donc à une contradiction et $\{n^2 | n \in \mathbb{N}\}$ n'est donc pas k-reconnaissable.

On peut réécrire les éléments de Σ_k^* de la façon suivante : à $u \in \Sigma_k^*$ on associe la paire (x, y) où $x = \nu_k(u)$ et $y = |u|$ est la longueur du mot u. On remarque de façon évidente qu'une telle représentation est injective au sens où deux mots de Σ_k^* ne peuvent être représentés par la même paire. De plus si (x, y) est une paire associée au mot $u \in \Sigma_k^*$ on a $x < k^y$ et réciproquement si une paire $(x, y) \in \mathbb{N}$ est donnée telle que $x < k^y$ alors le mot $u = 0^m\sigma_k(x)$, pour un entier m bien choisi, est associé à la paire (x, y). La concaténation de deux mots de Σ_k^* s'exprime de façon simple au niveau des paires d'entiers par :

$$(x, y)(x', y') = (k^{y'}x + x', y + y')$$

Il est alors facile de démontrer la proposition suivante :

Proposition $I.3$: Soit $l = k^p$ avec $k > 1, p > 0$. Alors il existe un morphisme injectif $\phi : \Sigma_l^* \to \Sigma_k^*$ rendant le diagramme suivant commutatif :

$$\begin{tikzcd}
\Sigma_l^* \arrow[rr, "\phi"] \arrow[dr, "\nu_l"'] & & \Sigma_k^* \arrow[dl, "\nu_k"] \\
& \mathbb{N} &
\end{tikzcd}$$

démonstration : On note $(x,y)_k$ pour les paires d'entiers associées aux éléments de Σ_k^*. Il suffit alors de poser $\phi((x,y)_l) = (x,py)_k$ et on vérifie que si $x < l^y$ alors $x < k^{py}$ car $l = k^p$ donc ϕ est bien définie. Les autres propriétés sont évidentes.

Un corollaire immédiat de la proposition précédente est l'équivalence entre les notions de k-reconnaissabilité et de k^p-reconnaissabilité :

Corollaire $I.4$: Avec les notations de la proposition précédente, un ensemble $A \subset \mathbb{N}$ est k-reconnaissable si et seulement si il est l-reconnaissable.

démonstration : Si A est k-reconnaissable alors $\nu_k^{-1}(A)$ est rationnel et puisque $\nu_l^{-1}(A) = \phi^{-1}(\nu_k^{-1}(A))$ on en déduit que $\nu_l^{-1}(A)$ est rationnel i.e. A est l-reconnaissable.

Si maintenant A est l-reconnaissable alors $\sigma_l(A)$ est rationnel et par conséquent $\phi(\sigma_l(A))$ l'est aussi. Puisque $\nu_k(\phi(\sigma_l(A))) = \nu_l(\sigma_l(A)) = A$ on en déduit que A est k-reconnaissable.

Maintenant, et avant d'énoncer le théorème de Cobham, on va dévelloper quelques résultats basiques concernant les ensembles k-reconnaissables. Il s'agira principalement de traduire au niveau arithmétique les résultats bien connus en ce qui concerne les langages rationnels. Ainsi l'utilisation du lemme de l'étoile fournit immédiatement le résultat suivant :

Proposition $I.5$: Soit $A \subset \mathbb{N}$ un ensemble k-reconnaissable infini $(k > 1)$. Alors il existe des entiers a, b, c, d positifs avec $b > 0, d > 0$ tels que

$$\forall n \in \mathbb{N},\, e_n = ak^{nd} + b\tfrac{k^{nd}-1}{k^d-1} + c \in A$$

démonstration : On pose $L = \sigma_k(A)$ qui est un langage rationnel, A étant infini L l'est aussi et par le lemme de l'étoile on en déduit immédiatement l'existence de $u, v, w \in \Sigma_k^*$ avec $v \neq \epsilon$ tels que $\forall n \in \mathbb{N}$ $uv^nw \in L$ et la proposition s'en suit immédiatement puisque $\nu_k(uv^nw) = e_n$ avec $d = |w|$, $a = \nu_k(u)k^{|v|}$, $b = \nu_k(w)k^{|v|}$ et $c = \nu_k(v)$.

Il est alors facile d'en déduire que l'ensemble des nombres premiers n'est pas k-reconnaissable pour tout $k > 1$. Plus précisément on a le résultat suivant :

Corollaire $I.6$: Si A est un ensemble constitué uniquement de nombres premiers et si A est k-reconnaissable $(k > 1)$, alors A est fini.

démonstration : On reprend les notations de la propositions précédentes et on suppose A infini. Alors $\forall n$, $e_n \in A$ or :

$$e_{n+r} = e_n + ak^{nd}(k^{rd} - 1) + bk^{nd}\tfrac{k^{rd}-1}{k^d-1}$$

On peut toujours choisir n tel que ni k^d, ni $k^d - 1$ ne soient divisible par le nombre premier e_n. Alors il existe $r > 0$ tel que $e_n | (k^{rd} - 1)$. On a alors pour un tel choix de n et de r, $e_n | e_{n+r}$ et $e_n < e_{n+r}$ ce qui contredit que e_{n+r} est premier.

Afin d'avancer plus loin dans notre étude des ensembles k-reconnaissables, on introduit deux grandeurs associées à un ensemble d'entiers :

Si $A = \{a_0, \ldots, a_i, \ldots\}$ est un ensemble infini d'entiers les a_i étant classés par ordre croissant on pose alors :

$$R_A = \limsup_{i\to\infty} \frac{a_{i+1}}{a_i}$$

et

$$D_A = \limsup_{i\to\infty} (a_{i+1} - a_i)$$

La proposition $I.5$ nous permet immédiatement d'énoncer un premier résultat :

Proposition $I.7$: Si A est un ensemble infini d'entiers k-reconnaissable alors il existe un sous ensemble $\{a'_1 < a'_2 < \ldots < a'_i < \ldots\}$ de A qui vérifie

$$lim_{i\to\infty} \frac{a'_{i+1}}{a'_i} = k^d$$

pour un certain entier $d > 0$

Et A vérifie $R_A < \infty$.

démonstration : Pour la première partie de la proposition il suffit de prendre $a_i = e_i$ où les e_i sont définis comme dans la proposition $I.5$.

Ensuite pour i assez grand il existe un entier j tel que :

$$a'_j \leq a_i < a_{i+1} \leq a'_{j+1}$$

Et par conséquent $\frac{a_{i+1}}{a_i} \leq \frac{a'_{j+1}}{a'_j}$ et donc

$$R_A \leq k^d = lim_{i\to\infty} \frac{e_{i+1}}{e_i}$$

.

Il est alors facile d'en déduire par exemple que l'ensemble $\{i! | i \in \mathbb{N}\}$ n'est pas k-reconnaissable pour tout $k > 1$.

Dans la même direction Eilenberg montre dans son livre ([6]) ce qu'il appelle "the gap theorem"' dont on ne donnera pas la démonstration ici (voir [6]) :

Théorème $I.8$: Soit $A \subset \mathbb{N}$, si A est k-reconnaissable pour un certain $k > 1$ alors :

$$R_A > 1$$
ou
$$D_A < \infty$$
le ou étant exclusif

Une application simple du théorème précédent est la suivante : $\forall b > 1$ l'ensemble $A = \{i^b | i \in \mathbb{N}\}$ n'est k-reconnaissable pour aucun $k > 1$. En effet on a alors $R_A = 1$ et $D_A = \infty$.

On va maintenant énoncer le théorème de Cobham mais avant il faut encore introduire une dernière notion : celle d'entiers multiplicativement indépendants.

Définition $I.9$: Deux entiers k et l sont dits multiplicativement indépendants si il n'existe pas d'entiers $q > 0$ et $p > 0$ tels que $k^p = l^q$. Si ça n'est pas le cas on dit alors qu'il sont multiplicativement dépendants.

Définition $I.10$: Un ensemble A d'entiers est dit ultimement périodique si $\exists N, p \in \mathbb{N}\ p > 0$ tels que $\forall n \in A,\ n \geq N \Rightarrow n + p \in A$.

Théorème de Cobham(1969) $I.11$: Soient k et l deux entiers multiplicativement indépendants, un ensemble d'entiers à la fois k- et l-reconnaissable est ultimement périodique.

Remarque : i)En utilisant $I.4$ il est facile de voir que si k et l sont multiplicativement dépendants alors un ensemble est k-reconnaissable si et seulement si il est l-reconnaissable.

ii) Il n'est pas très dur de montrer, et nous le verrons au cours de dévellopements ultérieurs, que tout ensemble ultimement périodique est k-reconnaissable pour tout $k > 1$.

Chapitre 2

généralisation à plusieurs dimensions, p-substitutions logique et automates

Dans cette section nous allons essayer d'étendre la notion de p-reconnaissabilité à des sous-ensembles de $\mathbb{N}^n$, puis nous verrons deux autres définitions équivalentes : celle d'ensemble p-substitutif et une de définissabilité dans une strusture logique.

2.1 Quelques notions de logique

On fait ici quelques rappels de logique du premier ordre qui nous serviront par la suite.

Définition $II.1$: Une structure logique du premier ordre consiste en la donnée de $S = \langle D, (R_i)_{i\in I}, (f_j)_{j\in J}, (c_k)_{k\in K}\rangle$ où D est le domaine c'est à dire un ensemble, les R_i sont des relations sur D c'est à dire des parties de D^{n_i}, les f_j des fonctions de D^{n_j} dans D et les c_k des constantes c'est-à-dire des éléments de D.

exemples : On donne tout de suite les exemples qui nous serviront : $\langle \mathbb{N}, +\rangle$ est une structure logique du premier ordre ; on a aussi $\langle \mathbb{N}, +, V_p\rangle$ où V_p est une fonction $\mathbb{N} \to \mathbb{N}$ telle que $V_p(x)$ est la plus grande puissance de p qui divise x (on a $p > 1$) si $x \neq 0$ et $V_p(0) = 1$.

A partir d'une structure logique du premier ordre on peut construire les formules du premier ordre qui vont avec. Afin de construire ces formules on introduit des variables en nombre dénombrable $x_1, \ldots, x_i, \ldots$. Les formules se construisent alors de façon inductive :

1- Toute constante et toute variable est un terme. Si f_j est une fonction n-aire et que $t_1, \ldots, t_n$ sont des termes alors $f_j(t_1, \ldots, t_n)$ est un terme.

2- Si t_1 et t_2 sont des termes alors $t_1 = t_2$ est une formule.

3- Si R_i est une relation $n - aire$ et que $t_1, \ldots, t_n$ sont des termes alors $R_i(t_1, \ldots, t_n)$ est une formule.

4- Si ϕ et ψ sont des formules et x une variable alors : $\phi \vee \psi$, $\neg\phi$ et $\exists x \phi$ sont des formules.

exemples : $(\exists z)(x + z = y)$ ou encore $\neg\exists x((x + y = z) \vee (z + x = y))$ sont des formules du premier ordre dans la structure $\langle \mathbb{N}, + \rangle$. La première définit la relation $x \leq y$.

Si ϕ est une formule on la note généralement $\phi(x_1, \ldots, x_n)$ où les x_i sont les variables libres (c'est-à-dire qui ne sont pas sous le joug d'un quantificateur $\exists$) apparaissant dans la formule ϕ. Si ϕ est une formule sans variable libre alors on note $S \models \phi$ si la formule ϕ est vérifiée dans S en interprétant les signes logiques $\neg$,$\vee$ et $\exists$ de la façon naturelle. Alors à toute formule $\phi(x_1, \ldots, x_n)$ est associé un sous-ensemble M_ϕ de $\mathbb{N}^n$ par :

$$M_\phi = \{(l_1, \ldots, l_n) \in D^n \mid S \models \phi(l_1, \ldots, l_n)\}.$$

Ainsi ϕ définit une relation sur D. Puisque qu'on peut voir une fonction $f : D^n \to D$ comme un sous ensemble de D^{n+1} (son graphe), de même on peut définir une constante c grâce à une relation unaire qui est $x = c$.

Si $S = \langle D, (R_i)_{i \in I}, (f_j)_{j \in J}, (c_k)_{k \in K} \rangle$ est une structure logique du premier ordre on dit alors qu'une relation R (resp. une fonction f, une constante c) est définissable dans cette structure s'il existe une formule du premier ordre ϕ telle que M_ϕ soit le sous-ensemble de D^n associé à R (resp. la fonction f, la constante c). Un sous-ensemble de D^n est dit définissable s'il s'écrit sous la forme M_ϕ.

Par exemple, on a déjà vu dans les exemples précédents que la relation $x \leq y$ est une relation définissable dans la structure $\langle \mathbb{N}, + \rangle$. La constante 0 est définissable dans cette même structure par la formule : $\neg\,(\exists y \,\neg\,(x \leq y))$.

2.2 k-reconnaissabilité en dimension supérieure

On va ici étendre la notion de k-reconnaissabilité à des sous-ensembles de $\mathbb{N}^n$ mais pour cela il va falloir commencer par définir les automates correspondant. La solution que l'on adoptera (et qui est communément admise) est d'utiliser des automates qui lisent une lettre de chaque mot du n-uplet en même temps c'est-à-dire qu'on va considérer des automates sur l'alphabet Σ_k^n. On étend alors la définition de ν_k à $\Sigma_k^{n*} \to \mathbb{N}^n$ composante par composante (on ne peut pas par contre étendre la définition de σ_k puisque pour tout élément de Σ_k^{n*} les mots du n-uplet ont tous la même longueur). On dit alors qu'une partie $A \subset \mathbb{N}^n$ est k-reconnaissable si il existe un langage rationnel $L \subset \Sigma_k^{n*}$ tel que $A = \nu_k(L)$. Si c'est le cas et si Λ est un automate qui reconnait le langage L on dira par abus de langage qu'il reconnait A.

Exemple : On considère ici l'ensemble qui nous servira d'exemple tout au long des développements : $A = \{(n,m)\,|aucun\ 2^p\ n'apparait\ \ la\ fois\ dans\ la\ decomposition\ binaire\ de\ n\ et\ de\ m\}$ (appelé l'ensemble de Pascal). alors l'automate suivant reconnait A, ce qui montre que A est 2-recconnaissable :

(Les lettres qui sont des vecteurs à deux composantes sont notées ici verticalement).

Maintenant qu'on a généralisé la k-reconnaissabilité à des dimensions supérieures, il ne reste plus qu'à définir la notion de k-substitution.

2.3 k-substitutions

Une k-substitution au départ c'est juste une application $\phi : A \to A^k$ où A est un alphabet et qui se prolonge de façon unique en un morphisme $\phi : A^* \to A^*$. Si de plus il existe une lettre $a \in A$ tel que $\phi(a)$ commence par la lettre de a alors on peut définir le mot $\phi^\omega(a)$ qui est la limite de la suite $a, \phi(a), \ldots, \phi^i(a), \ldots$ (puisque chaque terme de cette suite est préfixe du suivant et que la longueur des mots de la suite est strictement croissante). Si maintenant $\chi : A \to \{0,1\}$ est une application on peut l'étendre d'une unique façon en un morphisme $\chi : A \to \{0,1\}^*$ et on peut donc définir $c = \chi(\phi^\omega(a))$ qui est un mot infini sur l'alphabet $\{0,1\}$.

Maintenant, un ensemble $X \subset \mathbb{N}$ est dit k-substitutif s'il existe ϕ et χ comme précédemment tels que $n \in X \Leftrightarrow c_n = 1$.

exemple : L'ensemble des puissances de 2 est 2-substitutif via $\phi :\ a \to ab\ b \to bc\ c \to cc$ et $\chi :\ a \to 0; b \to 1\ c \to 0$.

On peut d'ores et déjà énoncer une première équivalence entre k-reconnaissabilité et k-substitution qui sera un cas particulier d'un théorème qu'on verra plus loin (il s'agit ici juste du cas à une dimension).

Théorème $II.2$: Un ensemble $X \subset \mathbb{N}$ est k-reconnaissable si et seulement si il est k-substitutif.

démonstration : Il s'agit d'une démonstration constructive dans les deux sens. Supposons tout d'abord que X est k-reconnaissable on peut alors se donner un automate déterministe Λ qui reconnaît le langage $\sigma_k(X)$. On peut de plus supposer cet automate émondé (c'est-à-dire qu'il existe de tout état un chemin vers un état final et un chemin de l'état initial vers tout état). On note alors $Q = \{q_0, \ldots, q_n\}$ l'ensemble des états de l'automate et où q_0 est l'état initial. On peut alors rajouter à l'automate une transition de q_0 vers lui-même et qui lit la lettre 0 (puisque l'automate est émondé au départ il n'y a pas de transition partant de q_0 qui lit 0 car sinon un mot de $0\Sigma_k^*$ serait dans $\sigma_k(X)$). Le nouvel automate reconnait le langage $0^*\sigma_k(X)$et on peut le compléter en ajoutant un état puit q_{n+1}. On prend alors Q comme alphabet et on définit la k-substitution par :

$$\phi : Q^* \to Q^* \ \phi(q) = (q.0)\ldots(q.(k-1)) \text{ et on a que } \phi(q_0) \text{ commence par } q_0$$
$$\text{et } \chi : Q \to \{0,1\} \text{ par } \chi(q) = 1 \text{ si } q \text{ est final, 0 sinon.}$$

Il est alors facile de voir que $\phi^\omega(q_0)_n = q_0.(\sigma_k(n))$ ce qui montre que l'on a bien défini une k-substitution qui reconnaît X.

Réciproquement, partant d'une k-substitution donné par $\phi : A \to A^k$ et $\chi : A \to \{0,1\}$ qui reconnaît X, il n'est pas très dur de construire un automate reconnaissant $\nu_k^{-1}(X)$ en opérant la construction inverse (B est l'ensemble des états de l'automate, a l'état initial les états finaux étant les $b \in A$ tels que $\chi(b) = 1$ puis on définit les transitions comme précédemment).

Maintenant il s'agit d'étendre cette notion de k-substitution pour pouvoir y reconnaître des sous-ensembles de $\mathbb{N}^n$. On ne le fait ici que dans le cas où $n = 2$ la généralisation étant immédiate.

Afin de définir ce qu'est une k-substitution en dimension deux il faut considérer des applications $\phi : B \to B^{k\times k}$: ces applications associe à un élément de B associe un carré de coté k rempli de k^2 lettres de B. Par exemple :

$$f : \{a,b\} \to \{a,b\}^{2\times 2} \text{ définit par}$$
$$a \to \begin{smallmatrix} a & b \\ a & a \end{smallmatrix} \text{ et } b \to \begin{smallmatrix} b & b \\ b & b \end{smallmatrix}$$

Il s'agit maintenant comme dans le cas à une dimension de prolonger l'application de ϕ afin de pourvoir l'itérer et ainsi obtenir un carré infini de deux cotés composé de lettres de B et qui soit point fixe de ϕ. On doit donc prolonger ϕ en une application sur les carrés composés d'éléments de B. Or ceci est simple, il suffit de remplacer chaque lettre du carré initial par son image par ϕ obtenant ainsi un carré de longueur multipliée par k. Un exemple étant ici plus parlant que de longs discours, montrons par exemple comment itérer la fonction définie dans l'exemple précédent sur la lettre a :

$$a \rightarrow \begin{array}{cc} a & b \\ a & a \end{array} \rightarrow \begin{array}{cccc} a & b & b & b \\ a & a & b & b \\ a & b & a & b \\ a & a & a & a \end{array} \rightarrow \begin{array}{cccccccc} a & b & b & b & b & b & b & b \\ a & a & b & b & b & b & b & b \\ a & b & a & b & b & b & b & b \\ a & a & a & a & b & b & b & b \\ a & b & b & b & a & b & b & b \\ a & a & b & b & a & a & b & b \\ a & b & a & b & a & b & a & b \\ a & a & a & a & a & a & a & a \end{array} \rightarrow \ldots$$

Ainsi pour obtenir un carré infini point fixe de ϕ, il faut trouver une lettre a telle que $\phi(a)$ possède a comme lettre dans le coin en bas à gauche. Alors on peut définir $\phi^{\omega}(a)$. Il suffit ensuite de définir $\chi : B \rightarrow \{0, 1\}$, on prolonge alors immédiatement χ au carré d'éléments de B : $\chi(\phi^{\omega}(a))$ représente alors la fonction caractéristique d'une certaine partie de $\mathbb{N}^2$ noté X ($(n, m) \in X$ si et seulement si la valeur à l'intersection de la n-ième colonne et de la m-ième ligne de $\chi(\phi^{\omega}(a))$ est un 1). On dit alors que la k-substitution précédemment définie reconnaît l'ensemble X.

Ainsi il n'est pas très difficile de vérifier que la 2-substitution précédemment définie en posant $\chi :\ a \rightarrow 1\ b \rightarrow 0$ reconnaît l'ensemble de Pascal.

2.4 Différentes façon de voir la k-reconnaissabilité

Cette section tourne principalement autour d'un théorème qui est le suivant :

Théorème $II.3$: Soit $X \subset \mathbb{N}^n$ et $k > 1$ un entier alors il y a équivalence entre les trois propositions suivantes :

(i) : L'ensemble X est k-reconnaissable.

(ii) : L'ensemble X est k-substitutif.

(iii) : L'ensemble X est définissable dans la structure logique $\langle \mathbb{N}, +, V_k \rangle$.

démonstration : L'équivalence $(i) \Leftrightarrow (ii)$ a déjà était vue dans le cas $n = 1$ et dans le cas général c'est juste une adaptation de la démonstration de la section précédente (pour une démonstration complète voir par exemple [4]).

On va donc ici surtout se focaliser sur la démonstration de l'équivalence $(i) \Leftrightarrow (iii)$. Et dans un premier temps il s'agira de montrer l'implication $(iii) \Rightarrow (i)$ par induction sur les formules logiques. Au lieu d'utiliser la structure $\langle \mathbb{N}, +, V_k \rangle$ on va partir de la structure équivalente (c'est-à-dire qu'on peut y définir exactement les mêmes relations) $\langle \mathbb{N}, R_+, R_{V_k} \rangle$ où $R_+(x, y, z)$ est la relation $x + y = z$ et $R_{V_k}(x, y)$ est la relation $V_k(x) = y$. Les formules atomiques que l'on peut construire à partir de la structure $\langle \mathbb{N}, R_x, R_{V_k} \rangle$ sont $x = y$, $R_{V_k}(x, y)$ et $R_+(x, y, z)$; et les langages associés sont bien rationnels : on a ainsi une expression rationnel pour $\sigma_k(M_=)$ $(\sigma_k(M_=) = (\substack{0 \\ 0} + \cdots + \substack{k-1 \\ k-1})^*)$, une pour $\sigma_k(M_{V_k})$ $(\sigma_k(M_{V_k}) = (\substack{0 \\ 0} + \cdots + \substack{k-1 \\ 0})^*(\substack{1 \\ 1} + \cdots + \substack{k-1 \\ 1})(\substack{0 \\ 0})^*)$ et pour $\sigma_k(M_+)$ il suffit de montrer que son langage miroir est rationnel (ce qui est plus simple pour gérer les retenues) et on peut donner par exemple un automate pour ce langage dans le cas $k = 2$ (dans le cas général l'automate se construit de la même manière puisqu'il y a un état qui gère l'addition sans retenue, un état qui gère les retenues (qui sont toutes de au plus 1) et un état puit) :

Maintenant il s'agit partant de deux formules ϕ et ψ et de deux automates Λ_ϕ et Λ_ψ (qui reconnaissent les langages associés à ϕ et ψ) de construire des automates pour les formules $\neg\phi$, $\exists x\phi$ et $\phi \vee \psi$.

Pour la formule $\neg\phi$ l'automate $\Lambda_{\neg\phi}$ sera simplement le complémentaire de l'automate Λ_ϕ.

On construit maintenant l'automate $\Lambda_{\phi\vee\psi}$. Pour cela on notera $x_1, \ldots, x_p, y_1, \ldots, y_l$ les variables libres apparaissant dans ϕ et $y_1, \ldots, y_l, z_1, \ldots, z_m$ les variables libres apparaissant dans ψ. Toutes les arêtes de l'automate Λ_ϕ lisent une lettre de la forme $(a_1, \ldots, a_p, b_1, \ldots, b_l)$, on remplace alors cette arête par plusieurs autres identiques mais étiquetées par tous les éléments de l'ensemble $\{(a_1, \ldots, a_p, b_1, \ldots, b_l)\} \times \{0, \ldots, k-1\}^m$.

De même, on remplace chaque arête de Λ_ψ étiquetée par $(b_1, \ldots, b_l, c_1, \ldots, c_m)$ par un ensemble d'arêtes identiques étiquetées par tous les éléments de l'ensemble $\{0, \ldots, k-1\}^k \times \{(b_1, \ldots, b_l, c_1, \ldots, c_m)\}$. Les nouveaux automates obtenus reconnaissent des parties de $\mathbb{N}^{p+l+m}$ et, pour obtenir $\Lambda_{\phi\vee\psi}$, il suffit de construire l'automate union des deux précédents.

Reste à construire l'automate $\Lambda_{\exists x\phi}$. Si x n'apparaît pas dans les variables libres de ϕ alors il suffit de garder l'automate Λ_ϕ (car les deux formules sont équivalentes). Sinon on note $x, x_1, \ldots, x_p$ les variables libres de ϕ : $\phi(x, x_{1,l}\, dots, x_p)$. Alors chaque arête de Λ_ϕ est étiquetée par une lettre $(a, a_1, \ldots, a_p)$ qu'on remplace alors par l'étiquette $(a_1, \ldots, a_p)$: l'automate obtenu n'est pas forcément déterministe mais reconnaît un langage L tel que $\nu_k(L) = M_{\exists x\phi}$ (qui n'est pas forcément $\nu_k^{-1}(M_{\exists x\phi})$ à cause des transitions de la forme $(a, 0, \ldots, 0)$).

Maintenant on va partir d'un automate reconnaissant un sous-ensemble de $\mathbb{N}^n$ pour construire une formule qui définit le même sous-ensemble.

On introduit pour cela les nouvelles relations $\epsilon_{0,k}(x, y), \ldots, \epsilon_{k-1,k}(x, y)$, la relation $\epsilon_{j,k}(x, y)$ signifiant que y est une puissance de k qui apparait dans le développement k-aire de x avec le coefficient j. Cette relation est définissable dans la structure $\langle \mathbb{N}, +, V_k \rangle$ par la formule :

$$(V_k(y) = y) \ \wedge \ [(\exists z, t)(x = z + j.y + t) \ \wedge \ (z < y) \ \wedge \ ((y < V_k(t)) \vee (t = 0))]$$

On définit aussi la nouvelle fonction λ_k telle que $\lambda_k(x)$ soit la plus grande puissance de k apparaissant avec un coefficient non nul dans le développement k-aire de x avec par convention $\lambda_k(0) = 1$. Il existe alors dans la structure $\langle \mathbb{N}, +, V_k \rangle$ une formule définissant la relation $\lambda_k(x) = y$:

$$[\,(V_k(y) = y) \ \wedge \ y \leq x \ \wedge \ ((\forall z)((V_k(z) = z) \wedge y < z) \Rightarrow (x < z))] \ \vee \\ [\,(x = 0) \ \wedge \ (y = 1)\,].$$

On pourra donc utiliser la fonction λ_k et les relations $\epsilon_{0,k}, \ldots, \epsilon_{k-1,k}$ dans les formules qui vont suivre sans sortir du cadre de $\langle \mathbb{N}, +, V_k \rangle$.

Soit maintenant $X \subset \mathbb{N}^n$ et Λ un automate reconnaissant le langage miroir de $\nu_k^{-1}(X)$ (on peut toujours supposer que c'est le langage miroir car un langage L est rationnel si et seulement si son miroir l'est). Alors $(x_1, \ldots, x_n) \in X$ si et seulement si il existe un n-uplet de mots $(w_1, \ldots, w_n)$ tel que $\forall i$, $\nu_k(w_i) = x_i$ et tel que $({w_1}^R, \ldots, {w_n}^R)$ soit reconnu par l'automate Λ. On remplace les états de Λ par des l-uplets de $\{0, \ldots, k-1\}$ (sans perte de généralité), par exemple $q_0 = (1, 0, \ldots, 0), \ldots, q_{l-1} = (0, \ldots, 0, 1)$, et donc un chemin fini $q_0 \ldots q$ peut être vu comme un mot $(u_1, \ldots, u_l)$ qui peut aussi être vu comme un l-uplet d'entiers $(\nu_k(u_1), \ldots, \nu_k(u_l))$.

Pour tout entier n on définira la suite $(n(i))_{i \geq 0}$ comme le développement k-aire de n i.e. $n = \sum_{i=0}^{\infty} n(i) k^i$. En utilisant les notations précédentes $(x_1, \ldots, x_n) \in X$ si et seulement si il existe un l-uplet d'entiers $(y_1, \ldots, y_l)$ tel que :

1- $(y_1(0), \ldots, y_l(0))$ est l'état initial $q_0 = (1, 0, \ldots, 0)$.

2- $(y_1(p), \ldots, y_l(p))$ est un état final pour un certain entier p tel que $k^p \geq max_{1 \leq j \leq n} \lambda_k(x_j)$.

3- Pour tout $0 \leq i < p$, si $(y_1(i), \ldots, y_l(i))$ est l'état q, alors $(y_1(i+1), \ldots, y_l(i+1))$ est l'état $\delta(q, (x_1(i), \ldots, x_n(i)))$ (où δ est la fonction de transition de l'automate).

Ces trois conditions peuvent s'exprimer grâce à une formule $\phi(x_1, \ldots, x_n)$:

$$\begin{gathered}(\exists y_1) \ldots (\exists y_l)(\exists z) \quad (V_k(z) = z) \\ \wedge \quad (z \geq max_{1 \leq j \leq n} \lambda_k(x_j)) \\ \wedge \quad \phi_1(y_1, \ldots, y_l) \\ \wedge \quad \phi_2(y_1, \ldots, y_l, z) \\ \wedge \quad \phi_3(x_1, \ldots, x_n, y_1, \ldots, y_l, z)\end{gathered}$$

avec :

$$\begin{gathered}\phi_1 : \bigwedge_{j=1}^{l} \epsilon_{q_0(j),k}(y_j, 1) \\ \phi_2 : \bigvee_{q \in F} \bigwedge_{j=1}^{l} \epsilon_{q(j),k}(y_j, z) \\ \phi_3 : (\forall t)(\,(V_k(t) = t) \ \wedge \ (t < z) \ \wedge \\ \bigwedge_{\delta(q,(a_1,\ldots,a_n))=q'} \left[\bigwedge_{j=1}^{l} \epsilon_{q(j),k}(y_j, t) \ \wedge \ \bigwedge_{j=1}^{n} \epsilon_{a_j,k}(x_j, t) \ \Rightarrow \ \bigwedge_{j=1}^{l} \epsilon_{q'(j),k}(y_j, k.t) \right])\end{gathered}$$

Clairement, les ensembles k-reconnaissables sont stables par les opérations booléennes usuelles sur les ensembles (puisque les langages rationnels le sont). Cependant le résultat précédent va nous permettre de trouver de nouvelles opérations pour lesquels les ensembles k-reconnaissables sont clos. Ainsi par exemple on a vu que la multiplication par un entier fixé était définissable dans la structure $\langle \mathbb{N}, +, V_k \rangle$: on en déduit que si X est k-reconnaissable il en est de même de $c.X$ puisque si X est définissable par la formule $\phi(y_1, \ldots, y_n)$ $c.X$ est définissable par la formule $(\exists y_1, \ldots, y_n)((\phi(y_1, \ldots, y_n)) \wedge (x_1 = c.y_1 \wedge \ldots \wedge x_n = c.y_n))$. On a en fait par le même argument le résultat plus général suivant :

Corollaire $II.4$: Soit $f : \mathbb{N}^m \to \mathbb{N}^n$ une fonction définissable dans la structure $\langle \mathbb{N}, +, V_k \rangle$. Alors, si $X \subset \mathbb{N}^m$ est k-reconnaissable il en est de même de $f(X)$.

On en déduit d'ailleurs que les termes d'une suite arithmétique de raison $q \geq 0$ et de premier terme $r \geq 0$ est k-reconnaissable pour tout entier $k > 1$ puisqu'un tel ensemble est définissable dans $\langle \mathbb{N}, + \rangle$ par :

$(\exists n)$ $(x = q.n + r)$ (la multiplication par un entier fixé est définissable dans $\langle \mathbb{N}, + \rangle$).

2.5 Généralisation du théorème de Cobham : théorème de Cobham-Semenov

Le dernier problème qu'il reste pour formuler une généralisation du théorème de Cobham c'est d'étendre à $\mathbb{N}^n$ la notion utilisée dans le théorème de cobham d'ensemble ultimement périodique. La proposition suivante va nous permettre de le faire :

Proposition $II.5$: Soit $X \subset \mathbb{N}$ alors les propositions suivantes sont équivalentes :
(i) l'ensemble X est ultimement périodique.
(ii) X est une union finie d'ensembles composés des termes d'une suite arithmétique.
(iii) X est définissable dans $\langle \mathbb{N}, + \rangle$.

démonstration : Pour prouver $(i) \Rightarrow (ii)$ soit $X \subset \mathbb{N}$ un ensemble ultimement périodique donc il existe des entiers N et $p > 0$ tels que $n \in X \wedge n \geq N \Rightarrow (n + p) \in X$ alors il suffit de considérer $R = \{i \,|\, 0 \leq i < p \wedge \exists x \in X \, : \, x = i \, mod \, p \ \wedge \ x \geq N\}$ on peut alors pour tout $i \in R$ il existe $x_i \in X$ tel que $x_i = i \; mod \, p$ et alors $X - (\bigcup_{i \in R} \{x_i + kp | k \in \mathbb{N}\})$ est clairement fini donc X est bien union de suites arithmétiques.

Pour prouver $(ii) \Rightarrow (i)$ il suffit de montrer que l'union de deux ensembles ultimement périodiques est ultimement périodique : Soient donc $X \subset \mathbb{N}$ et $X' \subset \mathbb{N}$ deux ensembles ultimement périodiques de périodes respectives p et p', alors clairement $X \cup X'$ est ultimement périodique de période $p + p'$.

Comme on a vu dans la section précédente une suite arithmétique est définissable dans $\langle \mathbb{N}, + \rangle$ donc on en déduit immédiatment que $(ii) \Rightarrow (iii)$.

Pour la preuve de $(iii) \Rightarrow (i)$ consulter par exemple [4].

On est maintenant en mesure de voir comment peut s'énoncer le théorème de Cobham en dimension supérieure : on remplace le fait d'être ultimement périodique par le fait d'être définissable dans $\langle \mathbb{N}, + \rangle$, on obtient alors le théorème suivant qui a été démontré pour la première fois en 1977 par A.Semenov dans [3] :

<u>Théorème de Cobham-Semenov $II.6$</u> : Soit $m \geq 1$ un entier et $p, q \geq 2$ deux entiers multiplicativement indépendants. Alors si $X \subset \mathbb{N}^m$ est à la fois p-reconnaissable et q-reconnaissable X est définissable dans $\langle \mathbb{N}, + \rangle$.

Le théorème se réénonce immédiatement de façon purement logique :

Si $X \subset \mathbb{N}^m$ est à la fois définissable dans $\langle \mathbb{N}, +, V_p \rangle$ et dans $\langle \mathbb{N}, +, V_q \rangle$ alors X est définissable dans $\langle \mathbb{N}, + \rangle$.

<u>remarque</u> : La preuve initiale du théorème de Cobham (c'est à dire le cas $m = 1$) qui se trouve dans [7] mais est très complexe. Dans son livre [6] S.Eilenberg mentionne le théorème de Cobham :Pour lui, il s'agit d'un défi de trouver une preuve plus raisonnable de ce joli résultat. La preuve de Semenov se construit par récurrence, le premier cas m=1 étant le théorème de Cobham , la preuve utilise 28 lemmes différents.

G.Hansel réussit en premier à trouver une démonstration plus simple du résultat de Cobham dans [1].

Chapitre 3

Autres systèmes de numération

On cherche ici à généraliser le problème dans une autre direction : au lieu d'écrire les entiers dans les bases k-aires on peut essayer de les décomposer dans d'autres bases. Par exemple, il est possible de décomposer les entiers sur la base des nombres de Fibonacci :

$$F_0 = 1,\ F_1 = 1 \text{ et } F_{n+2} = F_n + F_{n+1}$$
$$1 = F_1,\ 2 = F_2,\ 3 = F_3,\ 4 = F_3 + F_1 \text{ et } 5 = F_4$$

Pourtant, comme on peut le remarquer, on a $4 = F_3 + F_1 = F_2 + F_2$ donc l'unicité de la décomposition n'est pas forcément assurée. On doit donc définir d'une certaine manière l'unicité de la décomposition (comme d'ailleurs dans le cas des bases k-aires). Pour décomposer un entier n, il suffit de lui appliquer l'algorithme d'Euclide : On prend le plus grand entier k_0 tel que $F_{k_0} \leq n$ puis le plus grand entier c_0 tel que $c_0.F_{k_0} \leq n$ puis on recommence avec $n - c_0.F_{k_0}$ et on obtient la décomposition standard $n = c_0.F_{k_0} + c_1.F_{k_1} + \cdots + c_t.F_{k_t}$. Il faut cependant imposer quelques conditions sur la suite utilisée $(F_n)_{n\in\mathbb{N}}$ afin notamment que l'algorithme converge et que les entiers utilisés dans la décomposition $c_0, \ldots, c_t$ prennent un nombre de valeurs finis (afin que l'alphabet utilisé soit fini). On utilise donc la définition suivante :

Définition $III.1$: Un système de numération est une suite strictement croissante $(U_n)_{n\in\mathbb{N}}$ d'entiers telle que :

1.$U_0 = 1$ de façon à ce que tout $n \in \mathbb{N}$ ait une décomposition sur la base des $(U_n)_{n\in\mathbb{N}}$.

2.$sup\frac{U_{n+1}}{U_n} < \infty$ (de façon à ce que l'alphabet utilisé soit fini).

Alors la décomposition standard d'un entier n dans cette base est celle donnée par l'algorithme d'Euclide (on associe à 0 le mot vide) et on notera $\sigma_U(x)$ la réprésentation standard (en tant que mot) de l'entier x.

Par exemple, le système décimal classique est décrit par la suite définie par $U_0 = 1$ et $U_n = 10U_{n-1}$. Etant donné un système de numération $(U_n)_{n\in\mathbb{N}}$ on peut associer à chaque entier positif grâce à l'algorithme d'Euclide un mot sur l'alphabet $\{0,\ldots,\left\lceil sup\frac{U_{n+1}}{U_n}\right\rceil - 1\}$ où ici $\lceil x \rceil$ désigne le plus petit entier plus grand que x. On s'intéresse alors aux parties de $\mathbb{N}$ auxquelles sont associés des langages rationnels de $\{0,\ldots,\left\lceil sup\frac{U_{n+1}}{U_n}\right\rceil - 1\}^*$ (on dira alors d'une telle partie qu'elle est U-reconnaissable). La première question légitime qui vient se poser, et qui en quelque sorte permettra de discriminer certains sytèmes de numérations, c'est de savoir si $\mathbb{N}$ est lui-même U-reconnaissable. Le résultat suivant montre que finalement seul un nombre assez restreint de systèmes de numération vérifient cette condition :

Proposition $III.2$: Si l'ensemble $\mathbb{N}$ est reconnaissable par le système de numération $(U_n)_{n\in\mathbb{N}}$ alors la suite $(U_n)_{n\in\mathbb{N}}$ vérifie une relation de récurrence linéaire.

démonstration :Soit $L \subset \{0,\ldots,\left\lceil sup\frac{U_{n+1}}{U_n}\right\rceil - 1\}^*$ le langage associé à $\mathbb{N}$ alors si on note $t_n(L)$ le nombre de mots de L de longueur strictement inférieur à n il est clair via l'algorithme d'Euclide que $t_n(L) = U_n$. Or si L est rationnel la série formelle $\sum_{n=0}^{\infty} t_n(L)x^n$ est une fraction rationnelle car L peut être engendré par une grammaire non ambiguë. Donc il en est de même de $\sum_{n=0}^{\infty} U_n x^n$ ou encore il existe un polynôme $q(x)$ tel que $q(x).(\sum_{n=0}^{\infty} U_n x^n)$ soit un polynôme, en regardant terme à terme on en déduit que la suite $(U_n)_{n\in\mathbb{N}}$ vérifie une relation de récurrence linéaire.

Ainsi $\mathbb{N}$ est par exemple reconnaissable pour le système de numération décimal $(10^n)_{n\in\mathbb{N}}$ (qui vérifie la récurrence $U_n = 10U_{n-1}$) ou encore pour le système de Fibonacci $(F_n)_{n\in\mathbb{N}}$ puisqu'alors une expression rationnelle de $\sigma_F(\mathbb{N})$ est $0^*(10)^*$. Cependant la réciproque de la proposition précédente n'est pas vraie ainsi pour le système de numération défini par $U_0 = 1$, $U_1 = 2$, $U_2 = 4$ et $U_{n+3} = 2U_{n+1} + U_n$, $\sigma_U(\mathbb{N})$ n'est pas rationnel. Dans le cas où :

$$\lim_{n\to\infty} \frac{U_{n+1}}{U_n} = \theta \ (III.3)$$

pour un certain réel $\theta > 1$, Hollander ([12]) a donné une condition nécessaire et suffisante pour que $\mathbb{N}$ soit reconnaissable. Nous nous intéresserons ici principalement au cas où θ est un nombre de Pisot (dans ce cas-là $\mathbb{N}$ est toujours U-reconnaissable) :

Définition $III.4$: Un réel $\theta > 1$ est dit nombre de Pisot s'il est algébrique (c'est-à-dire racine d'un polynôme non nul de $\mathbb{Z}[X]$) et si tous ses conjugués (c'est-à-dire les autres racines que θ lui-même du polynôme minimal de θ) sont de module < 1.

exemples : Tout entier est un nombre de Pisot. Le nombre d'or $\phi = \frac{1+\sqrt{5}}{2}$ est un nombre de Pisot.

Plus particulièrement nous nous intéresserons aux systèmes de numération défini par une récurrence linéaire dont le polynôme caractéristique est le polynôme minimal d'un nombre de Pisot (ce qui implique notamment ($III.3$).On définit, de la même manière que dans la partie II, le fait pour une partie $X \subset \mathbb{N}^n$ d'être U-reconnaissable ($(x_1, \ldots, x_n)$ étant représenté par n'importe quel mot $(0^{l-k_1}\sigma_U(x_1), \ldots, 0^{l-k_n}\sigma_U(x_n))$ où $k_i = |\sigma_U(x_i)|$ et $l \geq max\{k_1, \ldots, k_n\}$). On cherche alors à obtenir des résultats analogues au théorème de Cobham pour des systèmes de numération non standards. Un premier résultat dans ce sens est le suivant ([10]) :

Théorème $III.5$:Soit U un système de numération défini par une récurrence linéaire dont le polynôme caractéristique est le polynôme minimal d'un nombre de Pisot θ, soit $X \subset \mathbb{N}^m$ alors X est U-reconnaissable si et seulement si X est définissable dans $\langle \mathbb{N}, +, V_U \rangle$.

Remarque : -Il nous faut définir la fonction V_U : $V_U(x) = y$ signifie que y est le plus petit U_n apparaissant dans la décomposition standard de x.

-Le fait que la relation $R_+(x, y, z) \Leftrightarrow x + y = z$ définisse une partie U-reconnaissable n'est pas évident à priori mais est fortement lié au fait que θ soit un nombre de Pisot.

-Les ensembles ultimement périodiques étant définissables dans $\langle \mathbb{N}, + \rangle$ le sont à priori dans $\langle \mathbb{N}, +, V_U \rangle$ donc sont U-reconnaissables.

D'autres résultats plus récents concernent la généralisation du théorème de Cobham à des systèmes de numération non standards : dans tout ce qui suit on supposera que U est un système de numération défini par une récurrence linéaire dont le polynôme caractéritique est le polynôme minimal d'un nombre de Pisot θ.

Théorème $III.6$: Si $X \subset \mathbb{N}$ est k-reconnaissable (k>1) et U-reconnaissable alors X est ultimement périodique.

démonstration : voir [13]

Théorème $III.7$: Soient θ et θ' deux nombres de Pisot multiplicativement indépendants et soient U et U' deux systèmes de numération dont les polynômes caractéristiques sont respectivement les polynômes minimaux de θ et θ'. Alors pour tout $n \geq 1$ et pour tout $X \subset \mathbb{N}^n$ si X est U- et U'-reconnaissable alors X est définissable dans $\langle \mathbb{N}, + \rangle$.

démonstration : voir [9].

On peut aussi retrouver pour les ensemble U-reconnaissables un point de vue substitutif (par ce que l'on nomme les U-substitutions : cf [11]).

Bibliographie

[1] G.Hansel, A propos d'un théorème de Cobham, in :*Actes de la fête des mots*,D.Perrin,Ed.,Greco de Programmation, CNRS, Rouen (1982).

[2] A.Muchnik, Definable criterion for definability in Presburger Arithmetic and its application, *preprint* in Russian, Institute of New Technologies (1991).

[3] A.L.Semenov, Presburgerness pf predicates regular in two number systems (in Russian), *Sibirsk. Math. Zh.* 18 (1977) 403-418, traduction en anglais : *Siberian Math. J.* 18 (1977) 289-299.

[4] V.Bruyere, G.Hansel, C.Michaux, R.Villemaire, Logic and p-recognizable sets of integers *Bull. Belg. Math. Soc. 1 (1994)*, 191-238.

[5] V.Bruyere *Automata and Numeration Systems*

[6] S.Eilenberg, Automata, Languages and Machines, *Vol.A, Academic Press*, New-York(1974).

[7] A.Cobham, On the base-dependence of sets of numbers recognizable by finite automata, *Math. Systems Theory* 3 (1969) 186-192.

[8] W.Ritchie, Finite automata and the set of squares, *J. Assoc. Comput. Mach.* 10 (1963) 528-531.

[9] A.Bes, An extension of the Cobham-Semenov theorem, *J. Symb. Logic* 65 (2000) 201-211.

[10] V.Bruyère,G.Hansel, Bertrand numeration systems and recognizability, submitted (1995) 22 pages.

[11] S.Fabre, Une généralisation du théorème de Cobham, *Acta Arithmetica* 67 (1994) 197-208.

[12] M.Hollander, Greedy numeration systems and regularity, *preprint* (1995) 21 pages.

[13] F.Point, V.Bruyère, On the Cobham-Semenov theorem, *Math.System Theory* (1996) 25 pages.