Syntactical and automatic properties of sets of polynomials over finite fields

Michel Rigo, University of Liège

Interregional Colloquium of Mathematics,
Trier, 12th October 2006

- Classically: integer base system $k \geq 2$,

$$n = \sum_{i=0}^{\ell} c_i \, k^{\ell-i} \text{ with } c_i \in \{0, \dots, k-1\}, c_0 \neq 0.$$

$$\rho_k : \mathbb{N} \to \{0, \dots, k-1\}^* : n \mapsto c_0 \cdots c_\ell$$

- From an algorithmic (formal languages theory) point of view:

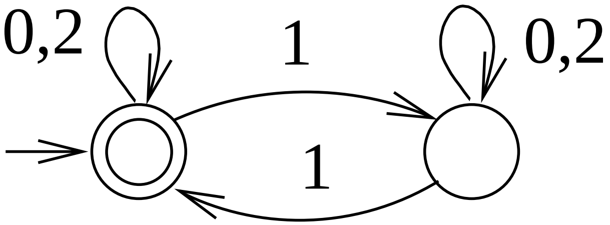
the *simplest sets* $X \subseteq \mathbb{N}$ are such that $\rho_k(X)$ is regular (accepted by some finite automaton) : k-*recognizable set*.

- Generalizations:

non-standard systems (e.g. Fibonacci), substitutive systems, abstract numeration systems

- Example : the set E_3 of even integers written in base 3

$u \in E_3$ iff u contains an even number of 1's.



- **Cobham's theorem** (1969) :

Let $p, q \geq 2$ be multiplicatively independent integers.
The only sets which are both p- and q-recognizable are ultimately periodic (i.e., finite union of arithmetic progressions).

G. Hansel, D. Perrin, F. Durand, V. Bruyère, F. Point,
C. Michaux, R. Villemaire, A. Bès, J. Bell, J. Honkala,
S. Fabre, C. Reutenauer, A.L. Semenov, L. Waxweiler, . . .

$\mathbb{F}_q$: finite field of characteristic p ($q = p^\alpha$)

In number theory, strong “analogy”
$\mathbb{N}$ (or $\mathbb{Z}$) $\leftrightarrow$ $\mathbb{F}_q[X]$
$\mathbb{Q}$ $\leftrightarrow$ $\mathbb{F}_q(X)$
$\mathbb{R}$ $\leftrightarrow$ $\mathbb{F}_q((X))$

Let $B \in \mathbb{F}_q[X]$ s.t. $\deg(B) = b > 0$, any $P \in \mathbb{F}_q[X]$

$$P = \sum_{i=0}^{\ell} C_i\, B^{\ell-i},\ C_0 \neq 0,\ C_i \in \mathbb{F}_q[X]_{<b}$$

Finite alphabet $A = \mathbb{F}_q[X]_{<b}$ set of polynomials of degree $< b$

$\rho_B : \mathbb{F}_q[X] \to A^* : P \mapsto C_0 \cdots C_\ell$

Let $B = X^2 + 2X + 2$ and $P = X^8 + 2X^7 + X^5 + 2X^4 + 2X^3 + X + 2$ over $\mathbb{Z}/3\mathbb{Z}$,

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

$$\rho_B(P) = (0, 1)(0, 1)(2, 2)(2, 1)(0, 1).$$

recognizable set of integers in base k

$\updownarrow$

recognizable set of polynomials in base B

$X \subseteq \mathbb{F}_q[X]$, $\rho_B(X)$ accepted by a finite automaton ?

Things turn out to be easier ! Let B be a polynomial of degree $b > 0$.

- If $\mathcal{S}, \mathcal{T}$ are two B-recognizable subsets of $\mathbb{F}_q[X]$, then $\mathcal{S} + \mathcal{T}$ is also B-recognizable. (no carry, single state automaton)

- Corollary: If $\mathcal{S}$ is a B-recognizable subset of $\mathbb{F}_q[X]$, then $\mathcal{S} + \{P\}$ is also B-recognizable, for any $P \in \mathbb{F}_q[X]$.

- Let Q be a polynomial. If $\mathcal{T} \subseteq \mathbb{F}_q[X]$ is B-recognizable then $Q.\mathcal{T}$ is also B-recognizable.

Special case : $\deg(Q) = 0$, $Q = \gamma$, letter-to-letter transformation :

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

- Let M, Q, B be polynomials over $\mathbb{F}_q$ with $\deg(B) \geq 1$. The set

$$\mathcal{A} = \{P.M + Q \mid P \in \mathbb{F}_q[X]\}$$

is B-recognizable. (*think about Cobham's theorem*.)

Base dependence properties :

- A set $\mathcal{T} \subseteq \mathbb{F}_q[X]$ is B-recognizable if and only if it is B^k-recognizable.

- Let P and Q be such that $P^k = Q^\ell$ for some $k, \ell > 0$. A set $\mathcal{T} \subseteq \mathbb{F}_q[X]$ is P-recognizable if and only if it is Q-recognizable.

(Wrong and first) conjecture for Cobham's theorem:

If P and Q are multiplicatively independent then the only subsets of $\mathbb{F}_q[X]$ which are both P- and Q-recognizable are the finite union of sets of the kind

$$\mathcal{A} = \{P.M + Q \mid P \in \mathbb{F}_q[X]\}$$

There is more…(suggested by D. Berend)

"Words" (or sequences) indexed by $\mathbb{F}_q[X]$ (instead of $\mathbb{N}$ or $\mathbb{Z}$)

Automaticity (F. von Haeseler): Let S be a finite set. A map $f : \mathbb{F}_q[X] \to S$ is B-*automatic* if for all $s \in S$, $f^{-1}\{s\}$ is a B-recognizable subset of $\mathbb{F}_q[X]$.

Special case: $S = \{0, 1\}$ (i.e., characteristic map of a set)

For each $R \in \mathbb{F}_q[X]_{<b}$, B-*decimation map*,

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

The B-*kernel* of $f = (f(P))_{P\in\mathbb{F}_q[X]}$ is

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

- Proposition: A map $f : \mathbb{F}_q[X] \to S$ is B-automatic if and only if its B-kernel is finite.

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

with characteristic map $f_{\mathcal{O}} : P \mapsto \begin{cases} 1, P \in \mathcal{O} \\ 0, P \notin \mathcal{O} \end{cases}$, $\boxed{\# \ker_B(f_{\mathcal{O}}) \leq 2}$

Therefore $\mathcal{O}$ is B-recognizable for any B of degree $b > 1$.

If b is even, then for all $P \in \mathcal{O}$ (resp. $P \notin \mathcal{O}$) and all $R \in \mathbb{F}_q[X]_{<b}$, $B.P + R \in \mathcal{O}$ (resp. $B.P + R \notin \mathcal{O}$) so $\partial_{B,R}(f_{\mathcal{O}}) = f_{\mathcal{O}}$.
If b is odd, $\partial_{B,R}(f_{\mathcal{O}}) = 1 - f_{\mathcal{O}}$ and $\partial_{B,R}(1 - f_{\mathcal{O}}) = f_{\mathcal{O}}$.

- $\{P \in \mathbb{F}_q[X] \setminus \{0\} \mid \deg(P) \equiv r \pmod s\}$ for any $0 \leq r < s$.

(Better) conjecture for Cobham's theorem:

If P and Q are multiplicatively independent then the only subsets of $\mathbb{F}_q[X]$ which are both P- and Q-recognizable are the boolean combinations of sets of the kind

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

or

$$\{P \in \mathbb{F}_q[X] \setminus \{0\} \mid \deg(P) \equiv r \pmod{s}\} \quad \text{for any } 0 \leq r < s.$$

("block"-) Complexity function

Let $f : \mathbb{F}_q[X] \to S$ be a map. For all $P \in \mathbb{F}_q[X]$ and $n \geq 0$,

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

The *complexity function* of f is $\mathfrak{C}_f : \mathbb{N} \to \mathbb{N}$ defined by

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

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

For any total ordering of $\mathbb{F}_q[X] = \{0 = R_1 < R_2 < \cdots\}$ such that $R_i \leq R_j \Rightarrow \deg(R_i) \leq \deg(R_j)$.

$$\mathfrak{C}_f(n) = \#\text{distinct words } f(P + R_1), f(P + R_2), \cdots, f(P + R_{q^n}).$$

- Morse-Hedlund's Theorem (for words over $\mathbb{N}$): an infinite word $w = w_0 w_1 w_2 \cdots$ is ultimately periodic iff $\exists C$ s.t. $p(n) < C$, $\forall n \geq 0$.

$$\{P.M + Q \mid P \in \mathbb{F}_q[X]\}, \quad \mathfrak{C}_f(n) = q^{\mathsf{deg}(M)}$$

$$\{P \in \mathbb{F}_q[X] \setminus \{0\} \mid \mathsf{deg}(P) \equiv r \pmod{s}\}, \quad \mathfrak{C}_f(n) = q^n - q^r + 3$$

Work under progress...

Another notion of complexity.

Let $w = w_0 w_1 w_2 \cdots$ be an infinite word. The arithmetical closure of w is

$$AC(w) = \{w_k w_{k+p} w_{k+2p} \cdots w_{k+np} \mid k \geq 0,\ p, n \geq 1\}$$

Van Der Waerden's theorem (1927): (unavoidable "pattern")
For all n, $AC(w)$ contains a^n for some a.

Arithmetical complexity (2000 Avgustinovich, Fon-Der-Flass, Frid)

$$A_w : n \mapsto AC(w) \cap \Sigma^n$$

Logical approach. . .

- Büchi-Bruyère's Theorem: $X \subseteq \mathbb{N}$ is k-recognizable iff it can be defined in $FO\langle\mathbb{N},+,V_k\rangle$.

- R. Villemaire (1992): $FO\langle\mathbb{N},+,V_k,V_\ell\rangle$ is undecidable.

- C. Michaux, R. Villemaire (1996) : logical proof of Cobham-Semenov's theorem.

- L. Waxweiler (ULg, 2006): extension of Büchi-Bruyère's Theorem to B-recognizable sets of $\mathbb{F}_q[X]$.

Exotic number systems...

Let's come back to sets of integers (another notion of recognizability)

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

Fix a one-to-one correspondence $\mu : \{0, \ldots, q-1\} \to \mathbb{F}_q$, s.t. $\mu(0) = 0$. It induces a one-to-one correspondence defined by

$$\mu : \mathbb{N} \to \mathbb{F}_q[X] : n \mapsto \mu(n) := \mu(c_0)X^\ell + \cdots + \mu(c_\ell)$$

(μ is not a morphism of monoids between $\mathbb{N}$ and $\mathbb{F}_q[X]$.)

Ingredients : q, μ, $B \in \mathbb{F}_q[X]$ with $\deg(B) \geq 1$, $n \mapsto \mu(n) \mapsto \rho_B(\mu(n))$

$X \subseteq \mathbb{N}$ is (q, μ, B)-*recognizable* if $\rho_B(\mu(n))$ is regular.

New notion but some well-known examples. . .

“linear cellular automata induced by a Laurent polynomial”
(J.-P. Allouche *et al.*, 1996)

Consider the set $\mathcal{T}$ of numbers obtained from Pascal’s triangle mod 2 converted to decimal (Sloane’s sequence `A001317`) :

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

$$\begin{array}{lllllll} 1 & \texttt{rules :} & 11 & 10 & 01 & 00 & \cdots\ 01101000110 \cdots \\ 11 & & \downarrow & \downarrow & \downarrow & \downarrow & \\ 101 & & 0 & 1 & 1 & 0 & \\ 1111 & & & & & & \end{array}$$

$$= \{1, 3, 5, 15, 17, 51, 85, 255, 257, 771, 1285, 3855, 4369, 13107, 21845, \ldots\}$$

Let us take $q = 2$, $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, $B = 1 + X$ and $\mu : \{0, 1\} \to \mathbb{F}$ mapping each integer coefficient $0, 1$ in base two onto its corresponding residue class also denoted $0, 1$.

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

and we get $\rho_B(\mu(\mathcal{T})) = 1\,0^*$