Répartition des fonctions Q-additives le long des carrés de polynômes sur un corps fini

Mireille Car, Christian Mauduit

Répartition des fonctions Q-additives le long des carrés de polynômes sur un corps fini [*] [†]

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

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.

Si $Q \in \mathbf{A}$ un polynôme de degré strictement positif, on note

$$\mathcal{C}_Q = \{X \in \mathbf{A} | \deg X < \deg Q\}$$

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

[*] AMS Classification 11 T 55

[†] 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.

somme

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

où $X_n \in \mathcal{C}_Q$ 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

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

Enfin, on notera $|\mathcal{X}|$ le nombre d'éléments de tout ensemble fini $\mathcal{X}$.

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 $R \in \mathcal{C}_Q$, on a $f(YQ + R) = f(Y) + f(R)$.

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

Drmota et Gutenbrunner ont étudié dans [6] 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], [9] et [5]). Madritsch et Thuswaldner ont étudié dans [10] le cas plus général des sommes de Weyl polynomiales associées aux fonctions Q-additives. Lorque B est égal à l'anneau $\mathbf{A} = \mathbb{F}[T]$, 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 [4] 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 des fonctions Q-additives à valeurs réelles.

Un exemple simple de fonctions complètement Q-additives à valeurs réelles 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 $X \in A$ 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 [6] l'existence d'un théorème central limite pour les fonctions Q-additives à valeurs réelles sur les puissances k-ièmes des éléments de $\mathbf{A}$:

Théorème Pour toute fonction 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 $\mu_f = q^{-\deg Q} \sum_{x \in \mathcal{C}_\mathcal{Q}} f(X)$, $\sigma_f^2 = q^{-\deg Q} \sum_{x \in \mathcal{C}_\mathcal{Q}} f(X)^2$ 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 q est un nombre entier impair, f une fonction complètement Q-additive à valeurs réelles définie sur $\mathbf{A}$ et on s'intéresse à la répartition des valeurs prises par $f(X^2)$, X décrivant l'anneau $\mathbf{A}$. Le but de cet article est de montrer que la méthode introduite par Mauduit et Rivat dans [12] (voir également [7] et [14]) peut être adaptée à A afin d'étudier le comportement de $f(X^k)$ lorsque $k = 2$. Notons que le cas général $k \geq 3$ semble hors d'atteinte par les techniques connues à ce jour.

La situation est rendue plus complexe que dans le cas des nombres entiers par l'existence d'obstructions de nature arithmétique propres à 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 pour tout nombre entier $k > 0$, la suites $(\frac{k}{p} f(X^2))_{X \in \mathbf{A}}$ a un comportement pathologique.

Par exemple, dans le cas où $\mathbf{A} = \mathbb{F}_3[T]$, $Q = T$ et f est l'application de A dans $\mathbb{R}$ définie par $f(0) = 0$, $f(1) = 1$, $f(2) = 2$, on a

$$|\{X \in \mathbb{F}_3[T]| \deg X < n,\ f(X^2) \equiv a \pmod 3\}| = \begin{cases} 3^{n-1} \text{ si } a = 0, \\ 2 \times 3^{n-1} \text{ si } a = 1, \\ 0 \text{ si } a = 2. \end{cases}$$

et f n'est donc pas équidistribuée sur les carrés.

A toute forme linéaire $\lambda : F^d \mapsto F$, on associe l'application $\lambda^\star$ de $\mathcal{C}_Q$ dans $\mathbb{F}_p$ définie par

$$\lambda^\star(\sum_{i=0}^{d-1} x_i Y^i) = \mathrm{tr}(\lambda(x_0, \ldots, x_{d-1})),$$

où tr désigne la trace de F sur $\mathbb{F}_p$.

Définition On dira qu'une application w de $\mathcal{C}_Q$ dans $\mathbb{Z}$ est dans la classe $\mathcal{L}$ s'il existe une forme linéaire $\lambda : F^d \mapsto F$ telle que pour tout $X \in \mathcal{C}_Q$, $\lambda^\star(X)$ soit la classe de $w(X)$ modulo p. Les fonctions Q-additives f pour lesquelles $f_{|\mathcal{C}_Q}$ décrit $\mathcal{L}$ seront dites dégénérées. Notons $\mathcal{D}$ l'ensemble de ces fonctions pour lesquelles nous démontrerons :

Théorème 1.1 *Soit f une fonction complètement Q-additive à valeurs entières dégénérée. Alors il existe une constante $\gamma(q, Q, f) > 0$ ne dépendant que de q, Q, f telle que pour tout nombre entier k et tout nombre entier $N > \deg Q$, on ait*

$$|\sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \exp(2\pi i\frac{k}{p}f(X^2))| \geq \gamma(q,Q,f)q^N.$$

Le principal théorème établi dans cet article est le suivant :

Théorème 1.2 *Soit f une fonction complètement Q-additive à valeurs entières non dégénérée. Alors, pour tout nombre réel α non entier, il existe un nombre réel $0 < a(q, Q, f, \alpha) < 1$ et un nombre entier $N(q, Q, f, \alpha)$ ne dépendant que de q, Q, f et α tel que pour tout nombre entier $N \geq N(Q, f, \alpha)$ on ait*

$$|\sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \exp(2\pi i\alpha f(X^2))| \leq b(q,Q)N^{\frac{\omega(Q)+1}{4}}q^{N(1-a(q,Q,f,\alpha))},$$

$\omega(Q)$ désignant le nombres de polynômes irréductibles distincts divisant Q et $b(q, Q) > 0$ étant une constante ne dépendant que de q et de Q.

On déduira de ce théorème le corollaire ci dessous :

Corollaire 1.3 *Soit f une fonction complètement Q-additive à valeurs entières non dégénérée. Alors, pour tout nombre entier $m > 0$, il existe un nombre réel $0 < h(q, Q, f, m) < 1$, tel que pour tout nombre entier rationnel a, on ait*

$$|\{X \in \mathbf{A}| \deg X < n,\ f(X^2) \equiv a \pmod m\}| = \frac{q^n}{m} + O(q^{n(1-h(q,Q,f,m))}),$$

les constantes impliquées par le symbole O ne dépendant que de q, Q, f et m.

La preuve du Théorème 1.1 sera donnée à la section 3. Pour obtenir la majoration du Théorème 1.2 prouvée à la section 6, nous majorerons les sommes

$$\Sigma_f(N) = \sum_{\substack{X \in \mathbf{A} \\ \nu \deg Q \leq \deg X < N}} \mathrm{e}(\alpha f(X^2)),$$

$\nu = \nu(N)$ étant le nombre entier déterminé par la condition $\nu \deg Q < N \leq (\nu+1)\deg Q$. Ceci sera fait à la section 5. Les outils nécessaires à ces preuves seront établis aux sections 2 et 4. Ce sont essentiellement des majorations de sommes de caractères faisant intervenir le caractère E défini à la section 2.1.

Pour $\alpha \in \mathbb{R}$, on pose $\mathrm{e}(\alpha) = \exp(2\pi i\alpha)$ et on note $\|\alpha\|$ la distance de α au nombre entier le plus proche. Pour alléger l'écriture, d'une part, dans les estimations de sommes de caractères, un élément x de $\mathbb{F}_p$ sera identifié à son image $j(x) \in \{0, \ldots, p-1\}$ et d'autre part, la dépendance des constantes à q ne sera pas précisée.

2 Rappels et lemmes techniques concernant le caractère exponentiel E

2.1 Le caractère E

On note $\mathbf{K}$ le corps $F(T)$. La valuation à l'infini sur le corps $\mathbf{K}$ est l'application v_∞ de $\mathbf{K}$ dans $\mathbb{Z} \cup \{\infty\}$ définie par $v_\infty(0) = \infty$ et $v_\infty(G/H) = \deg H - \deg G$, si G et H sont des polynômes non nuls. Le complété de $\mathbf{K}$ pour la valuation v_∞ est le corps $\mathbf{K}_\infty = F((T^{-1}))$ des séries de Laurent formelles

$$y = \sum_{n=-\infty}^{+\infty} y_n T^n, \ y_n \in F,$$

les coefficients y_n étant tous nuls pour n assez grand. On prolonge v_∞ à $\mathbf{K}_\infty$ en posant pour $y \neq 0$,

$$v_\infty(y) = -\sup\{n \in \mathbb{Z} \mid y_n \neq 0\}.$$

Soit $\mathcal{P}$ l'idéal de valuation de $\mathbf{K}_\infty$. Tout $y \in \mathbf{K}_\infty$ s'écrit de façon unique comme somme

$$y = [y] + \{y\}, \quad [y] \in \mathbf{A}, \quad \{y\} \in \mathcal{P},$$

où $[y]$ et $\{y\}$ peuvent être vus commes les parties entière et fractionnaire de y. Soit $\psi : F \mapsto \mathbb{C}$ le caractère non trivial du groupe additif de F défini par

$$\psi(x) = \exp(2\pi i \frac{j(\mathrm{tr}(x))}{p}),$$

j étant la bijection naturelle de $\mathbb{F}_p$ sur $\{0, 1, \ldots, p-1\}$. On associe à ψ un caractère additif non trivial de $\mathbf{K}_\infty$ en posant pour tout $y = \sum_{n=-\infty}^{+\infty} y_n T^n \in \mathbf{K}_\infty$,

$$E(y) = \psi(\mathrm{Res}(y)),$$

où

$$\mathrm{Res}(y) = y_{-1}.$$

Ce caractère est trivial sur l'anneau $\mathbf{A}$. Dans la suite de ce travail nous utiliserons souvent une conséquence immédiate de cette propriété à savoir, l'implication : Si A, B, H sont dans $\mathbf{A}$ avec $H \neq 0$

$$A \equiv B \pmod{H} \Rightarrow E(\frac{A}{H}) = E(\frac{B}{H}).$$

2.2 Sommes associées au caractère E

Tout d'abord rappelons sans démonstration le résultat fondamental suivant (voir [8]).

Proposition 2.1 *Soit, pour $y \in \mathbf{K}_\infty$ et N un nombre entier naturel*

$$S(y, N) = \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} E(yX). \tag{2.1}$$

Alors,

$$S(y, N) = \begin{cases} q^N & \text{si} \quad v_\infty(\{y\}) > N, \\ 0 & \text{sinon.} \end{cases} \tag{2.2}$$

d'où l'on déduit le corollaire

Corollaire 2.2 *Soit $H \in \mathbf{A}$ un polynôme non nul et soit $G \in \mathbf{A}$. Alors,*

$$\sum_{X \in \mathcal{C}_H} E(\frac{GX}{H}) = \begin{cases} \langle H \rangle & \text{si} \quad G \equiv 0 \pmod{H}, \\ 0 & \text{sinon.} \end{cases} \tag{2.3}$$

Proposition 2.3 *Pour tout $H \in \mathbf{A}$ non nul, on désigne par $v_Q(H)$ le plus grand nombre entier m tel que Q^m divise H. Soient m, n et ℓ des nombres entiers tels que $0 \leq m \leq n \leq \ell$ et soit $\theta \in \mathbb{R}$. Alors,*

$$\sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ m \leq v_Q(D) \leq n}} \langle D \rangle^{1/2} \langle Q \rangle^{\theta v_Q(D)} \tag{2.4}$$

$$\leq (n-m+1)\tau(Q^{\ell-m}) \left(\frac{\langle Q \rangle}{q}\right)^{\ell/2} \max\left((\langle Q \rangle^\theta q^{1/2})^m, (\langle Q \rangle^\theta q^{1/2})^n\right).$$

Preuve. Analogue à celle du lemme 19 de [12]

□

Lemme 2.4 *Pour tout $u \in \mathbb{R}$, on a*

$$|1 + \mathrm{e}(u)| \leq 2 - 4\|u\|^2, \tag{2.5}$$

Preuve. On a $|1 + \mathrm{e}(u)|^2 = 4(1 - \sin(\pi u)^2) \leq 4(1 - 4\|u\|^2)$, d'où $|1 + \mathrm{e}(u)| \leq 2(1 - 2\|u\|^2)$.

□

Proposition 2.5 *Soit w une application de $\mathcal{C}_Q$ dans $\mathbb{Z}$ n'appartenant pas à la classe $\mathcal{L}$. Pour $\alpha \in \mathbb{R}$, $H \in \mathcal{C}_Q$, soit*

$$\phi = \phi_1(Q, w, \alpha, H) = \sum_{X \in \mathcal{C}_Q} \mathrm{e}(\alpha w(X)) E(-\frac{HX}{Q}). \tag{2.6}$$

Alors, pour tout nombre réel $\alpha \notin \mathbb{Z}$, il existe une constante $0 < c_{Q,w,\alpha} < 1$ telle que pour tout $H \in \mathcal{C}_Q$, on ait

$$|\phi_1(Q, w, \alpha, H)| \leq \langle Q \rangle - c_{Q,w,\alpha}. \tag{2.7}$$

Preuve. Posons $d = \deg Q$. Dans le corps $\mathbf{K}_\infty$, $\frac{H}{Q}$ se développe en série de Laurent

$$\frac{H}{Q} = \sum_{i \leq -1} \frac{a_i}{T^i}.$$

Pour tout $X = \sum_{j=0}^{d-1} x_j T^j$ appartenant à $\mathcal{C}_Q$, on a

$$E(-\frac{HX}{Q}) = \psi(-(a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1}))$$

$$= \mathrm{e}(\frac{\mathrm{tr}(-(a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1}))}{p}),$$

d'où

$$e(\alpha w(X))E(-\frac{HX}{Q}) = e(\alpha w(X) - \frac{\mathrm{tr}(a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1})}{p}).$$

Notons $L_H(X) = a_{-1}x_0 + a_{-2}x_1 + \cdots + a_{-d}x_{d-1}$. Soit α un nombre réel non entier. Si α n'est pas un nombre rationnel de la forme ℓ/p, ℓ premier à p alors, pour tout chiffre $X \in \mathcal{C}_Q$ non nul, on a $(\alpha w(X) - \frac{\mathrm{tr}(L_H(X))}{p}) \notin \mathbb{Z}$. Si $\alpha = \ell/p$, ℓ étant premier à p, comme $w \notin \mathcal{L}$, il existe $X \in \mathcal{C}_Q$ non nul tel que $(w(X) - \mathrm{tr}(L_H(X))) \notin \mathbb{Z}p$ et donc tel que $(\alpha w(X) - \frac{\mathrm{tr}(L_H(X))}{p}) \notin \mathbb{Z}$. Dans l'un ou l'autre cas on peut choisir $X_H \in \mathcal{C}_Q - \{0\}$ maximisant $\|\alpha w(X) - \frac{\mathrm{tr}(L_H(X)}{p}\|$. On pose $\Delta_{w,\alpha,H} = \|\alpha w(X_H) - \frac{\mathrm{tr}(L_H(X_H)}{p}\|$ et $\delta_{w,\alpha} = \min_{H \in \mathcal{C}_Q} \Delta_{w,\alpha,H}$ (on note que $\delta_{w,\alpha} > 0$). La somme $\phi = \phi_1(Q, w, \alpha, H)$ s'écrit

$$\phi = 1 + \mathrm{e}(\alpha w(X_H)) - \frac{\mathrm{tr}(L_H(X_H))}{p}) + \sum_{\substack{X \in \mathcal{C}_Q \\ X \notin \{0, X_H\}}} \mathrm{e}(\alpha w(X) E(-\frac{HX}{Q}),$$

d'où

$$|\phi| \leq |1 + \mathrm{e}(\alpha w(X_H)) - \frac{\mathrm{tr}(L_H(X_H))}{p})| + \langle Q \rangle - 2.$$

Avec (2.5), il vient

$$|\phi| \leq \langle Q \rangle - 4\|\alpha w(X_H) - \frac{\mathrm{tr}(L_H(X_H))}{p})\|^2$$

$$= \langle Q \rangle - 4\Delta_{w,\alpha,H} \leq \langle Q \rangle - 4\delta_{w,\alpha}^2.$$

□

Pour des commodités d'écriture, posons $c_{w,\alpha} = 0$ dans le cas où $\alpha \in \mathbb{Z}$.

Proposition 2.6 *Soit w une application de $\mathcal{C}_Q$ dans $\mathbb{Z}$ n'appartenant pas à la classe $\mathcal{L}$. Soient $\alpha \in \mathbb{R}$, $(Q,H) \in \mathbf{A}^2$ avec $\deg Q > 0$. Pour tout nombre entier $j > 0$, soit*

$$\phi_j = \phi_j(Q,w,\alpha,H) = \sum_{R\in\mathcal{C}_Q} \mathrm{e}(\alpha w(R))E(-\frac{HR}{Q^j}). \tag{2.8}$$

Alors on a

$$\phi_j \leq \langle Q\rangle - c_{Q,w,\alpha}. \tag{2.9}$$

Preuve. Soit

$$H = \sum_{k=0}^{m} H_k Q^k,\ H_k \in \mathcal{C}_Q$$

le développement de H en base Q. Le caractère E étant trivial sur $\mathbf{A}$, on a

$$E(\frac{HR}{Q^j}) = E(\sum_{k=0}^{\min(m,j-1)} \frac{H_k R}{Q^{j-k}}) = \prod_{k=0}^{\min(m,j-1)} E(\frac{H_k R}{Q^{j-k}})).$$

Pour $0 \leq k \leq j-2$, on a $v_\infty(\frac{H_k R}{Q^{j-k}}) \geq 2$, d'où $E(\frac{H_k}{Q^{j-k}}) = 1$. Par suite,

$$\phi_j = \sum_{R\in\mathcal{C}_Q} \mathrm{e}(\alpha w(R))E(-\frac{H_j R}{Q}) = \phi_1(w,\alpha,Q,H_j).$$

La proposition précédente nous donne

$$\phi_j \leq \langle Q\rangle - c_{Q,w,\alpha}.$$

□

2.3 Sommes de Gauss quadratiques associées au caractère E

Pour $H \in \mathbf{A}$ non nul et $(A,B) \in \mathbf{A}^2$, soit

$$\Gamma(H;A,B) = \sum_{X\in\mathcal{C}_H} E(\frac{AX^2+BX}{H}). \tag{2.10}$$

Proposition 2.7 *Soient $H \in \mathbf{A}, A \in \mathbf{A}$ et $B \in \mathbf{A}$ avec $H \neq 0$. Alors, on a*
(1) $\Gamma(H;A,B) = \langle (A,H)\rangle \Gamma(\frac{H}{(A,H)}, \frac{A}{(A,H)}, \frac{B}{(A,H)})$ si (A,H) divise B ;
(2) $\Gamma(H;A,B) = 0$ si (A,H) ne divise pas B.

Preuve. On pose $H = H_1(A,H), A = A_1(A,H)$. Tout $X \in \mathcal{C}_H$ s'écrivant de façon unique $X = Y + ZH_1$ avec $Y \in \mathcal{C}_{H_1}$ et $Z \in \mathcal{C}_{(A,H)}$, on a

$$\Gamma(H;A,B) = \sum_{Y\in\mathcal{C}_{H_1}} \sum_{Z\in\mathcal{C}_{(A,H)}} E\left(\frac{A_1(Y+ZH_1)^2}{H_1} + \frac{B(Y+ZH_1)}{H_1(A,H)}\right)$$

$$= \sum_{Y\in\mathcal{C}_{H_1}} E\left(\frac{A_1Y^2}{H_1} + \frac{BY}{H_1(A,H)}\right) \sum_{Z\in\mathcal{C}_{(A,H)}} E(\frac{BZ}{(A,H)}).$$

Le corollaire 2.2 nous donne alors

$$\Gamma(H;A,B) = \left(\sum_{Y\in\mathcal{C}_{H_1}} E\left(\frac{A_1Y^2}{H_1} + \frac{BY}{H_1(A,H)}\right)\right) \times \begin{cases} \langle (A,H)\rangle & \text{si} \quad (A,H)|B, \\ 0 & \text{sinon.} \end{cases}$$

ce qui prouve (2). Si (A,H) divise B, on pose $B = B_1(A,H)$. On a alors

$$\Gamma(H;A,B) = \langle (A,H)\rangle \sum_{Y\in\mathcal{C}_{H_1}} E\left(\frac{A_1Y^2}{H_1} + \frac{B_1Y}{H_1}\right) = \langle (A,H)\rangle \Gamma(H_1;A_1,B_1).$$

□

Proposition 2.8 *Soient $H \in \mathbf{A}, A \in \mathbf{A}$ et $B \in \mathbf{A}$ avec $H \neq 0$. Alors, on a*

$$|\Gamma(H;A,B)| \leq \langle (A,H)\rangle^{1/2} \langle H\rangle^{1/2}. \tag{2.11}$$

Preuve. Si (A,H) ne divise pas B, la relation (2.11) est triviale. On suppose que (A,H) divise B. Comme ci-dessus, on pose $H = H_1(A,H), A = A_1(A,H), B = B_1(A,H)$. Les polynômes A_1 et H_1 étant premiers entre eux, il existe $C_1 \in \mathcal{C}_{H_1}$ tel que $B_1 \equiv 2A_1C_1 \pmod{H_1}$. Par suite,

$$\Gamma(H_1;A_1,B_1) = \sum_{Y\in\mathcal{C}_{H_1}} E\left(\frac{A_1(Y^2+2C_1Y)}{H_1}\right) = \sum_{Y\in\mathcal{C}_{H_1}} E(\frac{A_1(Y+C_1)^2}{H_1}) E(-\frac{C_1^2}{H_1}).$$

L'application $Y \to Y + C_1$ étant une permutation de l'ensemble $\mathcal{C}_{H_1}$, on a $\Gamma(H_1;A_1,B_1) = E(-\frac{C_1^2}{H_1})\Gamma(H_1;A_1,0)$, d'où $|\Gamma(H_1;A_1,B_1)| = |\Gamma(H_1;A_1,0)|$. Les propositions III.2 et III.3 de [2] nous donnent $|\Gamma(H_1;A_1,0)| = \langle H_1\rangle^{1/2}$ d'où,

$$|\Gamma(H_1;A_1,B_1)| = \langle (A,H)\rangle \langle H_1\rangle^{1/2} = \langle (A,H)\rangle^{1/2} \langle H\rangle^{1/2}.$$

□

3 Démonstration du Théorème 1.1

Soit λ une application linéaire non nulle de F^d dans F, $\lambda^\star$ l'application de $\mathcal{C}_Q$ dans $\mathbb{F}_p$ définie par

$$\lambda^\star(\sum_{i=0}^{d-1} x_i T^i) = \mathrm{tr}(\lambda(x_0, x_1, \ldots, x_{d-1}))$$

et $f^\star$ la fonction complètement Q-additive à valeurs dans $\mathbb{F}_p$ prolongeant $\lambda^\star$ à l'anneau $\mathbf{A}$.

Proposition 3.1 *Les applications $\lambda^\star$ et $f^\star$ sont linéaires et*

$$\mathrm{Ker} f^\star = \mathrm{Ker}\lambda^\star + (Q-1),$$

$(Q-1)$ désignant l'idéal de $\mathbf{A}$ engendré par le polynôme $Q-1$.

Preuve. La linéarité de $\lambda^\star$ est évidente et on vérifie facilement celle de $f^\star$. L'inclusion $\mathrm{Ker}\lambda^\star \subset \mathrm{Ker} f^\star$ est également évidente et pour montrer l'inclusion $(Q-1) \subset \mathrm{Ker} f^\star$, on remarque que si $X = \sum_{m=0}^{\infty} X_m Q^m$ est la représentation en base Q de $X \in \mathbf{A}$, alors

$$X(Q-1) = -X_0 + \sum_{m=0}^{\infty} (X_m - X_{m+1}) Q$$

et par suite

$$f^\star(X(Q-1)) = \lambda^\star(-X_0) + \sum_{m=0}^{\infty} \lambda^\star(X_m - X_{m+1})$$

$$= -\lambda^\star(X_0) + \sum_{m=0}^{\infty} (\lambda^\star(X_m) - \lambda^\star(X_{m+1})) = 0.$$

Montrons maintenant l'inclusion inverse. Soit $Y \in \mathrm{Ker} f$. On fait la division euclidienne de Y par $Q-1$:

$$Y = R + X(Q-1),\ R \in \mathcal{C}_{Q-1},\ X \in \mathbf{A}.$$

On a vu que $X(Q-1) \in \mathrm{Ker} f^\star$. Il s'en suit que $R \in \mathrm{Ker} f^\star$. Comme $\deg R < \deg(Q-1) = \deg Q$, on a $f(R) = w(R)$, c'est à dire $R \in \mathrm{Ker}\lambda^\star$.

□

On pose pour tout nombre entier N strictement positif et tout $a \in \mathbb{F}_p$,

$$U_N(a) = |\{X \in \mathbf{A}\ ; \deg X < N \text{ et } f^\star(X^2) = a\}|. \tag{3.1}$$

Proposition 3.2 *Soient $(u_1, \dots, u_d)$ l'élément non nul de F^d tel que pour $(x_0, \dots, x_{d-1}) \in F^d$,*

$$\lambda(x_0, \dots, x_{d-1}) = u_1 x_0 + \cdots + u_d x_{d-1}$$

et $(z_{-m})_{m\geq 1}$ la suite d'éléments de F définie par

$$\frac{Y_\lambda}{Q-1} = \sum_{m=1}^{\infty} z_{-m} T^{-m},$$

où

$$Y_\lambda = [(Q-1)(u_1 T^{-1} + u_2 T^{-2} + \cdots + u_d T^{-d})].$$

Soit φ la forme quadratique à d variables définie sur F^d par

$$\varphi(x_0, \dots, x_{d-1}) = \sum_{k=0}^{2d-2} z_{-k-1} \Big(\sum_{i+j=k} x_i x_j \Big).$$

Alors,
(i) la forme φ n'est pas nulle ;
(ii) pour tout $a \in \mathbb{F}_p$ et tout nombre entier $N > d$, on a

$$U_N(a) = q^{N-d} |\{(x_0, \dots, x_{d-1}) \in F^d\ ;\ \mathrm{tr}(\varphi(x_0, \dots, x_{d-1})) = a\}|.$$

Preuve. Posons $D = Q - 1$. La forme linéaire λ n'étant pas nulle, elle est surjective. La trace l'étant aussi, $\lambda^\star$ est surjective et il existe $R \in \mathcal{C}_Q$ tel que $\lambda^\star(R) = a$. Soit $X \in \mathbf{A}$ tel que $\deg X < N$. Comme

$$\mathrm{Ker} f^\star = \mathrm{Ker}\lambda^\star + (Q-1) = \mathrm{Ker}\lambda^\star + (D),$$

on en déduit

$$U_N(a) = \sum_{A \in \mathrm{Ker}\lambda^\star} |\{X \in \mathbf{A}\ ; \deg X < N \text{ et } X^2 \equiv R + A \pmod D\}|.$$

Supposons $N > d$. La division euclidienne par D nous donne l'égalité

$$|\{X \in \mathbf{A}\ ; \deg X < N \text{ et } X^2 \equiv R + A \pmod D\}| = q^{N-d} v(R, A),$$

où

$$v(R, A) = |\{X \in \mathcal{C}_D;\ X^2 \equiv R + A \pmod D\}|.$$

Si $A \in \mathrm{Ker}\lambda^\star$, on a par orthogonalité,

$$v(R,A) = \sum_{X \in \mathcal{C}_D} \frac{1}{\langle D \rangle} \sum_{Y \in \mathcal{C}_D} E(\frac{(X^2 - R - A)Y}{D}),$$

d'où avec (3.1)

$$q^{2d-N} U_N(a) = \sum_{Y \in \mathcal{C}_D} E(-\frac{RY}{D}) \sum_{X \in \mathcal{C}_D} E(\frac{X^2 Y}{D}) \sigma_Y, \tag{3.2}$$

où

$$\sigma_Y = \sum_{A \in \mathrm{Ker}\lambda^\star} E(-\frac{AY}{D}).$$

Pour tout $Y \in \mathcal{C}_D$, l'application $A \to E(-\frac{AY}{D})$ est un caractère du groupe additif $\mathrm{Ker}\lambda^\star$ et la somme σ_Y vaut donc 0 ou $|\mathrm{Ker}\lambda^\star| = q^d/p$. D'autre part,

$$\sum_{Y \in \mathcal{C}_D} \sum_{A \in \mathrm{Ker}\lambda^\star} E(-\frac{AY}{D}) = \sum_{A \in \mathrm{Ker}\lambda^\star} \sum_{Y \in \mathcal{C}_D} E(-\frac{AY}{D}) = q^d$$

et donc, il y a exactement $q^d/|\mathrm{Ker}\lambda^\star| = p$ polynômes $Y \in \mathcal{C}_D$ pour lesquels la somme σ_Y est non nulle. Déterminons ces polynômes.

Comme $Y_\lambda = [D(u_1 T^{-1} + u_2 T^{-2} + \cdots + u_d T^{-d}]$, on a $v_\infty(\frac{Y_\lambda}{D} - (u_1 T^{-1} + u_2 T^{-2} + \cdots + u_d T^{-d})) > d$. Donc, pour tout $A \in \mathcal{C}_D$ et tout $b \in \mathbb{F}_p$ on a $v_\infty(b(\frac{Y_\lambda}{D} - (u_1 T^{-1} + u_2 T^{-2} + \cdots + u_d T^{-d}))A) > 1$ d'où $E(b\frac{Y_\lambda A}{D}) = E(b(u_1 T^{-1} + u_2 T^{-2} + \cdots + u_d T^{-d})A)$. Si $A = \sum_{i=0}^{d-1} a_i T^i$, alors

$$E(b\frac{Y_\lambda A}{D}) = \mathrm{e}(\frac{\mathrm{tr}(b(u_1 a_0 + \cdots + u_d a_{d-1}))}{p}) = \mathrm{e}(\frac{b\mathrm{tr}(u_1 a_0 + \cdots + u_d a_{d-1})}{p}).$$

En particulier, $E(\frac{bY_\lambda A}{D}) = 1$ pour tout $b \in \mathbb{F}_p$ et tout $A \in \mathrm{Ker}\lambda^\star$. Par suite, pour tout $b \in \mathbb{F}_p$, la somme σ_{bY_λ} est non nulle. Les p polynômes $Y \in \mathcal{C}_D$ pour lesquels $\sigma_Y \neq 0$ sont donc les polynômes bY_λ, b décrivant $\mathbb{F}_p$. Avec (3.2) il vient

$$pq^{d-N} U_N(a) = \sum_{b \in \mathbb{F}_p} E(-\frac{bRY_\lambda}{D}) \sum_{X \in \mathcal{C}_D} E(\frac{bX^2 Y_\lambda}{D}) = \sum_{X \in \mathcal{C}_D} \Theta_X, \tag{3.3}$$

où

$$\Theta_X = \sum_{b \in \mathbb{F}_p} E(b(\frac{Y_\lambda(X^2 - R)}{D})). \tag{3.4}$$

Les sommes Θ_X valent 0 ou p. Posons

$$R = \rho_0 + \rho_1 T + \cdots + \rho_{2d-2} T^{2d-2} \text{ avec } \rho_d = \rho_{d+1} = \cdots = \rho_{2d-2} = 0.$$

Pour $X = \sum_{i=0}^{d-1} x_i T^i$ appartenant à $\mathcal{C}_D$,

$$E(bY_\lambda(X^2 - R)/D)) = \mathrm{e}(\mathrm{tr}(\sum_{k=0}^{2d-2} z_{-k-1}(\sum_{i+j=k} x_i x_j - \rho_k))/p).$$

D'après (3.4), on a

$$\Theta_X = p \Leftrightarrow \mathrm{tr}(\sum_{k=0}^{2d-2} z_{-k-1}(\sum_{i+j=k} x_i x_j - \rho_k)) = 0,$$

soit en posant

$$\varphi(x_0, \ldots, x_{d-1}) = \sum_{k=0}^{2d-2} z_{-k-1}(\sum_{i+j=k} x_i x_j) \text{ et } b(a) = \sum_{k=0}^{d-1} z_{-k-1}\rho_k,$$

$$\Theta_X = p \Leftrightarrow \mathrm{tr}(\varphi(x_0, \ldots, x_{d-1}) - b(a)) = 0.$$

Observons que dans l'écriture

$$\frac{Y_\lambda}{D} = \sum_{m=1}^{\infty} z_{-m} T^{-m}$$

on a $z_{-m} = u_m$ pour $m = 1, \ldots, d$. Cela montre d'une part que la forme φ n'est pas nulle et que d'autre part

$$b(a) = \sum_{k=0}^{d-1} u_{-k-1}\rho_k = \lambda(\rho_0, \ldots, \rho_{d-1}).$$

On a donc $\mathrm{tr}(b(a)) = a$, d'où, avec (3.3),

$$q^{d-N} U_N(a) = |\{(x_0, \ldots, x_{d-1}) \in F^d \ \ \mathrm{tr}(\varphi(x_0, \ldots, x_{d-1}) = a\}|,$$

ce qui est le résultat annoncé.

□

On s'intéresse maintenant aux fonctions Q-additives à valeurs entières.

Proposition 3.3 *Soit $f \in \mathcal{D}$. Alors, pour tout nombre entier k, on a*

$$|\sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\frac{k}{p}f(X^2))| >> q^N,$$

la constante impliquée par le symbole $>>$ ne dépendant que de q, Q et f.

Preuve. Posons

$$S_k(N) = \sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\frac{k}{p}f(X^2)).$$

La fonction f étant à valeurs entières, on peut supposer $0 \leq k < p$. Si $k = 0$, alors $S_k(N) = q^N$. Il reste à prouver la proposition dans le cas où $0 < k < p$, ce que l'on supposera maintenant. Comme $f \in \mathcal{D}$, on a $w = f_{|\mathcal{C}_Q} \in \mathcal{L}$. Il existe λ, application linéaire non nulle de F^d dans F telle que pour tout $X \in \mathcal{C}_{\mathcal{Q}}$, $\lambda^\star(X)$ soit la classe de $w(X)$ modulo p. Par Q-additivité, pour tout $X \in \mathbf{A}$, la classe de $f(X)$ modulo p est $f^\star(X)$. Donc,

$$S_k(N) = \sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\frac{k}{p}(f(X^2)) = \sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\frac{k}{p}f^\star(X^2)) = \sum_{a\in\mathbb{F}_p} \mathrm{e}(\frac{ak}{p})U_N(a).$$

Si l'on suppose $N > d$, il s'en suit que

$$S_k(N) = q^{N-d}\sum_{a\in\mathbb{F}_p} \mathrm{e}(\frac{ak}{p})u(a).$$

La forme φ_λ n'est pas nulle. Soit $r \in [1, d]$ son rang et δ son discriminant. Elle est équivalente à une forme diagonale $\phi(y_1, \ldots, y_d) = y_1^2 + \cdots + y_{r-1}^2 + a_r y_r^2$ où a_r est un élément non nul de F. Par suite, pour tout $a \in \mathbb{F}_p$, on a

$$u(a) = q^{d-r}\nu(a),$$

où

$$\nu(a) = |\{(y_1, \ldots, y_r \in F^r \ \ \mathrm{tr}(\theta(y_1, \ldots, y_r)(\theta(y_1, \ldots, y_r)) = a\}|$$

et

$$\theta(y_1, \ldots, y_r) = y_1^2 + \cdots + y_{r-1}^2 + a_r y_r^2.$$

On a donc

$$\nu(a) = \sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}} n_\theta(x),$$

où

$$n_\theta(x) = |\{(y_1,\dots,y_r \in F^r \ \ \theta(y_1,\dots,y_r) = x\}|.$$

Les propositions 6.26 et 6.27 de [11] nous donnent les valeurs des nombres $n_\theta(x)$. Pour cela, notons η le caractère quadratique du corps F et remarquons que $|\mathrm{Ker(tr)}| = q/p$. .

Supposons d'abord r pair. La proposition 6.26 de [11] nous donne

$$n_\theta(x) = q^{r-1} + v(x)q^{(r-2)/2)}\eta((-1)^{r/2}\delta) \text{ avec } v(x) = \begin{cases} -1 \text{ si } x \neq 0, \\ q-1 \text{ si } x = 0. \end{cases}$$

Si $a \neq 0$, les $x \in F$ intervenant dans la somme $\nu(a)$ sont non nuls. Si $a = 0$, 0 intervient dans la somme $\nu(a)$ et il y a exactement $\frac{q}{p} - 1$ éléments x non nuls intervenant dans $\nu(a)$. D'où,

$$S_k(N) = q^{N-r}(\frac{q}{p}(q^{r-1} - q^{(r-2)/2}\eta((-1)^{r/2}\delta)) \sum_{\substack{a\in\mathbb{F}_p\\ a\neq 0}} \mathrm{e}(\frac{ak}{p})$$

$$+(\frac{q}{p}-1)(q^{r-1} - q^{(r-2)/2}\eta((-1)^{r/2}\delta)) + q^{r-1} + (q-1)q^{(r-2)/2}\eta((-1)^{r/2}\delta))$$

$$= q^{N-r}(\frac{q}{p}(q^{r-1} - q^{(r-2)/2)}\eta((-1)^{r/2}\delta)) \sum_{a\in\mathbb{F}_p} \mathrm{e}(\frac{ak}{p}) + q^{r/2}\eta((-1)^{r/2}\delta))$$

$$= q^{N-r/2}\eta((-1)^{r/2}\delta)),$$

ce qui donne le résultat annoncé lorsque r est pair.

Supposons maintenant r impair. La proposition 6.27 de [11] nous donne

$$n_\theta(x) = q^{r-1} + q^{(r-1)/2)}\eta((-1)^{(r-1)/2}x\delta),$$

d'où

$$S_k(N) = q^{N-r}\sum_{a\in\mathbb{F}_p} \mathrm{e}(\frac{ak}{p})(\frac{q^r}{p} + q^{(r-1)/2)}\eta((-1)^{(r-1)/2}\delta) \sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}} \eta(x),$$

$$= q^{N-(r+1)/2}\eta((-1)^{(r-1)/2}\delta)\sum_{a\in\mathbb{F}_p}\mathrm{e}(\frac{ak}{p})\sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}}\eta(x).$$

Posons

$$\sigma=\sum_{a\in\mathbb{F}_p}\mathrm{e}(\frac{ak}{p})\sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}}\eta(x).$$

On a

$$\sigma=\frac{q}{p}\sum_{a\in\mathbb{F}_p}\mathrm{e}(\frac{ak}{p})+\sum_{a\in\mathbb{F}_p}\mathrm{e}(\frac{ak}{p})\sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}}\eta(x)$$

$$=\sum_{a\in\mathbb{F}_p}\mathrm{e}(\frac{ak}{p})\sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}}(1+\eta(x))=\sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}}\mathrm{e}(\frac{\mathrm{tr}(x)k}{p})(1+\eta(x))$$

$$=\sum_{\substack{x\in F\\ \mathrm{tr}(x)=a}}\mathrm{e}(\frac{\mathrm{tr}(x)k}{p})|\{y\in F;\ y^2=x\}|=\sum_{y\in F}\mathrm{e}(\frac{\mathrm{tr}(y^2)k}{p})=\sum_{y\in F}\psi(ky^2),$$

ψ étant le caractère additif de F défini dans l'introduction. On a $|\sigma|=q^{1/2}$ (voir par exemple [11, Théorème 5.15]) et il s'en suit que

$$|S_k(N)|=q^{N-r/2},$$

ce qui donne le résultat annoncé lorsque r est impair.

□

4 Transformées de Fourier des fonctions Q-additives tronquées

Dans ce paragraphe ainsi que dans les paragraphes suivants w est une application de $\mathcal{C}_Q$ dans $\mathbb{Z}$ n'appartenant pas à l'ensemble $\mathcal{L}$. On note encore w la fonction Q-additive non dégénérée prolongeant w à $\mathbf{A}$. On introduit les

fonctions tronquées. Soient λ et μ des nombres entiers tels que $0 \leq \mu \leq \lambda$. Pour tout $X \in \mathbf{A}$ dont le développement en base Q est

$$X = \sum_{i=0}^{\infty} X_i Q^i,$$

on définit $w_\lambda(X)$ et $w_{\mu,\lambda}(X)$ par

$$w_\lambda(X) = \sum_{n=0}^{\lambda-1} w(X_n), \quad w_{\mu,\lambda}(X) = \sum_{n=\mu}^{\lambda-1} w(X_n). \tag{4.1}$$

Soit $\alpha \in \mathbb{R}$, fixé. On pose pour tout $H \in \mathbf{A}$,

$$F_\lambda(H) = F_\lambda^{(w)}(\alpha, H) = \langle Q \rangle^{-\lambda} \sum_{X \in \mathcal{C}_{Q^\lambda}} \mathrm{e}(\alpha w_\lambda(X)) E(-\frac{HX}{Q^\lambda}), \tag{4.2}$$

$$F_{\mu,\lambda}(H) = F_{\mu,\lambda}^{(w)}(\alpha, H) = \langle Q \rangle^{-\lambda} \sum_{X \in \mathcal{C}_{Q^\lambda}} \mathrm{e}(\alpha w_{\mu,\lambda}(X)) E(-\frac{HX}{Q^\lambda}). \tag{4.3}$$

Bien qu'élémentaire la proposition suivante sera très utilisée dans la suite de ce travail.

Proposition 4.1 *Soit un nombre entier $\lambda \geq 0$.*
(i) Si $X \in \mathcal{C}_{Q^\lambda}$, alors $w_\lambda(X) = w(X)$.
(ii) Si $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in C_Q$, alors $w_{\lambda+1}(QX + Y) = w_\lambda(X) + w(Y) = w(X) + w(Y)$.
(iii) Si $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in \mathbf{A}$, alors $w_\lambda(X + YQ^\lambda) = w(X) = w_\lambda(X)$.
(iv) Si μ est un nombre entier tel que $\mu < \lambda$, si $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$ et si $Z \in \mathcal{C}_{Q^\mu}$, alors $w_{\mu,\lambda}(YQ^\mu + Z) = w(Y) = w_{\lambda-\mu}(Y)$.
(v) Si $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in \mathbf{A}$, alors $F_\lambda(X + YQ^\lambda) = F_\lambda(X)$.
(vi) Si $X \in \mathbf{A}$ et $Y \in \mathbf{A}$ sont congrus modulo Q^λ, alors, $F_\lambda(X) = F_\lambda(Y)$.
(vii) Si μ est un nombre entier tel que $\mu < \lambda$, si $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$ et si $Z \in \mathcal{C}_{Q^\mu}$, alors $F_{\mu,\lambda}(YQ^\mu + Z) = F_{\lambda-\mu}(Y)$.

Preuve. Les points (i), (iii), et (iv) sont évidents ; (v) et (vii) découlent de (4.2), (iii) et de la définition du caractère E ; (vi) est une conséquence de (v). Pour démontrer (ii), il suffit de vérifier que pour $X \in \mathcal{C}_{Q^\lambda}$ et $Y \in \mathcal{C}_Q$ on a $w_{\lambda+1}(QX + Y) = w(QX + Y) = w(X) + w(Y) = w(X) + w(Y) = w_\lambda(X) + w(Y)$.

□

Proposition 4.2 *On a*

$$F_0(H) = 1,$$

et pour tout nombre entier $\lambda \geq 1$, on a

$$\langle Q\rangle^{\lambda} F_\lambda(H) = \prod_{j=1}^{\lambda} \phi_j(Q, w, \alpha, H),$$

les fonctions ϕ_j étant définies par (2.8).

Preuve. Utilisant la proposition 4.1-(ii), la preuve est analogue à celle de la relation (17) de [12].

□

Proposition 4.3 *Soient un nombre entier $\lambda > 0$ et $H \in \mathbf{A}$. Alors,*

$$|F_\lambda(H)| \leq \langle Q\rangle^{-C(Q,w,\alpha)\lambda}, \tag{4.4}$$

avec

$$C(Q, w, \alpha) = \frac{c_{Q,w,\alpha}}{\langle Q\rangle \deg Q \log q}, \tag{4.5}$$

où $c_{Q,w,\alpha}$ est défini dans la Proposition 2.5.

Preuve. La proposition précédente donne le résultat quand $\lambda = 0$. Lorsque $\lambda > 0$, la proposition 4.2 jointe à la majoration (2.9) donne

$$|F_\lambda(H)| = \langle Q\rangle^{-\lambda} \prod_{j=1}^{\lambda} |\phi_j(Q, w, \alpha, H)| \leq (1 - \frac{c_{Q,w,\alpha}}{\langle Q\rangle})^{\lambda}.$$

Soit $C = C_{Q,w,\alpha} = c_{Q,w,\alpha}/\langle Q\rangle \log\langle Q\rangle$. Alors, $C \log\langle Q\rangle \leq \log\left(\frac{1}{1-c_{Q,w,\alpha}/\langle Q\rangle}\right)$, d'où $1 - c_{Q,w,\alpha}/\langle Q\rangle \leq \langle Q\rangle^{-C}$.

□

Proposition 4.4 *Soient $A \in \mathbf{A}$ et δ et λ des nombres entiers tels que $0 \leq \delta \leq \lambda$. Alors,*

$$\sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A (\mathrm{mod} Q^\delta)}} |F_\lambda(X)|^2 = |F_\delta(A)|^2.$$

Preuve. Utilisant la proposition 4.1-(ii), la preuve est analogue à celle du lemme 19 de [13].

□

Proposition 4.5 *Soient λ et μ des nombres entiers tels que $0 \leq \mu < \lambda$. Alors, pour tout $H \in \mathbf{A}$, on a*

$$\langle Q\rangle^{\mu} F_{\mu,\lambda}(H) = F_{\lambda-\mu}(H) S(\frac{H}{Q^{\lambda}}, \mu \deg Q).$$

Preuve. Utilisant la proposition 4.1-(iv), la preuve est analogue à celle à celle du lemme 10 de [12].

□

Proposition 4.6 *Soient λ et μ des nombres entiers tel que $0 \leq \mu < \lambda$. Alors,*

$$\sum_{X \in \mathcal{C}_{Q^{\lambda}}} |F_{\mu,\lambda}(X)| = \sum_{R \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(R)| \leq \langle Q\rangle^{\lambda-\mu}.$$

Preuve. Ici on fait la division euclidienne par $Q^{\lambda-\mu}$ des polynômes $X \in \mathcal{C}_{Q^{\lambda}}$, Avec la proposition précédente, il vient

$$\langle Q\rangle^{\mu} \sum_{X \in \mathcal{C}_{Q^{\lambda}}} |F_{\mu,\lambda}(X)| = \sum_{\substack{R \in \mathcal{C}_{Q^{\lambda-\mu}} \\ L \in \mathcal{C}_{Q^{\mu}}}} |F_{\lambda-\mu}(R+LQ^{\lambda-\mu})||S(\frac{R+LQ^{\lambda-\mu}}{Q^{\lambda}}, \mu \deg Q)| =$$

$$\sum_{\substack{R \in \mathcal{C}_{Q^{\lambda-\mu}} \\ L \in \mathcal{C}_{Q^{\mu}}}} |F_{\lambda-\mu}(R+LQ^{\lambda-\mu})| S(\frac{R+LQ^{\lambda-\mu}}{Q^{\lambda}}, \mu \deg Q)$$

puisque d'après la proposition 2.1, les sommes $S(\frac{R+LQ^{\lambda-\mu}}{Q^{\lambda}}, \mu \deg Q)$ sont positives ou nulles. La partie (v) de la proposition 4.1 nous donne ensuite

$$\langle Q\rangle^{\mu} \sum_{H \in \mathcal{C}_{Q^{\lambda}}} |F_{\mu,\lambda}(H)| = \sum_{R \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(R)| \sum_{L \in \mathcal{C}_{Q^{\mu}}} S(\frac{R+LQ^{\lambda-\mu}}{Q^{\lambda}}, \mu \deg Q).$$

Or,

$$\sum_{L \in \mathcal{C}_{Q^{\mu}}} S(\frac{R+LQ^{\lambda-\mu}}{Q^{\lambda}}, \mu \deg Q) = \sum_{L \in \mathcal{C}_{Q^{\mu}}} \sum_{X \in \mathcal{C}_{Q^{\mu}}} E((\frac{R}{Q^{\lambda}} + \frac{L}{Q^{\mu}})X)$$

$$= \sum_{X \in \mathcal{C}_{Q^\mu}} E(\frac{RX}{Q^\lambda}) \sum_{L \in \mathcal{C}_{Q^\mu}} E(\frac{LX}{Q^\mu}) = \langle Q \rangle^\mu$$

d'après le corollaire 2.2. En reportant cette égalité dans la somme précédente, on obtient

$$\sum_{H \in \mathcal{C}_{Q^\lambda}} |F_{\mu,\lambda}(H)| = \sum_{R \in \mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(R)|$$

et on majore trivialement $|F_{\lambda-\mu}(R)|$ par 1.

□

Proposition 4.7 *Soient λ, δ et μ des nombres entiers tels que $1 \leq \mu < \lambda, \lambda - \mu \leq \delta \leq \lambda$. Si $A \in \mathbf{A}$, alors*

$$\sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A \pmod{Q^\delta}}} |F_{\mu,\lambda}(X)| = \begin{cases} |F_{\lambda-\mu}(A)| & \text{si } v_\infty(\{A/Q^\delta\}) > (\mu + \delta - \lambda) \deg Q, \\ 0 & \text{sinon.} \end{cases}$$

Preuve. Soit $R \in \mathcal{C}_{Q^\delta}$ congru à A modulo Q^δ. Alors A et R sont congrus modulo $Q^{\lambda-\mu}$. Les polynômes $X \in \mathcal{C}_{Q^\lambda}$ congrus à A modulo Q^δ sont de la forme $X = R + LQ^\delta$ avec $L \in \mathcal{C}_{Q^{\lambda-\delta}}$; ils sont congrus à R modulo $Q^{\lambda-\mu}$ et vérifient, d'après la proposition 4.5, la relation

$$\langle Q \rangle^\mu F_{\mu,\lambda}(X) = F_{\lambda-\mu}(R) S(\frac{R + LQ^\delta}{Q^\lambda}, \mu \deg Q).$$

La positivité des sommes $S(\frac{R+LQ^\delta}{Q^\lambda}, \mu \deg Q)$ jointe à la proposition 4.1-(vi) permet d'écrire

$$\langle Q \rangle^\mu \sum_{\substack{X \in \mathcal{C}_{Q^\lambda} \\ X \equiv A (\mathrm{mod} Q^\delta)}} |F_{\mu,\lambda}(X)| = |F_{\lambda-\mu}(A)| \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} S(\frac{R}{Q^\lambda} + \frac{L}{Q^{\lambda-\delta}}, \mu \deg Q).$$

Par ailleurs,

$$\sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} S(\frac{R}{Q^\lambda} + \frac{L}{Q^{\lambda-\delta}}, \mu \deg Q) = \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} \sum_{X \in \mathcal{C}_{Q^\mu}} E((\frac{R}{Q^\lambda} + \frac{L}{Q^{\lambda-\delta}})X)$$

$$= \sum_{X \in \mathcal{C}_{Q^\mu}} E(\frac{RX}{Q^\lambda}) \sum_{L \in \mathcal{C}_{Q^{\lambda-\delta}}} E(\frac{LX}{Q^{\lambda-\delta}}) = \langle Q \rangle^{\lambda-\delta} \sum_{\substack{X \in \mathcal{C}_{Q^\mu} \\ X \equiv 0 (\mathrm{mod} Q^{\lambda-\delta})}} E(\frac{RX}{Q^\lambda}).$$

D'après le corollaire 2.2, la proposition 2.1 donne alors

$$\sum_{L\in\mathcal{C}_{Q^{\lambda-\delta}}} S(\frac{R}{Q^\lambda}+\frac{L}{Q^{\lambda-\delta}},\mu\deg Q)$$

$$=\langle Q\rangle^{\lambda-\delta}\times\begin{cases}\langle Q\rangle^{\mu+\delta-\lambda} & \text{si}\quad v_\infty(R/Q^\delta)>(\mu+\delta-\lambda)\deg Q,\\ 0 & \text{sinon.}\end{cases}$$

On a donc

$$\sum_{\substack{H\in\mathcal{C}_{Q^\lambda}\\ H\equiv A(\mathrm{mod}Q^\delta)}} |F_{\mu,\lambda}(H)|=|F_{\lambda-\mu}(A)|\times\begin{cases}1 & \text{si}\quad v_\infty(R/Q^\delta)>(\mu+\delta-\lambda)\deg Q,\\ 0 & \text{sinon}\end{cases}$$

et on conclut en observant que $v_\infty(R/Q^\delta)=v_\infty(\{A/Q^\delta\})$.

□

Proposition 4.8 *Soient λ,δ et μ des nombres entiers tels que $1\le\mu<\lambda$ et $\delta\le\lambda-\mu$. Si $(A,L)\in\mathbf{A}^2$, alors*

$$\sum_{\substack{X\in\mathcal{C}_{Q^\lambda}\\ X\equiv A(\mathrm{mod}Q^\delta)}} |F_{\mu,\lambda}(X)F_{\lambda-\mu}(X+L)|\le|F_\delta(A)||F_\delta(A+L)|.$$

Preuve. Notons B la somme à majorer et $R\in\mathcal{C}_{Q^\delta}$ le reste de A modulo Q^δ. Les polynômes $X\in\mathcal{C}_{Q^\lambda}$ congrus à R modulo Q^δ sont de la forme $X=Y+ZQ^{\lambda-\mu}$ avec $Y\in\mathcal{C}_{Q^{\lambda-\mu}}, Y\equiv R\pmod{Q^\delta}$ et $Z\in\mathcal{C}_{Q^\mu}$. D'après les propositions 4.5 et 4.1-(v), on obtient comme ci-dessus

$$\langle Q\rangle^\mu B=\sum_{\substack{Y\in\mathcal{C}_{Q^{\lambda-\mu}}\\ Y\equiv R(\mathrm{mod}Q^\mu)}} |F_{\lambda-\mu}(Y)||F_{\lambda-\mu}(L+Y)|\sum_{Z\in\mathcal{C}_{Q^\mu}} S(\frac{Y}{Q^\lambda}+\frac{Z}{Q^\mu}),\mu\deg Q).$$

Mais, pour tout $Y\in\mathcal{C}_{Q^{\lambda-\mu}}$, on a

$$\sum_{Z\in\mathcal{C}_{Q^\mu}} S(\frac{Y}{Q^\lambda}+\frac{Z}{Q^\mu}),\mu\deg Q)=\sum_{Z\in\mathcal{C}_{Q^\mu}}\sum_{W\in\mathcal{C}_{Q^\mu}} E((\frac{Y}{Q^\lambda}+\frac{Z}{Q^\mu})W)$$

$$=\sum_{W\in\mathcal{C}_{Q^\mu}} E(\frac{YW}{Q^\lambda})\sum_{Z\in\mathcal{C}_{Q^\mu}} E(\frac{ZW}{Q^\mu})=\langle Q\rangle^\mu$$

d'après le corollaire 2.2. On a donc,

$$B = \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R (\mathrm{mod} Q^{\mu})}} |F_{\lambda-\mu}(Y)||F_{\lambda-\mu}(L+Y)|$$

L'inégalité de Cauchy-Schwarz donne

$$B^2 \leq \Big(\sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R (\mathrm{mod} Q^{\delta})}} |F_{\lambda-\mu}(Y)|^2 \Big) \Big(\sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R (\mathrm{mod} Q^{\delta})}} |F_{\lambda-\mu}(L+Y)|^2 \Big).$$

Notons V le reste de L modulo $Q^{\lambda-\mu}$. Pour tout $Y \in \mathcal{C}_{Q^{\lambda-\mu}}$, on a avec la proposition 4.1-(vi) $F_{\lambda-\mu}(L+Y) = F_{\lambda-\mu}(V+Y)$, d'où

$$\sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R (\mathrm{mod} Q^{\delta})}} |F_{\lambda-\mu}(L+Y)|^2 = \sum_{\substack{Y \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Y \equiv R (\mathrm{mod} Q^{\delta})}} |F_{\lambda-\mu}(V+Y)|^2$$

$$= \sum_{\substack{Z \in \mathcal{C}_{Q^{\lambda-\mu}} \\ Z \equiv V+R (\mathrm{mod} Q^{\delta})}} |F_{\lambda-\mu}(Z)|^2.$$

La proposition 4.4 donne alors

$$B^2 \leq |F_{\delta}(R)|^2 |F_{\delta}(V+R)|^2$$

On conclut en remarquant que puisque $R \equiv A \pmod{Q^{\delta}}$ et $V + R \equiv L + A \pmod{Q^{\delta}}$, on a $F_{\delta}(R) = F_{\delta}(A), F_{\delta}(R+V) = F_{\delta}(A+L)$.

□

Proposition 4.9 *Soient λ, δ et μ des nombres entiers tels que $1 \leq \mu < \lambda, \lambda - \mu \leq \delta \leq \lambda$. Si $A \in \mathbf{A}$, alors*

$$\sum_{\substack{X,Y \in \mathcal{C}_{Q^{\lambda}} \\ X-Y \equiv A (\mathrm{mod} Q^{\delta})}} |F_{\mu,\lambda}(X) F_{\mu,\lambda}(Y)| \leq \begin{cases} 1 & \textit{si} \quad v_{\infty}(\{A/Q^{\delta}\}) > (\mu + \delta - \lambda) \deg Q, \\ 0 & \textit{sinon.} \end{cases}$$

Preuve. Posons

$$B' = \sum_{\substack{X,Y\in\mathcal{C}_{Q^\lambda}\\ X-Y\equiv A(\mathrm{mod}Q^\delta)}} |F_{\mu,\lambda}(X)F_{\mu,\lambda}(Y)|.$$

Alors avec les proposition 4.5 et 2.1, il vient

$$B' = \sum_{\substack{Y\in\mathcal{C}_{Q^\lambda}\\ X\equiv A+Y(\mathrm{mod}Q^\delta)\\ v_\infty(\frac{R(Y)}{Q^\lambda})>\mu\deg Q}} |F_{\mu,\lambda}(Y)||F_{\lambda-\mu}(R(Y))|.$$

Comme $\delta \geq \lambda - \mu$, la proposition 4.1-(vi) nous donne

$$B' = \sum_{\substack{Y\in\mathcal{C}_{Q^\lambda}\\ X\equiv A+Y(\mathrm{mod}Q^\delta)\\ v_\infty(\frac{R(Y)}{Q^\lambda})>\mu\deg Q}} |F_{\mu,\lambda}(Y)||F_{\lambda-\mu}(A+Y))|. \qquad (\star)$$

Soit $A' \in \mathcal{C}_{Q^\delta}$ congru à A modulo Q^δ. Pour $Y \in \mathcal{C}_{Q^\lambda}$ on a

$$v_\infty(\{\frac{R(Y)}{Q^\lambda}\}) > \mu\deg Q \Leftrightarrow v_\infty(\{\frac{A+Y}{Q^\delta}\}) > (\mu+\delta-\lambda)\deg Q.$$

Un tel Y s'écrit $Y = R + ZQ^\delta$ avec $R \in \mathcal{C}_{Q^\delta}$ et $Z \in \mathcal{C}_{Q^{\lambda-\delta}}$, ce qui donne $\{\frac{A+Y}{Q^\delta}\} = \frac{A'+V}{Q^\delta}$. On a alors

$$v_\infty(\{\frac{R(y)}{Q^\lambda}\}) > \mu\deg Q \Leftrightarrow \deg(A'+V) < (\lambda-\mu)\deg Q.$$

La relation $(\star)$ devient

$$B' = \sum_{Z\in\mathcal{C}_{Q^{\lambda-\delta}}} \sum_{\substack{V\in\mathcal{C}_{Q^\delta}\\ A'+V\in\mathcal{C}_{Q^{\lambda-\mu}}}} |F_{\mu,\lambda}(V+ZQ^\delta)F_{\lambda-\mu}(A'+V+ZQ^\delta)|.$$

Comme $\lambda - \mu \leq \delta$, en posant $S = A' + V$, on obtient

$$B' = \sum_{Z\in\mathcal{C}_{Q^{\lambda-\delta}}} \sum_{S\in\mathcal{C}_{Q^{\lambda-\mu}}} |F_{\mu,\lambda}(S-A'+ZQ^\delta)F_{\lambda-\mu}(S+ZQ^\delta)|.$$

D'après la proposition 4.1-(vi), pour $S \in \mathcal{C}_{Q^{\lambda-\mu}}$, on a $F_{\lambda-\mu}(S+ZQ^{\delta}) = F_{\lambda-\mu}(S)$, d'où,

$$B' = \sum_{Z\in\mathcal{C}_{Q^{\lambda-\delta}}} \sum_{S\in\mathcal{C}_{Q^{\lambda-\mu}}} |F_{\mu,\lambda}(S-A'+ZQ^{\delta})F_{\lambda-\mu}(S)|$$

$$= \sum_{S\in\mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(S)| \sum_{Z\in\mathcal{C}_{Q^{\lambda-\delta}}} |F_{\mu,\lambda}(S-A'+ZQ^{\delta})|.$$

Lorsque Z décrit l'ensemble $\mathcal{C}_{Q^{\lambda-\delta}}$, le polynôme $S-A'+ZQ^{\delta}$ décrit l'ensemble des polynômes $X \in \mathcal{C}_{Q^{\lambda}}$ congrus à $S-A'$ modulo Q^{δ}. Par suite,

$$B' = \sum_{S\in\mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(S)| \sum_{\substack{X\in\mathcal{C}_{Q^{\lambda}} \\ X\equiv S-A'(\mathrm{mod}Q^{\delta})}} |F_{\mu,\lambda}(X)|.$$

La proposition 4.7 nous donne pour $S \in \mathcal{C}_{Q^{\lambda-\mu}}$ fixé,

$$\sum_{\substack{X\in\mathcal{C}_{Q^{\lambda}} \\ X\equiv S-A'(\mathrm{mod}Q^{\delta})}} |F_{\mu,\lambda}(X)| = \begin{cases} |F_{\lambda-\mu}(S-A')| & \text{si } v_{\infty}(\{\frac{S-A'}{Q^{\delta}}\}) > (\mu+\delta-\lambda)\deg Q, \\ 0 & \text{sinon.} \end{cases}$$

Par ailleurs on a

$$v_{\infty}(\{\frac{S-A'}{Q^{\delta}}\}) > (\mu+\delta-\lambda)\deg Q \Leftrightarrow \deg(S-A') < (\lambda-\mu)\deg Q$$

$$\Leftrightarrow \deg(A') < (\lambda-\mu)\deg Q.$$

Donc, si $\deg A' \geq (\lambda-\mu)\deg Q$, alors $B'=0$ et si $\deg A' < (\lambda-\mu)\deg Q$, alors

$$B' = \sum_{S\in\mathcal{C}_{Q^{\lambda-\mu}}} |F_{\lambda-\mu}(S)||F_{\lambda-\mu}(S-A')|$$

et la proposition 4.8 donne $B' \leq |F_0(0)||F_0(-A')| = 1$.

□

5 Majoration de la somme $\Sigma(N)$

Le nombre réel α étant toujours fixé. Soient un nombre entier $N>0$ et $\mathcal{X} = \mathcal{X}(N)$ l'ensemble des polynômes $X \in \mathbf{A}$ tels que

$$\nu \deg Q \leq \deg X < N, \tag{5.1}$$

où $\nu = \nu(N)$ est le nombre entier déterminé par la condition

$$\nu \deg Q < N \leq (\nu + 1) \deg Q. \tag{5.2}$$

Observons que l'ensemble $\mathcal{X}$ a au plus q^N éléments. Posons

$$\Sigma = \Sigma(N) = \sum_{X \in \mathcal{X}} \mathrm{e}(\alpha w(X^2)). \tag{5.3}$$

Nous supposerons N assez grand pour que $\nu(N) \geq 30 \deg Q$. Soient des nombres entiers r et m tels que

$$\begin{cases} 1 < r \leq \frac{\nu - 3}{5 \deg Q - 1} \quad (i) \\ m < \nu - r, \quad (ii) \\ m < \nu + r + 3 - 2r \deg Q, \quad (iii) \\ 2m > \nu + r(1 + \deg Q). \quad (iv) \end{cases} \tag{5.4}$$

Observons qu'à l'exception du cas $\deg Q = 1$, la condition (iii) implique la condition (ii). Observons aussi que la condition (i) assure la compatibilité des conditions (ii) et (iv) et celle des conditions (iii) et (iv). On pose

$$\ell = \nu + r + 1 \tag{5.5}$$

5.1 Utilisation des fonctions de poids tronquées

La proposition suivante est un analogue polynomial de l'inégalité de Van der Corput (Voir [6, Lemme 3.2]).

Proposition 5.1 *On a*

$$|\Sigma(N)|^2 \leq q^N \max_{R \in \mathcal{C}_{Q^r}} \Big| \sum_{X \in \mathcal{X}} \mathrm{e}\left(\alpha(w((X+R)^2)) - w(X^2))\right) \Big| \tag{5.6}$$

Preuve. Soit $R \in \mathcal{C}_{Q^r}$. Puisque $r < \nu$, l'application $X \to X + R$ est une permutation de l'ensemble $\mathcal{X}$. On a donc

$$\sum_{X \in \mathcal{X}} \mathrm{e}(\alpha w(X^2)) = \sum_{X \in \mathcal{X}} \mathrm{e}(\alpha w((X+R)^2)).$$

Par suite,

$$\langle Q \rangle^r \Sigma = \langle Q \rangle^r \sum_{X \in \mathcal{X}} \mathrm{e}(\alpha w(X^2)) = \sum_{R \in \mathcal{C}_{Q^r}} \sum_{X \in \mathcal{X}} \mathrm{e}(\alpha w((X+R)^2))$$

$$= \sum_{X\in\mathcal{X}} \sum_{R\in\mathcal{C}_{Q^r}} \mathrm{e}(\alpha w((X+R)^2)).$$

L'inégalité de Cauchy-Schwarz donne

$$\langle Q\rangle^{2r}|\Sigma|^2 \le |\mathcal{X}| \sum_{X\in\mathcal{X}} |\sum_{R\in\mathcal{C}_{Q^r}} \mathrm{e}(\alpha w((X+R)^2))|^2$$

$$\le q^N \sum_{X\in\mathcal{X}} \sum_{\substack{R_1\in\mathcal{C}_{Q^r}\\ R_2\in\mathcal{C}_{Q^r}}} \mathrm{e}\left(\alpha(w((X+R_1)^2) - w((X+R_2)^2))\right)$$

$$= q^N \sum_{\substack{R_1\in\mathcal{C}_{Q^r}\\ R_2\in\mathcal{C}_{Q^r}}} \sum_{X\in\mathcal{X}} \mathrm{e}\left(\alpha(w((X+R_1)^2) - w((X+R_2)^2))\right).$$

L'application $X \to Y = X + R_2$ est une permutation de $\mathcal{X}$ et l'application $R_1 \to R = R_1 - R_2$ est une permutation de $\mathcal{C}_{Q^r}$; donc,

$$\langle Q\rangle^{2r}|\Sigma|^2 \le q^N \sum_{\substack{R_2\in\mathcal{C}_{Q^r}\\ R\in\mathcal{C}_{Q^r}}} \sum_{Y\in\mathcal{X}} \mathrm{e}\left(\alpha(w((Y+R)^2) - w(Y^2))\right),$$

d'où,

$$\langle Q\rangle^{r}|\Sigma|^2 \le q^N \sum_{R\in\mathcal{C}_{Q^r}} \sum_{Y\in\mathcal{X}} \mathrm{e}\left(\alpha(w((Y+R)^2) - w(Y^2))\right)$$

$$\le q^N \langle Q\rangle^r \max_{R\in\mathcal{C}_{Q^r}} |\sum_{Y\in\mathcal{X}} \mathrm{e}\left(\alpha(w((Y+R)^2) - w(Y^2))\right).$$

□

On en déduit

Proposition 5.2 *On a*

$$|\Sigma(N)|^2 \le q^N \max_{R\in\mathcal{C}_{Q^r}} (|T(N,r,R)|), \tag{5.7}$$

où

$$T = T(N,r,R) = \sum_{X\in\mathcal{X}} \mathrm{e}\left(\alpha(w_\ell((X+R)^2)) - w_\ell(X^2))\right), \tag{5.8}$$

w_ℓ étant la fonction tronquée introduite à la section 4.

Preuve. Soient $X \in \mathcal{X}$ et $R \in \mathcal{C}_{Q^r}$. On a $\deg X < N \leq (\nu+1)\deg Q$, d'où $\deg(XR) \leq (\nu+r+1)\deg Q - 2 = \ell \deg Q - 2$. On a aussi $\deg(R^2) \leq 2r\deg Q - 2 \leq \ell \deg Q - 2$. Par suite, $\deg\left((X+R)^2 - X^2\right) \leq \ell \deg Q - 2$. Si $X^2 = \sum_{n=0}^{\infty} Y_n Q^n$ et $(X+R)^2 = \sum_{n=0}^{\infty} Z_n Q^n$ sont les représentations respectives de X^2 et $(X+R)^2$ en base Q, on a $Y_j = Z_j$ pour tout nombre entier $j \geq \ell$, d'où, avec (4.1), $w((X+R)^2) - w_\ell((X+R)^2) = w(X^2) - w_\ell(X^2)$ ou encore $w((X+R)^2) - w(X^2) = w_\ell((X+R)^2) - w_\ell(X^2)$. On conclut avec (5.6).

□

En appliquant une deuxième fois l'inégalité de Van der Corput, on obtient

Proposition 5.3 *Soit $R \in \mathcal{C}_{Q^r}$. Alors*

$$T^2(N,r,R) \leq q^N \max_{S \in \mathcal{C}_{Q^r}} U(N,r,m,R,S), \tag{5.9}$$

où

$$U(N,r,m,R,S) = \tag{5.10}$$

$$\Big|\sum_{X\in\mathcal{X}} \mathrm{e}\left(\alpha(w_{m,\ell}((X+R+SQ^m)^2) - w_{m,\ell}((X+R)^2) - w_{m,\ell}((X+SQ^m)^2) + w_{m,\ell}(X^2))\right)\Big|.$$

Preuve. Soit $S \in \mathcal{C}_{Q^r}$. Alors, avec (5.4-(ii)), $\deg(SQ^m) < (m+r)\deg Q < \nu \deg Q$. L'application $X \to X + SQ^m$ est donc une permutation de l'ensemble $\mathcal{X}$. De ce fait,

$$T = \sum_{X\in\mathcal{X}} \mathrm{e}(\alpha(w_\ell((X+R+SQ^m)^2) - w_\ell((X+SQ^m)^2))).$$

Par suite, on a

$$\langle Q\rangle^r T = \sum_{S\in\mathcal{C}_{Q^r}} \sum_{X\in\mathcal{X}} \mathrm{e}(\alpha(w_\ell((X+R+SQ^m)^2) - w_\ell((X+SQ^m)^2)))$$

$$= \sum_{X\in\mathcal{X}} \sum_{S\in\mathcal{C}_{Q^r}} \mathrm{e}(\alpha(w_\ell((X+R+SQ^m)^2) - w_\ell((X+SQ^m)^2)))$$

et l'inégalité de Cauchy-Schwarz donne

$$\langle Q\rangle^{2r}|T|^2 \leq q^N \sum_{X\in\mathcal{X}} \Big|\sum_{S\in\mathcal{C}_{Q^r}} \mathrm{e}(\alpha(w_\ell((X+R+SQ^m)^2) - w_\ell((X+SQ^m)^2)))\Big|^2$$

$$= q^N \sum_{X\in\mathcal{X}} \sum_{\substack{S_1\in\mathcal{C}_{Q^r}\\ S_2\in\mathcal{C}_{Q^r}}} \mathrm{e}\left(\theta_X(S_1)-\theta_X(S_2)\right),$$

où pour $S\in\mathcal{C}_{Q^r}$, $\theta_X(S)=\alpha(w_\ell((X+R+SQ^m)^2)-w_\ell((X+SQ^m)^2))$. En inversant l'ordre des sommations on obtient

$$\langle Q\rangle^{2r}|T|^2 \le q^N \sum_{\substack{S_1\in\mathcal{C}_{Q^r}\\ S_2\in\mathcal{C}_{Q^r}}} \sum_{X\in\mathcal{X}} \mathrm{e}\left(\theta_X(S_1)-\theta_X(S_2)\right).$$

Les applications $X\to Y=X+S_2Q^m$ et $S_1\to S=S_1-S_2$ sont des permutations de $\mathcal{X}$ et $\mathcal{C}_{Q^r}$ respectivement. Donc,

$$\langle Q\rangle^{2r}|T|^2 \le q^N \sum_{\substack{S_2\in\mathcal{C}_{Q^r}\\ S\in\mathcal{C}_{Q^r}}} \sum_{Y\in\mathcal{X}} \mathrm{e}\left(\theta_{Y-S_2Q^m}(S_2+S)-\theta_{Y-S_2Q^m}(S_2)\right),$$

d'où

$$\langle Q\rangle^{2r}|T|^2 \le q^N \sum_{S_2\in\mathcal{C}_{Q^r}} \sum_{S\in\mathcal{C}_{Q^r}} \sum_{Y\in\mathcal{X}} \mathrm{e}\left(\alpha(w_\ell((Y+R+SQ^m)^2)-w_\ell((Y+SQ^m)^2)\right.$$
$$\left.-w_\ell((Y+R)^2)+w_\ell(Y^2))\right),$$

ce qui nous donne

$$|T|^2 \le q^N \max_{S\in\mathcal{C}_{Q^r}} U(N,r,m,R,S),$$

avec

$$U=U(N,r,m,R,S)=|\sum_{Y\in\mathcal{X}} \mathrm{e}\left(\alpha(w_\ell((Y+R+SQ^m)^2)-w_\ell((Y+SQ^m)^2)\right.$$
$$\left.-w_\ell((Y+R)^2)+w_\ell(Y^2))\right)|.$$

Montrons que U vérifie l'égalité (5.10). Soient $Z\in\mathcal{X}$ et $S\in\mathcal{C}_{Q^r}$. Si $Z^2=\sum_{n=0}^{\infty} V_nQ^n$ et $(Z+SQ^m)^2=\sum_{n=0}^{\infty} W_nQ^n$ sont les représentations respectives de Z^2 et $(Z+SQ^m)^2$ en base Q, alors $V_j=W_j$ pour tout nombre entier $j<m$, d'où $w_m((Z+SQ^m)^2)=w_m(Z^2)$. D'autre part, $w_\ell(Z^2)=w_m(Z^2)+w_{m,\ell}(Z^2)$ et $w_\ell((Z+SQ^m)^2)=w_m((Z+SQ^m)^2)+w_{m,\ell}((Z+SQ^m)^2)$. Il s'en suit que

$$w_\ell((Z+SQ^m)^2)-w_\ell(Z^2)=w_{m,\ell}((Z+SQ^m)^2))-w_{m,\ell}(Z^2).$$

On reporte cette égalité dans la formule définissant U en prenant Z égal à $Y+R$ puis à Y et on obtient (5.10).

□

5.2 Fonction caractéristique des carrés

Proposition 5.4 *Pour R et S dans $\mathcal{C}_{Q^r}$, on a*

$$\langle Q\rangle^{\ell} U(N,r,m,R,S) \tag{5.11}$$

$$= |\sum_{L\in\mathcal{C}_{Q^m}} \sum_{X\in\mathcal{X}} E(-\frac{LX}{Q^{\ell}}) \sum_{(A,B,G,H)\in(\mathcal{C}_{Q^{\ell}})^4} F_{m,\ell}(A)F_{m,\ell}(-B)F_{m,\ell}(-G)F_{m,\ell}(H)\Lambda(L)|,$$

où

$$\Lambda(L) = \Lambda(N,r,R,S,L,A,B,G,H) = \tag{5.12}$$

$$\sum_{M\in\mathcal{C}_{Q^{\ell}}} E\left(\frac{(M+R+SQ^m)^2A + (M+R)^2B + (M+SQ^m)^2G + M^2H + LM}{Q^{\ell}}\right).$$

Preuve. On pose $U = U(N,r,m,R,S)$ et pour $X\in\mathcal{X}, Y\in\mathcal{C}_{Q^{\ell}}, \rho\in\{0,1\} et \sigma\in\{0,1\}$,

$$\Theta = \Theta(X,Y,\rho,\sigma) = \sum_{Z\in\mathcal{C}_{Q^{\ell}}} E\left(\frac{((X+\rho R+\sigma SQ^m)^2 - Y)Z}{Q^{\ell}}\right).$$

D'après le corollaire 2.2, on a

$$\Theta = \begin{cases} \langle Q\rangle^{\ell} & \text{si } Y\equiv (X+\rho R+\sigma SQ^m)^2 \pmod{Q^{\ell}}, \\ 0 & \text{sinon,} \end{cases}$$

d'où $\Theta = \overline{\Theta}$ et

$$\langle Q\rangle^{-\ell}\mathrm{e}(\alpha w_{m,\ell}(Y))\Theta = \begin{cases} \mathrm{e}(\alpha w_{m,\ell}(Y)) & \text{si } Y\equiv (X+\rho R+\sigma SQ^m)^2 \pmod{Q^{\ell}}, \\ 0 & \text{sinon.} \end{cases}$$

D'autre part, d'après la proposition 4.1-(iv), si $Y\equiv (X+\rho R+\sigma SQ^m)^2 \pmod{Q^{\ell}}$, alors $w_{m,\ell}(Y) = w_{m,\ell}((X+\rho R+\sigma SQ^m)^2)$. Par suite, pour $X\in\mathcal{X}$ et $(\rho,\sigma)\in\{0,1\}^2$, on a

$$\mathrm{e}(\alpha w_{m,\ell}((X+\rho R+\sigma SQ^m)^2)) = \sum_{Y\in\mathcal{C}_{Q^{\ell}}} \langle Q\rangle^{-\ell}\mathrm{e}(\alpha w_{m,\ell}(Y))\Theta(X,Y,\rho,\sigma).$$

On porte cette relation dans l'égalité (5.10). Il vient

$$\langle Q\rangle^{4\ell} U = |\sum_{X\in\mathcal{X}} \sum_{(Y,Z,V,W)\in(\mathcal{C}_{Q^{\ell}})^4} \mathrm{e}(\alpha w_{m,\ell}(Y))\Theta(X,Y,1,1)\mathrm{e}(-\alpha w_{m,\ell}(Z))\Theta(X,Z,1,0)$$

$$\times \mathrm{e}(-\alpha w_{m,\ell}(V))\Theta(X,V,0,1)\mathrm{e}(\alpha w_{m,\ell}(W))\Theta(X,W,0,0)|$$

On inverse l'ordre des sommations après avoir remplacé les $\Theta(X,.,\rho,\sigma)$ par leurs valeurs et on obtient :

$$\langle Q\rangle^{4\ell}U = |\sum_{Y,A\in\mathcal{C}_{Q^\ell}} \mathrm{e}(\alpha w_{m,\ell}(Y))E(\frac{-YA}{Q^\ell}) \sum_{Z,B\in\mathcal{C}_{Q^\ell}} \mathrm{e}(-\alpha w_{m,\ell}(Z))E(\frac{-ZB}{Q^\ell})$$

$$\times \sum_{V,G\in\mathcal{C}_{Q^\ell}} \mathrm{e}(-\alpha w_{m,\ell}(V))E(\frac{-VG}{Q^\ell}) \sum_{W,H\in\mathcal{C}_{Q^\ell}} \mathrm{e}(\alpha w_{m,\ell}(W))E(\frac{-WH}{Q^\ell}) \times \Psi|,$$

où

$$\Psi = \Psi(A,B,G,H) =$$

$$\sum_{X\in\mathcal{X}} E\left(\frac{(X+R+SQ^m)^2A + (X+R)^2B + (X+SQ^m)^2G + X^2H}{Q^\ell}\right).$$

Avec (4.3), on a

$$U = |\sum_{A\in\mathcal{C}_{Q^\ell}} F_{m,\ell}(A) \sum_{B\in\mathcal{C}_{Q^\ell}} F_{m,\ell}(-B) \sum_{G\in\mathcal{C}_{Q^\ell}} F_{m,\ell}(-G) \sum_{H\in\mathcal{C}_{Q^\ell}} F_{m,\ell}(H)\Psi| \quad (\star)$$

Il nous reste à transformer la somme $\Psi(A,B,G,H)$. Pour cela, on répartit les $X\in\mathcal{X}$ dans les différentes classes modulo Q^ℓ. On a

$$\Psi(A,B,G,H) =$$

$$\sum_{M\in\mathcal{C}_{Q^\ell}} \sum_{\substack{X\in\mathcal{X}\\ X\equiv M(\mathrm{mod}Q^\ell)}} E\left(\frac{(X+R+SQ^m)^2A + (X+R)^2B + (X+SQ^m)^2G + X^2H}{Q^\ell}\right)$$

$$= \sum_{M\in\mathcal{C}_{Q^\ell}} \sum_{\substack{X\in\mathcal{X}\\ X\equiv M(\mathrm{mod}Q^\ell)}} E\left(\frac{(M+R+SQ^m)^2A + (M+R)^2B + (M+SQ^m)^2G + M^2H}{Q^\ell}\right).$$

Le corollaire 2.2 nous donne alors

$$\langle Q\rangle^{\ell}\Psi(A,B,G,H) = \sum_{M\in\mathcal{C}_{Q^\ell}} \sum_{X\in\mathcal{X}} \sum_{L\in\mathcal{C}_{Q^\ell}} E\left(\frac{L(M-X)}{Q^\ell}\right)$$

$$\times E\left(\frac{(M+R+SQ^m)^2A + (M+R)^2B + (M+SQ^m)^2G + M^2H}{Q^\ell}\right)$$

$$= \langle Q\rangle^{\ell}\Psi(A,B,G,H) = \sum_{L\in\mathcal{C}_{Q^\ell}}\sum_{X\in\mathcal{X}} E(-\frac{LX}{Q^\ell})$$

$$\times \sum_{M\in\mathcal{C}_{Q^\ell}} E\left(\frac{(M+R+SQ^m)^2A+(M+R)^2B+(M+SQ^m)^2G+M^2H+LM}{Q^\ell}\right).$$

En reportant cette valeur dans $(\star)$ on obtient (5.11), ce qui achève la preuve de la proposition 5.4.

□

Lemme 5.5 *On a*

$$\sum_{L\in\mathcal{C}_{Q^\ell}} |\sum_{X\in\mathcal{X}} E(-\frac{LX}{Q^\ell})| \leq 2(1-\frac{1}{q})\langle Q\rangle^{\ell}. \tag{5.13}$$

Preuve. Posons pour tout $L\in\mathcal{C}_{Q^\ell}$, $\sigma_L = \sum_{X\in\mathcal{X}} E(-\frac{LX}{Q^\ell})$. On a

$$\sigma_L = \sum_{\substack{X\in\mathbf{A}\\ \nu\deg Q\leq\deg X<N}} E(\frac{LX}{Q^\ell}) = \sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} E(\frac{LX}{Q^\ell}) - \sum_{\substack{X\in\mathbf{A}\\ \deg X<\nu\deg Q}} E(\frac{LX}{Q^\ell}).$$

La proposition 2.1 donne la valeur de σ_L en fonction de $v_\infty(L/Q^\ell) = \ell\deg Q - \deg L$:

$$\sigma_L = \begin{cases} q^N - q^{\nu\deg Q} & \text{si} \quad \deg L < \ell\deg Q - N,\\ -q^{\nu\deg Q} & \text{si} \quad \ell\deg Q - N \leq \deg L < (\ell-\nu)\deg Q,\\ 0 & \text{si} \quad \deg L \geq (\ell-\nu)\deg Q.\end{cases}$$

Par suite,

$$\sum_{L\in\mathcal{C}_{Q^\ell}} |\sum_{X\in\mathcal{X}} E(-\frac{LX}{Q^\ell})| = \sum_{\substack{L\in\mathbf{A}\\ deg L<\ell\deg Q-N}} (q^N-\langle Q\rangle^{\nu}) + \sum_{\substack{L\in\mathbf{A}\\ \ell\deg Q-N\leq deg L<(\ell-\nu)\deg Q}} \langle Q\rangle^{\nu}$$

$$= \langle Q\rangle^{\ell}q^{-N}(q^N-\langle Q\rangle^{\nu}) + (\langle Q\rangle^{\ell-\nu}-\langle Q\rangle^{\ell}q^{-N})\langle Q\rangle^{\nu} = 2\langle Q\rangle^{\ell}(1-\langle Q\rangle^{\nu}q^{-N}) \leq 2(1-\frac{1}{q})\langle Q\rangle^{\ell}.$$

□

Proposition 5.6 *Pour tout* $(R,S)\in(\mathcal{C}_{Q^r})^2$ *on a*

$$U(N,r,m,R,S)\leq 2(1-\frac{1}{q})\langle Q\rangle^{\ell/2}\max_{L\in\mathcal{C}_{Q^{-\ell}}}(\sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell}}|D|^{1/2}W(L,D)),\tag{5.14}$$

avec

$$W(L,D)=\sum_{(A,B,G,H)\in\mathcal{G}(L,D)}|F_{m,\ell}(A)F_{m,\ell}(-B)F_{m,\ell}(-G)F_{m,\ell}(H)|,\tag{5.15}$$

$\mathcal{G}(L,D)$ *désignant l'ensemble des* $(A,B,G,H)\in(\mathcal{C}_{Q^\ell})^4$ *vérifiant les conditions*

$$\begin{cases}(A+B+G+H,Q^\ell)=D\quad(i),\\ L+2R(A+B)+2SQ^m(A+G)\equiv 0\ (\mathrm{mod}\ D)\quad(ii).\end{cases}\tag{5.16}$$

Preuve. Si $(R,S)\in(\mathcal{C}_{Q^r})^2$, on pose $U=U(N,r,m,R,S)$ et pour $L\in\mathcal{C}_{Q^\ell}$

$$u(L)=\sum_{(A,B,G,H)\in(\mathcal{C}_{Q^\ell})^4}F_{m,\ell}(A)F_{m,\ell}(-B)F_{m,\ell}(-G)F_{m,\ell}(H)\Lambda(L).$$

Alors, avec (5.11),

$$\langle Q\rangle^\ell U=|\sum_{L\in\mathcal{C}_{Q^m}}\sum_{X\in\mathcal{X}}E(-\frac{LX}{Q^\ell})u(L)|\leq\sum_{L\in\mathcal{C}_{Q^m}}|u(L)||\sum_{X\in\mathcal{X}}E(-\frac{LX}{Q^\ell}|$$

$$\leq\max_{L\in\mathcal{C}_{Q^m}}|u(L)|\sum_{L\in\mathcal{C}_{Q^m}}|\sum_{X\in\mathcal{X}}E(-\frac{LX}{Q^\ell}|,$$

d'où, avec (5.13),

$$U\leq 2(1-\frac{1}{q})\max_{L\in\mathcal{C}_{Q^m}}|u(L)|.$$

Avec (5.12) et (2.10), on a

$$|u(L)|\leq\sum_{(A,B,G,H)\in(\mathcal{C}_{Q^\ell})^4}|F_{m,\ell}(A)F_{m,\ell}(-B)F_{m,\ell}(-G)F_{m,\ell}(H)|$$

$$\times|\Gamma(Q^\ell,A+B+G+H,L+2R(A+B)+2SQ^m(A+G))|.$$

On divise la somme ci-dessus en sommes partielles, suivant les valeurs de $D = (A+B+G+H, Q^\ell)$. La Proposition 2.7 jointe à la majoration (2.11) nous donnent alors

$$|u(L)| \leq \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell}} \sum_{\substack{(A,B,G,H)\in(\mathcal{C}_{Q^\ell})^4\\ (A+B+G+H,Q^\ell)=D\\ D|(L+2R(A+B)+2SQ^m(A+G))}} |F_{m,\ell}(A)F_{m,\ell}(-B)F_{m,\ell}(-G)F_{m,\ell}(H)|\langle D\rangle^{1/2}\langle Q\rangle^{\ell/2},$$

ce qui donne le résultat annoncé.

□

Soit, pour $R \in \mathcal{C}_{Q^r}$, $S \in \mathcal{C}_{Q^r}$ et $L \in \mathcal{C}_{Q^\ell}$,

$$V = V(R,S,L) = \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell}} \langle D\rangle^{1/2} W(L,D). \tag{5.17}$$

On pose

$$\rho = \rho(Q) = r\deg Q - 1 \tag{5.18}$$

et

$$\Delta = \ell - m + \rho(Q). \tag{5.19}$$

La condition (5.4-(ii)) jointe à (5.5) entraîne $\Delta > 0$. La condition (5.4-(iv)) entraîne $r\deg Q - 1 < 2m - \nu - r - 1$, d'où $\rho(Q) < 2m - \nu - r - 1$ et, avec (5.19) et (5.5), $\Delta < m$. On divise V en trois sommes partielles suivant les valeurs de $v_Q(D)$: $V = V_1 + V_2 + V_3$, avec

$$V_1 = V_1(R,S,L) = \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ v_Q(D)<\Delta}} \langle D\rangle^{1/2} W(L,D). \tag{5.20}$$

$$V_2 = V_2(R,S,L) = \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ \Delta\leq v_Q(D)<m}} \langle D\rangle^{1/2} W(L,D). \tag{5.21}$$

$$V_3 = V_3(R,S,L) = \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ v_Q(D)\geq m}} \langle D\rangle^{1/2} W(L,D). \tag{5.22}$$

On fixe momentanément les polynômes R, S et L et on majore ces trois sommes. La majoration de V_1 est facile.

Proposition 5.7 *Pour tout $(R,S)\in(\mathcal{C}_{Q^r})^2$ et $L\in\mathcal{C}_{Q^\ell}$ on a*

$$V_1(R,S,L) \leq \Delta\tau(Q^\ell)\langle Q\rangle^{4(\ell-m)}\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2} q^{(\Delta-1)/2}. \tag{5.23}$$

Preuve. On majore les sommes $W(L,D)$ intervenant dans V_1 en remplaçant la condition $(A,B,G,H)\in\mathcal{G}(L,D)$ par la condition moins restrictive $(A,B,G,H)\in(\mathcal{C}_{Q^\ell})^4$. Cela donne

$$V_1 \leq \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ \omega_Q(D)<\Delta}} \langle D\rangle^{1/2} \sum_{(A,B,G,H)\in(\mathcal{C}_{Q^\ell})^4} |F_{m,\ell}(A)F_{m,\ell}(B)F_{m,\ell}(G)F_{m,\ell}(H)|,$$

d'où, avec la proposition 4.6,

$$V_1 \leq \langle Q\rangle^{4(\ell-m)} \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ \omega_Q(D)<\Delta}} \langle D\rangle^{1/2}.$$

On applique alors la proposition 2.3 avec $m=\theta=0$ et $n=\Delta-1$ et il vient

$$\sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ \omega_Q(D)<\Delta}} \langle D\rangle^{1/2} \leq \Delta\tau(Q^\ell)\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2} \max(1, q^{(\Delta-1)/2}).$$

□

Les majorations de V_2 et V_3 demandent quelques notations supplémentaires.

D'après (5.15), si D est un polynôme unitaire divisant Q^ℓ tel que $\mathcal{G}(L,D) = \emptyset$, $W(L,D) = 0$ et n'intervient pas dans les sommes V_i. On n'a donc à considérer que les polynômes D pour lesquels $\mathcal{G}(L,D) \neq \emptyset$. Pour tout polynôme unitaire D divisant Q^ℓ, on pose

$$\tilde{D} = (D, R). \tag{5.24}$$

Les facteurs irréductibles de $\tilde{D}$ sont facteurs irréductibles de Q. Soit P l'un de ces facteurs. Alors $P^{v_P(\tilde{D})}$ divise (D,R), donc divise R. On a donc $v_P(\tilde{D}) \deg P \leq \deg R < r \deg Q$, ou encore avec (5.18), $v_P(\tilde{D}) \leq \rho$. Par suite,

$$\tilde{D} = \prod_{\substack{P \in \mathbf{I} \\ P|D}} P^{v_P(\tilde{D})} \quad | \quad \prod_{\substack{P \in \mathbf{I} \\ P|Q}} P^{\rho} \quad | \quad Q^\rho. \tag{5.25}$$

Avec (5.4-(ii)) et (5.4-(iv)) on a $\rho < m$, d'où $\tilde{D}|Q^m$. D'après (5.16), si $(A,B,G,H) \in \mathcal{G}(L,D)$, alors $D|Q^\ell$ et $L + 2R(A+B) + 2SQ^m(A+G) \equiv 0 \pmod{D}$, d'où, avec (5.24), $L + 2SQ^m(A+G) \equiv 0 \pmod{\tilde{D}}$, ce qui implique que $\tilde{D}$ divise L. Les polynômes D tels que $\mathcal{G}(L,D) \neq \emptyset$ sont tels que $\tilde{D}$ divise L. Quand cette condition est réalisée, on pose

$$2R = R'\tilde{D}, \quad 2SQ^\rho = S'\tilde{D}, \quad L = L'\tilde{D}, \quad D = D'\tilde{D}. \tag{5.26}$$

La deuxième des conditions (5.16) s'écrit alors

$$L'\tilde{D} + R'\tilde{D}(A+B) + S'Q^{m-\rho}\tilde{D}(A+G) \equiv 0 \pmod{D'\tilde{D}},$$

d'où

$$L' + R'(A+B) + S'Q^{m-\rho}(A+G) \equiv 0 \pmod{D'}. \tag{$5.16-(iii)$}$$

Les polynômes R' et D' sont premiers entre eux. Soit $R" \in \mathcal{C}_{D'}$, inverse de R' modulo D'. Posons

$$L" = R"L', \quad S" = R"S' = \frac{2R"SQ^\rho}{(D,R)}. \tag{5.27}$$

La condition (5.16-(iii)) devient

$$L" + A + B + S"Q^{m-\rho}(A+G) \equiv 0 \pmod{D'}. \tag{$5.16-(iv)$}$$

On peut maintenant majorer V_2 et V_3 :

Proposition 5.8 *Pour tout* $(R,S) \in (\mathcal{C}_{Q^r})^2$ *et* $L \in \mathcal{C}_{Q^\ell}$, *on a*

$$V_2(R,S,L) \leq (m-\Delta)\tau(Q^{\ell-\Delta}) \left(\frac{\langle Q\rangle}{q}\right)^{\ell/2} q^{(m-1)/2}. \tag{5.28}$$

Preuve. Soit $D \in \mathbf{M}$ divisant Q^ℓ et tel que $\Delta \leq v_Q(D) < m$. Nous supposerons que $\tilde{D}$ divise L. Soit $\delta = v_Q(D)$. D'après (5.19), on a

$$v_Q(D'\tilde{D}) = v_Q(D) \geq \Delta = \ell - m + \rho,$$

et d'après (5.25), $v_Q(\tilde{D}) \leq \rho$. Donc $v_Q(D') \geq \delta - \rho \geq \ell - m$. On majore la somme $W(L,D)$ en remplaçant les conditions (5.16) par les conditions moins restrictives

$$A+B+G+H \equiv 0 \pmod{Q^{\delta-\rho}};\ L" + A + B \equiv 0 \pmod{Q^{\delta-\rho}}$$

impliquées par (5.16-(i)) et (5.16-(iv)). On obtient avec (5.21) et (5.15)

$$V_2 \leq \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ \Delta\leq v_Q(D)<m}} \langle D\rangle^{1/2} \times \sum_{\substack{(A,B,G,H)\in(\mathcal{C}_{Q^\ell})^4\\ A+B+G+H\equiv 0 \pmod{Q^{\delta-\rho}}\\ A+B\equiv -L" (\mathrm{mod} Q^{\delta-\rho})}} |F_{m,\ell}(A)F_{m,\ell}(-B)F_{m,\ell} - (G)F_{m,\ell}(H)|,$$

d'où

$$V_2 \leq \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ \Delta\leq v_Q(D)<m}} \langle D\rangle^{1/2} \{ \sum_{\substack{(A,B)\in(\mathcal{C}_{Q^\ell})^2\\ A+B\equiv -L" (\mathrm{mod} Q^{\delta-\rho})}} |F_{m,\ell}(A)F_{m,\ell}(-B)|\}$$

$$\times \{ \sum_{\substack{(G,H)\in(\mathcal{C}_{Q^\ell})^2\\ G+H\equiv L" (\mathrm{mod} Q^{\delta-\rho})}} |F_{m,\ell}(-G)F_{m,\ell}(H)|\}.$$

Comme $\ell - m \leq \delta - \rho$, on peut appliquer la proposition 4.9 aux deux dernières sommes. On obtient

$$V_2 \leq \sum_{\substack{D\in\mathbf{M}\\ D|Q^\ell\\ \Delta\leq v_Q(D)<m}} \langle D\rangle^{1/2},$$

d'où, avec la proposition 2.3,

$$V_2 \leq (m-\Delta)\tau(Q^{\ell-\Delta})\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2}\max(q^{\Delta/2}, q^{(m-1)}/2).$$

□

Pour majorer V_3, on majore d'abord les $W(L,D)$ intervenant dans V_3.

Proposition 5.9 *Soit D un diviseur unitaire de Q^ℓ tel que $\tilde{D}$ divise L et tel que $\delta = v_Q(D) \geq m$. Alors,*

$$W(L,D) \leq \begin{cases} \langle Q\rangle^{-2C(Q,w,\alpha)(\delta-m-2\rho(Q))} & \text{si } \delta - m - 2\rho(Q) > 0, \\ 1 & \text{sinon.} \end{cases} \tag{5.29}$$

Preuve. Soit $(A,B,G,H) \in \mathcal{G}(L,D)$. Avec (5.16-(iv)) on a

$$L" + A + B + S"Q^{m-\rho}(A+G) \equiv 0 \pmod{D'}$$

et avec (5.16-(i)) on a

$$A + B + G + H \equiv 0 \pmod{D}$$

On a $v_Q(D') \geq \delta - \rho$, d'où

$$\begin{cases} L" + A + B + S"Q^{m-\rho}(A+G) \equiv 0 \pmod{Q^{\delta-\rho}} \\ A + B + G + H \equiv 0 \pmod{Q^{\delta-\rho}}, \end{cases}$$

système équivalent au système $(\mathcal{E})$ suivant

$$\begin{cases} L" + A + B + S"Q^{m-\rho}(A+G) \equiv 0 \pmod{Q^{\delta-\rho}} \\ G + H - S"Q^{m-\rho}(A+G) - L" \equiv 0 \pmod{Q^{\delta-\rho}}. \end{cases}$$

On majore $W = W(L,D)$ en remplaçant la condition $(A,B,G,H) \in \mathcal{G}(L,D)$ par la condition moins restrictive $(A,B,G,H) \in (\mathcal{C}_{Q^\ell})^4$ et vérifie $(\mathcal{E})$. On obtient

$$W \leq \sum_{(A,G)\in(\mathcal{C}_{Q^\ell})^2} |F_{m,\ell}(A)F_{m,\ell}(-G)| \sum_{\substack{B\in\mathcal{C}_{Q^\ell} \\ -B\equiv L"+A+S"Q^{m-\rho}(A+G)(\mathrm{mod}Q^{\delta-\rho})}} |F_{m,\ell}(-B)|$$

$$\times \sum_{\substack{H\in\mathcal{C}_{Q^\ell} \\ H\equiv L"-G+S"Q^{m-\rho}(A+G)(\mathrm{mod}\ Q^{\delta-\rho})}} |F_{m,\ell}(H)|).$$

Avec (5.4-(iv)), (5.5) et (5.18), on a $\delta - \rho \geq m - \rho \geq \ell - m$. En appliquant la proposition 4.7 aux deux dernières sommes on obtient que la somme

$$\sum_{\substack{B \in \mathcal{C}_{Q^\ell} \\ -B \equiv L" + A + S" Q^{m-\rho}(A+G) (\mathrm{mod}\ Q^{\delta-\rho}}} |F_{m,\ell}(-B)|$$

vaut $|F_{\ell-m}(L" + A + S" Q^{m-\rho}(A+G))|$ si $v_\infty(\{\frac{L"+A+S"Q^{m-\rho}(A+G)}{Q^{\delta-\rho}}\}) > (m + \delta - \rho - \ell) \deg Q$ et 0 sinon ainsi que la majoration

$$\sum_{\substack{H \in \mathcal{C}_{Q^\ell} \\ H \equiv L" - G + S" Q^{m-\rho}(A+G) (\mathrm{mod} Q^{\delta-\rho})}} |F_{m,\ell}(H)| \leq |F_{\ell-m}(L" - G + S" Q^{m-\rho}(A+G))|$$

On définit le sous ensemble $\mathcal{H}$ de $(\mathcal{C}_{Q^\ell})^2$ par la condition

$$(A,G) \in \mathcal{H} \Leftrightarrow \nu(\{\frac{L" + A + S" Q^{m-\rho}(A+G)}{Q^{\delta-\rho}}\}) > (m + \delta - \rho - \ell) \deg Q.$$

Alors,

$$W \leq \sum_{(A,G) \in \mathcal{H}} |F_{m,\ell}(A) F_{m,\ell}(-G)|$$

$$\times |F_{\ell-m}(L" + A + S" Q^{m-\rho}(A+G))| |F_{\ell-m}(L" - G + S" Q^{m-\rho}(A+G))|.$$

Fixons $A \in \mathcal{C}_{Q^\ell}$ et montrons que les $G \in \mathcal{C}_{Q^\ell}$ tels que $(A,G) \in \mathcal{H}$ sont dans une même classe de congruence modulo $Q^{\delta-m-2\rho}$. En effet, supposons que $(A,G) \in \mathcal{H}$ et $(A,G') \in \mathcal{H}$. Alors on a

$$v_\infty(\{\frac{S"(G-G')}{Q^{\delta-m}}\}) > (m + \delta - \rho - \ell) \deg Q.$$

Avec (5.4-(iv)) on a $2m > r(\deg Q + 1) + \nu$, d'où $m + \delta - \rho - \ell > \delta - m$. Par suite $S"(G - G') \equiv 0 \pmod{Q^{\delta-m}}$ d'où, avec (5.27), $\frac{R" S Q^\rho}{(D,R)}(G - G') \equiv 0 \pmod{Q^{\delta-m}}$. Le polynôme $R"$ étant l'inverse de R' modulo D', il est donc premier à tout diviseur de D'. En particulier, il est premier à Q et donc inversible modulo $Q^{\delta-m}$, d'où $SQ^\rho(G - G') \equiv 0 \pmod{Q^{\delta-m}}$. Par ailleurs, si P est un facteur irréductible de (S,Q), on $v_P(S) \deg P \leq \deg S < r \deg Q$, d'où avec (5.18), $v_P(S) \leq \rho$. On a donc

$$\prod_{\substack{P \in \mathbf{I} \\ P | (S,Q)}} P^{v_P(S)} \mid Q^\rho,$$

d'où

$$Q^{2\rho}(G-G') \equiv 0 \pmod{Q^{\delta-m}} \text{ et } G' \equiv G \pmod{Q^{\delta-m-2\rho}}.$$

Pour tout $A \in \mathcal{C}_{Q^\ell}$, notons $G_0(A)$ l'élément de $\mathcal{C}_{Q^{\delta-m-2\rho}}$ tel que pour tout $G \in \mathcal{C}_{Q^\ell}$ on ait

$$(A,G) \in \mathcal{H} \Rightarrow G \equiv G_0(A) \pmod{Q^{\delta-m-2\rho}}.$$

On majore $W = W(L,D)$ en remplaçant la condition $(A,H) \in \mathcal{H}$ par la condition $G \equiv G_0(A) \pmod{Q^{\delta-m-2\rho}}$. On obtient

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} \sum_{\substack{G \in \mathcal{C}_{Q^\ell} \\ G \equiv G_0(A) (\mathrm{mod} Q^{\delta-m-2\rho})}} |F_{m,\ell}(A)|$$

$$\times |F_{\ell-m}(L"+A+S"Q^{m-\rho}(A+G))||F_{m,\ell}(-G)|F_{\ell-m}(L"-G)+S"Q^{m-\rho}(A+G))|$$

Avec (5.4-(iv)) on a $m-\rho > \ell-m$ et la proposition 4.1-(vi) nous donne

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} \sum_{\substack{G \in \mathcal{C}_{Q^\ell} \\ G \equiv G_0(A) (\mathrm{mod} Q^{\delta-m-2\rho})}} |F_{m,\ell}(A)F_{\ell-m}(L"+A)||F_{m,\ell}(-G)|F_{\ell-m}(L"-G)|,$$

soit

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L" + A)|$$

$$\times \sum_{\substack{G \in \mathcal{C}_{Q^\ell} \\ G \equiv G_0(A) (\mathrm{mod} \mathbb{Q}^{\delta-m-2\rho})}} |F_{m,\ell}(-G)F_{\ell-m}(L" - G)|.$$

(I) Supposons d'abord que $\gamma = \delta - m - 2\rho > 0$. On a alors $\gamma < \ell - m$ et $m < \ell$. On applique la proposition 4.8 à la somme intérieure et on obtient

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L" + A)||F_\gamma(-G_0(A))F_\gamma(L" - G_0(A))|.$$

La proposition 4.3 donne alors

$$W \leq \langle Q \rangle^{-2C\gamma} \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L" + A)|$$

où $C = C(Q, w, \alpha)$ et les propositions 4.8 et 4.2 nous donnent

$$W \leq \langle Q\rangle^{-2C\gamma} |F_0(0)F_0(L")| = \langle Q\rangle^{-2C\gamma}.$$

(II) Supposons maintenant que $\gamma = \delta - m - 2\rho \leq 0$. Dans ce cas, la condition de congruence dans la somme majorant W n'apportant aucune restriction, on majore W trivialement et on obtient

$$W \leq \sum_{A \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(A)F_{\ell-m}(L" + A)| \sum_{G \in \mathcal{C}_{Q^\ell}} |F_{m,\ell}(-G)F_{\ell-m}(L" - G)|$$

et la proposition 4.8 nous donne $W \leq 1$.

□

Proposition 5.10 *Pour tout $(R, S) \in (\mathcal{C}_{Q^r})^2$ et $L \in \mathcal{C}_{Q^\ell}$, on a*

$$V_3(R, S, L) \leq (\ell - m + 1)\tau(Q^{\ell-m})\langle Q\rangle^{\ell/2}\langle Q\rangle^{-C'(Q,w,\alpha)(\ell-m-2\rho(Q))}, \tag{5.30}$$

avec

$$C'(Q, w, \alpha) = \min(2C(Q, w, \alpha), \frac{1}{2\deg Q}). \tag{5.31}$$

Preuve. Observons d'abord que la condition (5.4-(iii)) entraîne la relation $m + 2\rho < \ell$. Avec (5.22) et (5.29), on a

$$V_3 \leq \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ m \leq v_Q(D) \leq m+2\rho}} \langle D\rangle^{1/2} + \sum_{\substack{D \in \mathbf{M} \\ D|Q^\ell \\ m+2\rho < v_Q(D)}} \langle D\rangle^{1/2}\langle Q\rangle^{2(m+2\rho-v_Q(D))C},$$

où l'on a posé $C = C(Q, w, \alpha)$. Comme $\tau(Q^{\ell-m-2\rho-1}) \leq \tau(Q^{\ell-m})$, la proposition 2.3 donne

$$V_3 \leq \tau(Q^{\ell-m})\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2}\left((2\rho+1)q^{\rho+m/2} + (\ell - m - 2\rho)\langle Q\rangle^{2(m+2\rho)C}\right.$$

$$\left. \times \max\left((\langle Q\rangle^{-2C\|\alpha\|^2}q^{1/2})^{m+2\rho+1}, (\langle Q\rangle^{-2C\|\alpha\|^2}q^{1/2})^\ell\right)\right.$$

Si $\langle Q\rangle^{-2C}q^{1/2} < 1$, on a

$$V_3 \leq \tau(Q^{\ell-m})\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2}\left((2\rho+1)q^{\rho+m/2} + (\ell - m - 2\rho)q^{(m+1+2\rho)/2}\langle Q\rangle^{-2C}\right),$$

d'où

$$V_3 \leq \tau(Q^{\ell-m})\langle Q\rangle^{\ell/2}(\ell-m+1)q^{\rho+m/2-\ell/2}.$$

Si $\langle Q\rangle^{-2C}q^{1/2} \geq 1$, on a

$$V_3 \leq \tau(Q^{\ell-m})\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2}\left((2\rho+1)q^{\rho+m/2}+(\ell-m-2\rho)q^{\ell/2}\langle Q\rangle^{2(m+2\rho-\ell)C}\right),$$

$$\leq \tau(Q^{\ell-m})\langle Q\rangle^{\ell/2}\left((2\rho+1)q^{\rho+\frac{m-\ell}{2}}+(\ell-m-2\rho)\langle Q\rangle^{-2C(\ell-m-2\rho)})\right).$$

Si on pose $C'=C'(Q,w,\alpha)$, on a

$$V_3 \leq \tau(Q^{\ell-m})\langle Q\rangle^{\ell/2}(\ell-m+1)\langle Q\rangle^{-C'(\ell-m-2\rho)}.$$

□

Proposition 5.11 *On a*

$$V(R,S,L) \leq m\tau(Q^\ell)\langle Q\rangle^{\ell/2}\left(q^{-1}\langle Q\rangle^{4\nu+9r/2-(4+1/2\deg Q)m+4}\right.$$

$$\left.+q^{-1-r/2}\langle Q\rangle^{-(\nu-m)/2\deg Q}+\langle Q\rangle^{-C'(Q,w,\alpha)(\ell-m-2\rho)}\right). \tag{5.32}$$

Preuve. La proposition 5.7 nous donne

$$V_1 \leq \Delta\tau(Q^\ell)\langle Q\rangle^{4(\ell-m)}\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2}q^{(\Delta-1)/2},$$

d'où, avec (5.19), (5.18), (5.4) et (5.5),

$$V_1 \leq m\tau(Q^\ell)\langle Q\rangle^{\ell/2}\langle Q\rangle^{4(\nu+r+1-m)+r/2}q^{-1-m/2},$$

$$\leq \frac{m}{q}\tau(Q^\ell)\langle Q\rangle^{\ell/2}\langle Q\rangle^{4\nu+9r/2-m(4+1/2\deg Q)+4}.$$

La proposition 5.8 nous donne

$$V_2 \leq m\tau(Q^{\ell-\Delta})\left(\frac{\langle Q\rangle}{q}\right)^{\ell/2}q^{(m-1)/2},$$

d'où, avec (5.5),

$$V_2 \leq \frac{m}{q}\tau(Q^\ell)\langle Q\rangle^{\ell/2}q^{-r/2}\langle Q\rangle^{-(\nu-m)/2\deg Q}.$$

D'après la proposition 5.10, on a

$$V_3 \leq (\ell - m + 1)\tau(Q^{\ell-m})\langle Q\rangle^{\ell/2}\langle Q\rangle^{-C'(Q,w,\alpha)(\ell-m-2\rho)},$$

d'où, avec (5.18), (5.4) et (5.5),

$$V_3 \leq m\tau(Q^{\ell})\langle Q\rangle^{\ell/2}\langle Q\rangle^{-C'(Q,w,\alpha)(\ell-m-2\rho)}.$$

Les majorations de V_1, V_2, V_3 jointes aux relations (5.17), (5.20), (5.21), (5.22), nous donnent

$$V \leq m\tau(Q^{\ell})\langle Q\rangle^{\ell/2}\left(q^{-1}\langle Q\rangle^{4\nu+9r/2-m(4+1/2\deg Q)+4}\right.$$
$$\left.+q^{-1-r/2}\langle Q\rangle^{-(\nu-m)/2\deg Q}+\langle Q\rangle^{-C'(Q,w,\alpha)(\ell-m-2\rho}\right).$$

□

5.3 Fin de la Majoration

On est en mesure de démontrer la proposition suivante :

Proposition 5.12 *On suppose α non entier. Soient*

$$\eta(Q) = \left(\frac{4q^{99/100}\exp(\frac{1}{48\deg Q})(1-\frac{1}{q})(1+\frac{2}{q})\tau(Q)\langle Q\rangle^5}{(\deg Q)^{\omega(Q)+1}}\right)^{1/4} \tag{5.33}$$

et

$$\xi(Q,w,\alpha) = \frac{11}{15}\min\left(\frac{1}{48(\deg Q)^2+11\deg Q-1},\right.$$
$$\left.\frac{1}{16(\deg Q)^2+7\deg Q+\frac{1+8\deg Q}{C(Q,w,\alpha)}-1}\right), \tag{5.34}$$

où $C(Q,w,\alpha)$ est définie par (4.5). Alors, pour $\nu(N) > 100/\xi(Q,w,\alpha)$, on a

$$|\Sigma(N)| \leq \eta(Q)N^{\frac{\omega(Q)+1}{4}}q^{N(1-\frac{99}{400}\xi(Q,w,\alpha))}. \tag{5.35}$$

Preuve. On pose $C' = C'(Q,w,\alpha)$ défini par (5.31). On va imposer des conditions supplémentaires aux paramètres r et m afin que les conditions suivantes soient réalisées :

$$\begin{cases} (4\nu+13r/2)-m(4+1/2\deg Q)\leq 0,\\ (m-\nu-r)/2\deg Q+2r-4\leq 0,\\ C'(m-\nu-r-3)+2r(1+C'\deg Q)-4\leq 0. \end{cases} \tag{5.36}$$

Ces conditions réalisées, on déduit des relations (5.14), (5.17) et (5.32) que pour $R \in \mathcal{C}_Q$ et $S \in \mathcal{C}_{Q^r}$,

$$U = U(N, r, m, R, S) \leq 2(1 - \frac{1}{q})m\tau(Q^\ell)\langle Q\rangle^\ell \left(q^{-1}\langle Q\rangle^{4\nu+9r/2-(4+1/2\deg Q)m+4}\right.$$

$$\left. +q^{-1-r/2}\langle Q\rangle^{-(\nu-m)/2\deg Q} + \langle Q\rangle^{-C'(\ell-m-2\rho)}\right),$$

d'où, avec (5.5), (5.18) et (5.36),

$$U \leq 2(1 - \frac{1}{q})(\frac{2}{q} + 1)m\tau(Q^\ell)\langle Q\rangle^{\nu-r+5}. \tag{5.37}$$

Compte tenu de (5.31), les conditions (5.36) sont réalisées dès que les conditions

$$\begin{cases} (8\nu + 13r)\deg Q \leq m(8\deg Q + 1), \\ m \leq \nu + r - \frac{2r}{C'} - 2r\deg Q + 8\deg Q. \end{cases} \tag{5.38}$$

le sont.

On se donne un paramètre $\xi \in]0, 1]$ et on impose

$$1 < r \leq \xi\nu. \tag{5.39}$$

Les conditions (5.38) sont satisfaites si

$$\nu\left(\frac{1 + \frac{13\xi}{8}}{1 + \frac{1}{8\deg Q}}\right) \leq m \leq \nu(1 + \xi - \frac{2\xi}{C'} - 2\xi\deg Q).$$

On exigera donc que ξ vérifie la condition

$$\frac{1 + \frac{13\xi}{8}}{1 + \frac{1}{8\deg Q}} \leq 1 + \xi - 2\xi\deg Q - \frac{2\xi}{C'} \tag{5.40}$$

et que l'intervalle

$$J_{\xi,\nu} = [\nu\frac{1 + \frac{13\xi}{8}}{1 + \frac{1}{8\deg Q}}, \nu(1 + \xi - 2\xi\deg Q - \frac{2\xi}{C'})]$$

contienne des nombres entiers m tels que $r \leq \xi\nu$ et m vérifient les conditions (5.4). On prend

$$\xi = \xi(Q, w, \alpha) = \frac{\frac{11}{15}}{16(\deg Q)^2 + 7\deg Q + \frac{2+16\deg Q}{C'} - 1}. \tag{5.41}$$

et la condition (5.40) est vérifiée. Observons que, $C' = C'(Q, w, \alpha)$ étant défini par (5.31), $\xi(Q, w, \alpha)$ vérifie (5.34). On suppose que N est assez grand pour que $\nu = \nu(N) > 100/\xi$. Alors on a $\nu > 30 \deg Q$ et

$$\nu \geq \frac{1}{1 + \xi - 2\xi \deg Q - \frac{2\xi}{C'} - \frac{1+\frac{13\xi}{8}}{1+\frac{1}{8\deg Q}}}. \tag{5.42}$$

L'intervalle $J_{\xi,\nu}$ contient alors des nombres nombres entiers. Si $r \leq \xi\nu$, alors $\frac{1-3/\nu}{5\deg Q-1} > \frac{1-1/10\deg Q}{5\deg Q-1} > \xi$, d'où $r \leq \xi\nu < \frac{\nu-3}{5\deg Q-1}$, ce qui est la relation (5.4-(i)). Soit un nombre entier $m \in J_{\xi,\nu}$. Alors

$$m \leq \nu(1 + \xi - 2\xi \deg Q - 2\xi/C') \leq \nu(1 + \xi - 6\xi \deg Q),$$

d'où, d'une part $m \leq \nu(1 - 5\xi) < \nu - r$ et d'autre part,

$$m \leq \nu(1 + \xi(1 - 2\deg Q)) \leq \nu + r(1 - 2\deg Q) < \nu + r(1 - 2\deg Q)) + 3.$$

Les relations (5.4-(ii)) et (5.4-(iii)) sont vérifiées. Avec (5.41), on a

$$\xi < \frac{1 - 1/8\deg Q}{(1 + \deg Q)(1 + 1/8\deg Q)},$$

d'où

$$2m > \nu(1 + \xi(1 + \deg Q)) \geq \nu + r(1 + \deg Q)$$

et (5.4)-(iv) est vérifiée. Par suite, (5.37) est vérifiée. Majorons $\tau(Q^\ell)$. On a

$$\tau(Q^\ell) = \prod_{\substack{P \in \mathbf{I} \\ P|Q}} (\ell v_P(Q) + 1) \leq \prod_{\substack{P \in \mathbf{I} \\ P|Q}} (\ell v_P(Q) + \ell) = \ell^{\omega(Q)} \tau(Q).$$

Avec (5.5) puis (5.39), on a

$$\ell^{\omega(Q)} = (\nu + r + 1)^{\omega(Q)} \leq \nu^{\omega(Q)} (1 + \xi + \frac{1}{\nu})^{\omega(Q)}.$$

Comme $\nu = \nu(N) \geq 100/\xi$, on a

$$\ell^{\omega(Q)} \leq \nu^{\omega(Q)} (1+2\xi)^{\omega(Q)} = \nu^{\omega(Q)} \exp(\omega(Q) \log(1+\frac{101}{100}\xi) \leq \nu^{\omega(Q)} \exp(\frac{101}{100}\xi \deg Q).$$

Avec (5.41) et (5.31),

$$\ell^{\omega(Q)} \leq \nu^{\omega(Q)} \exp(\frac{1}{48 \deg Q}),$$

d'où

$$\tau(Q^\ell) \leq \exp(\frac{1}{48\deg Q})\tau(Q)\nu^{\omega(Q)}. \tag{5.43}$$

Avec (5.4) on a a $m \leq \nu + r - 6r\deg Q + 8\deg Q \leq \nu + r < 2\nu$, d'où, avec (5.37), (5.42) et (5.43),

$$U \leq \kappa(Q)\tau(Q)\nu^{\omega(Q)+1}\langle Q\rangle^{\nu-r+5},$$

où

$$\kappa(Q) = 4\exp(\frac{1}{48\deg Q})(1-\frac{1}{q})(1+\frac{2}{q}).$$

La proposition 5.3 nous donne

$$T(N,R,S)^2 \leq \kappa(Q)\tau(Q)q^N\nu^{\omega(Q)+1}\langle Q\rangle^{\nu-r+5},$$

puis, la proposition 5.2 nous donne

$$|\Sigma(N)|^4 \leq \kappa(Q)\tau(Q)q^{3N}\nu^{\omega(Q)+1}\langle Q\rangle^{\nu-r+5},$$

d'où, en majorant ν par $N/\deg Q$,

$$|\Sigma(N)| \leq \left(\kappa(Q)\tau(Q)\langle Q\rangle^5\right)^{1/4}\left(\frac{N}{\deg Q}\right)^{\frac{\omega(Q)+1}{4}} q^N\langle Q\rangle^{-r/4}.$$

L'intervalle $[\frac{99}{100}\xi\nu, \xi\nu]$ contient des nombres entiers. On prend r dans cet intervalle et on obtient la majoration

$$|\Sigma(N)| \leq \left(\kappa(Q)\tau(Q)\langle Q\rangle^5\right)^{1/4}\left(\frac{N}{\deg Q}\right)^{\frac{\omega(Q)+1}{4}} q^{N(1-\frac{99}{400}\xi)+\frac{99}{400}}.$$

□

6 Démonstration du théorème 1.2

Proposition 6.1 *Soit N un nombre entier, $N > 100\deg Q/\xi(Q,w,\alpha)$. Alors*

$$|\sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\alpha w(X^2))| \leq \eta(Q)\left(1+\frac{\langle Q\rangle^{1-99\xi/400}}{\langle Q\rangle^{1-99\xi/400}-1}\right)N^{\frac{\omega(Q)+1}{4}}q^{N(1-99\xi/400)}$$

$$+\langle Q\rangle^{[100/\xi]} - \eta(Q)N^{\frac{\omega(Q)+1}{4}}\frac{\langle Q\rangle^{([100/\xi]+1)(1-99\xi/400)}}{\langle Q\rangle^{1-99\xi/400}-1},$$

où $\xi = \xi(Q,w,\alpha)$.

Preuve. Posons

$$\mathfrak{S}(N) = \sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\alpha w(X^2)).$$

Avec (5.1), (5.2) et (5.3), on a

$$\mathfrak{S}(N) = 1 + \sum_{j=1}^{\nu(N)} \Sigma(j\deg Q) + \Sigma(N).$$

La proposition 5.12 nous donne

$$|\mathfrak{S}(N)| \leq 1 + \sum_{j=1}^{[100/\xi]} |\Sigma(j\deg Q)| +$$

$$\eta(Q)\left(\sum_{j=1+[100/\xi]}^{\nu(N)} (j\deg Q)^{\frac{\omega(Q)+1}{4}} q^{j\deg Q(1-99\xi/400)} + N^{\frac{\omega(Q)+1}{4}} q^{N(1-99\xi/400)}\right).$$

On majore la première somme en majorant trivialement $|\Sigma(j\deg Q)|$ par $q^{j\deg Q} - q^{(j-1)\deg Q}$ et la deuxième somme en majorant $(j\deg Q)^{\frac{\omega(Q)+1}{4}}$ par $N^{\frac{\omega(Q)+1}{4}}$. On obtient

$$|\mathfrak{S}(N)| \leq \langle Q\rangle^{[100/\xi]} + \eta(Q) N^{\frac{\omega(Q)+1}{4}} \left(\sum_{j=1+[100/\xi]}^{\nu(N)} \langle Q\rangle^{j(1-99\xi/400)} + q^{N(1-99\xi/400)}\right),$$

d'où,

$$|\mathfrak{S}(N)| \leq \langle Q\rangle^{[100/\xi]} +$$

$$\eta(Q) N^{\frac{\omega(Q)+1}{4}} \left(\frac{\langle Q\rangle^{(\nu(N)+1)(1-99\xi/400)} - \langle Q\rangle^{(1+[100/\xi])(1-99\xi/400)}}{\langle Q\rangle^{(1-99\xi/400)} - 1} + q^{N(1-99\xi/400)}\right).$$

Avec (5.2), on obtient

$$|\mathfrak{S}(N)| \leq \langle Q\rangle^{[100/\xi]} + \eta(Q)\left(1 + \frac{\langle Q\rangle^{1-99\xi/400}}{\langle Q\rangle^{1-99\xi/400} - 1}\right) N^{\frac{\omega(Q)+1}{4}} q^{N(1-99\xi/400)}$$

$$-\eta(Q) N^{\frac{\omega(Q)+1}{4}} \frac{\langle Q\rangle^{([100/\xi]+1)(1-99\xi/400)}}{\langle Q\rangle^{1-99\xi/400} - 1}.$$

□

Corollaire 6.2 *Soit α un nombre réel non entier. Alors il existe un nombre entier $N(Q,w,\alpha)$ tel que pour tout nombre entier $N \geq N(Q,w,\alpha)$ on ait*

$$|\sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\alpha w(X^2))| \leq \beta(Q,w,\alpha)N^{\frac{\omega(Q)+1}{4}}q^{N(1-99\xi/400)},$$

où $\xi = \xi(Q,w,\alpha)$ et

$$\beta(Q,w,\alpha) = \eta(Q)\left(1+\frac{\langle Q\rangle^{1-99\xi/400}}{\langle Q\rangle^{1-99\xi/400}-1}\right). \tag{6.1}$$

Preuve. Pour $N \geq n(Q,\xi) = n(Q,\xi(Q,w,\alpha))$, on a

$$\eta(Q)N^{\frac{\omega(Q)+1}{4}}\frac{\langle Q\rangle^{([100/\xi]+1)(1-99\xi/400)}}{\langle Q\rangle^{1-99\xi/400}-1} > \langle Q\rangle^{[100/\xi]}.$$

On prend $N(Q,w,\alpha) = \max(n(Q,\xi(Q,w,\alpha)), 1+100\deg Q/\xi(Q,w,\alpha))$.

□

Nous pouvons maintenant démontrer le Théorème 1.2 avec

$$a(Q,w,\alpha) = \frac{363}{2000}\min(\frac{1}{48(\deg Q)^2+11\deg Q-1}, \tag{6.2}$$

$$\frac{C(Q,w,\alpha)}{C(Q,w,\alpha)(16(\deg Q)^2+7\deg Q-1)+1+8\deg Q})$$

et

$$b = b(Q) = \eta(Q)\left(1+\frac{\langle Q\rangle^{1-363/2000(48(\deg Q)^2+11\deg Q-1)}}{\langle Q\rangle^{1-99/400(48(\deg Q)^2+11\deg Q-1)}-1}\right). \tag{6.3}$$

Posons $a = a(Q,w,\alpha)$ et minorons d'abord $\xi = C(Q,w,\alpha)$. On a

$$\frac{1}{48(\deg Q)^2+11\deg Q-1} \geq \frac{2000}{363}a$$

ainsi que

$$\frac{1}{16(\deg Q)^2+7\deg Q+\frac{1+8\deg Q}{C(Q,w,\alpha)-1}} \geq \frac{2000}{363}a.$$

D'après (5.34)

$$\xi(Q,w,\alpha) \geq \frac{2000}{363}a,$$

d'où

$$1 - 99\xi/400 \leq 1 - a.$$

D'autre part, la fonction $t \to \frac{\langle Q\rangle^t}{\langle Q\rangle^t - 1}$ étant décroissante sur l'ensemble des nombres réels, on a avec (5.34)

$$\frac{\langle Q\rangle^{1-99\xi/400}}{\langle Q\rangle^{1-99\xi/400} - 1} \leq \frac{\langle Q\rangle^{1-363/2000(48(\deg Q)^2+11\deg Q-1)}}{\langle Q\rangle^{1-363/2000(48(\deg Q)^2+11\deg Q-1)} - 1},$$

d'où, avec (6.1)

$$\beta(Q,w,\alpha) \leq \eta(Q)\left(1 + \frac{\langle Q\rangle^{1-363/2000(48(\deg Q)^2+7\deg Q-1)}}{\langle Q\rangle^{1-363/2000(48(\deg Q)^2+7\deg Q-1)} - 1}\right),$$

soit

$$\beta(Q,w,\alpha) \leq b(Q).$$

D'après le corollaire 6.2, pour tout nombre entier $N \geq N(Q,w,\alpha)$, on a

$$|\sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \mathrm{e}(\alpha w(X^2))| \leq b(Q)N^{\frac{\omega(Q)+1}{4}}q^{N(1-a)}.$$

□

Terminons cette section par la preuve du corollaire 1.3. Soient m un nombre entier strictement positif et $a \in \{0,1,\dots m-1\}$. Poson

$$z(m,a,N) = \mathrm{Card}\{X \in \mathbf{A} | \deg X < n,\ f(X^2) \equiv a \pmod m\}.$$

On a

$$z(m,a,N) = \sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} \frac{1}{m}\sum_{h=0}^{m-1} e(\frac{h(f(X^2)-a)}{m}).$$

En inversant l'ordre des sommations on obtient

$$mz(m,a,N) = \sum_{h=0}^{m-1} e(\frac{-ha}{m}) \sum_{\substack{X\in\mathbf{A}\\ \deg X<N}} e(\frac{hf(X^2)}{m})$$

$$= q^N + \sum_{h=1}^{m-1} e(\frac{-ha}{m}) \sum_{\substack{X \in \mathbf{A} \\ \deg X < N}} e(\frac{h}{m} f(X^2)).$$

Le théorème 1.2 nous donne alors

$$|mz(m,a,N) - q^N| \leq \sum_{h=1}^{m-1} b(q,Q) N^{\frac{\omega(Q)+1}{4}} q^{N(1-a(q,Q,f,h/m))}$$

$$\leq (m-1) b(q,Q) N^{\frac{\omega(Q)+1}{4}} q^{N(1-\eta(q,Q,f,m))},$$

avec $\eta(q,Q,f,m) = \min_{1 \leq h \leq m-1}\{a(q,Q,f,h/m)\}$, d'où le résultat annoncé.

□

Références

[1] N.L. Bassily, I. Kátai, *Distribution of the values of q-additive functions on polynomial sequences*, Acta Math. Hung. **68** (1995), 353-361.

[2] M. Car, *Quadratic forms on* $\mathbf{F}_q[T]$, J. Number Theory **61**, $n\,°1$, (1996), 145-180.

[3] L. Carlitz, *Diophantine approximations in fields of characteristic p*, Proc. Amer. Math. Soc. (1952), 187-208.

[4] M. Car, C. Mauduit, *Sur les puissances des polynômes sur un corps fini*, Uniform Distribution Theory, **8**, No 2, (2013), 171-182.

[5] M. Drmota, *The joint distribution of q-additive functions*, Acta Arith. **100** (2001), 17-39

[6] M. Drmota, G. Gutenbrunner, *The joint distribution of Q-additive functions on polynomials over finite fields*, J. Theor. Nombres Bordeaux **17** (2005), 125-150.

[7] M. Drmota, J.F. Morgenbesser, *Generalized Thue-Morse sequences of squares*, Israel J. Math. **190** (2012), 157-193

[8] D. R. Hayes, *The expression of a polynomial as the sum of three irreducibles,* Acta Arith **11** (1966), 461-488.

[9] D. H. Kim, *On the joint distribution of q-additive functions in residue classes*, J. Number Theeory **74** (1999), 307-336.

[10] M. Madritsch, J. Thuswaldner *Weyl sums in* $\mathbf{F}_q[X]$ *with digital restrictions* , Finite Fields and Their Applications **14**, $n\,°1$, (2008), 877-896.

[11] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, vol 20, (1983), (Reprinted 1987).

[12] C. Mauduit, J. Rivat, *La somme des chiffres des carrés*, Acta Math., **203** (2009), 107-148.

[13] C. Mauduit, J. Rivat, *Sur un problème de Gelfond : la somme des chiffres des nombres premiers*, Ann. of Math. **171** (2010), 1591-1646.

[14] C. Mauduit, J. Rivat, *Rudin-Shapiro sequences along squares*, preprint.