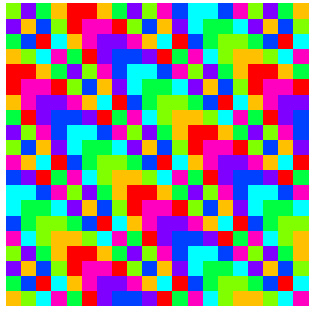
ENSEMBLES RECONNAISSABLES DE POLYNÔMES SUR UN CORPS FINI

Michel Rigo

Département de Mathématique, Université de Liège
http://www.discmath.ulg.ac.be/



COMMENÇONS AVEC LES ENTIERS...

NUMÉRATION EN BASE ENTIÈRE $k \geq 2$

$$n = \sum_{i=0}^{\ell} c_i\, k^i, \quad \text{avec} \quad c_i \in \Sigma_k = \{0, \ldots, k-1\},\ c_\ell \neq 0$$

tout entier n correspond à un mot $\mathrm{rep}_k(n) = c_\ell \cdots c_0$ sur Σ_k.

ensemble X d'entiers $\longleftrightarrow$ ensemble $\mathrm{rep}_k(X)$ de mots, langage

QUESTION NATURELLE

Explorer les liens entre

- propriétés arithmétiques des nombres

et

- propriétés syntaxiques de leurs représentations

Connexion avec la théorie des langages formels

La hiérarchie de Chomsky :

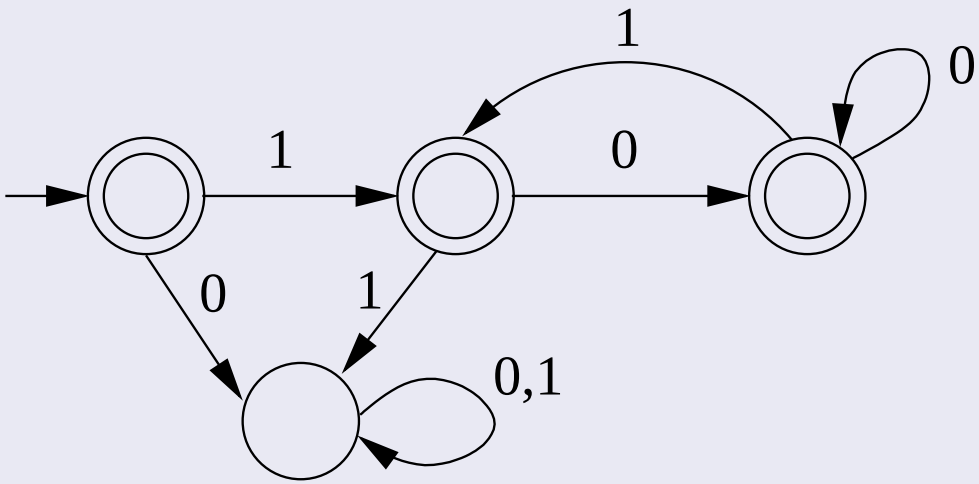
- Langages Récursivement énumérables (M. de Turing)
- Langages “Context-sensitive” (M.T. bornées linéairement)
- Langages algébriques (automates à pile)
- Langages réguliers (ou rationnels) (automates finis)

AUTOMATE FINI DÉTERMINISTE

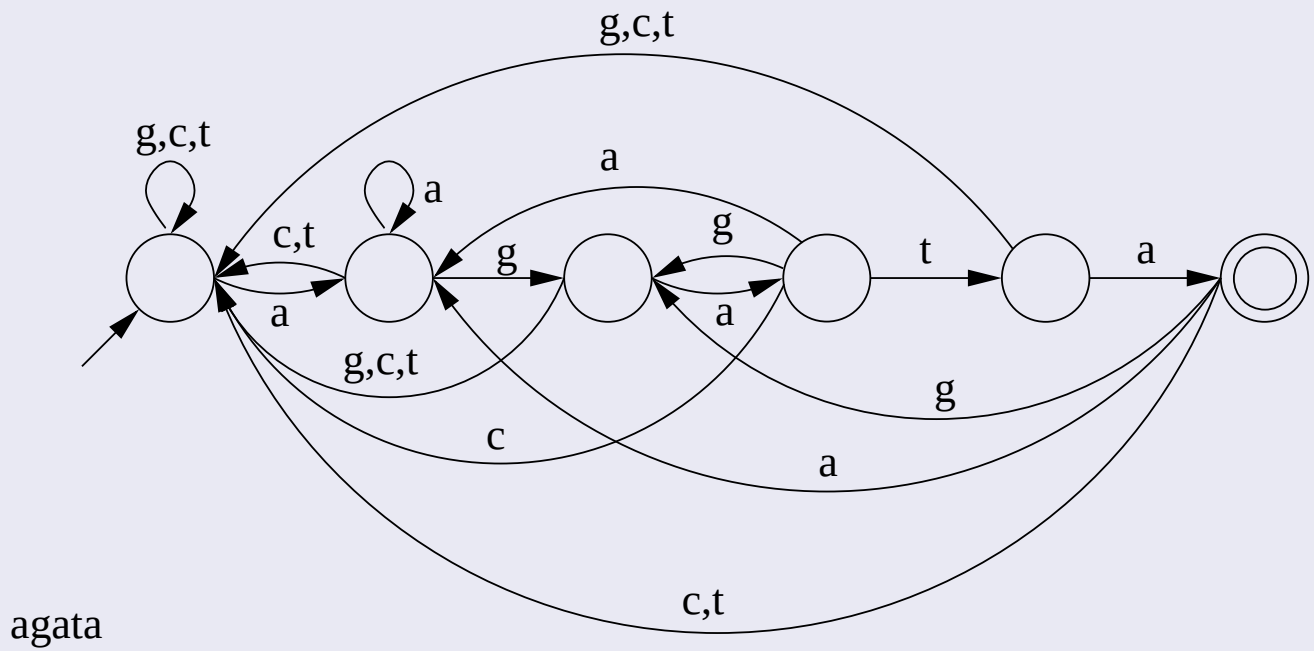
$\mathcal{A} = (Q, q_0, \Sigma, \delta, F)$

- Q ensemble fini d'états, $q_0 \in Q$ état initial
- $\delta : Q \times \Sigma \to Q$ fonction de transition
- $F \subseteq Q$ ensemble d'états finals (ou accepteurs)

EXEMPLE (FIBONACCI)



Exemple (Bioinformatique, ADN : a, c, g, t)



Exemple Informatique

Solution algorithmique pour le “model checking”
Vérification “automatique” de programmes, . . .

Retour aux ensembles d'entiers

Que recherche-t-on ?

Les ensembles X d'entiers "les plus simples" sont tels que

$$\mathrm{rep}_k(X) \text{ est régulier,}$$

i.e., les représentations en base k sont acceptées par un automate fini.

De tels ensembles sont dits k-reconnaissables.

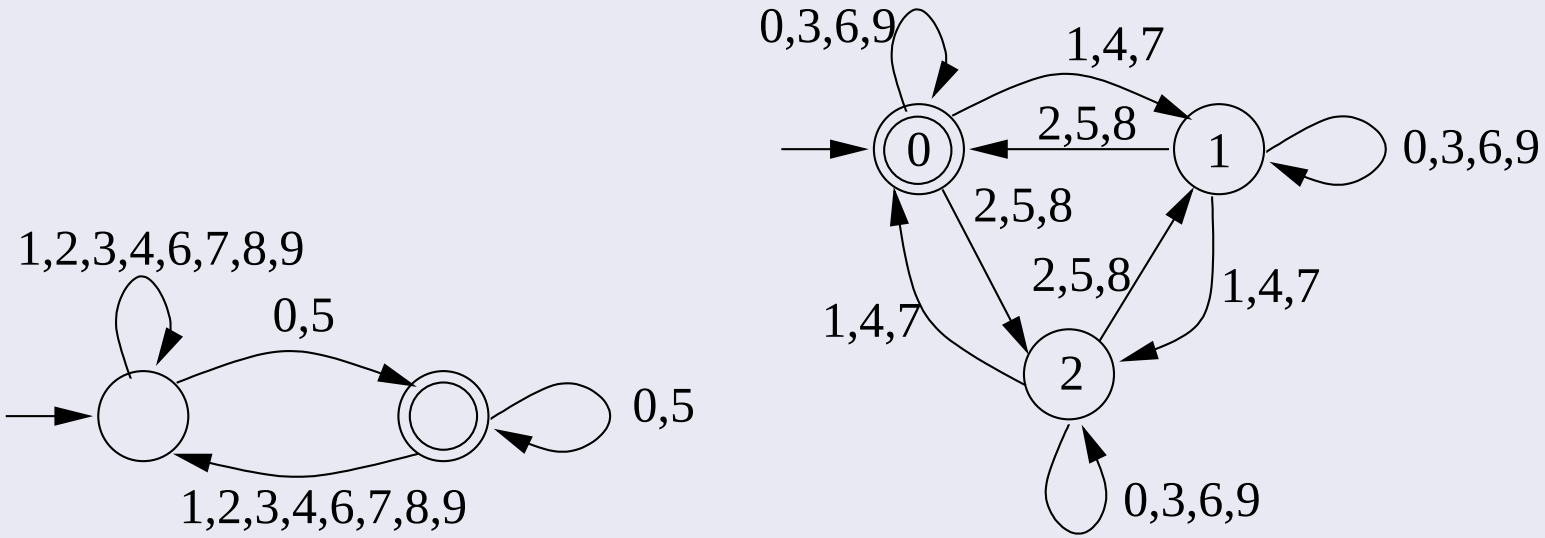
Critère de divisibilité en base k

Soient $k \geq 2$ et $0 \leq r < s$. L'ensemble

$$X = \{n \mid n \equiv r \pmod{s}\}$$

est k-reconnaissable. $t \xrightarrow{a} t.k + a \pmod{s}$

Exemple



UNE QUESTION "NATURELLE"

Si $X \subseteq \mathbb{N}$ est p-reconnaissable, est-il aussi q-reconnaissable ?

p, q sont *multiplicativement indépendants* si
$p^k = q^\ell \Rightarrow k = \ell = 0$, i.e., si $\log p / \log q$ est irrationnel.

"être multiplicativement dépendant" est une relation d'équivalence,

2	3	5	6	7	10	11	$\cdots$
4	9	25	36	49	100	121	$\cdots$
8	27	125	216	343	1000	1331	$\cdots$

PROPOSITION

Si $p, q \geq 2$ sont multiplicativement dépendants,
alors $X \subset \mathbb{N}$ est p-reconnaissable SSI il est q-reconnaissable.

UNE QUESTION "NATURELLE"

Si $X \subseteq \mathbb{N}$ est p-reconnaissable, est-il aussi q-reconnaissable ?

p, q sont *multiplicativement indépendants* si
$p^k = q^\ell \Rightarrow k = \ell = 0$, i.e., si $\log p / \log q$ est irrationnel.

"être multiplicativement dépendant" est une relation d'équivalence,

2	3	5	6	7	10	11	$\cdots$
4	9	25	36	49	100	121	$\cdots$
8	27	125	216	343	1000	1331	$\cdots$

PROPOSITION

Si $p, q \geq 2$ sont multiplicativement dépendants,
alors $X \subset \mathbb{N}$ est p-reconnaissable SSI il est q-reconnaissable.

UNE QUESTION "NATURELLE"

Si $X \subseteq \mathbb{N}$ est p-reconnaissable, est-il aussi q-reconnaissable ?

p, q sont *multiplicativement indépendants* si
$p^k = q^\ell \Rightarrow k = \ell = 0$, i.e., si $\log p / \log q$ est irrationnel.

"être multiplicativement dépendant" est une relation d'équivalence,

2	3	5	6	7	10	11	$\cdots$
4	9	25	36	49	100	121	$\cdots$
8	27	125	216	343	1000	1331	$\cdots$

PROPOSITION

Si $p, q \geq 2$ sont multiplicativement dépendants,
alors $X \subset \mathbb{N}$ est p-reconnaissable SSI il est q-reconnaissable.

UNE QUESTION "NATURELLE"

Si $X \subseteq \mathbb{N}$ est p-reconnaissable, est-il aussi q-reconnaissable ?

p, q sont *multiplicativement indépendants* si
$p^k = q^\ell \Rightarrow k = \ell = 0$, i.e., si $\log p / \log q$ est irrationnel.

"être multiplicativement dépendant" est une relation d'équivalence,

2	3	5	6	7	10	11	$\cdots$
4	9	25	36	49	100	121	$\cdots$
8	27	125	216	343	1000	1331	$\cdots$

PROPOSITION

Si $p, q \geq 2$ sont multiplicativement dépendants,
alors $X \subset \mathbb{N}$ est p-reconnaissable SSI il est q-reconnaissable.

Théorème [Cobham '69]

Soient $p, q \geq 2$ deux entiers multiplicativement indépendants.
Si $X \subseteq \mathbb{N}$ est simultanément p- et q-reconnaissable,
alors X est ultimement périodique (union finie de P.A.).

Corollaire

Il existe des ensembles

- k-reconnaissables pour tout k
  (ens. ultimement périodiques),
- k-reconnaissables pour un certain k (minimal) et
  exactement tous les k^m,
- k-reconnaissables pour aucun k.

Théorème [Cobham '69]

Soient $p, q \geq 2$ deux entiers multiplicativement indépendants.
Si $X \subseteq \mathbb{N}$ est simultanément p- et q-reconnaissable,
alors X est ultimement périodique (union finie de P.A.).

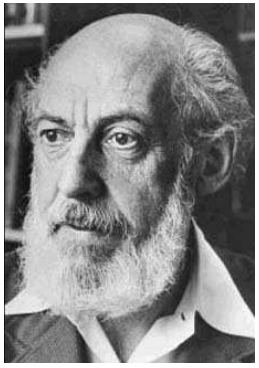
Corollaire

Il existe des ensembles

- k-reconnaissables pour tout k
  (ens. ultimement périodiques),
- k-reconnaissables pour un certain k (minimal) et
  exactement tous les k^m,
- k-reconnaissables pour aucun k.

Exemple

- L'ensemble des nombres pairs est k-reconnaissable pour tout k.
- L'ensemble $\{2^n \mid n \geq 0\}$ est 2-reconnaissable mais pas 3-reconnaissable.
- L'ensemble des nombres premiers n'est jamais k-reconnaissable.



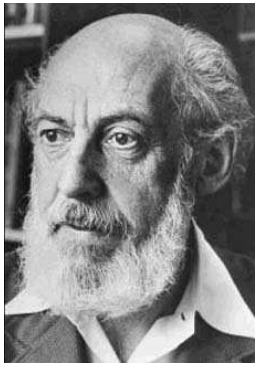
S. Eilenberg'74 (p.118)

"*The proof is correct, long and hard. It is a challenge to find a more reasonable proof of this fine theorem*"

$$\{p^m/q^n \mid m,n \geq 0\} \text{ est dense dans } [0,+\infty)$$

NOMBREUX TRAVAUX, SIMPLIFICATIONS, GÉNÉRALISATIONS (SYSTÈMES NON STANDARDS, CAS MULTI-DIMENSIONNEL,...)

G. Hansel'82, D. Perrin'90, F. Durand'05, V. Bruyère'97, F. Point, C. Michaux'96, R. Villemaire, A. Bès'00, J. Bell'05, J. Honkala, S. Fabre, C. Reutenauer, A.L. Semenov'77, L. Waxweiler'06, M.R.'06...



S. Eilenberg'74 (p.118)

"*The proof is correct, long and hard. It is a challenge to find a more reasonable proof of this fine theorem*"

$$\{p^m/q^n \mid m,n \geq 0\} \text{ est dense dans } [0,+\infty)$$

NOMBREUX TRAVAUX, SIMPLIFICATIONS, GÉNÉRALISATIONS (SYSTÈMES NON STANDARDS, CAS MULTI-DIMENSIONNEL,...)

G. Hansel'82, D. Perrin'90, F. Durand'05, V. Bruyère'97, F. Point, C. Michaux'96, R. Villemaire, A. Bès'00, J. Bell'05, J. Honkala, S. Fabre, C. Reutenauer, A.L. Semenov'77, L. Waxweiler'06, M.R.'06...

Anneau des polynômes

Analogie classique

$q = p^t$, $\mathbb{F}_q := \mathbb{F}$

- $\mathbb{N}, \mathbb{Z} \longleftrightarrow \mathbb{F}_q[X]$ anneau des polynômes sur $\mathbb{F}_q$
- $\mathbb{Q} \longleftrightarrow \mathbb{F}_q(X)$ corps des fractions rationnelles
- $\mathbb{R} \longleftrightarrow \mathbb{F}_q((X))$ corps des séries de Laurent

Décomposition d'un polynôme

base B : polynôme de degré $b > 0$ et

$$P = \sum_{i=0}^{\ell} C_i B^{\ell-i}, \; C_0 \neq 0$$

avec $\deg C_i < b$ pour tout $i \leq \ell$.

Remarque

On peut voir les C_i comme des éléments de $\mathbb{F}^b$.

Exemple

Soient $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$ et les polynômes $B = X^2 + 2X + 2$ et $P = X^8 + 2X^7 + X^5 + 2X^4 + 2X^3 + X + 2$ sur $\mathbb{F}$.
Par divisions euclidiennes successives,

$$P = 1.B^4 + 1.B^3 + (2X + 2).B^2 + (2X + 1).B + 1$$

La B-représentation de P est le mot sur $(\mathbb{Z}/3\mathbb{Z})^2$,

$$\rho_B(P) = \underbrace{(0,1)}_{\in \mathbb{F}^2}(0,1)(2,2)\overbrace{(2,1)}^{\Phi(2X+1)}(0,1).$$

$$\pi_B : (\mathbb{F}^b)^* \to \mathbb{F}[X]$$

Définition

L'ensemble $\mathcal{T} \subseteq \mathbb{F}[X]$ est *B-reconnaissable*, si le langage

$$\rho_B(\mathcal{T}) = \{\rho_B(P) \mid P \in \mathcal{T}\} \subseteq (\mathbb{F}^b)^*$$

est régulier (i.e., accepté par automate fini).

Remarque

$\mathcal{T} \subset \mathbb{F}[X]$ est B-reconnaissable ssi $\mathbf{0}^* \rho_B(\mathcal{T})$ l'est.

$\mathbf{0} = (\underbrace{0, \ldots, 0}_{b})$

Opérations élémentaires

Proposition

Soit B un polynôme de degré $b > 0$ sur $\mathbb{F}$.

Si $\mathcal{S}, \mathcal{T}$ sont des ensembles B-reconnaissables de $\mathbb{F}[X]$, alors $\mathcal{S} + \mathcal{T}$ est aussi B-reconnaissable.

Corollaire (translation)

Soit B un polynôme de degré $b > 0$ sur $\mathbb{F}$.

Si $\mathcal{S} \subseteq \mathbb{F}[X]$ est B-reconnaissable,
alors $\mathcal{S} + \{P\}$ l'est aussi, pour tout $P \in \mathbb{F}[X]$.

Construire un automate à un seul état lisant des triplets de lettres dans $\mathbb{F}^b$ et reconnaissant L

$$\left\{ \begin{pmatrix} u \\ v \\ w \end{pmatrix} : u, v, w \in (\mathbb{F}^b)^*, |u| = |v| = |w|, \pi_B(u) + \pi_B(v) = \pi_B(w) \right\}.$$

Les boucles ont pour label

$$\begin{pmatrix} (& f_0 & , & \cdots & , & f_{b-1} &) \\ (& g_0 & , & \cdots & , & g_{b-1} &) \\ (& f_0 + g_0 & , & \cdots & , & f_{b-1} + g_{b-1} &) \end{pmatrix}$$

avec $f_i, g_i \in \mathbb{F}$ et l'addition $f_i + g_i$ est considérée dans $\mathbb{F}$

REMARQUE

Contrairement à $\mathbb{N}$, pas de report dans $\mathbb{F}[X]$.

morphismes canoniques $p_j : (\mathbb{F}^b)^3 \to \mathbb{F}^b$, $j = 1, 2, 3$, définis par

$$p_j \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_j .$$

$p_1^{-1}[\mathbf{0}^* \rho_B(\mathcal{S})]$ et $p_2^{-1}[\mathbf{0}^* \rho_B(\mathcal{T})]$ sont réguliers et

$$p_3 \left(p_1^{-1}[\mathbf{0}^* \rho_B(\mathcal{S})] \cap p_2^{-1}[\mathbf{0}^* \rho_B(\mathcal{T})] \cap L \right)$$

est un langage régulier.

Proposition (multiplication par polynôme fixé)

Soient B, Q deux polynômes, avec $\deg(B) \geq 1$.

Si $\mathcal{T} \subseteq \mathbb{F}[X]$ est B-reconnaissable, alors $Q.\mathcal{T}$ l'est aussi.

cas 1 : $\deg(Q)=0$. $P = \sum_{i=0}^{k} C_i B^{k-i}$ et $\gamma.P = \sum_{i=0}^{k} (\gamma.C_i) B^{k-i}$
La multiplication par γ induit une permutation
$\nu : \Phi(C_i) \mapsto \Phi(\gamma.C_i)$ sur $\mathbb{F}^b$

cas 2 : $\deg(Q) = n > 0$.
$P = C_0 B^k + \cdots + C_k$ avec $C_0 \neq 0$ et $\deg(C_i) < b$.

$$P.Q = \sum_{i=0}^{k} (C_i.Q) B^{k-i} \text{ avec } \deg(C_i.Q) \leq n + b - 1.$$

$n + b - 1 = \beta b + r$ avec $\beta \in \mathbb{N} \setminus \{0\}$ et $0 \leq r < b$.

Pour chaque $C_i \in \mathbb{F}[X]_{<b}$,

$$C_i.Q = D_{i,0}B^\beta + \cdots + D_{i,\beta} \text{ avec } \deg(D_{i,j}) < b$$

Les polynômes $D_{i,j}$ sont déterminés par C_i, Q et B.
Construire un automate $\mathcal{A}$ acceptant le miroir du langage

$$L := \left\{ \begin{pmatrix} u \\ v \end{pmatrix} : u, v \in (\mathbb{F}^b)^*, |u| = |v|, Q.\pi_B(u) = \pi_B(v) \right\}.$$

- ensemble des états de $\mathcal{A}$: $(\mathbb{F}^b)^\beta$,
- état initial = état final : $(0, \ldots, 0)$

Pour chaque C_i (il y en a q^b),
on a un arc de $(r_{\beta-1}, \ldots, r_0)$ ayant pour label

$$\begin{pmatrix} \Phi(C_i) \\ r_{\beta-1} + \Phi(D_{i,\beta}) \end{pmatrix}$$

vers

$$(r_{\beta-2} + \Phi(D_{i,\beta-1}), \ldots, r_0 + \Phi(D_{i,1}), \Phi(D_{i,0})),$$

additions interprétées dans le $\mathbb{F}$-vectoriel $\mathbb{F}^b$.

$$P.Q = \sum_{i=0}^{k} \sum_{j=0}^{\beta} D_{i,j} B^{\beta+k-i-j}.$$

On conclut comme dans la proposition précédente (morphismes de projection).

Corollaire

Soient Q, R des polynômes de $\mathbb{F}[X]$. L'ensemble

$$\{Q.P + R \mid P \in \mathbb{F}[X]\}$$

est B-reconnaissable pour tout B de degré ≥ 1.

Rappel (critères de divisibilité)

Les ensembles

$$\{n \mid n \equiv r \pmod{s}\}$$

et

$$\{s.n + r \mid n \in \mathbb{N}\}$$

sont k-reconnaissables pour toute base $k \geq 2$.

AUTOMATICITÉ

DÉFINITION

Soit S un ensemble fini. Une application $f : \mathbb{F}[X] \to S$ est B-reconnaissable ou B-automatique si pour tout $s \in S$, $f^{-1}\{s\}$ est un ensemble B-reconnaissable de $\mathbb{F}[X]$.

Soit $S = \{s_1, \ldots, s_k\}$.
Pour tout $s_i \in S$, $i = 1, \ldots, k$, il existe un AFD

$$\mathcal{A}_i = (Q_i, q_{0,i}, \mathbb{F}^b, \delta_i, F_i)$$

acceptant $\mathbf{0}^* \rho_B(f^{-1}\{i\})$.

Automate produit :

- ensemble d'états $Q = Q_1 \times \cdots \times Q_k$
- état initial $q_0 = (q_{0,1}, \ldots, q_{0,k})$
- fonction de transition $\Delta : Q \times (\mathbb{F}^b)^* \to Q$

$$\Delta((q_1, \ldots, q_k), w) = (\delta_1(q_1, w), \ldots, (\delta_k(q_k, w)).$$

- fonction de sortie $\tau : Q \to S$
  l'image par τ de $(q_1, \ldots, q_k)$ est s_i ssi $q_i \in F_i$.

Conclusion

L'application $f : \mathbb{F}[X] \to S$ "est calculée" grâce à cet automate produit "nourri" avec les B-représentations des polynômes,

$$f(P) = \tau[\Delta(q_0, \mathbf{0}^n \rho_B(P))], \ \forall P \in \mathbb{F}[X], n \geq 0.$$

Noyau

Soit B un polynôme de degré $b > 0$.
Pour tout $R \in \mathbb{F}[X]$ de degré $< b$,
on définit des applications de "*B-décimation*"

$$\partial_{B,R} : S^{\mathbb{F}[X]} \to S^{\mathbb{F}[X]} : (f(P))_{P\in\mathbb{F}[X]} \mapsto (f(B.P + R))_{P\in\mathbb{F}[X]}.$$

Le B-noyau de $f = (f(P))_{P\in\mathbb{F}[X]}$ est l'ensemble

$$\ker_B(f) = \{\partial_{B,R_1} \circ \cdots \circ \partial_{B,R_n}(f) \mid \forall n \geq 0, R_1, \ldots, R_n \in \mathbb{F}[X]_{<b}\}.$$

Proposition

Une application $f : \mathbb{F}[X] \to S$ est B-reconnaissable
SSI son B-noyau est fini.

Application

Soit $\mathcal{O}$ l'ensemble des polynômes de degré impair,

$$\mathcal{O} = \{P \in \mathbb{F}[X] \setminus \{0\} \mid \deg(P) \equiv 1 \pmod 2\}.$$

Soit B un polynôme de degré $b > 1$.
Soit $f_{\mathcal{O}}$ l'application caractéristique de $\mathcal{O}$.

Proposition

$\# \ker_B(f_{\mathcal{O}}) \leq 2$ donc $\mathcal{O}$ est B-reconnaissable pour tout B.

Si b **est pair**,
pour tout $P \in \mathcal{O}$ (resp. $P \notin \mathcal{O}$) non nul et tout $R \in \mathbb{F}[X]_{<b}$,
$B.P + R \in \mathcal{O}$ (resp. $B.P + R \notin \mathcal{O}$) $\partial_{B,R}(f_{\mathcal{O}}) = f_{\mathcal{O}}$.

Si b **est impair**,
$\partial_{B,R}(f_{\mathcal{O}}) = 1 - f_{\mathcal{O}}$ et $\partial_{B,R}(1 - f_{\mathcal{O}}) = f_{\mathcal{O}}$.

En général

Pour tous $0 \leq r < s$,

$$\{P \in \mathbb{F}[X] \setminus \{0\} \mid \deg(P) \equiv r \pmod{s}\}$$

est B-reconnaissable.

A ce stade, voici les types d'ensembles reconnaissables "partout" :

Type 1

Soient Q, R des polynômes de $\mathbb{F}[X]$. L'ensemble

$$\{Q.P + R \mid P \in \mathbb{F}[X]\}$$

est B-reconnaissable pour tout B de degré ≥ 1.

Type 2

$$\{P \in \mathbb{F}[X] \setminus \{0\} \mid \deg(P) \equiv r \pmod{s}\}$$

est B-reconnaissable pour tout B de degré ≥ 1.

Type fini (cas particulier de 1)

Tout ensemble fini (tout langage fini est régulier).

Un ensemble infini $\mathcal{T} \subseteq \mathbb{F}[X]$ est *degré-syndétique* si $\exists C > 0$ tel que $\forall n \geq 0$,

$$\mathcal{T} \cap \{P \in \mathbb{F}[X] \mid \deg(P) \in [n, n + C)\} \neq \emptyset,$$

i.e., l'ensemble $\{\deg(P) \mid P \in \mathcal{T}\}$ est syndétique (ou à lacunes bornées) dans $\mathbb{N}$.

PROPOSITION

Si $\mathcal{T}$ est B-reconnaissable, il est degré-syndétique.

Le langage $\rho_B(\mathcal{T})$ étant régulier, l'ensemble des longueurs des mots y appartenant est ultimement périodique.

EXEMPLE

L'ensemble $\{X^{2^n} \mid n \geq 0\}$ n'est pas B-reconnaissable.

Dépendance à la base

Proposition

Soit B un polynôme de degré $b > 0$. $\mathcal{T} \subseteq \mathbb{F}[X]$ est B-reconnaissable ssi il est B^k-reconnaissable, $k \in \mathbb{N} \setminus \{0\}$.

$$P = C_0(B^k)^\ell + C_1(B^k)^{\ell-1} + \cdots + C_{\ell-1}B^k + C_\ell$$

$$P = C_{0,k-1}B^{k\ell+k-1} + \cdots + C_{0,0}B^{k\ell} + \cdots + C_{\ell,k-1}B^{k-1} + \cdots + C_{\ell,0}$$

$$C_i = C_{i,k-1}B^{k-1} + \cdots + C_{i,0},\ \forall i \in \{0, \ldots, \ell\}.$$

$\Phi_{B^k}(P) = C_0 \cdots C_\ell \in (\mathbb{F}^{kb})^*$ et
$\Phi_B(P) = C_{0,k-1} \cdots C_{0,0} \cdots C_{\ell,k-1} \cdots C_{\ell,0} \in (\mathbb{F}^b)^*$.
Correspondance codée par un morphisme uniforme

bases multiplicativement dépendantes

Corollaire

Soient P, Q deux polynômes de degré ≥ 1 tels qu'il existe $k, \ell > 0$ satisfaisant $P^k = Q^\ell$. Alors, $\mathcal{T} \subseteq \mathbb{F}[X]$ est P-reconnaissable ssi il est Q-reconnaissable.

Exemple

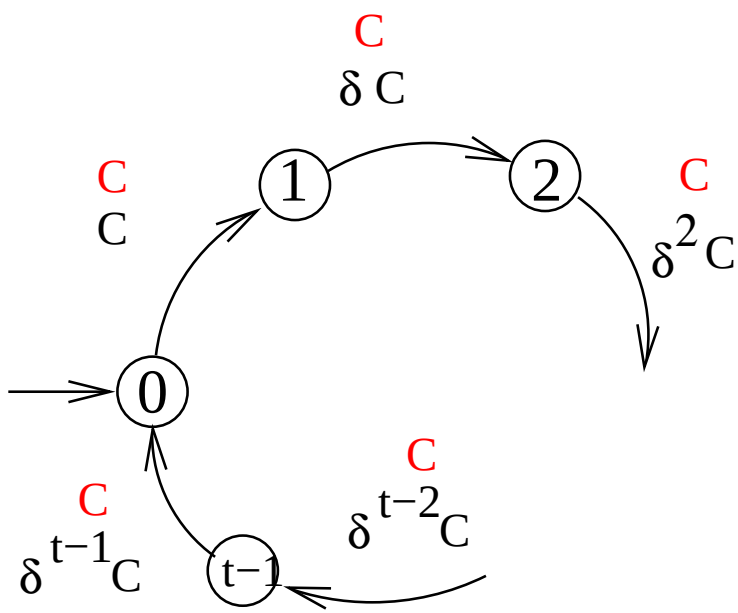
Soient $P = X^4 + X^3 + 2X^2 + 2X + 1$ et $Q = X^6 + 2X^3 + 2$ sur $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$.
On a $P^3 = Q^2 = (X^2 + 2X + 2)^6$.

PROPOSITION

Soit $\gamma \in \mathbb{F} \setminus \{0\}$. Un ensemble $\mathcal{T} \subset \mathbb{F}[X]$ est B-reconnaissable ssi il est (γB)-reconnaissable.

$$P = \sum_{i=0}^{k} C_i \, B^{k-i} = \sum_{i=0}^{k} (\gamma^{-1})^{k-i} \, C_i \, (\gamma B)^{k-i}.$$

Soit $\delta := \gamma^{-1}$, $\deg(C_i) = \deg(\delta^{k-i} \, C_i)$, soit t l'ordre de δ dans $\mathbb{F}$.



Cet automate accepte $(\rho_B(u), \rho_{\gamma B}(u))^R$, $u \in \mathbb{F}[X]$.

Exercice

Si e est l'ordre de $\gamma \in \mathbb{F}$ alors $(\gamma B)^e = B^e$,
donc B et γB sont multiplicativement dépendants.

Question

Analogue au théorème de Cobham ?

Type 3

Soient $a_1, \ldots, a_t \in \mathbb{F}$ fixés. L'ensemble

$$\{a_1 X^{n+t-1} + \cdots + a_t X^n + b_{n-1} X^{n-1} + \cdots + b_0 \mid \forall n \geq 0, b_i \in \mathbb{F}\}$$

est B-reconnaissable, quel que soit B.

Conjecture

Si P et Q sont multiplicativement indépendants, les seuls ensembles simultanément P- et Q-reconnaissables sont les unions booléennes d'ensembles des "types 1,2,3".

Exercice

Si e est l'ordre de $\gamma \in \mathbb{F}$ alors $(\gamma B)^e = B^e$,
donc B et γB sont multiplicativement dépendants.

Question

Analogue au théorème de Cobham ?

Type 3

Soient $a_1, \ldots, a_t \in \mathbb{F}$ fixés. L'ensemble

$$\{a_1 X^{n+t-1} + \cdots + a_t X^n + b_{n-1} X^{n-1} + \cdots + b_0 \mid \forall n \geq 0, b_i \in \mathbb{F}\}$$

est B-reconnaissable, quel que soit B.

Conjecture

Si P et Q sont multiplicativement indépendants, les seuls ensembles simultanément P- et Q-reconnaissables sont les unions booléennes d'ensembles des "types 1,2,3".

Complexité

Théorème de Cobham sur $\mathbb{N} \longrightarrow$ caractériser les ensembles ultimement périodiques

Théorème (Morse-Hedlund)

Un mot infini sur un alphabet fini $(x_n)_{n\in\mathbb{N}}$ est ultimement périodique ssi sa complexité est bornée.

$$00001011011011011 0 \cdots$$

7	000		001	010	101	011	110	101
8	0000	0001	0010	0101	1011	0110	1101	1011
8	00001	00010	00101	01011	10110	01101	11011	10110

$$01001010010010100101 \cdots$$

Ici, on remplace un mot infini par une application $f : \mathbb{F}[X] \to S$.
Une mesure possible : pour tout $P \in \mathbb{F}[X]$ et $n \geq 0$,

$$\zeta_f(P, n) : \mathbb{F}[X]_{<n} \to S : R \mapsto f(P + R)$$

et la fonction de complexité de f est

$$\mathfrak{C}_f(n) = \#\{\zeta_f(P, n) \mid P \in \mathbb{F}[X]\}.$$

$\mathfrak{C}_f(n) \leq \mathfrak{C}_f(n+1) \leq (\mathfrak{C}_f(n))^q$ et $1 \leq \mathfrak{C}_f(n) \leq (\#S)^{q^n}$.

PROPOSITION ;-(

Si $\mathcal{A}$ est de “type 1” et $\mathcal{B}$ de type “2”, alors

$$\mathfrak{C}_{f_\mathcal{A}}(n) \leq q^{\deg(Q)} \quad \text{et} \quad \mathfrak{C}_{f_\mathcal{B}}(n) \geq n - r.$$

Question

Peut-on espérer une mesure qui rende compte de la structure non linéaire de $\mathbb{F}[X]$?

$$1$$

$$X,\ X+1$$

$$X^2,\ X^2+1,\ X^2+X,\ X^2+X+1$$

$$\vdots$$

Retour sur des ensembles particuliers d'entiers

Ingrédient 0 : $q = p^t$

Ingrédient 1 : une bijection $\mu : \{0, \ldots, q-1\} \to \mathbb{F}$

A toute bijection μ entre $\{0, \ldots, q-1\}$ et $\mathbb{F} = \mathbb{F}_q$, $(\mu(0) = 0)$ correspond une bijection μ entre $\mathbb{N}$ et $\mathbb{F}[X]$

$$n = c_0\, q^\ell + \cdots + c_\ell \text{ avec } 0 \leq c_i < q.$$

$$\mu(n) := \mu(c_0) X^\ell + \cdots + \mu(c_\ell).$$

Remarque

μ n'est pas un morphisme de monoïdes entre $\mathbb{N}$ et $\mathbb{F}[X]$ (propagation de la retenue).

Ingrédient 2 : un polynôme $B \in \mathbb{F}[X]$ de degré ≥ 1

$$n \in \mathbb{N} \xrightarrow{\mu} \mu(n) \in \mathbb{F}[X] \xrightarrow{\rho_B} \rho_B(\mu(n))$$

$$X \subseteq \mathbb{N} \xrightarrow{\mu} \mu(X) \subseteq \mathbb{F}[X] \xrightarrow{\rho_B} \rho_B(\mu(X))$$

On peut définir des ensembles d'entiers (q, μ, B)-reconnaissables...

Sloane's sequence A001317 :

$$\left\{ t_n = \sum_{j=0}^{n} \left(\binom{n}{j} \mod 2 \right) 2^j \mid n \geq 0 \right\}$$

$$= \{1, 3, 5, 15, 17, 51, 85, 255, 257, 771, 1285, 3855, 4369, \ldots\}$$

$q = 2$, $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, $B = 1 + X$ and $\mu : \{0, 1\} \to \mathbb{F} : 0 \mapsto \overline{0}, 1 \mapsto \overline{1}$

$\mathcal{T}$ est $(2, \mu, 1 + X)$-reconnaissable :
Sur $\mathbb{Z}/2\mathbb{Z}$, on a

$$\mu(t_n) = \sum_{j=0}^{n} \left(\binom{n}{j} \mod 2 \right) X^j = (1 + X)^n$$

et $\rho_B(\mu(\mathcal{T})) = 1\,0^*$.

Par contre, $\mathcal{T}$ n'est pas 2-reconnaissable (ni $(2, \mu, X)$-reconnaissable).

Sloane's sequence A038184

000	001	010	011	100	101	110	111
0	1	1	0	1	0	0	1

$$\cdots 00100 \cdots$$

$$\cdots 0011100 \cdots$$

$$\cdots 001010100 \cdots$$

$$\mathcal{S} = \{1, 7, 21, 107, 273, 1911, 5189, 28123, \ldots\}$$

$$\mu(s_n) = (1 + X + X^2)^n.$$

$\mathcal{S}$ est $(2, \mu, 1 + X + X^2)$-reconnaissable.

- J.-P. Allouche, E. Cateland, W.-J. Gilbert, H.-O. Peitgen, J. Shallit, and G. Skordev, Automatic maps in exotic numeration systems, *Theory Comput. Syst.* **30** (1997), 285–331.
- J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, G. Skordev, Linear cellular automata, finite automata and Pascal's triangle, *Discrete Appl. Math.* **66** (1996), 1–22.
- M.R., Syntactical and automatic properties of sets of polynomials over finite field, à paraître *Finite Fields and their Applications*, `http ://www.discmath.ulg.ac.be/`