Systèmes de numération non-standard

Ilia Smilga

22 décembre 2008

1 Beta-expansions

La notion de β-expansion est une généralisation de l'écriture positionnelle standard d'un réel compris entre 0 et 1, par exemple en base 2 ou 10, à une base β pas forcément réelle.

Définition 1. Etant donné une base $\beta > 1$ et un réel $x \in [0;1]$, on appelle *développement en base* β de x tout mot infini (sur l'alphabet $\mathbb{Z}$) $(x_i)_{i\geq 1}$ tel qu'on a

$$x = \sum_{i\geq 1} x_i \beta^{-i}$$

On appelle *β-expansion* de x le développement particulier qu'on obtient avec l'algorithme glouton, à savoir le développement $d_\beta(x) = (x_i)_{i\geq 1}$ tel que pour tout $i \geq 1$, on a

$$x_i = \lfloor \beta^i \left(x - \sum_{j=1}^{i-1} x_j \beta^{-j} \right) \rfloor$$

Il est facile de voir qu'une β-expansion est en fait un mot sur l'alphabet plus restreint $\{0, \dots, \lceil \beta \rceil - 1\}$.

A partir de cette définition, il est immédiat de vérifier que parmi tous les développements en base β d'un réel donné, la β-expansion est la plus grande pour l'ordre lexicographique. On montre également sans peine que l'application qui à un réel associe sa β-expansion est strictement croissante pour l'ordre lexicographique. C'est d'ailleurs cette propriété qu'on utilise pour comparer "à la main" deux réels, étant données leurs écritures décimales.

On introduit maintenant le *décalage* σ :

Définition 2. $\sigma((x_i)_{i\geq 1}) = (x_{i+1})_{i\geq 1}$

Il est clair que pour tout $x \in [0;1]$ et pour tout entier $n \geq 1$, on a $\sigma^n(d_\beta(x)) \prec d_\beta(1)$ (où $\prec$ désigne l'ordre lexicographique). La réciproque est également vraie : tout mot qui vérifie cette propriété est une β-expansion valide, car il est clair qu'il est plus grand (dans l'ordre lexicographique) que tous les autres développements du réel qu'il représente. Ainsi, l'ensemble des β-expansions dans une base donnée est déterminé par la β-expansion de 1.

D'autre part, on peut caractériser de façon similaire les mots qui correspondent à l'expansion de 1 dans une certaine base. Il est clair que, pour tout $\beta > 1$ et pour tout entier $n \geq 1$, on a $\sigma^n(d_\beta(1)) \prec d_\beta(1)$: c'est un cas particulier de ce qui précède. La réciproque reste vraie, sauf pour 10^ω (qui donnerait

$\beta = 1$). En effet, étant donné une suite infinie de chiffres, on peut s'assurer que le réel qu'elle représente varie continûment de $+\infty$ à 0 quand β varie entre 1 et $+\infty$, ce qui montre qu'on peut ajuster β de sorte à ce que le mot représente 1 ; si, en plus, le mot vérifie la propriété mentionnée au-dessus, il sera bien une β-expansion de 1.

On va maintenant étudier la possibilité de reconnaître l'ensemble des β-expansions par automate fini. Pour cela, on introduit la notion de système dynamique symbolique :

Définition 3. Soit A un alphabet, $X \subset A^*$ un langage. On note $S_X = \{y \in A^{\mathbb{Z}} | \forall x \in X, y \neq uxv\}$, et on dit que S_X est le *système dynamique symbolique* qui évite le langage X.

On appelle *sous-décalage* de A^* toute partie de A^* stable par le décalage σ et fermée pour la topologie produit.

Il n'est pas difficile de montrer qu'en réalité, ces deux notions coïncident : tout système dynamique symbolique est fermé et stable par σ, et réciproquement, tout sous-décalage S peut s'écrire S_X où $X = A^+ \setminus F(S)$ est l'ensemble des facteurs évités par S.

On dit qu'un système S est *de type fini* s'il existe un langage fini X tel que $S = S_X$. On dit que S est *sofique* si le langage $A^+ \setminus F(S)$ est rationnel.

Malheureusement l'ensemble $D_\beta = \{d_\beta(x) | x \in [0,1]\} = \{s \in A^\omega | \forall n \geq 1, \sigma^n(s) \prec d_\beta(1)\}$ n'est pas un système dynamique symbolique, car il n'est pas fermé. En revanche, son adhérence S_β en est un ; c'est donc surtout cet objet qu'on va étudier.

De la caractérisation de D_β donnée plus haut, on peut en déduire une de S_β : on a
$$S_\beta = \{s \in A^\omega | \forall n \geq 1, \sigma^n(s) \preceq d^*_\beta(1)\}$$
où $d^*_\beta(1) = \sup_{x \in [0,1]} d_\beta(x)$; ce développement coïncide avec la β-expansion de 1 si celle-ci est infinie, il en diffère légèrement si la β-expansion de 1 est finie. En examinant les quotients à gauche de ce langage, on en déduit sans peine le premier résultat :

Proposition 1. *Etant donné $\beta > 1$, le système S_β est sofique ssi $d_\beta(1)$ est ultimement périodique ; il est de type fini ssi $d_\beta(1)$ est finie (i. e. appartient à A^*0^ω).*

Les valeurs intéressantes de β sont donc celles qui donnent lieu à une expansion ultimement périodique de 1 ; on va maintenant chercher à caractériser ces valeurs. On va commencer par quelques rappels et définitions :

Définition 4. Un *entier algébrique* est une racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. Le *polynôme minimal* d'un entier algébrique x est le polynôme qui engendre l'idéal des polynômes unitaires à coefficients dans $\mathbb{Z}$ annulés par x. Les *conjugués* d'un entier algébrique sont les autres racines de son polynôme minimal.

Un *nombre de Pisot* (resp. *de Perron*) est un entier algébrique x, réel, tel que $x > 1$ et pour tout y conjugué de x, on a $|y| < 1$ (resp. $|y| < x$)

On n'a malheureusement qu'une caractérisation partielle des bases β qui conviennent. On a seulement les deux résultats suivants :

Théorème 2. *Si β est un nombre de Pisot, le système S_β est sofique.*
Si S_β est sofique, β est de Perron.

Démonstration. Il est bien connu que tout rationnel a un développement ultimement périodique dans une base entière. On peut montrer un résultat plus fort : si β est de Pisot, tout élément de $\mathbb{Q}(\beta)$ a une β-expansion ultimement périodique. L'idée de la démonstration est la même que dans le cas entier : en utilisant le fait que β est un entier algébrique, on arrive à représenter les restes possibles par des d-uplets d'entiers, où d est le degré du polynôme minimal de β. En utilisant la borne sur les conjugués de β, on arrive à montrer que ces d-uplets sont bornés, ce qui montre qu'il n'y en a qu'un nombre fini et que donc il y a une répétition quelque part.

Quant à la condition nécessaire sur β, son obtention est beaucoup plus astucieuse. Il est clair que si S_β est sofique, β est un entier algébrique. En effet, l'ultime périodicité de la décomposition de 1 se traduit naturellement par une condition polynomiale sur β ; notons P le polynôme correspondant. Les coefficients de P s'expriment en fonction des chiffres du développement, et sont donc entiers ; on vérifie sans difficulté que P est également unitaire. Par ailleurs, β est la seule racine de P dans $]1, +\infty]$, car il est clair que la même écriture ne peut pas être une représentation de 1 dans une autre base.

En fait, il se trouve que P peut également être vu comme polynôme caractéristique d'une certaine matrice M, qui a la propriété d'être *primitive*, c'est-à-dire qu'il existe $k \in \mathbb{N}$ tel que $\forall i, j, (M^k)_{ij} > 0$. Il existe alors un théorème (le théorème de Perron-Frobenius) qui permet d'affirmer que la plus grande valeur propre de M (en valeur absolue) est réelle positive. Cette valeur propre ne peut donc être que β. Enfin, comme P est un polynôme unitaire à coefficients entiers qui a β pour racine, P a tous les conjugués de β pour racines, ce qui montre que β est de Perron. $\square$

Il existe effectivement des nombres de Perron qui ne sont pas de Pisot mais qui sont néanmoins la base d'un système sofique : par exemple, si β est la plus grande racine du polynôme $P = X^4 - 3X^3 - 2X^2 - 3$ ($\beta > 3$ car $P(3) = -15 < 0$), on peut vérifier que $d_\beta(1) = 3203$ mais que P a une racine entre -2 et -1 ($P(-2) = 29$ et $P(-1) = -1$).

2 U-représentations

La notion d'U-représentation est aussi une généralisation de l'écriture positionnelle standard, mais cette fois-ci pour les entiers.

Définition 5. Soit $U = (u_n)_{n \geq 0}$ une suite strictement croissante d'entiers commençant par 1, $N \in \mathbb{N}$. On appelle *U-représentation* de N une suite d'entiers naturels $(d_k d_{k-1} \dots d_0)$ telle que

$$N = \sum_{i=0}^{k} d_i u_i$$

On appelle *U-représentation normale* de N, notée $\langle N \rangle_U$, celle qui s'obtient par l'algorithme glouton, i. e. celle qui vérifie

$$\forall j \leq k, \sum_{i=0}^{j} d_i u_i < u_{j+1}$$

Dans le cas où U est une suite géométrique, on retombe sur l'écriture standard.

De même que pour les développements en base β, on montre que l'application qui à un entier associe son U-représentation normale est "strictement croissante" et que la représentation normale est "la plus grande" de toutes les représentations, sauf qu'il faut choisir le bon ordre. Ici, l'ordre qui convient est ce qu'on appelle en anglais le *radix order* : on compare d'abord les longueurs des mots, puis les mots eux-mêmes dans l'ordre lexicographique. C'est l'ordre qu'on utilise pour comparer à la main deux entiers, étant données leurs écritures décimales ou binaires.

On note $L(U)$ l'ensemble des U-représentations normales des entiers. On a également un résultat sur la reconnaissabilité par automate fini :

Proposition 3. *Si $L(U)$ est reconnaissable par automate fini, la suite U est, à partir d'un certain rang, définissable par une récurrence linéaire à coefficients entiers.*

Démonstration. Il est bien connu que, si L est un langage rationnel, la série $\sum_{n\geq 0} l_n X^n$, où $l_n = |\{x \in L||x| = n\}|$, est $\mathbb{Z}$-rationnelle, i. e. représente une fraction rationnelle à coefficients entiers (on le vérifie facilement par récurrence sur L). Donc la série dont la suite des coefficients est U est $\mathbb{Z}$-rationnelle, puisque $u_n = \sum_{k=0}^{n} l_n$ (en effet, l'U-représentation normale d'un entier naturel N est de longueur plus petite que n ssi $N < u_n$). On en déduit que les termes de U vérifient une récurrence linéaire à coefficients entiers. □

Avant d'aller plus loin, il faut dire qu'on remarque une certaine similitude entre les β-expansions et les U-représentations. Prenons, par exemple, $\beta = \phi = \frac{1+\sqrt{5}}{2}$ et U la suite de Fibonacci (commençant à $u_0 = 1, u_1 = 2$). Alors D_β est l'ensemble des mots infinis sur $\{0,1\}$ qui ne contiennent pas le facteur 11, et $L(U)$ est l'ensemble des mot finis sur le même alphabet qui évitent le même facteur ; on a ainsi $L(U) = F(D_\beta)$. Ce n'est pas si surprenant car asymptotiquement, on a $u_n \sim \phi^n$. En fait, on peut définir la notion de système de numération canoniquement associé à une base (réelle) donnée :

Définition 6. Soit $\beta > 1$, $(d_i)_{i\geq 1} = d^*_\beta(1) = \sup_{x\in[0,1]} d_\beta(x)$. On appelle alors *système de numération canonique associé à β* le système $U_\beta = (u_n)_{n\geq 0}$ choisi de telle sorte à ce qu'on ait :

$$\langle u_n - 1\rangle_{U_\beta} = d_1 \ldots d_n$$

soit explicitement, U_β est la suite définie par la relation de récurrence :

$$u_n = \sum_{i=1}^{n} d_i u_{n-i} + 1$$

Les systèmes de numération canoniques sont caractérisés par la proposition suivante :

Proposition 4. *Soit U une suite strictement croissante, telle que $u_0 = 1$ et la suite $\frac{u_{n+1}}{u_n}$ soit bornée. Alors les conditions suivantes sont équivalentes :*

1. *Il existe $\beta > 1$ tel que $U = U_\beta$*
2. *Il existe $\beta > 1$ tel que $L(U) = F(D_\beta)$*
3. *$\forall v \in U, v0 \in U$ (on dit que U est* extensible à droite*)*

Démonstration. Il est clair que la condition 2 implique 3. Il n'est pas difficile de voir que 1 implique 2, car avec cette définition de U, la condition d'être facteur d'une β-expansion et celle d'être une U-représentation normale s'écrivent de la même façon. Enfin, pour voir que 3 implique 1, on peut construire la β-expansion de 1 à partir des $\langle u_n - 1 \rangle_{U_\beta}$, en déduire la valeur de β et s'assurer qu'elle vérifie bien les bonnes propriétés. □

Il est clair que si β est un nombre de Pisot, puisque D_β est reconnaissable par un automate fini, $L(U)$ l'est aussi. Avec de bonnes hypothèses, on peut même obtenir un résultat plus fort : non seulement l'ensemble des U-représentations normales est reconnaissable, mais en plus, étant donné une suite de chiffres, on peut la transformer en U-représentation normale avec un transducteur fini.

Théorème 5. *Soit β un nombre de Pisot. On suppose que le polynôme caractéristique de U_β, c'est-à-dire le polynôme caractéristique de la récurrence linéaire qui définit cette suite, est égal au polynôme minimal de β (il est clair que β est une racine de ce premier polynôme, mais en général, le premier est seulement divisible par le deuxième). Soit $C \subset \mathbb{N}$ un alphabet. Alors il existe un transducteur fini qui prend en entrée un mot w sur C^*, et qui calcule l'U-représentation normale qui représente le même entier que w.*

La construction de ce transducteur est assez complexe ; elle passe par la construction d'un automate qui reconnaît les mots sur $C \cup -C$ qui représentent 0, et c'est cette construction qui utilise l'hypothèse sur la minimalité du polynôme.