ACTA ARITHMETICA
112.1 (2004)

Formes cubiques sur $\mathbb{F}_{2^h}[T]$

par

Mireille Car (Marseille)

Introduction. Soit q une puissance de 2 et $\mathbb{F}_q$ un corps fini à q éléments. Comme on le verra dans un article à paraître ultérieurement [3], l'étude de l'existence de représentations d'un polynôme $M \in \mathbb{F}_q[T]$ comme somme de cubes et de carrés et donc, puisque la caractéristique est 2, comme somme de cubes et d'un carré se ramène à l'étude de l'existence de représentations du polynôme M_1 associé à M par la relation $M = M_0^2 + TM_1^2$ comme somme

$$M_1 = \sum_{i=1}^{s} (V_i U_i^2 + T V_i^3).$$

L'étude de telles représentations nécessite la majoration du nombre de représentations de 0 comme somme

$$0 = \sum_{i=1}^{s} X_i Y_i^2,$$

X_i et Y_i étant des polynômes de $\mathbb{F}_q[T]$ vérifiant les conditions de degré

$$\deg X_i \le n, \quad \deg Y_i \le n,$$

ce qui conduit à l'étude des représentations d'un polynôme $M \in \mathbb{F}_q[T]$ comme somme

$$M = \sum_{i=1}^{s} X_i Y_i^2, \tag{1}$$

où X_i et Y_i sont des polynômes de $\mathbb{F}_q[T]$ soumis aux conditions de degré

$$\deg X_i \le n, \quad \deg Y_i \le n, \tag{2}$$

étude qui sera menée dans ce qui suit.

Notons $R(s, n, M)$ le nombre des représentations de $M \in \mathbb{F}_q[T]$ comme somme (1) où X_i et Y_i sont des polynômes de $\mathbb{F}_q[T]$ vérifiant les conditions de degré (2). Si le polynôme M admet une représentation (1) où les polynômes

2000 *Mathematics Subject Classification*: 11T06, 11T55.

X_i et Y_i vérifient les conditions (2), nécessairement $\deg M \leq 3n$. Suivant la terminologie introduite dans [4], nous dirons que la représentation (1) est *stricte* si les polynômes X_i et Y_i vérifient les conditions de degré les plus restrictives possibles, c'est-à-dire s'ils vérifient les conditions de degré (2), l'entier n étant déterminé par la relation

$$3n - 2 \leq \deg M \leq 3n. \tag{3}$$

Notons $Q(s, M)$ le nombre de représentations strictes de M comme somme (1). La méthode du cercle permet d'obtenir, sous l'hypothèse $s \geq 5$, une estimation asymptotique des nombres $R(s, n, M)$ pour n tendant vers ∞, d'où l'on déduit une estimation asymptotique des nombres $Q(s, M)$ pour $\deg M$ tendant vers ∞. Plus précisément, nous démontrons le théorème suivant.

THÉORÈME A. *Soit un entier $s \geq 5$. Alors, pour n tendant vers ∞ et pour tout polynôme M tel que* $\deg M \leq 3n$, *on a*

$$R(s, n, M) = C_s(M) q^{n(2s-3)} + O(q^{n(3s/2-1)}),$$

où

$$(q^s - 1)(q^{s-1} - 1) \leq C_s(M) \leq \frac{q^{(5s-7)/2}(q^s - 1)}{(q^{(s-3)/2} - 1)(q^{(s-1)/2} - 1)(q^{s-2} - 1)},$$

les constantes impliquées par le symbole O ne dépendant que de q et de s, et, pour $\deg M$ *tendant vers ∞, on a*

$$Q(s, M) = C_s(M) q^{n(2s-3)} + O(q^{n(3s/2-1)}),$$

l'entier n étant déterminé par la condition $3n - 2 \leq \deg M \leq 3n$.

De façon évidente, seule la représentation triviale est une représentation stricte du polynôme nul comme somme (1). La méthode utilisée ici ne nous permet pas d'obtenir une estimation asymptotique des nombres $R(s, n, 0)$ pour $s \leq 4$. Nous obtenons seulement une minoration et une majoration asymptotiques des nombres $R(4, n, 0)$ par des fonctions de même ordre de grandeur. Plus précisément, nous démontrons le théorème suivant.

THÉORÈME B. *Pour n tendant vers ∞, on a*

$$q^3(q^4 + 1)(q^2 + q + 1)q^{5n} + O(q^{9n/2})$$
$$\leq R(4, n, 0) \leq \left(q^3(q^4 + 1)(q^2 + q + 1) + \frac{q^8 + 5q^5 - 4q^6}{q - 1}\right) q^{5n} + O(q^{9n/2}),$$

les constantes impliquées par les symboles O ne dépendant que de q.

Pour établir ces théorèmes nous sommes amenés à majorer les nombres $R(2, n, 0)$. Cette majoration est obtenue par des méthodes élémentaires donnant aussi une minoration de ces nombres (voir le théorème IV.5 ci-desous). De façon évidente, $R(1, n, 0) = 2q^{n+1} - 1$. Pour compléter notre étude,

nous donnons au théorème IV.5 une majoration et une minoration asymptotiques des nombres $R(3,n,0)$. Notons aussi que tout polynôme M s'écrivant $M = 1^2 M$, pour tout polynôme M non nul on a $R(1, \deg M, M) \geq 1$.

Cette dernière remarque nous permet d'établir à l'aide de considérations élémentaires les relations

$$R(3,n,M) \geq (q-1)^2 q^{-1} q^{3n/2}, \qquad R(4,n,M) \geq (q-1)^2 q^{1+7n/2},$$

valables pour tout polynôme M tel que $\deg M \leq 3n$. Ceci nous montre que tout polynôme $M \in \mathbb{F}_q[T]$ non nul admet une représentation stricte comme somme

$$M = X_1 Y_1^2 + X_2 Y_2^2 + X_3 Y_3^2.$$

On a là une représentation stricte d'un polynôme de $\mathbb{F}_q[T]$ par une forme cubique à 6 variables. Rappelons ici que, par d'astucieuses méthodes élémentaires, L. Gallardo a démontré que si $q \neq 2, 4, 16$, tout polynôme de $\mathbb{F}_q[T]$ admet une représentation stricte comme somme de 5 formes cubiques $Q(A,B) = AB(A+B)$ (cf. [5]), que tout polynôme de $\mathbb{F}_q[T]$ admet une représentation stricte comme somme de 9 cubes, et que tout polynôme de $\mathbb{F}_{16}[T]$ admet une représentation stricte comme somme de 10 cubes (cf. [6]). D'autres considérations élémentaires nous permettront de démontrer que l'ensemble E_2 des polynômes M de degré au plus $3n$ admettant une représentation comme somme $M = X_1 Y_1^2 + X_2 Y_2^2$, où X_1, Y_1, X_2, Y_2 sont des polynômes de degré au plus n, est de densité strictement positive minorée par

$$\frac{q^5(q+1)}{q^7 + q^5 + 5q^4 + 6q^3 + 3q^2 + 2q + 1},$$

et que si E_1 designe l'ensemble des polynômes M de degré au plus $3n$, pouvant s'écrire comme produit $M = XY^2$ où $\deg X \leq n$, $\deg Y \leq n$, alors

$$\frac{q+1}{q^4 + 3q + 4}\, q^{2n+2} \leq \operatorname{card}(E_1) \leq q^{2n+2}.$$

I. La méthode du cercle

I.1. *Notations et conventions.* Dans ce qui suit le mot polynôme désigne un élément de $\mathbb{A} = \mathbb{F}_q[T]$. L'ensemble des polynômes unitaires est noté $\mathbb{M}$, l'ensemble des polynômes irréductibles unitaires est noté $\mathbb{I}$, tandis que l'ensemble des polynômes unitaires sans facteur carré est noté $\mathbb{S}$. On note $\mathbb{A}_n$ l'ensemble des polynômes de $\mathbb{A}$ de degré au plus n.

Soit H un polynôme non nul. On note $\mathcal{C}_H$ l'ensemble des polynômes de degré strictement inférieur à $\deg H$ identifié à l'ensemble des classes de congruence modulo H, et on note $\mathcal{C}_H^*$ l'ensemble des polynômes de $\mathcal{C}_H$ inversibles modulo H. Si Y est un polynôme, on note $H \mid Y$ la relation H divise Y.

Soit $v = v_\infty$ la valuation à l'infini définie sur le corps $\mathbb{K} = \mathbb{F}_q(T)$. On lui associe la valeur absolue $|\ |_\infty$ définie par

$$|a|_\infty = q^{-v(a)} \quad \text{si } a \neq 0, \qquad |0|_\infty = 0,$$

que l'on notera $|\ |$ pour simplifier. Notons $\mathbb{K}_\infty$ le complété de $\mathbb{K}$ pour la valeur absolue à l'infini et notons encore v, respectivement $|\ |$, l'extension au complété $\mathbb{K}_\infty$ de la valuation v, respectivement de la valeur absolue $|\ |$. Le corps $\mathbb{K}_\infty$ s'identifie au corps des séries de Laurent formelles en T^{-1}.

Si $u \in \mathbb{K}_\infty$ et si

$$u = \sum_{s=-\infty}^{\infty} u_s T^s,$$

on pose

$$\mathrm{Res}(u) = u_{-1}.$$

Si de plus $u \neq 0$, on pose

$$\mathrm{sgn}(u) = u_{-v(u)}.$$

Enfin, si B est un ensemble fini, on note $\#B$ le nombre d'éléments de B.

I.2. *Le caractère E et la mesure de Haar dt.* On définit un caractère E de $\mathbb{K}_\infty$ en posant

$$E(y) = \psi_q(\mathrm{Res}(y)), \tag{I.1}$$

où ψ_q est le caractère de $\mathbb{F}_q$ défini par

$$\psi_q(y) = (-1)^{\mathrm{tr}_{\mathbb{F}_q|\mathbb{F}_2}(y)}. \tag{I.2}$$

Le caractère ψ_q étant non trivial, il en est de même du caractère E.

On désigne par $\wp$ l'idéal de valuation de $\mathbb{K}_\infty$ et on désigne par dt la mesure de Haar sur $\mathbb{K}_\infty$ normalisée à 1 sur l'idéal de valuation $\wp$. Tout $u \in \mathbb{K}_\infty$ s'écrit de façon unique comme somme

$$u = [u] + \{u\}, \qquad [u] \in \mathbb{A},\ \{u\} \in \wp. \tag{I.3}$$

(On utilisera aussi la notation $[y]$ pour désigner la partie entière d'un nombre réel y, mais il y a peu de risque de confusion.)

La proposition suivante rappelle un certain nombre de résultats établis dans [7] ou se démontrant de façon analogue. Nous n'en donnons pas la démonstration.

Proposition I.1. (1) *Pour tout entier rationnel j, $\wp_j$ a pour mesure q^{-j}.*

(2) *On a $E(H) = 1$ pour tout $H \in \mathbb{A}$.*

(3) *Pour tout polynôme H non nul, si A et B sont des polynômes congrus modulo H, on a*

$$E(A/H) = E(B/H).$$

(4) *Pour $u \in \mathbb{K}_\infty$, on a l'implication*

$$v(u) \geq 2 \;\Rightarrow\; E(u) = 1. \tag{I.4}$$

(5) *Soient j un entier rationnel et $u \in \mathbb{K}_\infty$. Alors, on a*

$$\int_{v(t)>j} E(ut)\,dt = \begin{cases} q^{-j} & \text{si } v(u) > -j, \\ 0 & \text{sinon}, \end{cases} \tag{I.5}$$

$$\sum_{B \in \mathbb{A}_j} E(uB) = \begin{cases} q^{j+1} & \text{si } v(\{u\}) > j+1, \\ 0 & \text{sinon.} \end{cases} \tag{I.6}$$

(6) *Soient H un polynôme non nul et G un polynôme. Alors, on a*

$$\sum_{R \in \mathcal{C}_H} E(GR/H) = \begin{cases} |H| & \text{si } H \text{ divise } G, \\ 0 & \text{sinon.} \end{cases} \tag{I.7}$$

Proposition I.2. *Soient $a_0, a_1, \ldots, a_d$ des éléments de $\mathbb{K}_\infty$ et F l'application de $\mathbb{K}_\infty$ dans $\mathbb{K}_\infty$ définie par*

$$F(t) = a_0 + a_1 t + \ldots + a_d t^d.$$

Alors, pour tout entier rationnel j et tout $y \in \mathbb{K}_\infty^*$, on a

$$|y| \int_{v(t)>j} E(F(ty))\,dt = \int_{v(t)>j+v(y)} E(F(t))\,dt. \tag{I.8}$$

Preuve. C'est la proposition I.6 de [2].

Rappelons encore quelques résultats propres à la caractéristique 2 établis dans [2].

Proposition I.3. *Soient $\mathcal{G}$ un sous-groupe additif fini de $\mathbb{K}_\infty$, $a \in \mathbb{K}_\infty$ et $b \in \mathbb{K}_\infty$. Alors, on a*

$$\sum_{G \in \mathcal{G}} E(aG^2 + bG) \in \{0, \#\mathcal{G}\}. \tag{I.9}$$

Proposition I.4. *Soient j un entier rationnel, a et b des éléments de $\mathbb{K}_\infty$. Alors, on a*

$$\int_{v(t)>j} E(at^2 + bt)\,dt \in \{0, q^{-j}\}. \tag{I.10}$$

De plus, si l'on pose

$$I(a,b) = \int_{\wp} E(at^2 + bt)\,dt, \tag{I.11}$$

alors $I(a,b) = 1$ si et seulement si $[a] + T[b]^2$ est carré dans $\mathbb{A}$.

I.3. *La méthode du cercle et la dissection de Farey.* Soit un entier $n \geq 0$. Pour $t \in \mathbb{K}_\infty$ on pose

$$g(t) = \sum_{(A,B)\in \mathbb{A}_n \times \mathbb{A}_n} E(tAB^2). \tag{I.12}$$

D'après (I.5),

$$R(s,n,M) = \int_{\wp} g(t)^s E(tM)\, dt. \tag{I.13}$$

On approche t par des fractions rationnelles. On appelle *fraction de Farey à l'ordre n* toute fraction rationnelle G/H telle que $\deg H \leq n$, $\deg G < \deg H$, $\operatorname{pgcd}(H,G) = 1$. On désigne par $\mathcal{F}_n$ l'ensemble des fractions de Farey à l'ordre n. Si $G/H \in \mathcal{F}_n$ on appelle *arc de Farey de centre* G/H l'ensemble

$$\mathcal{U}_{n,G/H} = \{t \in \wp\,;\, v(t - G/H) > n + \deg H\}. \tag{I.14}$$

Proposition I.5. *Lorsque G/H décrit l'ensemble des fractions de Farey à l'ordre n, les arcs de Farey $\mathcal{U}_{n,G/H}$ forment une partition de $\wp$.*

Preuve. C'est le théorème 4.3 de [7].

Proposition I.6. *Soit $u \in \wp$ tel que $v(u) > 2n$. Alors, on a*

$$g(u) = \begin{cases} q^{2n+2} & \text{si } v(u) > 3n+1, \\ q^{n+1+[(v(u)-n)/2]} & \text{si } v(u) \leq 3n+1. \end{cases} \tag{I.15}$$

Preuve. Avec (I.12) et (I.4), la première des égalités (I.15) est immédiate. Avec (I.12) et (I.6) on a

$$g(u) = q^{n+1} \#\{X \in \mathbb{A}_n\,;\, v(\{uX^2\}) > n+1\},$$

d'où la deuxième des égalités (I.15).

II. Les arcs mineurs

Proposition II.1. *On a*

$$3q^{2n+2} \leq \int_{\wp} g(t)^2\, dt \leq \frac{q^6 + 3q^3 + 4q^2}{q+1}\, q^{2n}. \tag{II.1}$$

Preuve. D'après (I.13) l'intégrale $\int_\wp g(t)^2\, dt$ est égale au nombre $u(n)$ de solutions $(X,Y,U,V) \in \mathbb{A}_n \times \mathbb{A}_n \times \mathbb{A}_n \times \mathbb{A}_n$ de l'équation

$$XY^2 = UV^2. \tag{1}$$

Parmi ces solutions il y a $v(n)$ solutions (X,Y,U,V) telles que $XYUV \neq 0$ et $w(n)$ solutions (X,Y,U,V) telles que $XYUV = 0$. De façon évidente,

$$w(n) = (2q^{n+1} - 1)^2. \tag{2}$$

Pour $n > 0$, on minore $u(n)$ par $w(n)$ et $w(n)$ par $3q^{2n+2}$. On remarque que cette minoration de $u(n)$ reste vraie pour $n = 0$. Si (X,Y,U,V) est

une solution comptée dans $v(n)$, il existe des polynômes unitaires A et B premiers entre eux, des polynômes G et H unitaires et des éléments x, y, u, v non nuls dans $\mathbb{F}_q$ tels que

$$X = xA^2G, \quad U = uB^2G, \quad V = vAH, \quad Y = yBH \quad \text{et} \quad xy^2 = uv^2.$$

Par suite,

$$v(n) \le (q-1)^3 \sum_{\substack{(A,B)\in\mathbb{M}\times\mathbb{M}\\ 2\deg A\le n,\, 2\deg B\le n}} q^{2n+2-3\max(\deg A,\deg B)},$$

soit

$$v(n) \le \frac{q^3-1}{q+1}\, q^{2n+3}, \tag{3}$$

d'où le résultat annoncé.

Proposition II.2. *Soit G/H une fraction de Farey à l'ordre n et $t = u + G/H$ un élément de l'arc de Farey $\mathcal{U}_{n,G/H}$. Alors, on a*

$$|H|g(t) = \sum_{K\in\mathcal{C}_H} \sum_{Y\in\mathbb{A}_n} W(H, GY, K)\Gamma(uY, K/H), \tag{II.2}$$

avec

$$W(H, A, K) = \sum_{R\in\mathcal{C}_H} E\Big(\frac{AR^2 + KR}{H}\Big), \tag{II.3}$$

$$\Gamma(z, K/H) = \sum_{X\in\mathbb{A}_n} E(zX^2 + KX/H). \tag{II.4}$$

Preuve. On a

$$g(t) = \sum_{Y\in\mathbb{A}_n} \sum_{R\in\mathcal{C}_H} \sum_{\substack{X\in\mathbb{A}_n\\ X\equiv R \bmod H}} E((G/H + u)YX^2),$$

d'où, avec (I.7),

$$|H|g(t) = \sum_{Y\in\mathbb{A}_n} \sum_{R\in\mathcal{C}_H} E(GYR^2/H) \sum_{X\in\mathbb{A}_n} E(uYX^2) \sum_{K\in\mathcal{C}_H} E(K(R+X)/H).$$

On obtient (II.2) par inversion de l'ordre des sommations.

Soit H un polynôme unitaire de degré au plus n. On pose

$$H = \Lambda(H)\Psi(H)^2 = \Lambda\Psi^2, \tag{II.5}$$

où Λ et Ψ sont les fonctions multiplicatives définies pour tout $P \in \mathbb{I}$, tout entier $k \ge 0$, par

$$\Lambda(P^{2k}) = 1, \quad \Lambda(P^{2k+1}) = P, \tag{II.6}$$

$$\Psi(P^{2k}) = \Psi(P^{2k+1}) = P^k. \tag{II.7}$$

PROPOSITION II.3. *Soit $K \in \mathcal{C}_H$. Alors*

(i) $W(H,A,K) \in \{0, |H|\}$,

(ii) *si $\Psi(H)$ ne divise pas K, alors pour tout polynôme A, $W(H,A,K) = 0$,*

(iii) *si $\Psi(H)$ divise K, alors il y a exactement $|\Psi(H)|$ polynômes $A \in \mathcal{C}_H$ tels que $W(H,A,K) \neq 0$.*

Preuve. Le premier point est une conséquence de (I.9) et de la définition (II.3). Après inversion de l'ordre des sommations on obtient l'égalité

$$\sum_{A\in\mathcal{C}_H} W(H,A,K) = \sum_{R\in\mathcal{C}_H} E(KR/H) \sum_{A\in\mathcal{C}_H} E(AR^2/H),$$

d'où, avec (I.7),

$$\sum_{A\in\mathcal{C}_H} W(H,A,K) = |H| \sum_{\substack{R\in\mathcal{C}_H \\ H|R^2}} E(KR/H) = |H| \sum_{\substack{R\in\mathcal{C}_H \\ \Lambda\Psi|R}} E(KR/H)$$
$$= |H| \sum_{Z\in\mathcal{C}_\Psi} E(KZ/\Psi).$$

Finalement (I.7) nous donne

$$\sum_{A\in\mathcal{C}_H} W(H,A,K) = \begin{cases} |H|\,|\Psi| & \text{si } \Psi \text{ divise } K, \\ 0 & \text{sinon,} \end{cases}$$

ce qui établit les deux derniers points.

PROPOSITION II.4. *Soient $G \in \mathcal{C}_H$ premier à H, $K \in \mathcal{C}_H$ divisible par $\Psi(H)$ et Y un polynôme tel que $W(H,GY,K) \neq 0$. Soit Z un polynôme. Alors $W(H,G(Y+Z),K) \neq 0$ si et seulement si Z vérifie les deux conditions suivantes* :

(i) *$\Lambda(H)$ divise Z,*

(ii) *$GZ/\Lambda(H)$ est congru à un carré modulo $\Psi(H)^2$.*

Preuve. Compte tenu de (II.3) et du point (i) de la proposition précédente,

$$W(H,G(Y+Z),K) \neq 0 \;\Leftrightarrow\; W(H,GZ,0) \neq 0.$$

On a

$$W(H,GZ,0) = \sum_{Q\in\mathcal{C}_\Psi} \sum_{R\in\mathcal{C}_\Lambda} \sum_{S\in\mathcal{C}_\Psi} E\Big(\frac{GZ(Q+\Psi R+\Psi\Lambda S)^2}{\Psi^2\Lambda}\Big),$$

d'où

$$W(H,GZ,0) = |\Psi| \sum_{Q\in\mathcal{C}_\Psi} E\Big(\frac{GZQ^2}{\Psi^2\Lambda}\Big) \sum_{R\in\mathcal{C}_\Lambda} E(GZR^2/\Lambda). \tag{1}$$

Soit $V \in \mathcal{C}_\Lambda$ congru à GZ modulo Λ. D'après (I.4), puis (I.8),

$$\sum_{R\in\mathcal{C}_\Lambda} E(GZR^2/\Lambda) = \int\limits_{v(y)>-\deg\Lambda} E(Vy^2/\Lambda)\,dy = |\Lambda| \int\limits_{\wp} E(V\Lambda y^2)\,dy.$$

Enfin, d'après la proposition I.4,

$$\sum_{R\in\mathcal{C}_\Lambda} E(GZR^2/\Lambda) = \begin{cases} |\Lambda| & \text{si } V\Lambda \text{ est carré,} \\ 0 & \text{sinon.} \end{cases}$$

Comme Λ est sans facteur carré et que $V \in \mathcal{C}_\Lambda$, $V\Lambda$ est carré si et seulement si $V = 0$, c'est-à-dire si Λ divise GZ. Puisque G et H sont premiers entre eux,

$$\sum_{R\in\mathcal{C}_\Lambda} E(GZR^2/\Lambda) = \begin{cases} |\Lambda| & \text{si } \Lambda \text{ divise } Z, \\ 0 & \text{sinon.} \end{cases}$$

Supposons donc que Λ divise Z et posons $Z = \Lambda W$. Avec (1), il vient

$$W(H, GZ, 0) = |\Psi|\,|\Lambda| \sum_{Q\in\mathcal{C}_\Psi} E(GWQ^2/\Psi^2).$$

Soit $U \in \mathcal{C}_{\Psi^2}$ congru à GW modulo Ψ^2. En procédant comme ci-dessus, on démontre que

$$\sum_{Q\in\mathcal{C}_\Psi} E(GWQ^2/\Psi^2) = \begin{cases} |\Psi| & \text{si } U \text{ est carré,} \\ 0 & \text{sinon,} \end{cases}$$

établissant ainsi le résultat annoncé.

PROPOSITION II.5. *Soit $u \in \wp$ tel que*

$$n + \deg H < v(u) \le 2n + \deg H. \tag{II.8}$$

Alors

(i) $\Gamma(uY, K/H) \in \{0, q^{n+1}\}$,

(ii) $\Gamma(uY, K/H) \neq 0$ *si et seulement si* $[uYT^{2(n+1)}] + T[KT^{n+1}/H]^2$ *est carré*,

(iii) $\Gamma(uY, K/H) \neq 0 \;\Rightarrow\; 2\deg K \le \deg H - 2$.

De plus, soit $Y \in \mathbb{A}_n$ tel que $\Gamma(uY, K/H) \neq 0$ et soit $Z \in \mathbb{A}_n$. Alors, $\Gamma(u(Y+Z), K/H) \neq 0$ si et seulement si $[uZT^{2(n+1)}]$ est carré.

Preuve. Le premier point est une conséqunce de (I.9). D'après (I.4), puis (I.8),

$$\begin{aligned}\Gamma(uY, K/H) &= \int\limits_{v(x)\ge -n} (E(\{uY\})x^2 + Kx/H)\,dx \\ &= q^{n+1} \int\limits_{\wp} (E(T^{2(n+1)}\{uY\})x^2 + KT^{n+1}x/H)\,dx.\end{aligned}$$

D'après la proposition I.4,

$$\Gamma(uY, K/H) \neq 0 \;\Leftrightarrow\; [\{uY\}T^{2(n+1)}] + T[KT^{2n+1}/H]^2 \text{ est carré.}$$

On a $v(u) > n + \deg H$, d'où, pour tout $Y \in \mathbb{A}_n$, $v(uY) > 0$ et $\{uY\} = uY$. La deuxième partie de la proposition est établie. Si $\Gamma(uY, K/H) \neq 0$, alors $[uYT^{2(n+1)}] + T[KT^{n+1}/H]^2$ est carré, d'où

$$\deg[uYT^{2(n+1)}] \geq 1 + 2\deg[KT^{n+1}/H],$$
$$2\deg K \leq 2\deg H + n - v(u) - 1 \leq \deg H - 2,$$

ce qui démontre (iii). La dernière partie de la proposition se déduit de (ii).

PROPOSITION II.6. *Soit G/H une fraction de Farey à l'ordre n et t un élément de l'arc de Farey $\mathcal{U}_{n,G/H}$ tel que $n + \deg H < v(t - G/H) \leq 2n + \deg H$. Alors, on a*

$$g(t) \leq q^{3n/2+1}. \tag{II.9}$$

Preuve. Posons $u = t + G/H$. Alors,

$$v(u) > n + \deg H. \tag{1}$$

Soit $\mathcal{K}(t)$ l'ensemble des polynômes $K \in \mathcal{C}_H$ pour lesquels existe un polynôme $Y \in \mathbb{A}_n$ vérifiant

$$W(H, GY, K) \neq 0 \quad \text{et} \quad \Gamma(uY, K/H) \neq 0. \tag{2}$$

D'après les propositions II.2–II.5,

$$g(t) = q^{n+1}\#\mathcal{K}(t)\#\mathcal{Z}(u, H), \tag{3}$$

où $\mathcal{Z}(u, H)$ est l'ensemble des polynômes $Z \in \mathbb{A}_n$ tels que

$$[uZT^{2(n+1)}] \text{ soit carré}, \quad \Lambda \,|\, Z, \quad GZ/\Lambda \text{ soit carré mod } \Psi^2.$$

Soit $\mathcal{R}(H)$ l'ensemble des $R \in \mathcal{C}_H$ tels que $\Lambda \,|\, R$ et GR/Λ soit carré mod Ψ^2. Alors,

$$\#\mathcal{Z}(u, H) = \sum_{R \in \mathcal{R}(H)} \#\{Z \in \mathbb{A}_n\,;\, Z \equiv R \bmod H,\, [uZT^{2(n+1)}] \text{ carré}\}.$$

Les arguments utilisés pour établir la proposition II.5 nous donnent la caractérisation

$$[uZT^{2(n+1)}] \text{ carré} \;\Leftrightarrow\; \sum_{X \in \mathbb{A}_n} E(uZX^2) = q^{n+1},$$

d'où,

$$\begin{aligned} q^{n+1}\#\mathcal{Z}(u, H) &= \sum_{R \in \mathcal{R}(H)} \sum_{\substack{Z \in \mathbb{A}_n \\ Z \equiv R \bmod H}} \sum_{X \in \mathbb{A}_n} E(uZX^2) \\ &= \sum_{R \in \mathcal{R}(H)} \sum_{Z \in \mathbb{A}_{n-\deg H}} \sum_{X \in \mathbb{A}_n} E(u(R + ZH)X^2) \end{aligned}$$

$$= \sum_{R\in\mathcal{R}(H)} \sum_{X\in\mathbb{A}_n} E(uRX^2) \sum_{Z\in\mathbb{A}_{n-\deg H}} E(uZHX^2)$$

$$\leq \sum_{R\in\mathcal{R}(H)} \sum_{X\in\mathbb{A}_n} \sum_{Z\in\mathbb{A}_{n-\deg H}} E(uZHX^2),$$

d'où, après inversion de l'ordre des sommations,

$$q^{n+1}\#\mathcal{Z}(u,H) \leq \#\mathcal{R}(H) \sum_{Z\in\mathbb{A}_{n-\deg H}} \sum_{X\in\mathbb{A}_n} E(uZHX^2).$$

Comme ci-dessus

$$\sum_{X\in\mathbb{A}_n} E(uZHX^2) = q^{n+1} \;\Leftrightarrow\; [uZHT^{2(n+1)}] \text{ carré},$$

d'où

$$\#\mathcal{Z}(u,H) \leq \#\mathcal{R}(H)\#\{Z\in\mathbb{A}_{n-\deg H}\,;\,[uHZT^{2(n+1)}] \text{ carré}\}. \tag{4}$$

Les arguments utilisés pour établir la proposition II.4 conduisent à l'égalité

$$\#\mathcal{R}(H)|\Psi| = \sum_{Q\in\mathcal{C}_{\Psi^2}} \sum_{X\in\mathcal{C}_\Psi} E(GQX^2/\Psi^2)$$

$$= \sum_{X\in\mathcal{C}_\Psi} \sum_{Q\in\mathcal{C}_{\Psi^2}} E(GQX^2/\Psi^2) = |\Psi|^2,$$

d'où

$$\#\mathcal{R}(H) = |\Psi|. \tag{5}$$

Notons $\alpha(u)$ le nombre de polynômes $Z\in\mathbb{A}_{n-\deg H}$ tels que $[uZHT^{2n+2}]$ soit un carré et posons

$$k = v(u) - \deg H, \tag{6}$$

$$uH = \sum_{i=-\infty}^{-k} v_i T^i, \tag{7}$$

$$m = n - \deg H. \tag{8}$$

Alors $\alpha(u)$ est égal au nombre de solutions $(z_0, z_1, \ldots, z_m)\in\mathbb{F}_q^{m+1}$ du système d'équations linéaires (e_λ) suivant :

$$\sum_{\substack{i+j=2\lambda+1\\ i\leq -s,\, 0\leq j\leq d}} v_i z_j = 0, \tag{e_λ}$$

λ étant un entier tel que $-2n-1 \leq 2\lambda+1 \leq m-k$. Supposons $z_m, z_{m-1}, \ldots$ $\ldots, z_{m+2\lambda}$ déterminés. Comme v_{-k} est non nul, l'équation $(e_{\lambda-1})$ détermine alors $z_{m+2\lambda-1}$. Supposons $m-k$ pair, $m-k = 2\delta$. Si k est pair, $k =$

2κ, on choisit les coefficients $z_m, z_{m-2}, \dots, z_0$ et on détermine les coefficients $z_{m-1}, z_{m-3}, \dots, z_1$ par les équations $(e_{\delta-1}), \dots, (e_{-\kappa})$. Si k est impair, $k = 2\kappa + 1$, on choisit les coefficients $z_m, z_{m-2}, \dots, z_1$ et on détermine les coefficients $z_{m-1}, \dots, z_0$ par les équations $(e_{\delta-1}), \dots, (e_{-1-\kappa})$. Si les équations (e_λ) restantes sont vérifiées par le système $(z_0, z_1, \dots, z_m)$, celui-ci est compté dans $\alpha(u)$. Sous l'hypothèse $m - k$ pair, on a donc la majoration

$$\alpha(u) \le \begin{cases} q^{1+m/2} & \text{si } m \text{ est pair,} \\ q^{(m+1)/2} & \text{si } m \text{ est impair.} \end{cases}$$

On procède de façon analogue si $m - k$ est impair. On obtient

$$\alpha(u) \le \begin{cases} q^{m/2} & \text{si } m \text{ est pair,} \\ q^{(m+1)/2} & \text{si } m \text{ est impair.} \end{cases}$$

Dans tous les cas

$$\alpha(u) \le q^{1+(n-\deg H)/2},$$

c'est-à-dire

$$\#\{Z \in \mathbb{A}_{n-\deg H}\,;\, [uHZT^{2(n+1)}] \text{ carré}\} \le q^{1+(n-\deg H)/2}. \tag{9}$$

Avec (4), (5) et (9), puis (II.5), il vient

$$\#\mathcal{Z}(u, H) \le q^{1+(n-\deg H)/2}|\Psi| \le q^{1+n/2}|\Lambda|^{-1/2}.$$

L'égalité (3) donne alors

$$g(t) \le q^{3n/2+2}\#\mathcal{K}(t)|\Lambda|^{-1/2}. \tag{10}$$

Soit $K \in \mathcal{K}(t)$. Les conditions (iii) des propositions II.3 et II.5 montrent que K est divisible par Ψ et que $2\deg K \le \deg H - 2$. Par conséquent,

$$\#\mathcal{K}(t) \le q^{-1}|\Lambda|^{1/2},$$

ce qui donne le résultat annoncé.

Comme au paragraphe I.3, $\mathcal{F}_n$ désigne l'ensemble des fractions de Farey à l'ordre n. Si $G/H \in \mathcal{F}_n$, on appelle *arc mineur de centre* G/H l'ensemble des $t \in \wp$ tels que

$$n + \deg H < v(t - G/H) \le 2n + \deg H, \tag{II.10}$$

et on note $\wp^-$ la réunion des arcs mineurs de centre G/H, G/H parcourant $\mathcal{F}_n$.

Soit un entier $s \ge 4$. Posons, pour tout polynôme M,

$$R(s, n, M)^- = \int_{\wp^-} g(t)^s E(tM)\, dt. \tag{II.11}$$

Proposition II.7. *Pour tout polynôme M on a*

$$|R(s, n, M)^-| \le a_1(s) q^{n(3s/2-1)}, \tag{II.12}$$

avec

$$a_1(s) = \frac{q^6 + 3q^3 + 4q^2}{q+1}\, q^{s-2}. \tag{II.13}$$

Preuve. D'après (II.1) et (II.9),

$$|R(s,n,M)^-| \le q^{(s-2)(3n/2+1)} \int_{\wp} |g(t)|^2\, dt.$$

On conclut avec (II.1).

III. Les séries singulières. Soit un entier $s \ge 2$. Soit M un polynôme. Pour tout polynôme unitaire H, on pose

$$A(s,M,H) = |H|^{-s} |\Psi(H)|^s B(M,H) \tag{III.1}$$

où Ψ est la fonction multiplicative définie par la relation (II.7) et

$$B(M,H) = \sum_{G \in \mathcal{C}_H^*} E(GM/H). \tag{III.2}$$

Dans ce qui suit on s'intéresse aux séries

$$S_s(M) = \sum_{H \in \mathbb{M}} A(s,M,H). \tag{III.3}$$

Proposition III.1. *Soit P un polynôme irréductible unitaire. Le polynôme M étant supposé non nul, soit v la valuation P-adique de M. Alors, pour tout entier $m \ge 0$, on a*

$$B(M,P^m) = \begin{cases} 0 & \text{si } m > 1+v, \\ -|P|^v & \text{si } m = 1+v, \\ |P|^{m-1}(|P|-1) & \text{si } m \le v. \end{cases} \tag{III.4}$$

Preuve. La proposition VI.6 de [1] donne ce même résultat en caractéristique impaire. Le lecteur peut vérifier que la preuve reste valable en caractéristique 2.

Proposition III.2. (1) *Soient un entier $s \ge 4$ et M un polynôme. Alors, pour tout entier $m \ge 0$, on a*

$$\sum_{\substack{H \in \mathbb{M} \\ \deg H > m}} |A(s,M,H)| \le b_1(s) q^{m(3-s)/2}, \tag{III.5}$$

avec

$$b_1(s) = \frac{q^{(3-s)/2}}{(1-q^{(3-s)/2})(1-q^{(1-s)/2})}. \tag{III.6}$$

(2) *La série $S_s(M)$ est absolument convergente. De plus,*

$$S_s(0) = \frac{1-q^{1-s}}{1-q^{3-s}}, \tag{III.7}$$

et, pour tout polynôme M non nul, on a

$$b_2(s) \leq S_s(M) \leq b_1(s), \tag{III.8}$$

avec

$$b_2(q,s) = 1 - q^{1-s}. \tag{III.9}$$

Preuve. Soit un entier $j \geq 0$. Rappelons que $\mathbb{S}$ désigne l'ensemble des polynômes $Q \in \mathbb{M}$ sans facteur carré. Avec (III.1), (II.6), (II.7) et (III.2),

$$\begin{aligned}\sum_{\substack{H\in\mathbb{M}\\ \deg H=j}} |A(s,M,H)| &\leq \sum_{\substack{Q\in\mathbb{S},\, Y\in\mathbb{M}\\ \deg Q+2\deg Y=j}} |Q|^{1-s}|Y|^{2-s}\\ &\leq \sum_{\substack{Q\in\mathbb{S},\,\deg Q\leq j\\ \deg Q\equiv j \bmod 2}} |Q|^{1-s} \sum_{\substack{Y\in\mathbb{M}\\ \deg Q+2\deg Y=j}} |Y|^{2-s},\end{aligned}$$

d'où

$$\begin{aligned}\sum_{\substack{H\in\mathbb{M}\\ \deg H=j}} |A(s,M,H)| &\leq q^{j(3-s)/2} \sum_{\substack{Q\in\mathbb{S},\,\deg Q\leq j\\ \deg Q\equiv j \bmod 2}} |Q|^{-(s+1)/2}\\ &\leq q^{j(3-s)/2} \sum_{Q\in\mathbb{M}} |Q|^{-(s+1)/2},\end{aligned}$$

$$\sum_{\substack{H\in\mathbb{M}\\ \deg H=j}} |A(s,M,H)| \leq \frac{q^{j(3-s)/2}}{(1-q^{(1-s)/2})}.$$

La relation (III.5) ainsi que la deuxième des inégalités (III.8) est alors immédiate. On obtient (III.7) en développant la somme $S_s(0)$ en produit eulérien.

Supposons M non nul. En développant la somme $S_s(M)$ en produit eulérien, on obtient

$$S_s(M) = \prod_{P\in\mathbb{I}} \Theta(M,P), \tag{1}$$

où

$$\Theta(M,P) = 1 + \sum_{k=1}^{\infty} A(s,M,P^k). \tag{2}$$

Avec (III.1), (III.4), (II.5), (II.6) et (II.7), il s'ensuit que

$$\Theta(M,P) = \begin{cases} 1 - |P|^{-s} & \text{si } P \text{ ne divise pas } M,\\ (1-|P|^{-s})(1-|P|^{(2-s)(1+w(P,M))})(1-|P|^{2-s})^{-1} & \\ & \text{si } P \text{ divise } M,\end{cases}$$

où

$$w(P,M) = [v_P(M)/2]. \tag{3}$$

Avec (1) et (2), on en déduit que

$$S_s(M) = \Big\{ \prod_{P\in\mathbb{I}} (1-|P|^{-s}) \Big\} \times \Big\{ \prod_{\substack{P\in\mathbb{I}\\ P|M}} \frac{1-|P|^{(2-s)(1+w(P,M))}}{1-|P|^{2-s}} \Big\},$$

d'où, $S_s(M) \geq 1 - q^{1-s}$.

IV. Estimation de $R(s,n,M)$. Dans ce paragraphe M est un polynôme tel que

$$\deg M \leq 3n. \tag{IV.1}$$

Les notations du paragraphe II sont conservées. Si $G/H \in \mathcal{F}_n$, on appelle *arc majeur de centre* G/H l'ensemble des $t \in \wp$ tels que $v(t-G/H) > 2n+\deg H$. On désigne par $\wp^+$ la réunion des arcs majeurs.

Soit un entier $s \geq 4$. Rappelons que l'on a

$$R(s,n,M) = \int_{\wp} g(t)^s E(tM)\, dt. \tag{IV.2}$$

Posons

$$R(s,n,M)^+ = \int_{\wp^+} g(t)^s E(tM)\, dt. \tag{IV.3}$$

Proposition IV.1. *Soit H un polynôme unitaire de degré au plus n et soit*

$$J_{H,s}(M) = \int_{v(u)>2n+\deg H} g(u)^s E(uM)\, du. \tag{IV.4}$$

Si $\deg M < 2n$ *ou si* $\deg M \geq 2n$ *et* $\deg H > \deg M - 2n$, *alors*

$$J_{H,s}(M) = \Theta_s q^{n(2s-3)} - \gamma_s(M,H), \tag{IV.5}$$

avec

$$\Theta_s = \frac{q^{3s-3} - q^{2s-3}}{q^{s-2}-1}, \tag{IV.6}$$

$$0 \leq \gamma_s(M,H) \leq c_1(s) q^{n(3s/2-2)} |H|^{s/2-1}, \tag{IV.7}$$

où

$$c_1(s) = \frac{(q^2-1)q^{2s-3}}{q^{s-2}-1}. \tag{IV.8}$$

Si $2n + \deg H \leq \deg M$, *alors*

$$J_{H,s}(M) = \Theta_s q^{n(2s-3)} - \lambda_s q^{n(s-1)+\mu(s-2)}, \tag{IV.9}$$

où l'entier μ *est défini par la relation* $\deg M = n + 2\mu - \varrho$, $\varrho \in \{0,1\}$, *où*

$$\lambda_s = \frac{(q^{s+1}-q)q^{s-2}}{q^{s-2}-1}. \tag{IV.10}$$

Enfin, si $\deg M = 3n$ *ou si* $2n + \deg H \le \deg M = 3n-1$, *alors*

$$J_{H,s}(M) = q^{n(2s-3)}(q^{2s-1} - q^{s-1}). \tag{IV.11}$$

Preuve. D'après (I.15) et (I.5),

(1) $$J_{H,s}(M) = q^{s(2n+2)-3n-1} + \sum_{j=2n+\deg H+1}^{3n+1} \sum_{a\in\mathbb{F}_q^*} q^{s(n+1+[(j-n)/2])-j} \int\limits_{\substack{v(u)=j\\ \operatorname{sgn}(u)=a}} E(uM)\,du.$$

D'autre part,

$$\int\limits_{\substack{v(u)=j\\ \operatorname{sgn}(u)=a}} E(uM)\,du = E(aT^{-j}M) \int\limits_{v(u)>j} E(uM)\,du,$$

d'où, avec (1), (I.1) et (I.5),

(2) $$J_{H,s}(M) = q^{n(2s-3)+2s-1} + (q-1) \sum_{\substack{j>2n+\deg H\\ j>1+\deg M}}^{3n+1} q^{s(n+1+[(j-n)/2])-j} - \varepsilon(M,n,H) q^{s(n+1+[(1+\deg M-n)/2])-\deg M-1},$$

où

$$\varepsilon(M,n,H) = \begin{cases} 1 & \text{si } \deg M \ge 2n + \deg H,\\ 0 & \text{sinon.}\end{cases} \tag{3}$$

Posons, pour $v < w$ entiers,

$$B(v,w) = \sum_{k=v}^{w} q^{k(s-2)}. \tag{4}$$

Supposons $\deg M < 2n + \deg H$. Posons

$$1 + 2n + \deg H = n + 2m + r, \quad r \in \{-1, 0\}. \tag{5}$$

D'après (2), si $r = 0$, alors

$$J_{H,s}(M) = q^{n(2s-3)+2s-1} + (q^2-1)q^{(s-1)(n+1)}B(m,n),$$

et si $r = -1$, alors

$$J_{H,s}(M) = q^{n(2s-3)+2s-1} + (q^2-1)q^{(s-1)(n+1)}B(m,n) + (q-1)q^{n(s-1)}q^{m(s-2)+1}.$$

Donc, pour $r = 0$, on a

$$J_{H,s}(M) = q^{n(2s-3)}\,\frac{q^{3s-3} - q^{2s-3}}{q^{s-2}-1} - \frac{(q^2-1)q^{n(s-1)+m(s-2)+s-1}}{q^{s-2}-1},$$

et pour $r = -1$, on a

$$J_{H,s}(M) = q^{n(2s-3)}\,\frac{q^{3s-3} - q^{2s-3}}{q^{s-2}-1} - \frac{(q-1)(q^s+q)q^{n(s-1)+m(s-2)}}{q^{s-2}-1}.$$

Compte tenu de (5), on a prouvé la première partie de la proposition.

Supposons maintenant $\deg M \geq 2n + \deg H$. Traitons séparément le cas $\deg M \geq 3n-1$. Si $\deg M \in \{3n, 3n-1\}$, la relation (2) s'écrit

$$J_{H,s}(M) = q^{n(2s-3)}(q^{2s-1} - q^{s-1}), \tag{6}$$

ce qui est la relation (IV.11). Supposons $\deg M < 3n-1$. Posons

$$2 + \deg M = n + 2m + r, \quad r \in \{-1, 0\}. \tag{7}$$

Avec (2), on a pour $r = 0$,

$$J_{H,s}(M) = q^{n(2s-3)+2s-1} - q^{n(s-1)+m(s-2)+1} + (q^2-1)q^{(s-1)(n+1)}B(m,n),$$

et pour $r = -1$, on a

$$J_{H,s}(M) = q^{s(2n+2)-3n-1} - q^{n(s-1)+m(s-2)+2} + (q^2-1)q^{(s-1)(n+1)}B(m,n) + (q-1)q^{n(s-1)+m(s-2)+1},$$

d'où dans les deux cas

$$J_{H,s}(M) = q^{n(2s-3)}\,\frac{q^{3s-3} - q^{2s-3}}{q^{s-2}-1} - \frac{(q^{s+1}-q)q^{n(s-1)+m(s-2)}}{q^{s-2}-1}, \tag{8}$$

ce qui est la relation (IV.9). On remarque que si l'on écrit l'égalité (8) avec $m = n+1$, on retrouve la valeur de $J_{H,s}(M)$ donnée par la relation (6). La relation (IV.9) reste vraie pour les polynômes de degré $\geq 3n-1$.

On remarque que dans le cas où $2n + \deg H \leq \deg M$, la valeur de $J_{H,s}(M)$ ne dépend pas de H. On pose

$$\Lambda_s(M) = \begin{cases} \Theta_s & \text{si } \deg M < 2n, \\ \Theta_s - \lambda_s q^{(\mu-n)(s-2)} & \text{si } 2n \leq \deg M = n + 2\mu + \varrho \leq 3n-2,\ \varrho \in \{0,1\}. \end{cases} \tag{IV.12}$$

On note que

$$(q^{s+1}-q)(q^{s-2}+1) \leq \Lambda_s(M) \leq \Theta_s. \tag{IV.13}$$

Proposition IV.2. *Soit un entier $s \geq 4$. Alors il existe une constante $c_2(s)$ telle que pour tout polynôme M de degré $\leq 3n$, on ait*

$$|R(s,n,M)^+ - \Lambda_s(M)q^{n(2s-3)}S_s(M)| \leq c_2(s)q^{3n(s-1)/2}. \tag{IV.14}$$

Preuve. Soit $t = G/H + u$ appartenant à l'arc majeur de centre G/H. D'après (I.12),

$$g(t) = \sum_{(Q,R)\in\mathcal{C}_H\times\mathcal{C}_H} \sum_{\substack{X\in\mathbb{A}_n\\ X\equiv Q \bmod H}} \sum_{\substack{Y\in\mathbb{A}_n\\ Y\equiv R \bmod H}} E((G/H+u)XY^2),$$

c'est-à-dire,

$$g(t) = \sum_{(Q,R)\in\mathcal{C}_H\times\mathcal{C}_H} E(GQR^2/H) \times \sum_{X\in\mathbb{A}_{n-\deg H}} \sum_{Y\in\mathbb{A}_{n-\deg H}} E(u(Q+HX)(R+HY)^2).$$

Puisque $v(u) > 2n + \deg H$, on a

$$g(t) = \sum_{(Q,R)\in\mathcal{C}_H\times\mathcal{C}_H} E(GQR^2/H) \sum_{X\in\mathbb{A}_{n-\deg H}} \sum_{Y\in\mathbb{A}_{n-\deg H}} E(uH^3XY^2). \tag{1}$$

Avec (I.4), puis (I.8), il vient

$$|H|^2 \sum_{X\in\mathbb{A}_{n-\deg H}} \sum_{Y\in\mathbb{A}_{n-\deg H}} E(uH^3XY^2) = \int\limits_{\substack{v(x)\geq -n\\ v(y)\geq -n}} E(uxy^2)\,dx\,dy.$$

Enfin, avec à nouveau (I.4), on obtient la relation

$$|H|^2 \sum_{X\in\mathbb{A}_{n-\deg H}} \sum_{Y\in\mathbb{A}_{n-\deg H}} E(uH^3XY^2) = g(u),$$

d'où, avec (1),

$$|H|^2 g(t) = S(H,G)g(u), \tag{2}$$

où

$$S(H,G) = \sum_{(Q,R)\in\mathcal{C}_H^2} E(GQR^2/H). \tag{3}$$

Avec les notations (IV.3) et (IV.4) on a

$$R(s,n,M)^+ = \sum_{G/H\in\mathcal{F}_n} |H|^{-2s} S(H,G)^s E(GM/H) J_{H,s}(M)\,;$$

avec (I.7) et les notations (II.5)–(II.7), on a

$$S(H,G) = |H|\#\{R\in\mathcal{C}_H\,;\, H\mid R^2\} = |H|\#\{R\in\mathcal{C}_H\,;\, \Lambda\Psi\mid R\} = |H\Psi|,$$

d'où, avec (III.1) et (III.2),

$$R(s,n,M)^+ = \sum_{\substack{H\in\mathbb{M}\\ \deg H\leq n}} A(s,M,H)J_{H,s}(M). \tag{4}$$

On suppose $\deg M < 2n$. D'après (IV.5) et (IV.7),

$$\Big|R(s,n,M)^+ - \Theta_s q^{n(2s-3)} \sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} A(s,M,H)\Big| \le c_1(s) q^{n(3s/2-2)} \sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} |A(s,M,H)|\,|H|^{s/2-1}.$$

Avec (III.1), (III.2), (II.6) et (II.7) il vient

$$\sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} |A(s,M,H)|\,|H|^{s/2-1} \le \sum_{\substack{Q\in\mathbb{S},\, Y\in\mathbb{M}\\ \deg Q+2\deg Y\le n}} |Q|^{1-s}|Y|^{2-s}|QY^2|^{s/2-1} = \sum_{\substack{Q\in\mathbb{S},\, Y\in\mathbb{M}\\ \deg Q+2\deg Y\le n}} |Q|^{-s/2},$$

d'où

$$\sum_{H\in\mathbb{M},\,\deg H\le n} |A(s,M,H)|\,|H|^{s/2-1} \le \frac{q^{1+n/2}}{1-q^{1-s/2}}. \tag{5}$$

Par suite, avec (III.3) et (III.5),

$$|R(s,n,M)^+ - \Theta_s q^{n(2s-3)} S_s(M)| \le \Theta_s b_1(s) q^{3n(s-1)/2} + \frac{c_1(s)q}{1-q^{1-s/2}}\, q^{3n(s-1)/2}. \tag{6}$$

On suppose maintenant $2n \le \deg M \le 3n$. On pose

$$2 + \deg M = n + 2m + r, \quad r \in \{-1, 0\}, \quad \deg M = 3n - k. \tag{7}$$

D'après (IV.5), (IV.7) et (IV.9),

$$\Big|R(s,n,M)^+ - \Theta_s q^{n(2s-3)} \sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} A(s,M,H) - \lambda_s q^{n(s-1)+m(s-2)} \sum_{\substack{H\in\mathbb{M}\\ \deg H\le n-k}} A(s,M,H)\Big| \le c_1(s) q^{n(3s/2-2)} \sum_{\substack{H\in\mathbb{M}\\ n-k<\deg H<n}} A(s,M,H)|H|^{s/2-1},$$

puis, avec (5), la notation (IV.12), (III.3), (III.5) et la remarque (IV.13),

$$|R(s,n,M)^+ - \Lambda_s(M)q^{n(2s-3)}S_s(M)|$$
$$\leq \Theta_s b_1(s)q^{3n(s-1)/2}$$
$$+ \lambda_s b_1(s)q^{n(s+1)/2+m(s-2)+k(s-3)/2} + \frac{c_1(s)q}{1-q^{1-s/2}}\, q^{3n(s-1)/2}.$$

Avec (7) on a

$$|R(s,n,M)^+ - \Lambda_s(M)q^{n(2s-3)}S_s(M)| \tag{8}$$
$$\leq \Theta_s b_1(s)q^{3n(s-1)/2} + \lambda_s b_1(s)q^{(s-3)/2}q^{3n(s-1)/2-[k/2]} + \frac{c_1(s)q}{1-q^{1-s/2}}\, q^{3n(s-1)/2}.$$

L'entier k étant positif ou nul, les relations (6) et (8) donnent le résultat annoncé avec

$$c_2(s) = \Theta_s b_1(s) + \lambda_s b_1(s)q^{(s-3)/2} + \frac{c_1(s)q}{1-q^{1-s/2}}.$$

Nous pouvons conclure.

THÉORÈME IV.3. *Soit un entier $s \geq 5$. Alors, pour n tendant vers ∞, pour tout polynôme M tel que* $\deg M \leq 3n$, *on a*

$$R(s,n,M) = \Lambda_s(M)S_s(M)q^{n(2s-3)} + O(q^{n(3s/2-1)}),$$

les constantes impliquées par le symbole O ne dépendant que de q et de s.

Preuve. Avec (IV.2), (IV.3), (II.12) et (IV.14) on a

$$|R(s,n,M) - \Lambda_s(M)q^{n(2s-3)}S_s(M)| \leq a_1(s)q^{n(3s/2-1)} + c_2(s)q^{3n(s-1)/2}.$$

REMARQUE. D'après les relations (III.8) et (IV.13), on a

$$b_2(s)(q^{s+1}-q)(q^{s-2}+1) \leq \Lambda_s(M)S_s(M) \leq b_1(s)\Theta_s.$$

On obtient le théorème A annoncé dans l'introduction en remplaçant $b_1(s)$, $b_2(s)$ et Θ_s par leurs valeurs respectives.

Nous pouvons déduire très simplement de ce qui précède une majoration et une minoration asymptotiques des nombres $R(4,n,0)$.

THÉORÈME IV.4. *Pour n tendant vers ∞, on a*

$$\Theta_4 q^{5n}\left(1+\frac{1}{q}+\frac{1}{q^2}\right) + O(q^{9n/2})$$
$$\leq R(4,n,0) \leq \left(\Theta_4\left(1+\frac{1}{q}+\frac{1}{q^2}\right) + \frac{q^8+3q^5+4q^4}{q+1}\right)q^{5n} + O(q^{9n/2}),$$

les constantes impliquées par les symboles O ne dépendant que de q.

Preuve. On remarque que $R(4,n,0)^-$ est positif. Une minoration de $R(4,n,0)^+$ donnera donc une minoration de $R(4,n,0)$. La proposition IV.2

nous donne l'estimation

$$|R(4,n,0)^+ - \Theta_4 q^{5n} S_4(0)| \le c_2(4) q^{9n/2}.$$

L'identité (III.7) donne alors la minoration du théorème. Les relations (II.12) et (II.13) nous donnent

$$0 \le R(4,n,0)^- \le \frac{q^6+3q^3+4q^2}{q+1}\, q^{2+5n},$$

d'où la majoration.

On obtient le théorème B en remplaçant Θ_4 par sa valeur.

Les estimations des nombres $R(2,n,0)$ et $R(3,n,0)$ se déduisent des calculs faits au paragraphe II. Elles sont données par le théorème suivant. Il faut noter que l'ordre de grandeur exact des nombres $R(3,n,0)$ n'est pas déterminé.

THÉORÈME IV.5. *Pour tout entier positif n, on a*

$$3q^{2n+2} \le R(2,n,0) \le \frac{q^6+3q^3+4q^2}{q+1}\, q^{2n}$$

et pour n tendant vers ∞, on a

$$3q^{3+3n} \le R(3,n,0) \le \frac{q^7+3q^4+4q^3}{q+1}\, q^{7n/2} + O(nq^{3n}),$$

les constantes impliquées par les symboles O ne dépendant que de q.

Preuve. L'estimation de $R(2,n,0)$ se déduit de (IV.2) et de (II.1). Avec (IV.2) on a

$$R(3,n,0) = \int_{\wp} g(t)^3\, dt.$$

De (I.12) on déduit la minoration évidente $g(t) \ge q^{n+1}$, d'où

$$R(3,n,0) \ge q^{n+1} \int_{\wp} g(t)^2\, dt,$$

la minoration de $R(3,n,0)$ se déduit de (II.1). Les relations (II.12) et (II.13) nous donnent

$$0 \le R(3,n,0)^- \le \frac{q^7+3q^4+4q^3}{q+1}\, q^{7n/2}.$$

Compte tenu de (IV.5) et (IV.7), la relation (4) établie dans la preuve de la proposition IV.2 nous donne ici

$$0 \le R(3,n,0)^+ \le \sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} A(3,0,H)(\Theta_3 q^{3n} + c_1(3) q^{5n/2}|H|^{1/2})$$

$$\le (\Theta_3 + c_1(3)) q^{3n} \sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} A(3,0,H).$$

Avec (III.1), (II.6) et (II.7) on a

$$\sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} A(3,0,H) \le \sum_{\substack{Q\in\mathbb{S},\,Y\in\mathbb{M}\\ \deg Q+2\deg Y\le n}} |Q|^{-2}|Y|^{-1} \le \sum_{Q\in\mathbb{S}} |Q|^{-2} \sum_{\substack{Y\in\mathbb{M}\\ 2\deg Y\le n}} |Y|^{-1},$$

d'où

$$\sum_{\substack{H\in\mathbb{M}\\ \deg H\le n}} A(3,0,H) \le \frac{q^3-1}{q^3-q^2} \sum_{\substack{Y\in\mathbb{M}\\ 2\deg Y\le n}} |Y|^{-1} \le \frac{q^3-1}{2(q^3-q^2)}\,(2n+1).$$

Par suite,

$$R(3,n,0)^+ \le (\Theta_3 + c_1(3))\,\frac{q^3-1}{2(q^3-q^2)}\,(2n+1)q^{3n}.$$

Nous complétons cette étude en établissant par des méthodes élémentaires une majoration et une minoration des nombres $R(3,n,M)$ et $R(4,n,M)$, où M est non nul.

THÉORÈME IV.6. *Pour tout entier $n \ge 0$, pour tout polynôme M non nul tel que $\deg M \le 3n$, on a*

$$(q-1)^2 q^{-1} q^{3n/2} \le R(3,n,M) \ll q^{7n/2},$$
$$(q-1)^2 q^{1+7n/2} \le R(4,n,M) \ll q^{5n},$$

les constantes impliquées par les symboles $\ll$ ne dépendant que de q. De plus, tout polynôme M non nul admet une représentation stricte comme somme

$$M = X_1^2 Y_1 + X_2^2 Y_2 + X_3^2 Y_3.$$

Preuve. Soit M un polynôme non nul de degré au plus $3n$. Avec (IV.2) on a

$$R(s,n,M) = |R(s,n,M)| \le \int_{\wp} |g(t)^s|\,dt = \int_{\wp} g(t)^s\,dt = R(s,n,0).$$

Les théorèmes IV.4 et IV.5 donnent alors les majorations annoncées. Soit un entier $n \ge 0$. Soit M un polynôme non nul de degré $3n-r$, où $0 \le r \le 3$. Soit Y_1 un polynôme de degré n. Par division euclidienne, on a l'existence de polynômes X_1 et M_1 tels que

$$M = Y_1^2 X_1 + M_1, \quad \deg X_1 \le n,\ \deg M_1 < 2n. \tag{1}$$

Soit Y_2 un polynôme de degré $[n/2]$. Par division euclidienne, on a l'existence de polynômes X_2 et M_2 tels que

$$M_1 = Y_2^2 X_2 + M_2, \quad \deg X_2 \le n,\ \deg M_2 < n. \tag{2}$$

On a donc

$$M = Y_1^2 X_1 + Y_2^2 X_2 + 1^2 M_2, \tag{3}$$

les polynômes X_1, Y_1, X_2, Y_2, M_2 étant tous de degré au plus n. Chaque choix (Y_1, Y_2) de ce type conduisant à une représentation (3), on a

$$R(3,n,M) \geq (q-1)q^n(q-1)q^{[n/2]}.$$

Trivialement,

$$R(4,n,M) \geq \sum_{X\in\mathbb{A}_n}\sum_{Y\in\mathbb{A}_n} R(3,n,M+XY^2) \geq q^{2n+2}(q-1)q^n(q-1)q^{[n/2]}.$$

On a là les minorations annoncées. Lorsque $r \in \{0,1,2\}$, les représentations (3) sont des représentations strictes, d'où la deuxième partie du théorème.

Terminons par deux théorèmes de densité.

THÉORÈME IV.7. *L'ensemble E_2 des polynômes M de degré au plus $3n$ admettant une représentation comme somme $M = X_1Y_1^2 + X_2Y_2^2$, où X_1, Y_1, X_2, Y_2 sont des polynômes de degré au plus n, est de densité strictement positive. Plus précisément, l'ensemble E_2 est de densité supérieure à*

$$\frac{q^4(q+1)}{q^5+q^4+5q^2+4q+1}.$$

Preuve. On a

$$q^{4n+4} = \sum_{M\in\mathbb{A}_{3n}} R(2,n,M) = \sum_{M\in E_2} R(2,n,M).$$

L'inégalité de Cauchy–Schwarz donne alors

$$\begin{aligned} q^{8n+8} &\leq \#(E_2)\sum_{M\in E_2} R(2,n,M)^2 \leq \#(E_2)\sum_{M\in\mathbb{A}_{3n}} R(2,n,M)^2 \\ &= \#(E_2)R(4,n,0). \end{aligned}$$

Avec le théorème IV.4, il vient

$$\#(E_2) \geq q^{3n+8}\left(\Theta_4\left(1+\frac{1}{q}+\frac{1}{q^2}\right)+\frac{q^8+3q^5+4q^4}{q+1}\right)^{-1} + O(q^{5n/2}),$$

d'où la minoration annoncée.

THÉORÈME IV.8. *Soit E_1 l'ensemble des polynômes M de degré au plus $3n$ pouvant s'écrire comme produit $M = XY^2$, où X et Y sont des polynômes de degré au plus n. Alors, on a*

$$\frac{q+1}{q^4+3q+4}\,q^{2n+2} \leq \#(E_1) \leq q^{2n+2}.$$

Preuve. On a

$$q^{2n+2} = \sum_{M\in\mathbb{A}_{3n}} R(1,n,M) = \sum_{M\in E_1} R(1,n,M), \tag{1}$$

d'où

$$q^{2n+2} \geq \#(E_1).$$

On applique l'inégalité de Cauchy–Schwarz à la relation (1) et on obtient

$$q^{4n+4} \le \#(E_1) \sum_{M \in S_1} R(1,n,M)^2 \le \#(E_1) \sum_{M \in \mathbb{A}_{3n}} R(1,n,M)^2$$
$$= \#(E_1) R(2,n,0).$$

Le théorème IV.5 donne alors

$$\#(E_1) \ge \frac{q+1}{q^4+3q+4}\, q^{2n+2}.$$

Références

[1] M. Car, *Sommes de carrés dans* $\mathbb{F}_q[X]$, Dissertationes Math. 215 (1983).
[2] —, *Sommes d'exponentielles dans* $\mathbb{F}_{2^h}((X^{-1}))$, Acta Arith. 62 (1992), 303–328.
[3] M. Car et J. Cherly, *Sommes de cubes et de carrés dans* $\mathbb{F}_{2^h}[X]$, en préparation.
[4] G. W. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials over a Finite Field*, Oxford Math. Monogr., Oxford Univ. Press, 1991.
[5] L. Gallardo, *Une variante du problème de Waring sur* $\mathbb{F}_{2^n}[t]$, C. R. Acad. Sci. Paris Sér. I Math. 327 (1998), 117–121.
[6] —, *On the restricted Waring problem over* $\mathbb{F}_{2^n}[t]$, Acta Arith. 92 (2000), 109–113.
[7] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*, ibid. 11 (1966), 461–488.

L.A.T.P. – U.M.R. 6632
Bâtiment Henri Poincaré
Faculté des Sciences de St-Jérôme
Av. Escadrille Normandie-Niemen
13397 Marseille Cedex 20, France
E-mail: mireille.car@univ.u-3mrs.fr

Reçu le 29.4.2002
et révisé le 29.11.2002 (4275)