Astérisque

JØRGEN CHERLY

Sommes d'exponentielles cubiques dans l'anneau des polynomes en une variable sur le corps à 2 éléments, et application au problème de Waring

Astérisque, tome 198-199-200 (1991), p. 83-96

<http://www.numdam.org/item?id=AST_1991__198-199-200__83_0>

SOMMES D'EXPONENTIELLES CUBIQUES DANS L'ANNEAU DES POLYNOMES EN UNE VARIABLE SUR LE CORPS A 2 ELEMENTS, ET APPLICATION AU PROBLEME DE WARING

par

Jørgen CHERLY

En 1770, Waring a énoncé que tout nombre entier (positif) est somme de 4 carrés, 9 cubes, 19 bicarrés. Quelques années plus tard, il a étendu son affirmation au cas des puissances supérieures ; c'était le début d'une longue succession de variations sur le thème.

Bien que la touche finale du problème original ait été donnée - encore est-ce tout récemment en 1986, par les efforts conjoints de Balasubramanian, Deshouillers et Dress que le problème de Waring pour les bicarrés a été résolu - de nombreuses questions restent encore en suspens.

L'une des variantes consiste à étudier l'ensemble des sommes de puissances k-ièmes dans l'anneau $\mathbb{F}_q[X]$ des polynômes en une indéterminée sur le corps fini $\mathbb{F}_q$, anneau qui partage de nombreuses propriétés arithmétiques avec $\mathbb{Z}$. Les travaux de Matthews (1966), Kubota (1971) et Car (1971) conduisent à des résultats dont nous citons le dernier en date, qui est le meilleur possible concernant les restrictions imposées aux degrés des termes.

Tout élément M de $\mathbb{F}_q[X]$ de degré suffisamment grand peut s'écrire sous la forme

$$M = M_1^k + \cdots + M_s^k$$

où $s = \min(k2^{k-1}+1, 2[k(k-1)\log 2]+2k+3)$ et $\deg M_i < \frac{1}{k}\deg M + 1$, à la condition que k soit inférieur à la caractéristique de $\mathbb{F}_q$.

Ce travail a pour but d'apporter une première pierre à l'étude du cas où le degré est supérieur à la caractéristique de $\mathbb{F}_q$. Nous montrons le résultat suivant :

THÉORÈME I : *Tout élément M de $\mathbb{F}_2[X]$ de degré assez grand qui est congru à 0 ou 1 modulo $1+X+X^2$ est somme d'au plus 18 cubes de polynômes de degré inférieur à $\frac{1}{3}\deg M + 1$.*

On remarque que la condition de congruence est indispensable, car toute somme de cubes dans $\mathbb{F}_2[X]$ est congrue à 0 ou 1 modulo $1+X+X^2$. Le résultat a surtout une importance qualitative (nombre de termes finis) la valeur 18 n'est sûrement pas la meilleure possible.

La démonstration s'effectue en deux étapes ; la première partie, qui nous semble avoir un intérêt intrinsèque est l'estimation de sommes trigonométriques. La seconde partie est plus standard. On y met en oeuvre la "méthode du cercle" adaptée à l'anneau $\mathbb{F}_q[X]$ en suivant Carlitz. Pour cela, on introduit un caractère E sur le complété $\mathbb{F}_q((\frac{1}{X}))$ de $\mathbb{F}_q[X]$; le nombre de représentations de M en somme de s cubes prend une expression intégrale

$$R_s(M) = \int \Big(\sum_{\deg B \leq n} E(B^3 t)\Big)^s E(-Mt)dt$$

étendue à la boule unité de $\mathbb{F}_q((\frac{1}{X}))$.

Le traitement traditionnel des "arcs mineurs" par la méthode de Weyl s'avère inefficace, car il repose sur des différentiations successives et introduit un facteur 3 ! qui est nul dans $\mathbb{F}_2$. On a recours au traitement suggéré par Vaughan en 1977 dans le cas archimédien. La difficulté que l'on rencontre dans le cas présent est l'impossibilité d'utiliser une quelconque variété de la méthode de la phase stationnaire ; en effet, les termes résiduels qui interviennent dans la formule sommatoire de Poisson, loin d'être négligeable, peuvent avoir un ordre de grandeur maximal, comme nous le montrons. Dans la première partie nous prouvons également que peu de ces termes sont en fait non nuls. On obtient ainsi l'équivalent du lemme de Weyl.

THÉORÈME II : *Il existe un réel K tel que, pour tout couple de polynômes G et H premiers entre eux ($H \neq 0$), pour tout entier n et tout $u \in \mathbb{F}_2((\frac{1}{X}))$ vérifiant $n + \deg H < v(u) \leq 2n + \deg H$ on ait*

$$\left| \sum_{B \in \mathbb{F}_2[X], \deg B \leq n} E(B^3(\frac{G}{H} + u)) \right| \leq K.2^{\frac{19}{20}n}$$

où $v(u)$ désigne la valuation de u.

Commentaire.

La constante K peut être explicitée : $K = 2^{2^{540}}$ convient. La méthode utilisée ne permet pas d'obtenir l'exposant $\frac{3}{4}$ du cas archimédien au lieu de $\frac{19}{20}$; sa limite théorique, atteinte dans plusieurs cas, est $\frac{5}{6}$.

Remarque : L'intérêt du résultat provient de ce que tout élément t de $\mathbb{F}_2((\frac{1}{X}))$ peut s'écrire sous la forme

$$(1) \qquad \begin{cases} t = \frac{G}{H} + u. \text{ avec } (G, H) = 1, 0 \leq \deg H \leq n \\ (\text{et } v(u) > n + \deg H) \end{cases}$$

et que la somme

$$\sum_{B \in \mathbb{F}_2[X], \deg B \leq n} E(B^3(\frac{G}{H} + u))$$

notée $S_n(t)$ peut être calculée explicitement si $v(u) > 2n + \deg H$.

PREMIERE PARTIE : Une inégalité du type de celle de Weyl pour les sommes trigonométriques cubiques dans $\mathbb{F}_2((\frac{1}{X}))$

a) Notation

On note $F_2((\frac{1}{X}))$ le complété du corps $F_2(X)$ des fractions rationnelles en une indéterminée sur F_2, pour la valuation 0-adique v telle que $v(\frac{A}{B}) =$

$\deg B - \deg A$ lorsque A et B sont des polynômes non nuls. Un élément non nul u de $F_2((\frac{1}{X}))$ peut être représenté comme un série de Laurent

$$\sum_{m=-\infty}^{-v(u)} u_m X^m \ , \text{ où } u_m \in F_2.$$

A la valuation v est associée la valeur absolue $|.|$ telle que pour tout u dans $F_2((\frac{1}{X}))$, on ait $|u| = 2^{-v(u)}$.

On note E le caractère du groupe additif $F_2((\frac{1}{X}))$, défini par

$$E(\sum u_m X^m) = \begin{cases} 1 & \text{si } u_{-1} = 0 \\ -1 & \text{si } u_{-1} = 1. \end{cases}$$

Pour tout entier n, on note $\mathcal{P}_n$ le groupe additif compact des éléments de $\mathbb{F}_2((\frac{1}{X}))$ de valuation supérieure à n.
On note dt la mesure de Haar normalisée sur la boule unité $\mathcal{P}_0$; que l'on notera également $\mathcal{P}$.

b)Un lemme sur les sommes trigonométriques cubiques dans $\mathbb{F}_2((\frac{1}{X}))$

Pour un entier positif k, notons g_k l'ensemble des polynômes de degré au plus égal à k.

LEMME 1 : *Soient* $\alpha, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_2((\frac{1}{X}))$ *et* $\phi(y) = \alpha y^3 + \alpha_1 y^2 + \alpha_2 y + \alpha_3$, $y \in \mathbb{F}_2((\frac{1}{X}))$ *nous obtenons la relation*

$$\left|\sum_{B\in g_k} E(\phi(B))\right|^4 = \left|\sum_{B\in g_k} E(\phi(B))\right|^2 \sum_{R\in g_k} \sum_{Q\in g_k} E(\alpha(R^2Q + RQ^2)).$$

c)Formule sommatoire de Poisson et sommes de Gauss

Soit $t = \frac{G}{H} + u$ un élément de $\mathbb{F}_2((\frac{1}{X}))$ satisfaisant **(1)** et la condition **(2)** suivante

$$v(u) \leq 2n + \deg H \ . \tag{2}$$

On définit la fonction f par la relation

$$f(\eta) = \begin{cases} E(\eta^3 H^3 u) & \text{si } v(\eta) \geq \deg H - n \\ 0 & \text{sinon.} \end{cases} \tag{3}$$

La formule sommatoire de Poisson implique que l'on a

$$S_n(t) = \sum_{K \in \mathbb{F}_2[X]} \hat{f}(K) S(G, H, K) \tag{4}$$

où $\hat{f}(K)$ désigne la transformée de Fourier de f en K et où la somme de Gauss $S(G, H, K)$ est définie par

$$S(G, H, K) = \sum_{R (\mathrm{mod}\ H)} E\left[\frac{GR^3 + KR}{H}\right].$$

Il résulte du lemme 1 que si une somme de Gauss est non nulle, le carré de son module est égal à la somme double

$$\sum_{R (\mathrm{mod}\ H)} \sum_{Q (\mathrm{mod}\ H)} E\left(\frac{G(R^2Q + RQ^2)}{H}\right)$$

que nous noterons $T(G, H)$. Il résulte alors de (4) que l'on a

$$|S_n(t)| \leq T(G, H)^{\frac{1}{2}} \sum_{K \in \mathbb{F}_2[X]} |\hat{f}(K)|. \tag{5}$$

Nous terminerons cette section en mentionnant la majoration suivante pour les sommes de Gauss ; on a

$$T(G, H) \leq 2^{\frac{14}{3}} |H|^{\frac{4}{3}} \tag{6}$$

où l'exposant de $|H|$, ainsi que la constante sont les meilleurs possibles. Cette majoration s'obtient en remarquant que l'on a

$$T(G, H_1 H_2) = T(GH_2^2, H_1) T(GH_1^2, H_2)$$

dès que H_1 et H_2 sont premiers entre eux ; on calcule alors explicitement $T(G, P^\ell)$, où P est irréductible et ℓ entier.

d)<u>Evaluation d'une transformée de Fourier</u>

PROPOSITION 1 : *La fonction f étant définie par la relation* (3), *on a pour tout K dans $\mathbb{F}_2[X]$:*

$$|\hat{f}(K)| \in \left\{0, 2^{[(v(H^3 u)+2)/3]}\right\}. \tag{7}$$

Démonstration : A seule fin de simplifier les calculs, on se placera dans le cas où $v(u)$ est divisible par 3. Soit $\{w_j\}_{j\in J}$ un système de représentants de

$$\mathcal{P}_{\deg H-n-1}/\mathcal{P}_{\deg H-v(u)/3}.$$

On peut alors écrire :

$$\hat{f}(K)=\sum_{j\in J}a_jI_j \quad \text{où} \quad a_j=E(w_j^3H^3u+Kw_j) \text{ et}$$
$$I_j=\int_{v(\eta)\geq 1-\frac{v(u)}{3}+\deg H}E((\eta^2w_j+\eta w_j^2)H^3u+K\eta)d\eta$$

L'intégrale I_j vaut 0 ou $2^{v(H^3u)/3}$ et si $\hat{f}(K)$ est non nul, il existe un et un seul indice $k\in J$ tel que pour tout $j\in J$

on a
$$I_j=\begin{cases}2^{v(H^3u)/3} & \text{si } j=k\\ 0 & \text{si } j\neq k\end{cases}$$

d'où la proposition.

e) <u>Démonstration du théorème II dans le cas où</u> $v(u)>3\deg H$

On indique comment établir une version forte du théorème, dans le cas où l'élément $t=\dfrac{G}{H}+u$ est tel que l'on ait :

$$\max(n+\deg H,3\deg H)<v(u)\leq 2n+\deg H \quad (G,H)=1, 0\leq \deg H\leq n\ .$$

THEOREME A : *Sous les conditions précisées ci-dessus, on a :*

$$\left|S_n\left(\frac{G}{H}+u\right)\right|\leq 2^4.2^{\frac{5n}{6}}\ .$$

Démonstration : D'après les relations (5) (6), et (7) nous avons :

$$|S_n(t)|\leq 2^{\frac{7}{3}}|H|^{\frac{2}{3}}\sum_{\substack{K\in\mathbb{F}[X]\\ \hat{f}(K)\neq 0}}2^{[(v(H^3u)+2)/3]}\ .$$

Il ne nous reste plus qu'à majorer le cardinal des K tels que $\hat{f}(K)\neq 0$.
Les ensembles $B+\mathcal{P}$ où $B\in\mathbb{F}_2[X]$, $\deg B\leq n-\deg H$ forment une partition

de $\mathcal{P}_{\deg H-n-1}$.
Nous avons donc d'après la condition $v(u) > 3\deg H$:

$$\widehat{f}(K) = \int_{v(\eta)\geq \deg H-n} E(\eta^3 H^3 u)E(K\eta)d\eta =$$
$$\sum_{\deg B\leq n-\deg H} E(B^3H^3u)\int_{\mathcal{P}} E((\eta^2 B+\eta B^2)H^3u+K\eta)d\eta\ .$$

On peut donc majorer le cardinal des K tel que $\widehat{f}(K)$ soit non nul par le nombre des polynômes K tel qu'il existe

$$B\in \mathbb{F}_2[X],\ \deg B\leq n-\deg H \text{ avec } \int_{\mathcal{P}} E((\eta^2B+\eta B^2)H^3u+K\eta)d\eta$$

non nulle.

Or ce nombre peut être évalué explicitement. Il vaut $2^{n-\deg H+1-[(v(H^3u)+1)/2]}$.
Le théorème A en résulte.

f) Démonstration du théorème II dans le cas où $v(u)\leq 3\deg H$

On considère dans toute cette section un élément $t=\dfrac{G}{H}+u$ de $\mathbb{F}_2((\dfrac{1}{X}))$ tel que l'on ait

$$(8)\qquad \begin{cases} n+\deg H < v(u)\leq 3\deg H\\ (G,H)=1\ ,\ 0\leq \deg H\leq n\end{cases}$$

Introduisons maintenant la fonction arithmétique multiplicative Φ de $\mathbb{F}_2[X]$ dans lui-même, tel que, pour P irréductible, on ait

$$(9)\qquad \Phi(P^\ell)=\begin{cases} P^{[(\ell+1)/3]} & \text{si } \ell\neq 2\\ P^2 & \text{si } \ell=2\end{cases}$$

Cette fonction s'introduira de façon naturelle dans notre étude (cf. Proposition 3). Notre but dans cette section est d'établir le résultat suivant :
Théorème B : *Sous les conditions* (8), *on a pour*

$$n\geq 2^{541}\qquad |S_n(t)|\leq 2^3\ .2^{\frac{19}{20}n}\ .$$

Démonstration : Nous allons distinguer deux cas :

1er cas : $|\Phi(H)| \leq |H|^{\frac{1}{5}}$

et

2ème cas : $|\Phi(H)| > |H|^{\frac{1}{5}}$

Démonstration du 1er cas :

Nous partons de la relation **(5)**. D'après la condition $v(u) \leq 3 \deg H$ il découle du théorème de Plancherel

$$\sum_{K \in \mathbb{F}_2[X]} |\hat{f}(K)|^2 = 2^{n+1-\deg H} .$$

D'où

$$|S_n(t)| \leq T(G,H)^{\frac{1}{2}} \cdot 2^{n+1-[(v(u)+2)/3]} \tag{10}$$

Pour majorer $T(G,H)$ dans la relation **(10)** nous avons besoin du résultat suivant dû à Georges Rhin.

Lemme 2 : *Soit $Q \in \mathbb{F}_2[X]$ de degré $\chi \geq 2$. Le nombre $r = r(Q)$ de polynômes irréductibles qui divisent Q, vérifie l'inégalité*

$$r \leq \frac{3\chi \log 2}{\log \chi} . \tag{11}$$

Par des méthodes purement arithmétiques, en appliquant :

* d'une part, la définition de $\Phi(H)$ et les résultats concernant le module des sommes de Gauss $S(G,H,K)$,
* d'autre part, le résultat **(11)** de Georges Rhin,

nous obtenons la proposition suivante :

Proposition 2 : *Soient $H \in \mathbb{F}_2[X]$ et $|\Phi(H)| \leq |H|^{1/5}$ alors :*

$$T(G,H) \leq 2^{\frac{14}{3}} |H|^{\frac{11}{9} + \frac{6 \log 2}{\log \deg H}} .$$

Ainsi, pour $|\Phi(H)| \leq |H|^{\frac{1}{5}}$ le théorème B résulte de la relation **(10)** et de la proposition 2.

Démonstration du 2ème cas :

La somme $S_n(t)$ peut s'écrire

$$(\mathbf{12})\ S_n(t) = \sum_{\deg L \leq n - \deg H} E(L^3H^3u) \sum_{\deg R < \deg H} E\left(R^3\left(\frac{G}{H}+u\right)\right)E(R^2LHu)E(RL^2H^2u)$$

D'après le lemme 1 nous avons la majoration suivante :

$$(\mathbf{13}) \qquad |S_n(t)| \leq 2^{n+1-\deg H}T(G,H,u)^{\frac{1}{2}}$$

où

$$(\mathbf{14}) \qquad T(G,H,u) = \sum_{\deg R < \deg H} \ \sum_{\deg Q < \deg H} E\left(\left(\frac{G}{H}+u\right)(R^2Q+RQ^2)\right) .$$

Nous allons majorer $T(G,H,u)$ en considérant séparément les trois cas suivants. En fait nous avons divisé l'intervalle $n + \deg H < v(u) \leq 3\deg H$ en trois intervalles distincts qui varient en fonction du degré de $\Phi(H)$. Les intervalles considérés peuvent être vides.

cas (a) $\quad n + \deg H < v(u) \leq 3\deg \Phi(H)$

cas (b) $\quad 3\deg\Phi(H) + 1 \leq v(u) \leq 2\deg H + \deg \Phi(H) - 2$

cas (c) $\quad 2\deg H + \deg\Phi(H) - 2 < v(u) \leq 3\deg H$

on obtient :

$$(\mathbf{15}) \qquad T(G,H,u) \leq \begin{cases} \dfrac{|H|^3}{2^{2[(v(u)+2)/3]}} & \text{si } (a) \\ \dfrac{|H|^3}{2^{[(v(u)+\deg\Phi(H)+1)/2]}} & \text{si } (b) \\ \dfrac{|H|^2}{|\Phi(H)|} & \text{si } (c) \end{cases}$$

La relation **(15)** se démontre à l'aide de la proposition suivante :

PROPOSITION 3 : *Soient $(G,H)=1$ et R un polynôme de $\mathbb{F}_2[X]$ alors :*

$$\sum_{Q (\mathrm{mod}\ H)} E\left(\frac{G(R^2Q+RQ^2)}{H}\right) = |H| \Longrightarrow \Phi(H) \mid R$$

où Φ *désigne la fonction arithmétique multiplicative définie par la relation* **(9)**.

Il résulte alors de **(13)** et **(15)** que l'on a

$$\textbf{(16)} \qquad |S_n(t)| \leq \begin{cases} 2^{n+1}\dfrac{|H|^{1/2}}{2^{2[(v(u)+2)/3]}} & \text{si (a)} \\ 2^{n+1}\dfrac{|H|^{1/2}}{2^{[(v(u)+\deg\Phi(H)+1)/2]/2}} & \text{si (b)} \\ 2^{n+1}\dfrac{1}{2^{\deg\Phi(H)/2}} & \text{si (c)} \end{cases}$$

Ainsi, pour $|\Phi(H)| > |H|^{\frac{1}{5}}$, le théorème B résulte de la relation **(16)**.

DEUXIEME PARTIE : Méthode du cercle dans $\mathbb{F}_2[X]$ (Application au problème de Waring)

a) Méthode du cercle dans $\mathbb{F}_2[X]$

Soit M un polynôme de $\mathbb{F}_2[X]$ de degré $\deg M \in]3(n-1), 3n]$. Alors le nombre de représentations de M, noté $R_s(M)$, comme somme $M = M_1^3 + M_2^3 + \cdots + M_s^3$ où pour $i = 1, 2, \ldots s, M_i \in \mathbb{F}_2[X]$ avec $\deg M_i \leq n$ est égale à l'intégrale

$$\int_{\mathcal{P}} S_n^s(t) E(Mt)dt \text{ où } S_n(t) = \sum_{\substack{\deg B \leq n \\ B \in \mathbb{F}_2[X]}} E(B^3 t) \ .$$

On a une partition de $\mathcal{P}$ analogue à une dissection de Farey du segment $[0, 1]$.

$$\mathcal{P} = \bigcup_{\substack{H \in \mathbb{F}_2[X] \\ 0 \leq \deg H \leq n}} \ \bigcup_{\substack{G \in \mathbb{F}_2[X] \\ \deg G < \deg H \\ (G,H)=1}} \mathcal{M}_{G/H} \qquad \text{où}$$

$$\mathcal{M}_{G/H} = \left\{ t \in \mathcal{P} \mid v(t - \frac{G}{H}) > n + \deg H \right\} \ .$$

Notons qu'il n'y a que des arcs majeurs.

Posons

$$m = \bigcup_{\substack{H \in \mathbb{F}_2[X] \\ \deg H = 0}}^{n} \left(\bigcup_{\substack{(G,H)=1 \\ \deg G < \deg H}} \left\{ t \in P | t = \frac{G}{H} + u, n + \deg H < v(u) \leq 2n + \deg H \right\} \right)$$

$$\mathcal{M} = \mathcal{P} \setminus m$$

On obtient :

$$R_s(M) = \int_{\mathcal{M}} S_n^s(t)E(Mt)dt + \int_m S_n^s(t)E(Mt)dt \ .$$

b) <u>Un équivalent de l'intégrale</u> $\int_{\mathcal{M}}$ <u>sur l'ensemble</u> $\mathcal{M}$

L'intégrale $\int_{\mathcal{M}}$ sur l'ensemble $\mathcal{M}$ se calcule à l'aide du résultat suivant :

LEMME 3 : *Pour* $t = \dfrac{G}{H} + u \in \mathcal{M}$ *on a :*

$$S_n(\frac{G}{H} + u) = \begin{cases} S(G,H).2^{v(u)/3-\deg H} & \text{si } v(u) \equiv 0(3) \text{ et } v(u) \leq 3n+1 \\ 0 & \text{si } v(u) \equiv 1(3) \text{ et } v(u) \leq 3n+1 \\ S(G,H).2^{(v(u)+1)/3-\deg H} & \text{si } v(u) \equiv 2(3) \text{ et } v(u) \leq 3n+1 \end{cases}$$

$$S_n(\frac{G}{H} + u) = S(G,H).2^{n+1-\deg H} \ \text{si } v(u) \geq 3n+2$$

où

$$S(G,H) = \sum_{R(\mathrm{mod}\ H)} E(\frac{G}{H}R^3) \ .$$

On a :

$$\int_{\mathcal{M}} S_n^s(t)E(Mt)dt = 2^{n(s-3)}(2^{s-1} - \varepsilon) \sum_{0 \leq \deg H \leq n} \ \sum_{\substack{(G,H)=1 \\ \deg G < \deg H}} E(M\frac{G}{H})\frac{S(G,H)^s}{|H|^s}$$

$$\text{où } \varepsilon = \begin{cases} 0 & \text{si } \deg M = 3n \\ 1 & \text{si } \deg M = 3n-1 \text{ ou } \deg M = 3n-2. \end{cases}$$

L'intégrale $\int_{\mathcal{M}}$ fait apparaître les premiers termes d'une série singulière notée $G_s(M)$. On montrera le lemme suivant :

LEMME 4 : *Soit pour* $s \in \mathbb{N}$, *pour* $M \in \mathbb{F}_2[X]$:

$$G_s(M) = \sum_{\substack{H \in \mathbb{F}_2[X] \\ H \neq 0}} |H|^{-s} \sum_{\substack{G \in \mathbb{F}_2[X] \\ \deg G < \deg H \\ (G,H)=1}} [S(G,H)]^s E(M\frac{G}{H}).$$

Pour $s \geq 7$, pour M un polynôme congru à 0 ou 1 modulo $1+X+X^2$ on a :

$$a_1(s) \leq G_s(M) \leq a_2(s) \text{ avec } \begin{cases} a_1(s) & = 2(1-2^{4-s})^3(1-2^{2-s/3}) \\ a_2(s) & = 2(1+2^{4-s})^3(1-2^{3-2s/3})/1-2^{2-s/3} \end{cases}$$

A l'aide du lemme 4 on démontre pour $s \geq 7$, pour M congru à 0 ou 1 modulo $1+X+X^2$

$$\textbf{(17)} \qquad \int_{\mathcal{M}} S_n^s(t)E(Mt)dt = 2^{n(s-3)}(2^{s-1}-\varepsilon)G_s(M) + O_s(2^{n(s-3-\frac{s-6}{3})}).$$

c) <u>Majoration de l'intégrale sur</u> m

L'intégrale $\int_m$ sur l'ensemble m est majorée à l'aide du théorème II, l'équivalent du lemme de Weyl et l'identité de Parseval.

On a :

$$\textbf{(18)} \qquad \left|\int_m S_n^s(t)E(Mt)dt\right| \leq \max_{t\in m}\left|S_n^{s-2}(t)\right| \int_{\mathcal{P}} S_n^2(t)dt = O_s(2^{n(s-3-\frac{s-42}{20})})$$

d) <u>Un équivalent de</u> $R_s(M)$

On obtient ainsi d'après **(17)** et **(18)** un équivalent de $R_s(M)$ pour $s \geq 43$ et M congru à 0 ou 1 modulo $1+X+X^2$

$$R_s(M) = 2^{n(s-3)}(2^{s-1}-\varepsilon)G_s(M) + O_s(2^{n(s-3-\frac{s-42}{20})}).$$

Démonstration du Théorème I :

On désigne par $K_{\ell,n-1}$ l'ensemble des polynômes $\mathcal{U} \in \mathbb{F}_2[X]$ du degré $(\leq 3(n-1))$ de la forme

$$\mathcal{U} = A_1^3 + \cdots + A_\ell^3, \deg A_i \leq n-1, i = 1,2,\ldots \ell\ .$$

On a la minoration

$$\text{card } \mathcal{K}_{\ell,n-1} \geq b(\ell).2^{3n(1-(\frac{2}{3})^\ell)}$$

où

$$b(\ell) = 2^{3-2\ell-2(\frac{2}{3})^{\ell-1}}.$$

Soient $M \in \mathbb{F}_2[X]$ tel que $3(n-1) < \deg M \leq 3n$ et congru à 0 ou 1 modulo $1+X+X^2$,

$$R_{\ell,n-1}(t) = \sum_{\mathcal{U}\in\mathcal{K}_{\ell,n-1}} E(t\,\mathcal{U}) \text{ et } J_{s,\ell}(M) = \int_{\mathcal{P}} S_n^s(t)R_{\ell,n-1}^2(t)E(Mt)dt\ .$$

L'intégrale $J_{s,\ell}(M)$ est égale au nombre de représentations de M sous la forme

$$M = M_1^3 + \cdots + M_s^3 + A_1^3 + \cdots + A_\ell^3 + B_1^3 + \cdots B_\ell^3$$

avec $\deg M_i \leq n$ pour $i = 1, 2, \ldots s$ $\deg A_k \leq n-1$ pour $k = 1, 2, \ldots \ell$ $\deg B_j \leq n-1$ pour $j = 1, 2, \ldots \ell$.

Le nombre de cubes dans cette présentation de M est inférieur ou égal à $s + 2\ell$.
Il suffit donc de minimaliser $s + 2\ell$ sous la condition : $J_{s,\ell}(M)$ strictement positive.
Les calculs se font de la même manière que pour obtenir un équivalent de $R_s(M)$.
On obtient la condition supplémentaire $s > \sup(6, 10.2^{\ell+1}/2^{\ell-1})$. Il ne nous reste qu'à minimaliser $s + 2\ell$ sous cette condition, ce qui donne pour résultat 18. D'où le théorème.

Je tiens à remercier Monsieur Jean-Marc Deshouillers de l'Université de Bordeaux I qui par ses nombreux conseils et encouragements m'a permis de mener à bien ce travail.

REFERENCES

[1] BALASUBRAMANIAN R., DESHOUILLERS J.M., DRESS F., Problème de Waring pour les bicarrés, *CRAS Paris*, série I, n°4 et n°5, **303** (1986).

[2] CAR M., Le problème de Waring pour l'anneau des polynômes sur un corps fini, *CRAS Paris*, Série A, **273** (1971), 141-144.

[3] CHERLY J., *Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à 2 éléments, et application au problème de Waring*, Thèse soutenue à l'Université de Bordeaux I le 27/10/89.

[4] KUBOTA R.M., Waring's problem for $\mathbb{F}_q[X]$, *Dissertationes Math.* **117** (1974).

[5] MATTHEWS K.R., *Waring's theorem for polynomials over a finite field*, Thèse soutenue à l'Université du Queensland, (1966).

[6] RHIN G., Répartition modulo I dans un corps de séries formelles sur un corps fini, *Dissertationes Math.* **95** (1972).

[7] VAUGHAN R.C., *The Hardy-Littlewood Method*, Cambridge tracts in Mathematics **80** (1981).

Jørgen CHERLY
Université de Bretagne Occidentale
Département de Mathématiques
et Informatique
6, avenue le Gorgeu
29287 BREST CEDEX