Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

RÉPARTITION DES FONCTIONS COMPLÈTEMENT Q-ADDITIVES LE LONG DES CARRÉS DE È POLYNÔMES SUR UN CORPS FINI

Mireille Car & Christian Mauduit

Tome 144
Fascicule 4

2016

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique
pages 775-817

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 4, tome 144, décembre 2016

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
`smf@smf.univ-mrs.fr`

Hindustan Book Agency
O-131, The Shopping Mall
Arjun Marg, DLF Phase 1
Gurgaon 122002, Haryana
Inde

AMS
P.O. Box 6248
Providence RI 02940
USA
`www.ams.org`

Tarifs

Vente au numéro : 43 € ($ 64)

Abonnement Europe : 178 €, hors Europe : 194 € ($ 291)

Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Nathalie Christiaën

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
`revues@smf.ens.fr` • `http://smf.emath.fr/`

ISSN 0037-9484

Directeur de la publication : Stéphane Seuret

Bull. Soc. math. France
144 (4), 2016, p. 775–817

RÉPARTITION DES FONCTIONS COMPLÈTEMENT Q-ADDITIVES LE LONG DES CARRÉS DE POLYNÔMES SUR UN CORPS FINI

PAR MIREILLE CAR & CHRISTIAN MAUDUIT

RÉSUMÉ. — Soit F un corps fini à q éléments (q impair), $Q \in F[T]$ et f une fonction complètement Q-additive à valeurs entières. L'objet de ce travail est l'étude des sommes d'exponentielles $\sum_{\substack{X\in F[T]\\ \deg X<N}} \exp(2\pi i\alpha f(X^2))$ pour $\alpha \in \mathbb{R}$. Nous en déduisons en particulier une condition nécessaire et suffisante portant sur f pour que, pour tout $(a,m) \in \mathbb{N}\times\mathbb{N}^*$, on ait $\operatorname{card}\{X \in \mathbf{A} \mid \deg X < N,\ f(X^2) \equiv a \pmod m\} = \frac{q^N}{m} + O(q^{(1-h)N})$, avec $0 < h < 1$.

ABSTRACT (*Repartition of completely Q-additive functions along squares of polynomials over a finite field*)

Let F be a finite field with q elements (q odd), $Q \in F[T]$ and f an integer valued completely Q-additive function. The goal of this work is to study the exponential sums $\sum_{\substack{X\in F[T]\\ \deg X<N}} \exp(2\pi i\alpha f(X^2))$ for $\alpha \in \mathbb{R}$. In particular, this study provides a necessary and sufficient condition on f under which, for any $(a,m) \in \mathbb{N}\times\mathbb{N}^*$, we have $\operatorname{card}\{X \in \mathbf{A} \mid \deg X < N,\ f(X^2) \equiv a \pmod m\} = \frac{q^N}{m} + O(q^{(1-h)N})$, with $0 < h < 1$.

Texte reçu le 19 février 2015, révisé le 5 janvier 2016 accepté le 9 février 2016.

MIREILLE CAR, Université d'Aix-Marseille, Institut de Mathématiques de Marseille CNRS, UMR 7373, CMI, 39 rue F. Joliot-Curie 13453 Marseille Cedex 13, France

CHRISTIAN MAUDUIT, Université d'Aix-Marseille et Institut Universitaire de France, Institut de Mathématiques de Marseille CNRS, UMR 7373, 163 avenue de Luminy, Case 907, F-13288 Marseille Cedex 9, France

Classification mathématique par sujets (2000). — 11 T 55.

Mots clefs. — Polynômes sur un corps fini, fonctions Q-additives, sommes d'exponentielles.

Recherche effectuée avec le soutien de l'Agence Nationale de La Recherche, projet ANR-10-BLAN 0103 MUNUM et de Ciência sem Fronteiras, projet PVE 407308/2013-0.

1. Introduction et notations

Soit F un corps fini à q éléments et de caractéristisque p. On note $\mathbf{A}$ l'anneau $F[T]$ des polynômes à une variable sur le corps F, $\mathbf{M}$ l'ensemble des polynômes unitaires de $F[T]$ et $\mathbf{I}$ l'ensemble des polynômes irréductibles unitaires de $F[T]$. Si X et Y sont des polynômes non nuls, on note $\tau(X)$ le nombre de diviseurs unitaires de X et (X, Y) le plus grand commun diviseur unitaire de X et Y. Dans tout cet article, $Q \in \mathbf{A}$ est un polynôme de degré $d > 0$ et on note $\mathscr{C}_Q = \{X \in \mathbf{A} | \deg X < \deg Q\}$ l'ensemble des restes de la division euclidienne par Q où l'on convient que $\deg 0 = -\infty$. Tout polynôme $X \in \mathbf{A}$ admet une unique représentation comme somme

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

où $X_n \in \mathscr{C}_Q$ pour tout $n \in \mathbb{N}$, appelée représentation de X en base Q. La suite $(X_n)_{n\in\mathbb{N}}$ dont tous les termes sont nuls à partir d'un certain rang est la suite des chiffres de X en base Q. La valeur absolue d'un polynôme $X \in \mathbf{A}$ est définie par

$$\langle X \rangle = \begin{cases} q^{\deg X} & \text{si } X \neq 0, \\ 0 & \text{si } X = 0 \end{cases} \tag{1.2}$$

et on note $|\mathscr{X}|$ le nombre d'éléments de tout ensemble fini $\mathscr{X}$.

DÉFINITION. — *Une application f de $\mathbf{A}$ dans un groupe additif $\mathbf{B}$ est dite complètement Q-additive si pour tout $Y \in \mathbf{A}$ et tout $R \in \mathscr{C}_Q$, on a $f(YQ+R) = f(Y) + f(R)$.*

Observons qu'une fonction complètement Q-additive f à valeurs dans un groupe $\mathbf{B}$ est déterminée par les valeurs prises par f sur l'ensemble des chiffres $\mathscr{C}_Q$. En effet, si (1.1) est la représentation de X en base Q, alors $f(X) = \sum_{n=0}^{\infty} f(X_n)$.

Drmota et Gutenbrunner ont étudié dans [7] la distribution des fonctions Q-additives sur $\mathbf{A}$ et montré des résultats analogues à ceux obtenus par Bassily-Kátai, Kim et Drmota dans le cas des nombres entiers (voir [1], [12] et [5]). Madritsch et Thuswaldner ont étudié dans [14] le cas plus général des sommes de Weyl polynomiales associées aux fonctions Q-additives. Lorque $\mathbf{B}$ est égal à l'anneau $\mathbf{A} = F[T]$, la fonction « somme des chiffres en base Q » définie pour tout $X \in A$ écrit sous la forme (1.1) par $s(X) = \sum_{n\geq 0} X_n$, constitue un exemple typique de fonction Q-additive sur $\mathbf{A}$. Dans [3] nous avons étudié son comportement sur les puissances k-ièmes des éléments de $\mathbf{A}$. Dans cet article nous nous intéressons au cas plus difficile à traiter des fonctions Q-additives à valeurs réelles.

Un exemple simple de fonctions complètement Q-additives à valeurs entières est fourni par les fonctions de poids Q-adique $w_Q^{(\ell)}$, ℓ étant un paramètre réel, définies par

$$w_Q^{(\ell)}(X) = \sum_{n=0}^{\infty} \langle X_n \rangle^\ell \tag{1.3}$$

pour tout $X \in \mathbf{A}$ dont la représentation en base Q est donnée par (1.1). En particulier, $w_Q^{(0)}(X)$ est le nombre de chiffres de X différents de 0.

Drmota et Gutenbrunner ont montré dans [7] l'existence d'un théorème central limite pour les fonctions complètement Q-additives à valeurs réelles sur les puissances k-ièmes des éléments de $\mathbf{A}$:

THÉORÈME. — *Pour toute fonction complètement Q-additive $f : \mathbf{A} \to \mathbb{R}$ et pour tout nombre entier $k > 0$, on a pour y nombre réel et n nombre entier tendant vers $+\infty$,*

$$\frac{1}{q^n} |\{X \in \mathbf{A} | \deg X < n, f(X^k) \leq \frac{kn}{\deg Q}\mu_f + y\sqrt{\frac{nk}{\deg Q}}\sigma_f\}| = \Phi(y) + o(1),$$

avec $\mu_f = q^{-\deg Q} \sum_{x \in \mathscr{C}_Q} f(X)$, $\sigma_f^2 = q^{-\deg Q} \sum_{x \in \mathscr{C}_Q} f(X)^2$ et $\Phi(y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-t^2/2} dt$, la loi de distribution normale.

Dans ce qui suit, on suppose que f une fonction complètement Q-additive à valeurs entières définie sur $\mathbf{A}$ de caractéristique p impaire et on s'intéresse à la répartition des valeurs prises par $f(X^2)$, X décrivant l'anneau $\mathbf{A}$. Lorsque la caractéristique de $\mathbf{A}$ est égale à 2, les carrés de $\mathbf{A}$ ont des propriétés particulières qui peuvent conduire à des représentations Q-adiques très atypiques. Par exemple, si $p = 2$ et $Q = T^2$, la fonction complètement Q-additive f définie sur $\mathscr{C}_Q = \{x_0 + x_1 T, (x_0, x_1) \in \mathbb{F}^2\}$ par

$$f(x_0 + x_1 T) = \begin{cases} 0 \text{ si } x_1 = 0, \\ 1 \text{ si } x_1 \neq 0 \end{cases}$$

est nulle sur les carrés de $\mathbf{A}$.

Le but de cet article est de montrer que la méthode introduite par Mauduit et Rivat dans [17] (voir également [9] et [20] pour des généralisations) peut être adaptée à $\mathbf{A}$ afin d'étudier le comportement de $f(X^2)$ lorsque $p \neq 2$. Notons que l'étude du comportement de $f(X^k)$ pour $k \geq 3$ semble hors d'atteinte par les techniques connues à ce jour (sauf lorsque k est une puissance de p).

La situation est rendue plus complexe que dans le cas des nombres entiers par l'existence d'obstructions de nature arithmétique propres à $\mathbf{A}$ et qui n'apparaissaient pas dans le cas des nombres entiers. Plus précisément, nous allons identifier une classe de fonctions complètement Q-additives pour lesquelles,