Uniform Distribution Theory **8** (2013), no.2, 171–182

uniform distribution theory

SUR LES PUISSANCES DES POLYNÔMES SUR UN CORPS FINI

Mireille Car — Christian Mauduit

Résumé. Let $\mathbb{F}$ a finite field, Q a given element of $\mathbb{F}[T]$ with positive degree and k a positive integer. The goal of this work is to study the Q-automaticity of the set of kth powers of elements of $\mathbb{F}[T]$ and to calculate the number of polynomials $X \in \mathbb{F}[T]$ of degree N such that the sum of digits of X^k in base Q is fixed.

Communicated by András Sárközy

1. Introduction et notations

Soit $\mathbb{F}$ un corps fini à q éléments et de caractéristisque p et $\mathbb{F}[T]$ l'anneau des polynômes à une variable sur le corps $\mathbb{F}$. Dans tout cet article Q désigne un élément de $\mathbb{F}[T]$ de degré strictement positif. On note

$$\mathcal{C}_Q = \{X \in \mathbb{F}[T] | \deg X < \deg Q\}$$

où l'on convient que $\deg 0 = -\infty$. Tout polynôme non nul $X \in \mathbb{F}[T]$ admet une unique représentation sous la forme

$$X = \sum_{n=0}^{\ell} X_n Q^n, \tag{1.1}$$

où $\ell \in \mathbb{N}, X_n \in \mathcal{C}_Q$ pour tout $n \in \{0, \dots, \ell\}$ et $X_\ell \neq 0$ (voir par exemple [1]). Cette représentation est l'écriture de X en base Q. La suite $(X_n)_{0 \leq n \leq \ell}$ est la suite des chiffres de X en base Q. On peut considérer $\mathcal{C}_Q$ comme un alphabet fini dont les lettres sont les polynômes de degré strictement inférieur à $\deg Q$. Pour tout $j \in \mathbb{N}$, on désigne par $\mathcal{C}_Q^{(j)}$ l'ensemble des mots de longueur j, (i.e. constitués de j lettres). Si $\mathbf{m} \in \mathcal{C}_Q^{(j)}$, on note $|\mathbf{m}| = j$ sa longueur.

2010 Mathematics Subject Classification: 11T55, 11B85, 11A63, 68Q45.
Keywords: Polynômes, corps finis, automates.
Recherche effectuée avec le soutien de l'Agence Nationale de La Recherche, projet ANR-10-BLAN 0103 MUNUM.

L'ensemble de tous les mots finis construits sur l'alphabet $\mathcal{C}_Q$ est la réunion $\mathcal{C}_Q^\star = \bigcup_{j\in\mathbb{N}} \mathcal{C}_Q^{(j)}$. On appelle langage sur l'alphabet $\mathcal{C}_Q$ tout sous-ensemble de $\mathcal{C}_Q^\star$.
On peut alors noter

$$\mathrm{rep}_Q(X) = X_\ell \dots X_0 \in \mathcal{C}_Q^{(\ell+1)}$$

la représentation (1.1) du polynôme non nul X. On convient que $\mathrm{rep}_Q(0) = 0$.

2. Sous-ensemble de $\mathbb{F}[T]$ reconnaissable par un Q-automate fini

Définition 1 : Un Q-automate fini (déterministe) est un quadruplet $\mathcal{A} = \mathcal{A}_Q = (E, E_f, e_0, \varphi)$ où
i) E est un alphabet fini, (états) ;
ii) $E_f \subset E$, (états finaux) ;
iii) $e_0 \in E$, (état initial) ;
iv) φ est une application de $E \times \mathcal{C}_Q$ vers E.

Pour tout $(e, c) \in E \times \mathcal{C}_Q$, on pose $\varphi(e, c) = e.c$ et on prolonge φ en une application de $E \times \mathbb{F}[T]$ vers E ou de $E \times \mathcal{C}_Q^\star$ vers E notée encore φ par abus de notation, en procédant de la manière suivante : si la représentation en base Q de $X \in \mathbb{F}[T]$ est $\mathrm{rep}_Q(X) = X_\ell \dots X_0 \in \mathcal{C}_Q^{(\ell+1)}$, alors on pose pour tout $e \in E$,

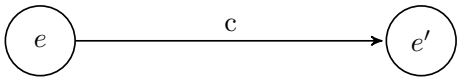
$$\varphi(e, X) = e \cdot X = \Big(\cdots \big((e \cdot X_\ell) \cdot X_{\ell-1}\big) \cdots \Big) \cdot X_0.$$

Remarque 1 : Cette définition correspond à la notion de $(\mathcal{C}_Q, Q)$-automate fini définie dans [1] (voir exemple 1.7) et a été étudiée de manière très détaillée par M. Rigo et L. Waxweiler dans [16], [19] et [18] (voir aussi [2] pour les notions générales concernant les automates finis).

Remarque 2 : Le "déterminisme" de $\mathcal{A}$ traduit le fait que $\mathcal{A}$ admet un seul état initial e_0 et que φ est une application.

Le graphe étiqueté $\mathcal{G}(\mathcal{A}) = \mathcal{G}(\mathcal{A}_Q)$ associé à l'automate fini $\mathcal{A}_Q$ est le graphe $\mathcal{G}(\mathcal{A}_Q) = (E, U)$ dans lequel
i) E est l'ensemble des sommets de $\mathcal{G}(\mathcal{A}_Q)$;
ii) $U = \{(e, e', c) \in E \times E \times \mathcal{C}_Q | \varphi(e, c) = e'\}$ est l'ensemble des arcs étiquetés de $\mathcal{G}(\mathcal{A}_Q)$.

On représente un arc étiqueté de la manière suivante :



Définition 2 : On dit qu'un langage $L \subset \mathcal{C}_Q^\star$ est Q-régulier ou reconnaissable par un Q-automate fini, s'il existe un Q-automate fini $\mathcal{A} = (E, E_f, e_0, \varphi)$ tel que

$$L = \{\mathbf{m} \in \mathcal{C}_Q^\star | \varphi(e_0, \mathbf{m}) \in E_f\}.$$

Définition 3 : On dit qu'un sous-ensemble $S \subset \mathbb{F}[T]$ est reconnaissable par un Q-automate fini, si le langage

$$\mathcal{L}_Q(S) = \{\mathrm{rep}_Q(X), X \in S\}$$

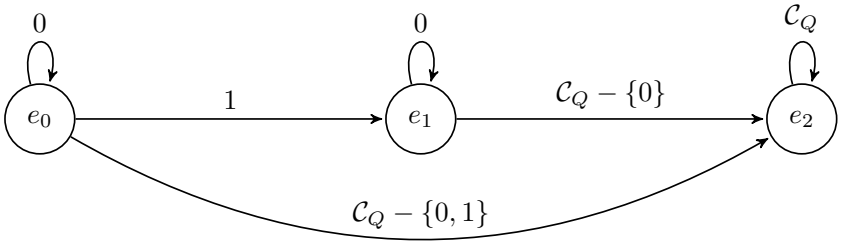
est Q-régulier.

Les deux exemples suivants sont les analogues polynomiaux d'exemples de sous ensembles de $\mathbb{N}$ reconnaissables par un automate fini (voir par exemple [6]).

Exemple 1 : L'ensemble $\mathcal{Q} = \{Q^n, n \in \mathbb{N}\}$ est reconnaissable par le Q-automate fini

$$\mathcal{A} = \big\{\{e_0, e_1, e_2\}, \{e_1\}, e_0, \varphi\big\}$$

dont le graphe $\mathcal{G}(\mathcal{A})$ est



De plus, si les polynômes Q et R sont multiplicativement indépendants, alors l'ensemble $\mathcal{Q}$ n'est pas reconnaissable par un R-automate fini (voir [18, Proposition 7]).

Exemple 2 : Le sous ensemble $\mathcal{I}$ de $\mathbb{F}[T]$ constitué des polynômes irréductibles n'est jamais reconnaissable par un Q-automate fini (voir [18, Theorem 9]).

Question 1 : L'ensemble des entiers naturels sans facteur carré ayant une densité irrationnelle, on sait d'après [6] qu'il n'est reconnaissable par aucun automate fini. Cet argument ne fonctionne pas pour l'ensemble $\mathfrak{Q}$ des polynômes sans facteur carré, c'est à dire ne possédant que des racines simples dans une clôture algébrique de $\mathbb{F}$ dont la densité égale à $1 - \frac{1}{q}$ est rationnelle. Est-il vrai que $\mathfrak{Q}$ n'est jamais reconnaissable par un Q-automate fini ?

Le résultat suivant est souvent utile :

Lemme 2.1. *Pour tout nombre entier strictement positif k, un sous-ensemble S de $\mathbb{F}[T]$ est reconnaissable par un Q^k-automate fini si et seulement si il est reconnu par un Q-automate fini.*

Preuve. Voir [16, Proposition 6]

□

3. L'ensemble $\mathcal{P}(k)$ des puissances k-ièmes des éléments de $\mathbb{F}[T]$

Dans le cadre des nombres entiers, il résulte des travaux de Büchi concernant l'arithmétique faible du second ordre que l'ensemble des carrés n'est reconnaissable par aucun automate fini, [3]. Ritchie a donné dans [17] une preuve élégante et élémentaire de cette non reconnaissabilité dans le cas particulier de la base 2. Minsky et Papert ont montré dans [14] qu'en utilisant l'ordre naturel sur les nombres entiers, il est possible de démontrer que pour tout nombre entier $k \geq 2$, l'ensemble des puissances k-ièmes d'entiers n'est reconnaissable par aucun automate fini. Leur preuve consiste à démontrer que si une suite $(u_n)_{n\in\mathbb{N}}$ d'entiers de densité nulle est telle que $\lim_{n\to+\infty} \frac{u_{n+1}}{u_n} = 1$, alors elle n'est reconnaissable par aucun automate fini, (voir aussi [6]). La situation est plus complexe dans le cas de $\mathbb{F}[T]$. L'objet de cette partie est de caractériser les entiers k pour lesquels l'ensemble $\mathcal{P}(k)$ des puissances k-ièmes de polynômes de $\mathbb{F}[T]$ est reconnaissable par un Q-automate fini. Nous allons démontrer le théorème suivant :

Théorème 3.1. *Soit un nombre entier $k \geq 2$ Le sous-ensemble $\mathcal{P}(k)$ de $\mathbb{F}[T]$ constitué des puissances k-ièmes d'éléments de $\mathbb{F}[T]$ est reconnaissable un Q-automate fini si et seulement si k est une puissance de la caractéristique p de $\mathbb{F}$.*

(A) *Condition nécessaire :* La preuve repose sur les lemmes suivants.

Lemme 3.2. *Soit un nombre entier $k \geq 2$ premier à p. Soit $A \in \mathbb{F}[T]$ un polynôme dont la représentation en base Q commence par le chiffre 1. Alors, il existe $n \in \mathbb{N}$ et $R \in \mathbb{F}[T]$ tels que $(AQ^n + R) \in \mathcal{P}(k)$ et $\deg R < n \deg Q$.*

Lemme 3.3. *Soit un langage $L \subset \mathcal{C}_Q^\star$ reconnaissable par un Q-automate fini tel que tout mot commençant par la lettre 1 se prolonge en un mot de L. Alors, il existe un entier $s = s(L) > 0$ tel que pour tout entier $n \geq s$,*

$$\mathrm{Card}\{\mathbf{m} \in L, |\mathbf{m}| \leq n\} \geq q^{(n-s)\deg Q}.$$

Remarque 3 : Le Lemme 3.3 reprend une stratégie utilisée à plusieurs reprises par Cassaigne afin de démontrer la non-automaticité de certaines suites (voir par exemple [5]).

Supposons démontrés ces deux lemmes et montrons que la reconnaissabilité de $\mathcal{P}(k)$ par un Q-automate fini conduirait à une contradiction lorsque k n'est pas une puissance de p.

1) Supposons d'abord que k est premier à p. La reconnaissabilité de $\mathcal{P}(k)$ par un automate fini impliquerait grâce au Lemme 3.2 et au Lemme 3.3 que

$$\mathrm{Card}\{\mathbf{m} \in \mathcal{L}\big(\mathcal{P}(k)\big), |\mathbf{m}| \leq n\} \gg q^{n \deg Q},$$

c'est-à-dire que

$$\mathrm{Card}\{X \in \mathcal{P}(k), \deg X \leq n\} \gg q^{n \deg Q},$$

ce qui conduirait à une contradiction puisque

$$\mathrm{Card}\{X \in \mathcal{P}(k), \deg X \leq n\} \leq q^{[n/k]+1}.$$

2) Traitons maintenant le cas général. Soit h un nombre entier strictement positif et soit $k \geq 2$ un nombre entier premier avec p. Observons que si $X \in \mathcal{C}_Q$, alors $X^{p^h} \in \mathcal{C}_{Q^{p^h}}$. Si $\mathbf{m} = X_1 \dots X_j \in \mathcal{C}^{(j)}$, on note $\mathbf{m}^{\langle p^h \rangle} = X_1^{p^h} \dots X_j^{p^h} \in \mathcal{C}^{(j)}_{Q^{p^h}}$. Si $X_0, \dots, X_\ell$ sont des éléments de $\mathcal{C}_Q$, on a l'identité

$$\left(\sum_{i=0}^{\ell} X_i Q^i\right)^{kp^h} = \left(\sum_{i=0}^{\ell} X_i^{p^h} \big(Q^{p^h}\big)^i\right)^k.$$

Il en résulte que

$$\mathcal{L}_{Q^{p^h}}\big(\mathcal{P}(k)\big) = \left\{\mathbf{m}^{\langle p^h \rangle}, \mathbf{m} \in \mathcal{L}_Q\big(\mathcal{P}(kp^h)\big)\right\}.$$

Si $\mathcal{P}(kp^h)$ était reconnaissable par un Q-automate fini, le langage $\mathcal{L}_Q(\mathcal{P}(kp^h))$ serait Q-régulier. Le langage $\mathcal{L}_{Q^{p^h}}(\mathcal{P}(k))$ serait donc Q^{p^h}-régulier, c'est à dire

que $\mathcal{P}(k)$ serait reconnaissable par un Q^{p^h}-automate fini. D'après le Lemme 2.1, $\mathcal{P}(k)$ serait reconnaissable par un Q-automate fini, ce qui est impossible d'après la première partie. Il nous reste à démontrer le Lemme 3.2 et le Lemme 3.3.

Preuve du Lemme 3.2. L'écriture de A en base Q est de la forme

$$A = Q^s + A_{s-1}Q^{s-1} + \cdots + A_1Q + A_0.$$

Soit un nombre entier $j \geq 0$ congru à $-s$ modulo k. Posons $B = AQ^j$. Alors,
(i) $\deg B$ est divisible par k,
(ii) le coefficient dominant de B est une puissance k-ième dans $\mathbb{F}$.

Considérons le corps $\mathbb{F}((\frac{1}{T}))$ des séries de Laurent formelles

$$y = \sum_{n=-\infty}^{+\infty} y_n T^n \qquad (\dagger)$$

où les coefficients y_n appartiennent au corps $\mathbb{F}$ et sont tous nuls pour n assez grand. On a l'inclusion $\mathbb{F}[T] \subset \mathbb{F}((\frac{1}{T}))$ et on prolonge la fonction degré au corps $\mathbb{F}((\frac{1}{T}))$ en posant pour $y \neq 0$, écrit sous la forme (†),

$$\deg(y) = \max\{n \in \mathbb{Z} | y_n \neq 0\}.$$

Si y est écrit sous la forme (†), on pose

$$\{y\} = \sum_{n=-\infty}^{-1} y_n T^n, \quad [y] = y - \{y\}$$

et on remarque que $[y] \in \mathbb{F}[T]$.
D'après [4, Proposition I.3.2], il existe $\beta \in \mathbb{F}((\frac{1}{T}))$ tel que $B = \beta^k$. Si N est l'entier défini par $kN = \deg B$, alors $\deg \beta = N$. Posons

$$\beta = \sum_{n=-\infty}^{N} \beta_n T^n.$$

Soit un entier m tel que $m \deg Q \geq (k-1)N$ et

$$C = \big[\beta Q^m T^{(k-1)N - m\deg Q}\big] T^{m\deg Q - (k-1)N}.$$

Alors $C \in \mathbb{F}[T]$ avec $\deg C = N + m\deg Q$ et on a

$$\begin{aligned}\deg(C - \beta Q^m) &= m\deg Q - (k-1)N + \deg\big(\{\beta Q^m T^{(k-1)N - m\deg Q}\}\big) \\ &< m\deg Q - (k-1)N,\end{aligned}$$

d'où

$$\deg\bigl(C^k - (\beta Q^m)^k\bigr) < m\deg Q - (k-1)N + (k-1)(N + m\deg Q) = km\deg Q,$$

soit

$$\deg(C^k - BQ^{km}) < km\deg Q.$$

On a donc $AQ^{km+j} = C^k + R$ où $R \in \mathbb{F}[T]$ est de degré $< km\deg Q$.

□

Preuve du Lemme 3.3. Notons $\mathcal{A} = (E, E_f, e_0, \varphi)$ le Q-automate fini reconnaissant le langage L et $E_1 \subset E$ l'ensemble des états atteignables par les mots commençant par la lettre 1 : $E_1 = \varphi(e_0, 1\mathcal{C}_Q^\star)$. Pour tout $e \in E_1$, il existe $\mathbf{m} \in \mathcal{C}_Q^\star$ tel que $\varphi(e, \mathbf{m}) \in E_f$. Parmi tous les $\mathbf{m}$ ayant cette propriété on en choisit un, noté $\mathbf{m}(e)$, de longueur minimale et on note

$$r = \max_{e \in E_1} |\mathbf{m}(e)|.$$

Soit un nombre entier $j \geq 0$. Pour tout mot $\mathbf{m} \in 1\mathcal{C}_Q^{(j)}$, il existe un mot $\mathbf{m}' \in \mathcal{C}_Q^\star$ tel que $|\mathbf{m}'| \leq r$ et $\mathbf{m}\mathbf{m}' \in L$. Le langage L contient donc au moins $(\mathrm{Card}(\mathcal{C}_Q))^j$ mots de longueur $j + i + 1$, où $i \in \{0, \ldots, r\}$. Si n est un nombre entier, $n \geq r + 1$, L contient au moins $(\mathrm{Card}(\mathcal{C}_Q))^{n-r-1}$ mots de longueur au plus n.

□

(B) *Condition suffisante :* Elle est donnée par la proposition suivante.

Proposition 3.4. *Soit $k = p^a$ avec a entier strictement positif. Alors $\mathcal{P}(k)$ est reconnaissable par un Q-automate fini.*

Preuve : Soit $Y \in \mathbb{F}[T]$. Alors Y est une puissance k-ième si et seulement si il existe $\ell \in \mathbb{N}$ et $X_0, \ldots, X_\ell \in \mathcal{C}_Q$ tels que

$$Y = X_\ell^{p^a} Q^{p^a \ell} + \cdots + X_0^{p^a} = X_\ell^k Q^{k\ell} + \cdots + X_0^k.$$

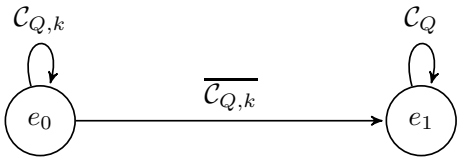
Notons $\mathcal{C}_{Q,k}$ l'ensemble des puissances k-ièmes des éléments de $\mathcal{C}_Q$ et $\overline{\mathcal{C}_{Q,k}} = \mathcal{C}_{Q^k} - \mathcal{C}_{Q,k}$. On a donc

$$\mathcal{P}(k) = \left\{ Y_\ell (Q^k)^\ell + \cdots + Y_0, \quad \ell \in \mathbb{N}, (Y_\ell \ldots, Y_0) \in \mathcal{C}_{Q,k}^{\ell+1} \right\}.$$

L'ensemble $\mathcal{P}(k)$ est donc reconnaissable par le Q^k-automate fini

$$\mathcal{A}_Q^{(k)} = \bigl\{\{e_0, e_1\}, \{e_0\}, e_0, \varphi\bigr\}$$

dont le graphe est



et la Proposition 3.4 résulte du Lemme 2.1.

□

Remarque 4 : Le Lemme 3.3 peut être utilisé pour donner une autre preuve de la non-automaticité de l'ensemble des polynômes irréductibles. En effet, on a aisément le

Lemme 3.5. *Soit $A \in \mathbb{F}[T]$ un polynôme non nul. Alors, il existe $n \in \mathbb{N}$ et $R \in \mathbb{F}[T]$ tels que $(AQ^n + R)$ soit un polynôme irréductible et $\deg R < n \deg Q$.*

Preuve : Notons $\Pi_Q(n, A)$ le nombre de polynômes irréductibles P de degré $n \deg Q + \deg A$ tels que $\deg(P - AQ^n) < n \deg Q$. Un théorème de Hsu [13] nous donne la minoration

$$\Pi_Q(n, A) \geq \frac{q^n}{n \deg Q + \deg A} - (3 + \deg A)\frac{q^{(n \deg Q + \deg A)/2}}{n \deg Q + \deg A},$$

d'où l'on déduit que $\Pi_Q(n, A) > 0$ dès que $q^{n/2} > \deg A q^{\deg A}$.

□

4. La fonction somme des chiffres sur $\mathcal{P}(k)$

Soient b, k et h des nombres entiers ≥ 2 et a un nombre entier. Le problème posé en 1968 par Gelfond dans [12] de l'estimation, pour tout nombre entier strictement positif N, du nombre d'entiers $n \in [0, N[$ tels que la somme des chiffres de n^k en base b soit congru à a modulo h, est encore largement ouvert. Voir [10], [11], [15] et [8] pour des résultats partiels concernant l'ensemble des nombres entiers et [9] pour le cas des corps finis. L'objet de cette partie est de répondre à une question analogue dans le cadre des polynômes sur un corps fini. Soit $X \in \mathbb{F}[T]$. Si $\mathrm{rep}_Q = X_\ell \dots X_0$, on note

$$s(X) = \sum_{n=0}^{\ell} X_n$$

la somme des chiffres de X en base Q. L'ensemble des chiffres $\mathcal{C}_Q$ étant un sous groupe fini de $\mathbb{F}[T]$, la fonction s est à valeurs dans $\mathcal{C}_Q$. C'est de plus

une fonction Q-additive. Elle diffère par son domaine de valeurs, des fonctions Q-additives sur $\mathbb{F}[T]$ étudiées par Drmota et Gutenbrunner dans [7]. La proposition suivante donne quelques propriétés utiles de la fonction s.

Proposition 4.1. *Pour tout $(X, Y) \in \mathbb{F}[T]^2$, on a*
(1) $s(X) \equiv X \pmod{((Q-1))}$;
(2) $s(X+Y) = s(X) + s(Y)$;
(3) $s(XY) = s(s(X)s(Y))$.

Preuve. (1) Soit

$$X = \sum_{n=0}^{\ell} X_n Q^n, \quad X_n \in \mathcal{C}_Q$$

l'écriture de $X \in \mathbb{F}[T]$ en base Q. Comme $Q \equiv 1 \pmod{(Q-1)}$, il en résulte que pour tout $n \in \mathbb{N}$ on a $Q^n \equiv 1 \pmod{(Q-1)}$, d'où

$$\sum_{n=0}^{\ell} X_n Q^n \equiv \sum_{n=0}^{\ell} X_n \ \big(\mathrm{mod}\ (Q-1)\big)$$

et donc $s(X) \equiv X \pmod{(Q-1)}$.

(2, 3) Si $(X, Y) \in \mathbb{F}[T]^2$, il résulte de (1) que l'on a d'une part

$$s(X) + s(Y) \equiv X + Y \equiv s(X+Y) \ \big(\mathrm{mod}\ (Q-1)\big)$$

et d'autre part

$$s\big(s(X)s(Y)\big) \equiv s(X)s(Y) \equiv XY \equiv s(XY) \ \big(\mathrm{mod}\ (Q-1)\big).$$

Comme $\deg s(X), \deg s(Y)$ et $\deg s(X+Y)$ sont strictement inférieurs à $\deg Q = \deg((Q-1))$, la congruence $s(X) + s(Y) \equiv s(X+Y) \pmod{(Q-1)}$ implique l'égalité (2).
Comme $\deg s(s(X)s(Y))$ et $\deg s(XY)$ sont strictement inférieurs à $\deg Q = \deg(Q-1)$, la congruence $s(s(X)s(Y)) \equiv s(XY) \pmod{(Q-1)}$ implique l'égalité (3).

□

Soit k un nombre entier strictement positif et soit $C \in \mathcal{C}_Q$. On désigne par $\mathcal{S}_Q^k(C)$ l'ensemble des polynômes $X \in \mathbb{F}[T]$ tels que $s(X^k) = C$. Le théorème suivant donne la valeur exacte du cardinal de l'ensemble

$$\{X \in \mathcal{S}_Q^k(C) | \deg X = N\}$$

pour tout nombre entier N assez grand.

Théorème 4.2. *Soit k un entier strictement positif et soit $C \in \mathcal{C}_Q$. Pour $N \in \mathbb{N}$, soit $u_{k,C}(N)$ le nombre de polynômes $X \in F[T]$ de degré N tels que $s(X^k) = C$. Alors,*
(1) si C n'est pas une puissance k-ième modulo $(Q-1)$, alors pour tout $N \in \mathbb{N}$ on a $u_{k,C}(N) = 0$;
(2) si C est une puissance k-ième modulo $(Q-1)$, alors pour tout $N \geq \deg Q$ on a

$$u_{k,C}(N) = (q-1)q^{N-\deg Q}\rho_k(C),$$

où $\rho_k(C)$ désigne le nombre de solutions de la congruence $C \equiv R^k \pmod{(Q-1)}$.

Preuve. Notons tout d'abord que $\deg(Q-1) = \deg Q$ et donc que $\mathcal{C}_{(Q-1)} = \mathcal{C}_Q$. Soit $C \in \mathcal{C}_Q$. S'il existe $X \in F[T]$ tel que $s(X^k) = C$, il résulte de la Proposition 4.1 que $C \equiv X^k \pmod{(Q-1)}$.
Réciproquement, supposons $C \equiv R^k \pmod{(Q-1)}$ avec $R \in \mathcal{C}_Q$ et considérons $X \in \mathbb{F}[T]$ congru à R modulo $(Q-1)$. Il résulte de la Proposition 4.1 que

$$s(X^k) \equiv X^k \equiv R^k \equiv C \ \big(\mathrm{mod}\ (Q-1)\big).$$

Comme $\deg(s(X^k) - C) < \deg Q = \deg(Q-1)$, on a $s(X^k) = C$. Donc, pour tout $N \in \mathbb{N}$,

$$u_{k,C}(N) \quad = \sum_{\substack{R \in \mathbb{F}[T] \\ \deg R < \deg Q \\ C \equiv R^k (\mathrm{mod}(Q-1))}} \nu_R(N),$$

où $\nu_R(N)$ désigne le nombre de $X \in \mathbb{F}[T]$ de degré N congrus à R modulo $(Q-1)$. Si $N \geq \deg Q$, alors $\nu_R(N)$ est égal au nombre de $Y \in \mathbb{F}[T]$ de degré $N - \deg(Q-1) = N - \deg Q$. Par suite, pour $N \geq \deg Q$, on a $\nu_R(N) = q^{N-\deg Q}$ et donc

$$u_{k,C}(N) \quad = \sum_{\substack{R \in \mathbb{F}[T] \\ \deg R < \deg(Q-1) \\ C \equiv R^k (\mathrm{mod}(Q-1))}} q^{n-\deg Q}.$$

□

Question 2 : Il serait intéressant de décrire de manière plus précise la structure de l'ensemble $\mathcal{S}_Q^k(C)$ lorsque k n'est pas une puissance de la caractéristique p et lorsque C est une puissance k-ième modulo $(Q-1)$. Par exemple est-il vrai sous ces hypothèses que l'ensemble $\mathcal{S}_Q^k(C)$ n'est jamais reconnaissable par un Q-automate fini ?

Références

[1] ALLOUCHE, J.-P.— CATELAND, E.— GILBERT, W.J.—PEITGEN, H.0. —SHALLIT, J.—SKORDEV, G.: *Automatic maps in exotic numeration systems*, Theory Comput. Syst. **30** (1997), 285–331.

[2] ALLOUCHE,J.-P.—SHALLIT, J.: *Automatic sequences. Theory, Applications, Generalizations*. Cambridge University Press, Cambridge, 2003.

[3] BÜCHI, J.R.: *Weak second-order arithmetic and finite automata*, Z. Math. Logik Grundlagen Math. **6** (1960), 66–92.

[4] CAR, M.: *Répartition modulo 1 dans un corps de séries formelles sur un corps fini*, Acta Arithmetica **49** (1995), 229–242.

[5] CASSAIGNE, J.—LE GONIDEC, M.: *Propriétés et limites de la reconnaissance d'ensembles d'entiers par automates dénombrables*, J. Theor. Nombres Bordeaux **22** (2010), 307–338.

[6] COBHAM, A.: *Uniform tag sequences*, Math. Syst Theory **6** (1972), 164–192.

[7] DRMOTA, M.—GUTENBRUNNER, G.: *The joint distribution of Q-additive functions on polynomials over finite fields*, J. Theor. Nombres Bordeaux **17**(2005), 125–150.

[8] DRMOTA, M.—MAUDUIT, C.—RIVAT, J.: *The sum-of-digits function of polynomial sequences*, J. Lond. Math. Soc. **84** (2011), 81–102.

[9] DARTYGE, C.—SÁRKÖZY, A.: *The sum of digits function in finite fields*, Proc. Amer. Math. Soc., à paraître.

[10] DARTYGE, C.—TENENBAUM, G.: *Sommes de chiffres de multiples d'entiers*, Ann. Inst. Fourier **55**(2005), 2423–2474.

[11] DARTYGE, C.—TENENBAUM, G.: *Congruences de sommes de chiffres de valeurs polynomiales*, Bull. London Math. Soc. **38** (2006), 61–69.

[12] GELFOND, A. O. : *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arithmetica, (1968), 259–265.

[13] HSU, C. N.: *The distribution of irreducible polynomials in* $\mathbb{F}_q[T]$, J. Number Theory **61** (1996), 85–96.

[14] MINSKY, M.—PAPERT, S.: *Unrecognizable sets of numbers*, J. Assoc. Comput. Mach. **13** (1966), 281–286.

[15] MAUDUIT, C.—RIVAT, J.: *La somme des chiffres des carrés*, Acta Math. **203** (2009), 107–148.

[16] RIGO, M.: *Syntactical and automatic properties of set of polynomials over finite fields*, Finite Fields Appl. **14** (2008), 258–276.

[17] RITCHIE, R.W.: *Finite automata and the set of squares*, J. Assoc. Comput. Mach. **10** (1963), 528–531.

[18] RIGO, M.—WAXWEILER, L.: *Logical characterization of recognizable sets of polynomials over a finite field*, International Journal of Foundations of Computer Science, (à paraître).

[19] WAXWEILER, L.: *Caractère reconnaissable d'ensembles de polynômes à coefficients dans un corps fini*, thèse de doctorat, Université de Liège, décembre 2009, `http:orbi,ulg.ac.be/handle/2268/11381`.

Received April 16, 2013
Accepted June 12, 2013

Mireille Car
Laboratoire d'Analyse, Topologie et Probablitités
CNRS, UMR 7353
CMI, 39 rue F. Joliot Curie
13453 Marseille Cedex 13
FRANCE
E-mail: mireille.car@univ-amu.fr

Christian Mauduit
Institut de Mathématiques de Luminy
CNRS, UMR 6206
163 avenue de Luminy, Case 907
F-13288 Marseille Cedex 9
FRANCE
et
Instituto de Matemática Pura e Aplicada,
IMPA–CNRS, UMI 2924
Estrada Dona Castorina 110
22460-320 Rio de Janeiro
BRASIL
E-mail: mauduit@iml.univ-mrs.fr