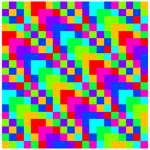
Jouer avec les mots, pourquoi et comment ?

Michel Rigo

http://www.discmath.ulg.ac.be/
http://orbi.ulg.ac.be/handle/2268/184489

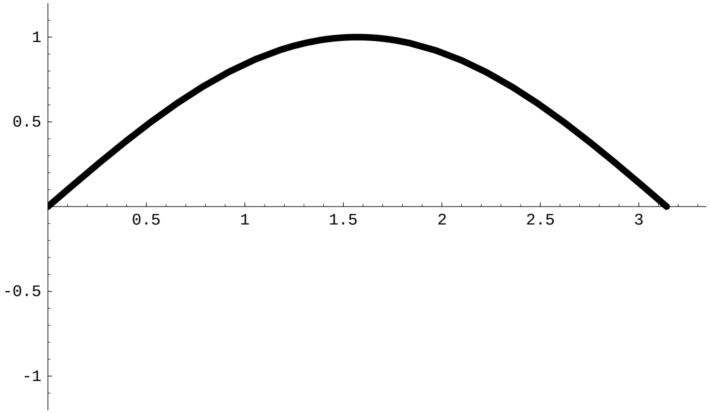
BSSM — 4 août 2015
Brussels Summer School of Mathematics

Université de Liège



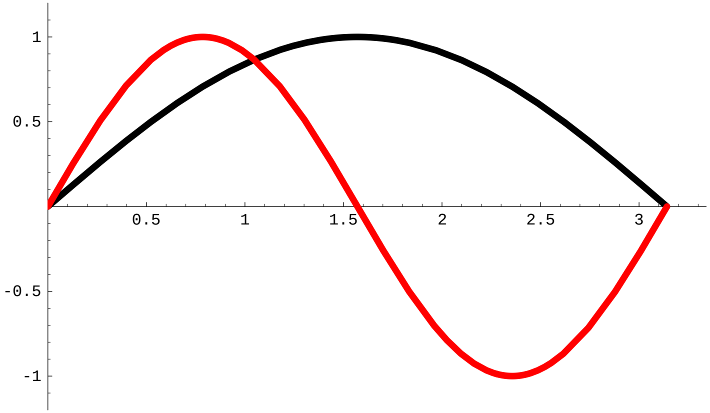
Exercice d'échauffement

Signe de la fonction $\sin(x)$ sur $[0, \pi]$?



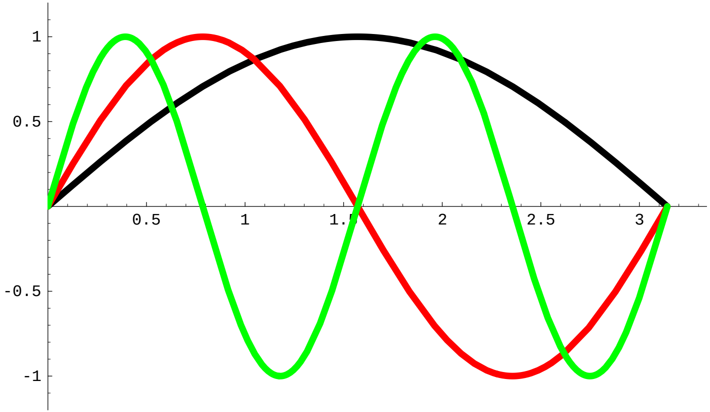
Exercice d'échauffement

Signe de la fonction $\sin(x)\sin(2x)$ sur $[0, \pi]$?



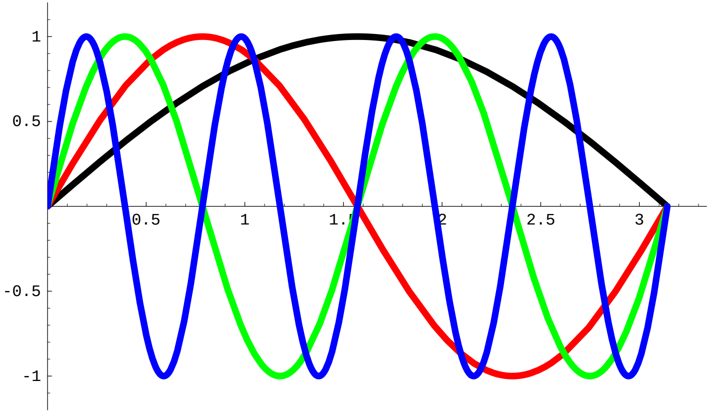
Exercice d'échauffement

Signe de la fonction $\sin(x)\sin(2x)\sin(4x)$ sur $[0, \pi]$?



Exercice d'échauffement

Signe de la fonction $\sin(x)\sin(2x)\sin(4x)\sin(8x)$ sur $[0,\pi]$?



Exercice d'échauffement

Question générale

Signe sur $[0, \pi]$ de la fonction

$$f_n(x) := \sin(x)\sin(2x)\sin(4x)\cdots\sin(2^n x)$$

L'intervalle $[0, \pi]$ est divisé en 2^n intervalles

$$I_j := \left[\frac{j\,\pi}{2^n}, \frac{(j+1)\,\pi}{2^n}\right] \qquad j = 0, \ldots, 2^n - 1$$

Comment caractériser *facilement*

le signe de f_n sur I_j pour n grand et $j < 2^n \ldots$

Pour les cosinus, on dispose d'une formule :

$$\cos(x)\cos(2x)\cos(4x)\cdots\cos(2^n x) = \frac{\sin(2^{n+1}x)}{2^{n+1}\sin(x)}$$

Un brin de formalisation

Un *alphabet* est un ensemble fini,
e.g., $\{+,-\}$, $\{a,b,c\}$, $\{0,1,\ldots,9\}$, $\{\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{T}\}$.

Soit A un alphabet. Un *mot (fini) de longueur $n \geq 0$* sur A est une application de $[\![0, n-1]\!]$ à valeurs dans A, i.e., une suite finie d'éléments de A.

$$+--+, \quad abcbca, \quad \mathtt{AGGCTACTTA}$$

La longueur d'un mot est notée $|w|$.

Le *mot vide* est la suite vide de longueur 0, noté ε.

Structure de monoïde

L'ensemble A^* des mots finis sur A muni de l'opération de *concaténation* est un monoïde dont le neutre est ε

$$bon \cdot jour = bonjour$$

Notion de convergence

Soit A un alphabet. Un *mot infini* sur A est une application $\mathbf{w} : \mathbb{N} \to A$, i.e., une suite d'éléments de A

$$14159265358979323846264338327950288419716939937 \cdots$$

- suite de mots infinis convergeant vers un mot infini limite
- suite de mots *finis* convergeant vers un mot infini limite

Espace métrique

Soit $A^{\mathbb{N}}$ l'ensemble des mots infinis sur A. Soient $\mathbf{x}, \mathbf{y} \in A^{\mathbb{N}}$

$\mathbf{x} \wedge \mathbf{y}$: plus long préfixe commun

$$d : A^{\mathbb{N}} \times A^{\mathbb{N}} \to \mathbb{R}_{\geq 0}, \quad d(\mathbf{x}, \mathbf{y}) = \begin{cases} 2^{-|\mathbf{x} \wedge \mathbf{y}|} & , \text{ si } \mathbf{x} \neq \mathbf{y} \\ 0 & , \text{ si } \mathbf{x} = \mathbf{y} \end{cases}$$

Notion de convergence

Soit A un alphabet. Un *mot infini* sur A est une application $\mathbf{w} : \mathbb{N} \to A$, i.e., une suite d'éléments de A

$$14159265358979323846264338327950288419716939937\cdots$$

- suite de mots infinis convergeant vers un mot infini limite
- suite de mots *finis* convergeant vers un mot infini limite

Espace métrique

Soit $A^{\mathbb{N}}$ l'ensemble des mots infinis sur A. Soient $\mathbf{x}, \mathbf{y} \in A^{\mathbb{N}}$

$\mathbf{x} \wedge \mathbf{y}$: plus long préfixe commun

$$d : A^{\mathbb{N}} \times A^{\mathbb{N}} \to \mathbb{R}_{\geq 0}, \quad d(\mathbf{x}, \mathbf{y}) = \begin{cases} 2^{-|\mathbf{x} \wedge \mathbf{y}|} & , \text{ si } \mathbf{x} \neq \mathbf{y} \\ 0 & , \text{ si } \mathbf{x} = \mathbf{y} \end{cases}$$

Distance ultramétrique

1. $d(\mathbf{x}, \mathbf{y}) \geq 0$,
2. $d(\mathbf{x}, \mathbf{y}) = 0$ si et seulement si $\mathbf{x} = \mathbf{y}$,
3. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$,
4. $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ (inégalité triangulaire),

$$\forall \mathbf{w}, \mathbf{x}, \mathbf{y} \in A^{\mathbb{N}}, \ d(\mathbf{w}, \mathbf{x}) \leq \max\{d(\mathbf{w}, \mathbf{y}), d(\mathbf{y}, \mathbf{x})\} .$$

Digression. Soient $p \geq 2$ premier et x entier. On a $x = p^n q$ et *la valuation p-adique* $\nu_p(x) = n$. Extension à $\mathbb{Q}$ par
$\nu_p(a/b) = \nu_p(a) - \nu_p(b)$ pour tous $a, b \in \mathbb{Z}$ avec $b \neq 0$.

La *valeur absolue p-adique* (non archimédienne) sur le champ $\mathbb{Q}$ est $|x|_p = p^{-\nu_p(x)}$ si $x \neq 0$ et $|0|_p = 0$.

On a $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ pour tous $x, y \in \mathbb{Q}$ et la distance correspondante $d(x, y) = |x - y|_p$ est ultramétrique.

Distance ultramétrique

1. $d(\mathbf{x},\mathbf{y}) \geq 0$,
2. $d(\mathbf{x},\mathbf{y}) = 0$ si et seulement si $\mathbf{x} = \mathbf{y}$,
3. $d(\mathbf{x},\mathbf{y}) = d(\mathbf{y},\mathbf{x})$,
4. $d(\mathbf{x},\mathbf{z}) \leq d(\mathbf{x},\mathbf{y}) + d(\mathbf{y},\mathbf{z})$ (inégalité triangulaire),

$$\forall \mathbf{w},\mathbf{x},\mathbf{y} \in A^{\mathbb{N}},\ d(\mathbf{w},\mathbf{x}) \leq \max\{d(\mathbf{w},\mathbf{y}), d(\mathbf{y},\mathbf{x})\}\,.$$

Digression. Soient $p \geq 2$ premier et x entier. On a $x = p^n q$ et *la valuation p-adique* $\nu_p(x) = n$. Extension à $\mathbb{Q}$ par
$\nu_p(a/b) = \nu_p(a) - \nu_p(b)$ pour tous $a, b \in \mathbb{Z}$ avec $b \neq 0$.

La *valeur absolue p-adique* (non archimédienne) sur le champ $\mathbb{Q}$ est $|x|_p = p^{-\nu_p(x)}$ si $x \neq 0$ et $|0|_p = 0$.

On a $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ pour tous $x, y \in \mathbb{Q}$ et la distance correspondante $d(x,y) = |x-y|_p$ est ultramétrique.

boule de centre $\mathtt{abbbbb}\cdots$ et de rayon $1/2$

$$\{\mathbf{x} \in A^{\mathbb{N}} \mid d(\mathbf{x}, \mathtt{abbbbb}\cdots) \leq 1/2\}$$

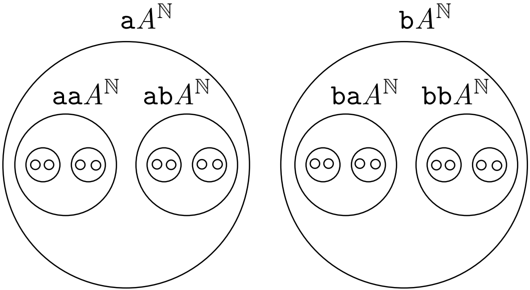


FIGURE : Une représentation de $\{\mathtt{a}, \mathtt{b}\}^{\mathbb{N}}$.

- *Tout point appartenant à une boule en est le centre ;*
- *si $\mathcal{B} \cap \mathcal{B}' \neq \emptyset$, alors $\mathcal{B} \subseteq \mathcal{B}'$ ou $\mathcal{B}' \subseteq \mathcal{B}$.*

Convergence

Soit $(\mathbf{x}_n)_{n\geq 0}$ une suite de mots infinis sur A.
Cette suite *converge* vers $\mathbf{y} \in A^{\mathbb{N}}$ si

$$\forall \epsilon > 0,\ \exists N\ :\ \forall n \geq N, d(\mathbf{x}_n, \mathbf{y}) < \epsilon.$$

Pour tout ℓ, il existe N tel que pour tout $n \geq N$, les mots infinis $\mathbf{x}_n$ ont tous le *même préfixe de longueur* ℓ.

NB : $A^{\mathbb{N}}$ est un espace métrique complet et compact.

Convergence de mots finis

Soit $(x_n)_{n\geq 0}$ une suite de mots finis sur A. Soit $z \notin A$.
Cette suite *converge* vers $\mathbf{y} \in A^{\mathbb{N}}$ si

la suite $(x_n z^\omega)_{n\geq 0}$ converge vers $\mathbf{y}$.

Convergence

Soit $(\mathbf{x}_n)_{n\geq 0}$ une suite de mots infinis sur A.
Cette suite *converge* vers $\mathbf{y} \in A^{\mathbb{N}}$ si

$$\forall \epsilon > 0, \exists N \ : \forall n \geq N, d(\mathbf{x}_n, \mathbf{y}) < \epsilon.$$

Pour tout ℓ, il existe N tel que pour tout $n \geq N$, les mots infinis $\mathbf{x}_n$ ont tous le *même préfixe de longueur* ℓ.

NB : $A^{\mathbb{N}}$ est un espace métrique complet et compact.

Convergence de mots finis

Soit $(x_n)_{n\geq 0}$ une suite de mots finis sur A. Soit $z \notin A$.
Cette suite *converge* vers $\mathbf{y} \in A^{\mathbb{N}}$ si

la suite $(x_n z^\omega)_{n\geq 0}$ converge vers $\mathbf{y}$.

Exemple dans $\{0,\ldots,9\}^{\mathbb{N}}$, développement en fractions continues de $\pi - 3$

$$\frac{1}{7} \qquad 142857142857\,142857142857\,142857142857\cdots$$

$$\cfrac{1}{7+\cfrac{1}{15}} \qquad 141509433962264\,1509433962264\,15094339\cdots$$

$$\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1}}} \qquad 141592920353982300884955752212389380\cdots$$

$$\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292}}}} \qquad 14159265301190260407226149477372968400\cdots$$

Suite convergente de mots finis

$$
\begin{array}{l}
1zzzzzzzzzzzzzzzzzzzz\cdots\\
14zzzzzzzzzzzzzzzzzzzz\cdots\\
141zzzzzzzzzzzzzzzzzzzz\cdots\\
1415zzzzzzzzzzzzzzzzzzzz\cdots\\
14159zzzzzzzzzzzzzzzzzzzz\cdots\\
141592zzzzzzzzzzzzzzzzzzzz\cdots\\
1415926zzzzzzzzzzzzzzzzzzzz\cdots\\
14159265zzzzzzzzzzzzzzzzzzzz\cdots\\
141592653zzzzzzzzzzzzzzzzzzzz\cdots\\
1415926535zzzzzzzzzzzzzzzzzzzz\cdots\\
14159265358zzzzzzzzzzzzzzzzzzzz\cdots\\
141592653589zzzzzzzzzzzzzzzzzzzz\cdots\\
1415926535897zzzzzzzzzzzzzzzzzzzz\cdots\\
\vdots\\
1415926535897932384626433832795028841971693993 7\cdots
\end{array}
$$

Si $\#A \geq 2$, $A^{\mathbb{N}}$ est non dénombrable.

Cependant, les "algorithmes pouvant engendrer un mot infini de $A^{\mathbb{N}}$" (i.e., si on fournit n par exemple en base 2, l'algorithme calcule le $n$ième symbole du mot) forment un ensemble dénombrable.

Turing, On computable numbers, with an application to the Entscheidungsproblem, Proc. London Math. Soc. 1937.

$\rightsquigarrow$ On va chercher des algorithmes "simples"
(hiérarchie de Chomsky, complexité de Chaitin–Kolmogorov).

Construction simple de mots infinis

Soit A^* le monoïde des mots finis sur A. Un *morphisme* est une application $f : A^* \to A^*$ telle que $f(uv) = f(u)f(v)$ pour tous $u, v \in A^*$.

Définition

Un *morphisme prolongeable sur a* est tel que

- $f(a) = au$ avec $u \neq \varepsilon$ et
- $\lim_{n\to+\infty} |f^n(a)| = +\infty$.

Exemple 1 (longueur constante)

$t : + \mapsto +-, \; - \mapsto -+$ est prolongeable, $|t^n(+)| = 2^n$.

Construction simple de mots infinis

Exemple 2

$u : a \mapsto abc, \ b \mapsto ac, \ c \mapsto bac$ est prolongeable sur a,
$|u^{n+1}(a)| \geq 2|u^n(a)|$.

Exemple 3 (morphisme de Fibonacci)

$f : a \mapsto ab, \ b \mapsto a$ est prolongeable sur a,
$|f^n(a)| = F_n$.

Exemple 4

$g : a \mapsto ba, \ b \mapsto ab$ n'est pas prolongeable.

Exemple 5

$h : a \mapsto ab, b \mapsto \varepsilon$ n'est pas prolongeable,
$|h^n(a)| = 2$ pour tout $n \geq 1$.

Construction simple de mots infinis

Soit $f : A^* \to A^*$ un morphisme prolongeable sur a.

Exercice

1. Si $f(a) = au$, exprimer $f^n(a)$.
2. Montrer que $f^n(a)$ est un préfixe de $f^{n+1}(a)$.
3. Conclure que $(f^n(a))_{n\geq 0}$ converge vers un mot infini limite.
4. Etendre f sur $A^{\mathbb{N}}$ et montrer que ce mot infini limite est un point fixe de f.

$$f^{\omega}(a) := \lim_{n\to+\infty} f^n(a).$$

Un morphisme prolongeable permet donc de définir aisément un mot infini (ensemble des mots purement morphiques).

Construction simple de mots infinis

Exemple 1

$t : + \mapsto +-, \; - \mapsto -+$

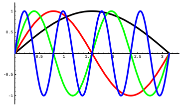
$$\begin{array}{rcl} t(+) & = & +- \\ t^2(+) & = & +--+ \\ t^3(+) & = & +--+-++- \\ t^4(+) & = & +--+-++--++-+--+ \\ & \vdots & \end{array}$$

Construction simple de mots infinis

Exemple 2

$f : a \mapsto abc,\ b \mapsto ac,\ c \mapsto bac$

$$
\begin{aligned}
f(a) &= abc \\
f^2(a) &= abcacbac \\
f^3(a) &= abcacbacabcbacacabcbac \\
f^4(a) &= abcacbacabcbacacabcbacabcacbacacabc \cdots bac \\
&\vdots
\end{aligned}
$$



Retour au problème initial

Comment caractériser *facilement*

le signe de f_n sur I_j pour n grand et $j < 2^n \dots$

En particulier, doit-on déterminer le signe de chaque intervalle pour déterminer le signe d'un seul d'entre eux ? Doit-on disposer de $sign(I_0), \dots, sign(I_{j-1})$ pour déterminer $sign(I_j)$?

$$+--+-++--++-+--+-++-+--++--+-++-\cdots$$

$$+ \mapsto +-, \quad - \mapsto -+$$

$$\begin{array}{cccccccccccccccc}
 & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & \cdots \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & \cdots \\
\hline
+ & - & - & + & - & + & + & - & - & + & + & - & + & - & - & \cdots
\end{array}$$

$$+ \mapsto +-, \quad - \mapsto -+$$

										1	1	1	1	1	$\cdots$
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	$\cdots$
$+$	$-$	$-$	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$\cdots$

$$+ \mapsto +-, \quad - \mapsto -+$$

										1	1	1	1	1	$\cdots$
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	$\cdots$
$\oplus$	$\ominus$	$-$	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$\cdots$

$$+ \mapsto +-, \qquad - \mapsto -+$$

										1	1	1	1	1	$\cdots$
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	$\cdots$
$+$	$\ominus$	$-$	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$\cdots$

$$+ \mapsto +-, \quad - \mapsto -+$$

$$\begin{array}{cccccccccccccccc}
 & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & \cdots \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & \cdots \\
\hline
+ & - & \ominus & \oplus & - & + & + & - & - & + & + & - & + & - & - & \cdots
\end{array}$$

$$+ \mapsto +-, \quad - \mapsto -+$$

										1	1	1	1	1	$\cdots$
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	$\cdots$
$+$	$-$	$\ominus$	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$\cdots$

$$+ \mapsto +-, \qquad - \mapsto -+$$

										1	1	1	1	1	$\cdots$
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	$\cdots$
$+$	$-$	$-$	$+$	$\ominus$	$\oplus$	$+$	$-$	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$\cdots$

$$+ \mapsto +-, \qquad - \mapsto -+$$

$$\begin{array}{cccccccccccccccc}
 & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & \cdots \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & \cdots \\
\hline
+ & - & - & \oplus & - & + & + & - & - & + & + & - & + & - & - & \cdots
\end{array}$$

$$+ \mapsto +-, \quad - \mapsto -+$$

$$
\begin{array}{cccccccccccccccc}
 & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & \cdots \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & \cdots \\
\hline
+ & - & - & + & - & + & \oplus & \ominus & - & + & + & - & + & - & - & \cdots
\end{array}
$$

$$+ \mapsto +-, \qquad - \mapsto -+$$

										1	1	1	1	1	$\cdots$
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	$\cdots$
$+$	$-$	$-$	$+$	$-$	$+$	$\oplus$	$-$	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$\cdots$

$$+ \mapsto +-, \qquad - \mapsto -+$$

										1	1	1	1	1	$\cdots$
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	$\cdots$
$+$	$-$	$-$	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$\cdots$

$$\boxed{t_{2n} = t_n, \quad t_{2n+1} = -t_n}$$

Morphismes de longueur constante

Soit $f : A^* \to A^*$ tel que $|f(a)| = k$ pour tout $a \in A$.

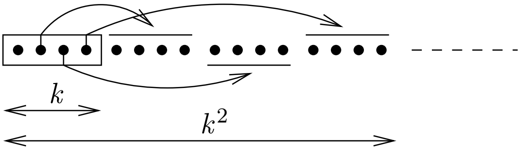


FIGURE : Morphisme de longueur constante $k = 4$.

$$\mathbf{x} = f^{\omega}(a) = x_0 x_1 x_2 \quad \cdots x_q \cdots \quad \cdots x_j \cdots \quad \cdots$$

Lemme fondamental (simple exercice)

Soit j, $k^m \leq j < k^{m+1}$. On a $j = kq + r$, $k^{m-1} \leq q < k^m$ et $0 \leq r < k$. Le symbole x_j est le $(r+1)$-ième symbole dans $f(x_q)$.

$$\boxed{t_{2n} = t_n, \quad t_{2n+1} = -t_n}$$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	$\cdots$
$\oplus$	$\ominus$	$-$	$\oplus$	$-$	$+$	$\oplus$	$-$	$-$	$+$	$+$	$-$	$+$	$\ominus$	$-$	$\cdots$

$$13 = 2.6 + 1 = 2.(2.3 + 0) + 1 = 2.(2.(2.1 + 1) + 0) + 1$$
$$= 2.(2.(2.(2.0 + 1) + 1) + 0) + 1$$

$$\mathrm{rep}_2(n) = 1101$$

Ainsi, connaissant l'écriture en base 2 de j, on détermine directement le signe de la fonction sur I_j.

$$\boxed{t_{2n} = t_n, \quad t_{2n+1} = -t_n}$$

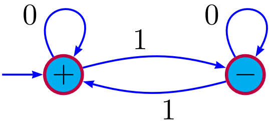
$$\begin{array}{cccccccccccccccc}
 & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & \cdots \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & \cdots \\
\hline
{\color{blue}\oplus} & {\color{red}\ominus} & - & {\color{blue}\oplus} & - & + & {\color{red}\oplus} & - & - & + & + & - & + & {\color{blue}\ominus} & - & \cdots
\end{array}$$

$$\begin{aligned}
{\color{blue}13} &= 2.{\color{red}6} + 1 = 2.(2.{\color{blue}3} + 0) + 1 = 2.(2.(2.{\color{red}1} + 1) + 0) + 1 \\
&= 2.(2.(2.(2.{\color{blue}0} + 1) + 1) + 0) + 1
\end{aligned}$$

$$\mathrm{rep}_2(n) = 1101$$

Ainsi, connaissant l'écriture en base 2 de j, on détermine directement le signe de la fonction sur I_j.

$$+ \mapsto +-, \quad - \mapsto -+$$

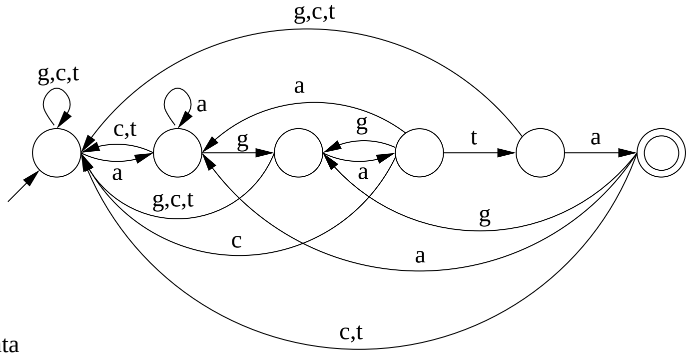


On introduit la notion d'*automate fini déterministe*

- Q ensemble d'états
- $q_0 \in Q$ état initial
- $\delta : Q \times A \to Q$ fonction de transition

On étend la fonction de transition à $\delta : Q \times A^* \to Q$

Recherche d'un mot dans un texte. . .



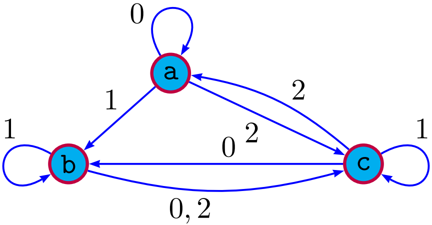
agata

Complexité linéaire par rapport à l'entrée

Morphismes de longueur constante

L'exemple de $+--+-++-\cdots$ se généralise :

$$f : \begin{cases} \mathtt{a} & \mapsto & \mathtt{abc} \\ \mathtt{b} & \mapsto & \mathtt{cbc} \\ \mathtt{c} & \mapsto & \mathtt{bca} \end{cases}$$



$$f^\omega(\mathtt{a}) = \mathtt{abccbcbcabcacbcbcacbcbcaabc}\cdots$$

Proposition (A. Cobham 1972)

Si $\mathbf{x} = x_0x_1x_2\cdots$ est point fixe d'un morphisme f de longueur constante $k \geq 2$ et débutant par a, alors pour l'automate associé

$$\forall j, \quad x_j = \delta_f(\mathtt{a}, \mathrm{rep}_k(j))$$

RÉCIPROQUE (A. COBHAM 1972)

Soient $k \geq 2$ et un automate fini déterministe

- A comme ensemble d'états,
- $\mathtt{a} \in A$ comme état initial,
- $[\![0, k-1]\!]$ comme alphabet, (k arcs sortant de chaque état)
- $\delta(\mathtt{a}, 0) = \mathtt{a}$.

Alors, le mot infini $\mathbf{x}$ défini par

$$\forall j, \quad x_j = \delta(\mathtt{a}, \mathrm{rep}_k(j))$$

est engendré par le morphisme prolongeable sur a de longueur constante k et associé à l'automate.

Ensemble des *mots infinis k-automatiques*.

Généralisations

- Ajout d'un codage (projection) / automates avec sortie

$$f^\omega(\mathtt{a}) = \mathtt{abccbcbcabcacbcbcacbcbcaabc}\cdots$$

$$g(f^\omega(\mathtt{a})) = \mathtt{0100101001000101000101000 10}\cdots$$

$$\{\text{mots purement morphiques}\} \subsetneq \{\text{mots morphiques}\}$$

- Etude des ensembles k-reconnaissables de nombres

$$\{1, 4, 6, 9, 13, 15, 19, 21, 25, \dots\}$$

- Longueur non constante, $a \mapsto ab,\ \ b \mapsto a$

$$abaababaabaababaab\cdots$$

  $\rightsquigarrow$ systèmes de numération non standards
- Cadre multi-dimensionnel
- Codage/représentation de systèmes dynamiques discrets

$$\{\text{mots automatiques}\} \subsetneq \{\text{mots morphiques}\}$$

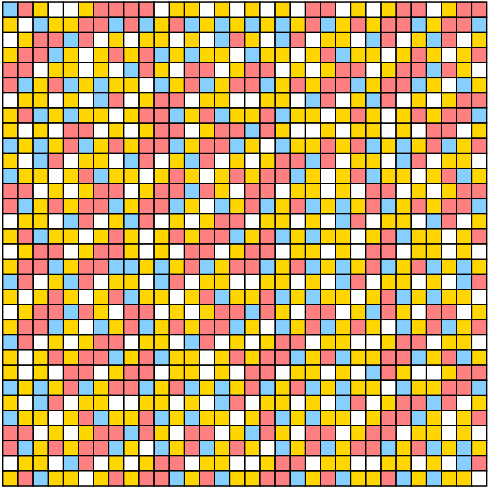
- fréquence d'apparition d'un symbole
- ordre de croissance, thm. de Cobham de 1969
- fonction de complexité

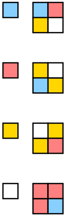
$f : a \mapsto ab, \;\; b \mapsto a$

$f^\omega(a) = abaababaabaababaababaabaababaabaababaababaabaabab \cdots$

Est-ce qu'un mot infini engendré par un morphisme de longueur 2 peut aussi l'être par un morphisme de longueur 3 ?

A. Cobham
`http://recursed.blogspot.com/2010/04/alan-cobham.html`





J.-P. Allouche, T. Johnson, Finite automata and morphisms in assisted musical composition, Journal of New Music Research (1995).

Tom Johnson : “Les automates finis n’occupent qu’un chapitre dans mon livre *Self-Similar Melodies* (1996), mais en 1997 j’eus envie d’étudier des suites de cette sorte plus rigoureusement et de composer une collection de *Automatic Music for six percussionists*. Les sept premiers mouvements furent créés à Moscou par l’ensemble de Marc Pekarsky. . . ”

Applications

1. Combinatoire des mots : *étude des configurations, motifs évitables, dénombrement, énumération, structure,...*
2. Théorie des nombres
3. Géométrie discrète

(4.) Système de numération, ensembles reconnaissables, vérification

(5.) Théorie des jeux combinatoires

Un carré : coco, $0120\underline{2121}01$, uu

Théorème

Si $\#A = 2$, tout mot suffisamment long contient un carré.

- Si $\#A > 2$?
- Peut-on éviter les cubes sur deux lettres ?

Un carré : coco, $0120\underline{2121}01$, uu

Théorème

Si $\#A = 2$, tout mot suffisamment long contient un carré.

- Si $\#A > 2$?
- Peut-on éviter les cubes sur deux lettres ?

Combinatoire des mots

Un chevauchement : $cvcvc$, `ananas`

Tout cube débute/se termine par un chevauchement

Théorème (Thue 1906)

Le mot de Thue–Morse ne contient pas de chevauchement

$$+--+-++--++-+--+-++-+--++--+-++-\cdots$$

M. Morse, Recurrent geodesics on a surface of negative curvature, *Trans. Amer. Math. Soc.* 22 (1921) 84–100.

Preuve (Lothaire)

Lemme

Soit $X = \{ab, ba\}$.
Si $x \in X^*$, alors axa et bxb n'appartiennent aucun des deux à X^*.

Par récurrence sur $|x|$.

Cas de base, $x = \varepsilon$.

Supposons le résultat OK pour les mots de longueur $< n$.

Soit $x \in X^*$ de longueur n.
Par l'absurde, supposons que $u = axa \in X^*$.

$$u = abyba, \quad |y| = |x| - 2$$

et $y \in X^*$ donc $x = byb \notin X^*$, absurde.

Preuve (Lothaire)

Lemme

Soit $X = \{ab, ba\}$.
Si $x \in X^*$, alors axa et bxb n'appartiennent aucun des deux à X^*.

Par récurrence sur $|x|$.

Cas de base, $x = \varepsilon$.

Supposons le résultat OK pour les mots de longueur $< n$.

Soit $x \in X^*$ de longueur n.
Par l'absurde, supposons que $u = axa \in X^*$.

$$u = abyba, \quad |y| = |x| - 2$$

et $y \in X^*$ donc $x = byb \notin X^*$, absurde.

Preuve (Lothaire)

Lemme

Soit $X = \{ab, ba\}$.
Si $x \in X^*$, alors axa et bxb n'appartiennent aucun des deux à X^*.

Par récurrence sur $|x|$.

Cas de base, $x = \varepsilon$.

Supposons le résultat OK pour les mots de longueur $< n$.

Soit $x \in X^*$ de longueur n.
Par l'absurde, supposons que $u = axa \in X^*$.

$$u = ab\,y\,ba, \quad |y| = |x| - 2$$

et $y \in X^*$ donc $x = byb \notin X^*$, absurde.

Lemme "overlap-free morphism"

Soit f tel que $f(a) = ab$, $f(b) = ba$.
Si w est sans chevauchement, $f(w)$ aussi.

Supposons que $f(w)$ contient un chevauchement

$$f(w) = x\,cvcvc\,y, \quad c \in \{a, b\},\ v, x, y \in \{a, b\}^*$$

Thèse : w contient un chevauchement.

$\leadsto$ exploiter le fait que f est de longueur constante.

$$f(w) = xcvcvcy$$

$|cvcvc| = 3 + 2|v|$ est impair, $|f(w)|$ pair $\Rightarrow$ $|xy|$ impair.

- Montrer que $|v|$ est impair
  - Si $|x|$ pair, alors $cvcv, cy \in X^*$.
    supposons $|v|$ pair, alors $cvc \in X^*$, contradiction.
  - Si $|x|$ impair, alors $vcvc, y \in X^*$.
    supposons $|v|$ pair, alors $cvc \in X^*$, contradiction.

$$f(w) = xcvcvcy$$

$|cvcvc| = 3 + 2|v|$ est impair, $|f(w)|$ pair $\Rightarrow$ $|xy|$ impair.

- Montrer que $|v|$ est impair
  - Si $|x|$ pair, alors $cvcv, cy \in X^*$.
    supposons $|v|$ pair, alors $cvc \in X^*$, contradiction.
  - Si $|x|$ impair, alors $vcvc, y \in X^*$.
    supposons $|v|$ pair, alors $cvc \in X^*$, contradiction.

Combinatoire des mots

On peut conclure

1. Si $|x|$ pair.

$$f(w) = \underbrace{x}_{\text{pair}} \underbrace{c \overbrace{v}^{\text{impair}}}_{\text{pair}} \underbrace{cv}_{\text{pair}} cy \in X^*$$

$$x, cv, cy \in X^* \Rightarrow \exists r, s, t : f(r) = x,\ f(s) = cv,\ f(t) = cy$$

$$w = rsst$$

s, t débutent par la même lettre,
donc sst débute par un chevauchement.

2. Si $|x|$ impair.

$$f(w) = \underbrace{xc}_{\text{pair}} \underbrace{\overbrace{v}^{\text{impair}} c}_{\text{pair}} \underbrace{vc}_{\text{pair}} y \in X^*$$

Combinatoire des mots

On peut conclure

1. Si $|x|$ pair.

$$f(w) = \underbrace{x}_{\text{pair}}\ \underbrace{c\ \overbrace{v}^{\text{impair}}}_{\text{pair}}\ \underbrace{cv}_{\text{pair}}\ cy \in X^*$$

$$x, cv, cy \in X^* \Rightarrow \exists r, s, t : f(r) = x,\ f(s) = cv,\ f(t) = cy$$

$$w = rsst$$

s, t débutent par la même lettre,
donc sst débute par un chevauchement.

2. Si $|x|$ impair.

$$f(w) = \underbrace{xc}_{\text{pair}}\ \underbrace{\overbrace{v}^{\text{impair}}\ c}_{\text{pair}}\ \underbrace{vc}_{\text{pair}}\ y \in X^*$$

On peut conclure

1. Si $|x|$ pair.

$$f(w) = \underbrace{x}_{\text{pair}}\ \underbrace{c\ \overbrace{v}^{\text{impair}}}_{\text{pair}}\ \underbrace{cv}_{\text{pair}}\ cy \in X^*$$

$$x, cv, cy \in X^* \Rightarrow \exists r, s, t : f(r) = x,\ f(s) = cv,\ f(t) = cy$$

$$w = rsst$$

s, t débutent par la même lettre,
donc sst débute par un chevauchement.

2. Si $|x|$ impair.

$$f(w) = \underbrace{xc}_{\text{pair}}\ \underbrace{\overbrace{v}^{\text{impair}}\ c}_{\text{pair}}\ \underbrace{vc}_{\text{pair}}\ y \in X^*$$

Combinatoire des mots

On peut conclure

1. Si $|x|$ pair.

$$f(w) = \underbrace{x}_{\text{pair}}\,\underbrace{c\,\overbrace{v}^{\text{impair}}}_{\text{pair}}\,\underbrace{cv}_{\text{pair}}\,cy \in X^*$$

$$x, cv, cy \in X^* \Rightarrow \exists r, s, t : f(r) = x,\ f(s) = cv,\ f(t) = cy$$

$$w = rsst$$

s, t débutent par la même lettre,
donc sst débute par un chevauchement.

2. Si $|x|$ impair.

$$f(w) = \underbrace{xc}_{\text{pair}}\,\underbrace{\overbrace{v}^{\text{impair}}\,c}_{\text{pair}}\,\underbrace{vc}_{\text{pair}}\,y \in X^*$$

Corollaire

Existence d'un mot sur 3 lettres sans carré

$$\{a, ab, abb\} \text{ code}$$

$$abb|ab|a|abb|a|ab|abb|ab|a|ab|abb|a|abb|ab|a|ab \cdots$$

$$321312321231321 \cdots$$

Un carré abélien : `abcbca`

Peut-on construire un mot infini sur 3 lettres sans carré abélien ?

$$0102010$$

$$0102101$$

Un carré abélien : `abcbca`
Peut-on construire un mot infini sur 3 lettres sans carré abélien ?

$$0102010$$

$$0102101$$

V. Keränen (ICALP'1992) fournit un morphisme de longueur 85 répondant à la question !

$$a \mapsto abcacdcbcdcadcdbdabacabadbabcbdbcbacbcdcacbabd$$
$$abacadcbcdcacdbcbacbcdcacdcbdcdadbdcbca;$$

$$b \mapsto bcdbdadcdadbadacabcbdbcbacbcdcacdcbdcdadbdcbca$$
$$bcbdbadcdadbdacdcbdcdadbdadcadabacadcdb;$$

$$c \mapsto cdacabadabacbabdbcdcacdcbdcdadbdadcadabacadcdb$$
$$cdcacbadabacabdadcadabacabadbabcbdbadac;$$

$$d \mapsto dabdbcbabcbdcbcacdadbdadcadabacabadbabcbdbadac$$
$$dadbdcbabcbdbcabadbabcbdbcbacbcdcacbabd;$$

J. Cassaigne, J. D. Currie, L. Schaeffer, J. Shallit, *Avoiding Three Consecutive Blocks of the Same Size and Same Sum*, arXiv:1106.5204

$$\varphi : 0 \mapsto 03,\ 1 \mapsto 43,\ 3 \mapsto 1,\ 4 \mapsto 01$$

$$\varphi^{\omega}(0) = 031430110343430310110110314303434303434 \cdots$$

ne contient aucun cube additif, e.g., 041340.

Le problème de Prouhet (1851) – Tarry – Escott
Mémoire sur quelques relations entre les puissances de nombres

Partitionner $\{0, \dots, 2^n - 1\}$ de telle sorte que

$$\{0, \dots, 2^n - 1\} = \{a_1, \dots, a_{2^{n-1}}\} \cup \{b_1, \dots, b_{2^{n-1}}\}$$

$$\sum_{j=1}^{2^{n-1}} a_j = \sum_{j=1}^{2^{n-1}} b_j, \; \sum_{j=1}^{2^{n-1}} a_j^2 = \sum_{j=1}^{2^{n-1}} b_j^2, \; \dots, \; \sum_{j=1}^{2^{n-1}} a_j^{n-1} = \sum_{j=1}^{2^{n-1}} b_j^{n-1}$$

$$\prod_{i=0}^{\infty} (1 - X^{2^i}) = \sum_{j=0}^{\infty} t_j \, X^j$$

Le problème de Prouhet (1851) – Tarry – Escott
Mémoire sur quelques relations entre les puissances de nombres

Partitionner $\{0, \ldots, 2^n - 1\}$ de telle sorte que

$$\{0, \ldots, 2^n - 1\} = \{a_1, \ldots, a_{2^{n-1}}\} \cup \{b_1, \ldots, b_{2^{n-1}}\}$$

$$\sum_{j=1}^{2^{n-1}} a_j = \sum_{j=1}^{2^{n-1}} b_j, \ \sum_{j=1}^{2^{n-1}} a_j^2 = \sum_{j=1}^{2^{n-1}} b_j^2, \ \ldots, \ \sum_{j=1}^{2^{n-1}} a_j^{n-1} = \sum_{j=1}^{2^{n-1}} b_j^{n-1}$$

$$\prod_{i=0}^{\infty}(1 - X^{2^i}) = \sum_{j=0}^{\infty} t_j \, X^j$$

Théorie des nombres

Exhiber des nombres transcendants (sur $\mathbb{Q}$)

- nombres de Liouville (approximations diophantiennes)

$$\sum_{j=1}^{\infty} \frac{1}{10^{j!}}, \qquad \sum_{k=1}^{\infty} \frac{a_j}{k^{j!}},\ k \geq 2,\, a_j \in [\![0, k-1]\!]$$

- e
- π

Quid des *nombres k-automatiques* ?

$$01101001100101101001011 0 \cdots \leftrightarrow 0,4124540314078330 \cdots$$

$$x_0 x_1 x_2 \cdots \leftrightarrow \sum_{j \geq 0} \frac{x_j}{k^{j+1}}$$

Conjecture Cobham, Hartmanis–Stearns'1965

- mot ultimement périodique $\leftrightarrow$ nombre rationnel
- mot k-automatique non périodique $\rightarrow$ *nombre transcendant* ?

- Si α est un nombre algébrique irrationnel, alors le développement en base k de α ne peut pas être engendré par un automate fini ?
- Existe-t-il un nombre algébrique irrationnel dont les n premiers chiffres puissent être calculés en $\mathcal{O}(n)$ opérations ?

Théorie des nombres

Fonction de complexité $\mathsf{p}_{\mathbf{w}} : \mathbb{N} \to \mathbb{N}, n \mapsto \#\mathsf{Fac}_{\mathbf{w}}(n)$

$$\mathsf{p}_{\mathbf{w}}(m+n) \leq \mathsf{p}_{\mathbf{w}}(m)\mathsf{p}_{\mathbf{w}}(n), \qquad \mathsf{p}_{\mathbf{w}}(n) \leq (\#A)^n$$

$$\mathsf{p}_{\mathbf{w}}(n) \leq \mathsf{p}_{\mathbf{w}}(n+1)$$

Théorème (Morse–Hedlund)

Les conditions suivantes sont équivalentes

- $\mathbf{w}$ est ultimement périodique, $\mathbf{w} = uv^{\omega}$
- il existe N tel que $\mathsf{p}_{\mathbf{w}}(N) \leq N$
- $\mathsf{p}_{\mathbf{w}}$ est borné
- il existe m tel que $\mathsf{p}_{\mathbf{w}}(m) = \mathsf{p}_{\mathbf{w}}(m+1)$

Si $\mathbf{w}$ non périodique, alors $\mathsf{p}_{\mathbf{w}}(n) \geq n+1$ pour tout n.

Complexité des mots automatiques

Si $\mathbf{w}$ est un mot k-automatique, alors $\mathsf{p}_{\mathbf{w}}(n)$ est en $\mathcal{O}(n)$

Preuve (*désubstitution*)

$f^\omega(a) = abbabaabbaababbabaababbaabbabaab\cdots$

$(f^2)^\omega(a) = ab|ba|ba|ab|ba|ab|ab|ba|ba|ab|ab|ba|ab|ba|ba|ab|\cdots$

$(f^3)^\omega(a) = ab\ ba|ba\ ab|ba\ ab|ab\ ba|ba\ ab|ab\ ba|ab\ ba|ba\ ab|\cdots$

$(f^4)^\omega(a) = ab\ ba\ ba\ ab|ba\ ab\ ab\ ba|ba\ ab\ ab\ ba|ab\ ba\ ba\ ab|\cdots$

$$4 < n \leq 8, \quad k^{m-1} < n \leq k^m, \quad (\#A)^2 k^m < (\#A)^2 k\, n$$

Remarque Pansiot (1984)

Soit $\mathbf{w}$ un mot purement morphique (non périodique),
alors $\mathsf{p}_{\mathbf{w}}(n)$ est en $\Theta(n)$, $\Theta(n\log n)$, $\Theta(n\log\log n)$ ou $\Theta(n^2)$.

Complexité des mots automatiques

Si $\mathbf{w}$ est un mot k-automatique, alors $\mathrm{p}_{\mathbf{w}}(n)$ est en $\mathcal{O}(n)$

<u>Preuve</u> (*désubstitution*)

$f^\omega(a) = abbabaabbaababbabaababbaabbabaab\cdots$

$(f^2)^\omega(a) = ab|ba|ba|ab|ba|ab|ab|ba|ba|ab|ab|ba|ab|ba|ba|ab|\cdots$

$(f^3)^\omega(a) = ab\ ba|ba\ ab|ba\ ab|ab\ ba|ba\ ab|ab\ ba|ab\ ba|ba\ ab|\cdots$

$(f^4)^\omega(a) = ab\ ba\ ba\ ab|ba\ ab\ ab\ ba|ba\ ab\ ab\ ba|ab\ ba\ ba\ ab|\cdots$

$$4 < n \leq 8, \quad k^{m-1} < n \leq k^m, \quad (\#A)^2 k^m < (\#A)^2 k\, n$$

Remarque Pansiot (1984)

Soit $\mathbf{w}$ un mot purement morphique (non périodique), alors $\mathrm{p}_{\mathbf{w}}(n)$ est en $\Theta(n)$, $\Theta(n\log n)$, $\Theta(n\log\log n)$ ou $\Theta(n^2)$.

Complexité des mots automatiques

Si $\mathbf{w}$ est un mot k-automatique, alors $\mathsf{p}_{\mathbf{w}}(n)$ est en $\mathcal{O}(n)$

Preuve (*désubstitution*)

$f^{\omega}(a) = abbabaabbaababbabaababbaabbabaab\cdots$

$(f^2)^{\omega}(a) = ab|ba|ba|ab|ba|ab|ab|ba|ba|ab|ab|ba|ab|ba|ba|ab|\cdots$

$(f^3)^{\omega}(a) = ab\ ba|ba\ ab|ba\ ab|ab\ ba|ba\ ab|ab\ ba|ab\ ba|ba\ ab|\cdots$

$(f^4)^{\omega}(a) = ab\ ba\ ba\ ab|ba\ ab\ ab\ ba|ba\ ab\ ab\ ba|ab\ ba\ ba\ ab|\cdots$

$$4 < n \leq 8, \quad k^{m-1} < n \leq k^m, \quad (\#A)^2 k^m < (\#A)^2 k\, n$$

Remarque Pansiot (1984)

Soit $\mathbf{w}$ un mot purement morphique (non périodique), alors $\mathsf{p}_{\mathbf{w}}(n)$ est en $\Theta(n)$, $\Theta(n\log n)$, $\Theta(n\log\log n)$ ou $\Theta(n^2)$.

Complexité des mots automatiques

Si $\mathbf{w}$ est un mot k-automatique, alors $\mathrm{p}_{\mathbf{w}}(n)$ est en $\mathcal{O}(n)$

<u>Preuve</u> (*désubstitution*)

$f^\omega(a) = abbabaabbaababbabaababbaabbabaab\cdots$

$(f^2)^\omega(a) = ab|ba|ba|ab|ba|ab|ab|ba|ba|ab|ab|ba|ab|ba|ba|ab|\cdots$

$(f^3)^\omega(a) = ab\ ba|ba\ ab|ba\ ab|ab\ ba|ba\ ab|ab\ ba|ab\ ba|ba\ ab|\cdots$

$(f^4)^\omega(a) = ab\ ba\ ba\ ab|ba\ ab\ ab\ ba|ba\ ab\ ab\ ba|ab\ ba\ ba\ ab|\cdots$

$$4 < n \leq 8, \quad k^{m-1} < n \leq k^m, \quad (\#A)^2 k^m < (\#A)^2 k\, n$$

Remarque Pansiot (1984)

Soit $\mathbf{w}$ un mot purement morphique (non périodique),
alors $\mathrm{p}_{\mathbf{w}}(n)$ est en $\Theta(n)$, $\Theta(n \log n)$, $\Theta(n \log\log n)$ ou $\Theta(n^2)$.

Complexité des mots automatiques

Si $\mathbf{w}$ est un mot k-automatique, alors $\mathsf{p}_{\mathbf{w}}(n)$ est en $\mathcal{O}(n)$

Preuve (*désubstitution*)

$f^\omega(a) = ab\,b\,a\,baabbaababbabaababbaabbabaab\cdots$

$(f^2)^\omega(a) = ab|ba|ba|ab|ba|ab|ab|ba|ba|ab|ab|ba|ab|ba|ba|ab|\cdots$

$(f^3)^\omega(a) = ab\ ba|ba\ ab|ba\ ab|ab\ ba|ba\ ab|ab\ ba|ab\ ba|ba\ ab|\cdots$

$(f^4)^\omega(a) = ab\ ba\ ba\ ab|ba\ ab\ ab\ ba|ba\ ab\ ab\ ba|ab\ ba\ ba\ ab|\cdots$

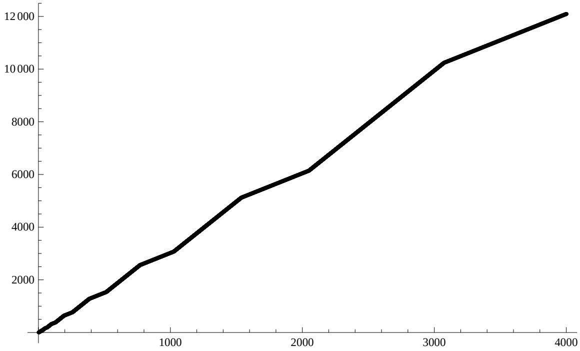
$$4 < n \le 8, \quad k^{m-1} < n \le k^m, \quad (\#A)^2 k^m < (\#A)^2 k\, n$$

Remarque Pansiot (1984)

Soit $\mathbf{w}$ un mot purement morphique (non périodique),
alors $\mathsf{p}_{\mathbf{w}}(n)$ est en $\Theta(n)$, $\Theta(n \log n)$, $\Theta(n \log\log n)$ ou $\Theta(n^2)$.

Complexité du mot de Thue–Morse
(de Luca, Varricchio ; Cassaigne ; Brlek)

$$\mathsf{p}_{\mathbf{t}}(n) = \begin{cases} 4n - 2\cdot 2^m - 4, & \text{if } 2\cdot 2^m < n \leq 3\cdot 2^m; \\ 2n + 4\cdot 2^m - 2, & \text{if } 3\cdot 2^m < n \leq 4\cdot 2^m. \end{cases}$$



THÉORÈME BUGEAUD–ADAMCZEWSKI 2007

Si $\mathbf{w}$ est le développement en base k d'un nombre algébrique irrationnel, alors

$$\lim_{n\to+\infty} \frac{\mathsf{p}_{\mathbf{w}}(n)}{n} = +\infty$$

COROLLAIRE

Les nombres automatiques non périodiques sont transcendants.

Théorie des nombres

Soient $\mathbb{K}$ un corps, $a(n) \in \mathbb{K}^{\mathbb{N}}$ et $k_1, \ldots, k_d \in \mathbb{K}$. La suite $a(n)$ satisfait une *relation de récurrence linéaire* sur $\mathbb{K}$ si

$$a(n) = k_1 a(n-1) + \cdots + k_d\, a(n-d), \quad \forall n >>$$

Skolem–Mahler–Lech

Soit $a(n)$ une suite linéaire récurrente sur un corps de caractéristique 0. Alors, l'ensemble

$$\mathcal{Z}(a) = \{n \in \mathbb{N} \mid a(n) = 0\} \text{ est ultimement périodique.}$$

Remarque

Si $\mathbb{K}$ est un corps fini, $a(n)$ (et donc $\mathcal{Z}(a)$) est trivialement ultimement périodique.

T. Tao, Effective Skolem–Mahler–Lech theorem in Structure and Randomness, **AMS**'08.

Si $\mathbb{K}$ est un corps infini de caractéristique $p > 0$...

Exemple 1 (Lech)

$$a(n) := (1+t)^n - t^n - 1 \in \mathbb{F}_p(t).$$

La suite a satisfait la relation linéaire sur $\mathbb{F}_p(t)$, pour $n > 3$

$$a(n) = (2+2t)\, a(n-1) + (1+3t+t^2)\, a(n-2) - (t+t^2)\, a(n-3).$$

On a

$$a(p^j) = (1+t)^{p^j} - t^{p^j} - 1 = 0$$

alors que $a(n) \neq 0$ si n n'est pas une puissance de p. Dès lors, on obtient

$$\mathcal{Z}(a) = \{1, p, p^2, p^3, \ldots\}.$$

Exemple 2 (Derksen)

Soit la suite $a(n)$ de $\mathbb{F}_p(x, y, z)$ définie par

$$a(n) := (x+y+z)^n - (x+y)^n - (x+z)^n - (y+z)^n + x^n + y^n + z^n.$$

On peut montrer que :

- La suite $a(n)$ satisfait une relation de récurrence linéaire.
- L'ensemble des zéros est donné par

$$\mathcal{Z}(a) = \{p^n \mid n \in \mathbb{N}\} \cup \{p^n + p^m \mid n, m \in \mathbb{N}\}.$$

$\mathcal{Z}(a)$ peut sembler *plus pathologique* qu'en caractéristique nulle. Cependant, on peut penser aux mots p-automatiques !

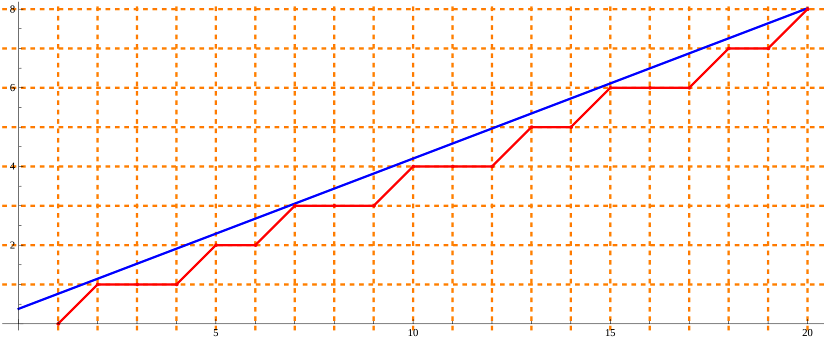
Théorème (H. Derksen'2007)

Soit $a(n)$ une suite linéaire récurrente sur un corps de caractéristique p. Alors la suite caractéristique de l'ensemble $\mathcal{Z}(a)$ est un mot p-automatique.

Derksen décrit précisément la forme des automates possibles :
Tout mot p-automatique n'est pas un ensemble $\mathcal{Z}(a)$ pour une suite linéaire récurrente sur un corps de caractéristique p.

Géométrie discrète

Discrétisation de droites (pente irrationnelle)



$abaababaabaababaababaabaababaabaababaababaabaabab \cdots$

$\rightsquigarrow$ Tester si une suite de “pixels” décrit un segment de droite ?

$\mathbb{Q}/\mathbb{Z}$ est l'ensemble des points d'ordre fini dans $\mathbb{R}/\mathbb{Z}$

$$\alpha \text{ rationnel} \Leftrightarrow \exists m, n \in \mathbb{Z},\ m \neq n,\ \{m\alpha\} = \{n\alpha\}.$$

Si $\alpha = p/q$, $\left\{\frac{(q+1)p}{q}\right\} = \{p/q\}$

Supposons qu'il existe $m < n$ tels que $\{m\alpha\} = \{n\alpha\}$.

Alors $(n-m)\alpha$ est un entier r et $\alpha = r/(n-m) \in \mathbb{Q}$

$\mathbb{Q}/\mathbb{Z}$ est l'ensemble des points d'ordre fini dans $\mathbb{R}/\mathbb{Z}$

$$\alpha \text{ rationnel} \Leftrightarrow \exists m, n \in \mathbb{Z},\ m \neq n,\ \{m\alpha\} = \{n\alpha\}.$$

Si $\alpha = p/q$, $\left\{\frac{(q+1)p}{q}\right\} = \{p/q\}$

Supposons qu'il existe $m < n$ tels que $\{m\alpha\} = \{n\alpha\}$.

Alors $(n-m)\alpha$ est un entier r et $\alpha = r/(n-m) \in \mathbb{Q}$

Géométrie discrète

Exercice (thm. de Kronecker)

Si α est irrationnel, alors
l'ensemble des $\{n\alpha\}$, $n \in \mathbb{N}$, est dense dans $[0, 1]$.

Soit N. On partitionne $[0, 1]$ en intervalles de longueur $1/N$.

"Pigeonhole principle" : deux éléments $\{\alpha\}, \{2\alpha\}, \ldots, \{(N+1)\alpha\}$ appartiennent au même intervalle.

Si $i < j \leq N+1$ tels que $k/N < \{i\alpha\} < \{j\alpha\} < (k+1)/N$,

$$\{(j-i)\alpha\} < 1/N \text{ et on considère les } \{n(j-i)\alpha\}$$

Si $i < j \leq N+1$ tels que $k/N < \{j\alpha\} < \{i\alpha\} < (k+1)/N$,

$$1 - 1/N < \{(j-i)\alpha\} < 1$$

Exercice (thm. de Kronecker)

Si α est irrationnel, alors
l'ensemble des $\{n\alpha\}$, $n \in \mathbb{N}$, est dense dans $[0,1]$.

Soit N. On partitionne $[0,1]$ en intervalles de longueur $1/N$.

"Pigeonhole principle" : deux éléments $\{\alpha\}, \{2\alpha\}, \ldots, \{(N+1)\alpha\}$ appartiennent au même intervalle.

Si $i < j \leq N+1$ tels que $k/N < \{i\alpha\} < \{j\alpha\} < (k+1)/N$,

$$\{(j-i)\alpha\} < 1/N \text{ et on considère les } \{n(j-i)\alpha\}$$

Si $i < j \leq N+1$ tels que $k/N < \{j\alpha\} < \{i\alpha\} < (k+1)/N$,

$$1 - 1/N < \{(j-i)\alpha\} < 1$$

Géométrie discrète

Exercice (thm. de Kronecker)

Si α est irrationnel, alors
l'ensemble des $\{n\alpha\}$, $n \in \mathbb{N}$, est dense dans $[0, 1]$.

Soit N. On partitionne $[0, 1]$ en intervalles de longueur $1/N$.

"Pigeonhole principle" : deux éléments $\{\alpha\}, \{2\alpha\}, \ldots, \{(N+1)\alpha\}$ appartiennent au même intervalle.

Si $i < j \leq N + 1$ tels que $k/N < \{i\alpha\} < \{j\alpha\} < (k+1)/N$,

$$\{(j-i)\alpha\} < 1/N \text{ et on considère les } \{n(j-i)\alpha\}$$

Si $i < j \leq N + 1$ tels que $k/N < \{j\alpha\} < \{i\alpha\} < (k+1)/N$,

$$1 - 1/N < \{(j-i)\alpha\} < 1$$

Exercice (thm. de Kronecker)

Si α est irrationnel, alors
l'ensemble des $\{n\alpha\}$, $n \in \mathbb{N}$, est dense dans $[0,1]$.

Soit N. On partitionne $[0,1]$ en intervalles de longueur $1/N$.

"Pigeonhole principle" : deux éléments $\{\alpha\}, \{2\alpha\}, \dots, \{(N+1)\alpha\}$ appartiennent au même intervalle.

Si $i < j \leq N+1$ tels que $k/N < \{i\alpha\} < \{j\alpha\} < (k+1)/N$,

$$\{(j-i)\alpha\} < 1/N \text{ et on considère les } \{n(j-i)\alpha\}$$

Si $i < j \leq N+1$ tels que $k/N < \{j\alpha\} < \{i\alpha\} < (k+1)/N$,

$$1 - 1/N < \{(j-i)\alpha\} < 1$$

On a même un résultat plus fort de "distribution uniforme"

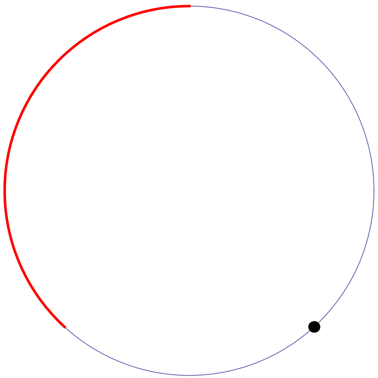
Théorème (Weyl 1916)

Soient $0 < a < b < 1$. Si α est irrationnel, alors

$$\lim_{n \to +\infty} \frac{\#\{k < n \mid a < \{k\alpha\} < b\}}{n} = b - a \,.$$

Réalisation de systèmes dynamiques discrets

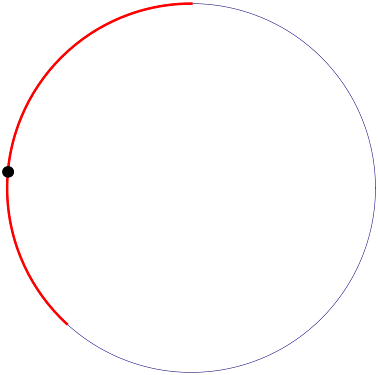
$\mathbb{T} = \mathbb{R}/\mathbb{Z}$, $R : \mathbb{T} \to \mathbb{T}$, $x \mapsto x + \alpha \pmod 1$



$I_a = [0, 1 - \alpha[$, $I_b = [1 - \alpha, 1[$, a

Réalisation de systèmes dynamiques discrets

$\mathbb{T} = \mathbb{R}/\mathbb{Z}$, $R : \mathbb{T} \to \mathbb{T}$, $x \mapsto x + \alpha \pmod 1$

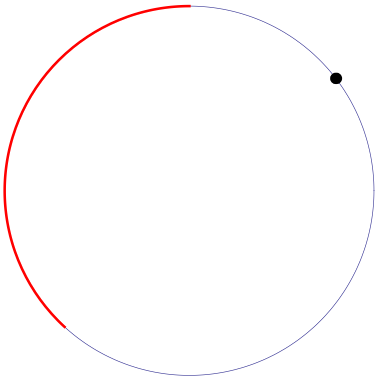


$I_a = [0, 1-\alpha[$, $I_b = [1-\alpha, 1[$, ab

Géométrie discrète

Réalisation de systèmes dynamiques discrets

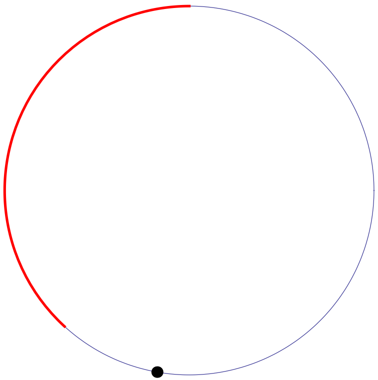
$\mathbb{T} = \mathbb{R}/\mathbb{Z},\ R : \mathbb{T} \to \mathbb{T},\ x \mapsto x + \alpha \pmod 1$



$I_a = [0, 1 - \alpha[,\ I_b = [1 - \alpha, 1[,\ aba$

Réalisation de systèmes dynamiques discrets

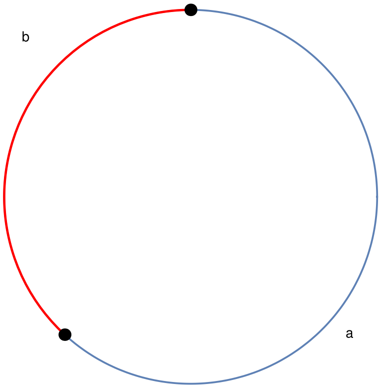
$\mathbb{T} = \mathbb{R}/\mathbb{Z},\ R : \mathbb{T} \to \mathbb{T},\ x \mapsto x + \alpha \pmod 1$



$I_a = [0, 1-\alpha[,\ I_b = [1-\alpha, 1[,\ abaa$

Géométrie discrète

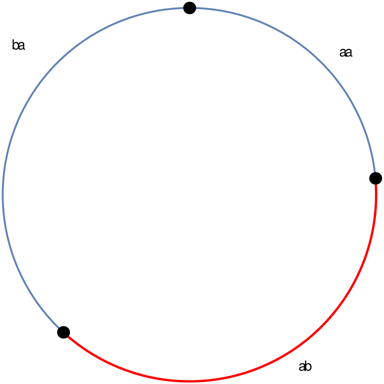
I_b



$I_a, \ I_b$

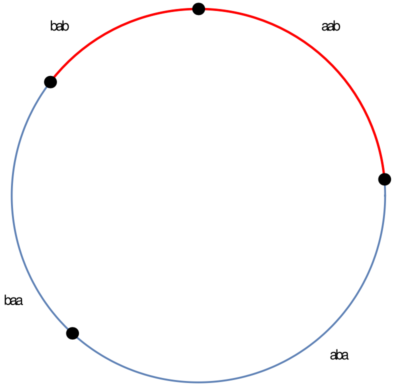
Géométrie discrète

$R^{-1}(I_b)$



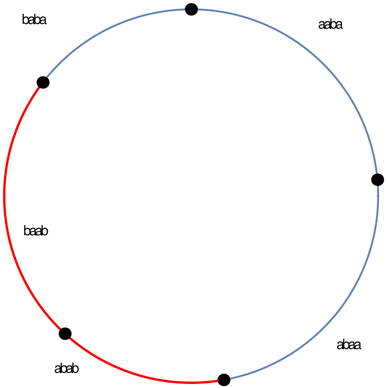
$$I_a \cap R^{-1}(I_a),\ I_a \cap R^{-1}(I_b),\ I_b \cap R^{-1}(I_a)$$

$R^{-2}(I_b)$



$I_a \cap R^{-1}(I_a) \cap R^{-2}(I_b),\ I_a \cap R^{-1}(I_b) \cap R^{-2}(I_a),$
$I_b \cap R^{-1}(I_a) \cap R^{-2}(I_a),\ I_b \cap R^{-1}(I_a) \cap R^{-2}(I_b)$

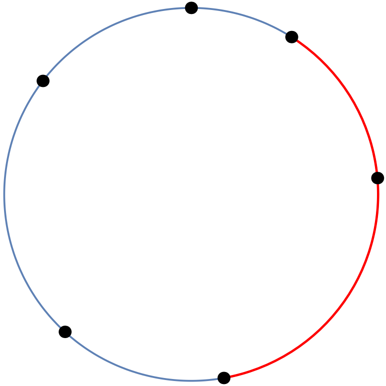
$R^{-3}(I_b)$



$I_{aab} \cap R^{-3}(I_a),\ I_{aba} \cap R^{-3}(I_a),\ I_{aba} \cap R^{-3}(I_b)$
$I_{baa} \cap R^{-3}(I_b),\ I_{bab} \cap R^{-3}(I_a)$

Géométrie discrète

$R^{-4}(I_b)$



I_{aabaa}, I_{aabab}, I_{abaab},
I_{ababa}, I_{baaba}, I_{babaa}

Les *mots sturmiens* sont caractérisés de diverses façons

- sont de complexité $\mathsf{p}(n) = n + 1$ (minimale)
- mots mécaniques de pente irrationnelle
- codage de rotations
- mots apériodiques et *équilibrés*,

$$\forall u, v \in \mathsf{Fac}_n, \quad -1 \leq |u|_a - |v|_a \leq 1.$$

cf. aussi les suites de Beatty

$$\lfloor (n+1)\varphi \rfloor - \lfloor n\varphi \rfloor$$

Complexité du mot de G. Rote (JNT 1994)

$$x_n = \begin{cases} a & \text{si } \{n\alpha\} < 1/2 \\ b & \text{sinon} \end{cases}$$

Si $\alpha = (1+\sqrt{5})/2$,

$$\mathbf{x}_\varphi = ababaababbabaababbaba\cdots$$

n'est pas sturmien, $\mathrm{p}(2) = 4$.

- J.-P. Allouche, M. Mendès France, Euler, Pisot, Prouhet-Thue-Morse, Wallis and the duplication of sines, *Monatsh. Math.* **155** (2008), 301-315.
- M. Lothaire, *Combinatorics on Words*, Cambridge University Press, 1983.
  ouvrage collectif jetant les bases de la combinatoire des mots
- F. Gouvêa, *p-adic Numbers - An Introduction*, Universitext, Springer
- M. Rigo, *Formal Languages, Automata and Numeration Systems*, vol. 1, ISTE-Wiley, 2014.
  se veut cours d'introduction à la combinatoire des mots
- M. Rigo, *Théorie des automates et langages formels*, notes de cours ULg, `http://www.discmath.ulg.ac.be/`
- A. Cobham, Uniform tag sequences, *Math. Systems Theory* 6 (1972), 164–192.
  article fondateur sur les suites automatiques

- J.-P. Allouche, J. Shallit, *Automatic Sequences : Theory, Applications, Generalizations*, Cambridge University Press, (2003).
  la bible des suites automatiques
- V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Logic and p-recognizable sets of integers, *Bull. Belg. Math. Soc.* 1 (1994), 191–238.
  très beau survol !
- J. Berstel, D. Perrin, The origins of combinatorics on words, *European J. Combin.* 28 (2007), 996–1022.
- J.-P. Allouche, J. Shallit, The ubiquitous Prouhet-Thue-Morse sequence, Sequences and their applications (Singapore, 1998), 1–16, Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London, 1999.
- M. Rigo, Le problème de Prouhet, *Losanges* 19 (2012), 42–53.
  article de vulgarisation autour du problème de Prouhet

- V. Berthé, M. Rigo (Eds), *Combinatorics, Automata and Number Theory*, vol. 135 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2010.
  ouvrage collectif : fonction de complexité, transcendance Bugeaud-Adamczewski,. . .
- H. Derksen, A Skolem-Mahler-Lech theorem in positive characteristic and finite automata, *Invent. Math.* 168 (2007), 175–224.
- G. Hansel, A simple proof of the Skolem-Mahler-Lech theorem, *Theoret. Comput. Sci.* 43 (1986), 91–98.
- M. Lothaire, *Algebraic Combinatorics on Words*, vol. 90 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2002.
  ouvrage collectif, chapitre sur les mots sturmiens
- V. Berthé, Discrete Geometry and Symbolic Dynamics, *The Kiselmanfest : An International Symposium in Complex Analysis and Digital Geometry* (2006).