

HOUDA AÏSSA

Formes quadratiques sur $\mathbb{F}_q[T]$

Annales mathématiques Blaise Pascal, tome 9, n° 1 (2002), p. 9-20

http://www.numdam.org/item?id=AMBP_2002__9_1_9_0

© Annales mathématiques Blaise Pascal, 2002, tous droits réservés.

L'accès aux archives de la revue « Annales mathématiques Blaise Pascal » (<http://math.univ-bpclermont.fr/ambp/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Formes quadratiques sur $\mathbb{F}_q[T]$

Houda Aïssa

Résumé

Dans ce travail nous étudions des formes quadratiques polynomiales à quatre variables, prolongeant ainsi un résultat de M.Car.

I Introduction

Soit \mathbb{F}_q le corps fini à q éléments, q étant une puissance d'un nombre premier impair.

Certaines analogies entre l'anneau $\mathbb{F}_q[T]$ des polynômes à une variable sur le corps \mathbb{F}_q et l'anneau des entiers relatifs \mathbb{Z} ont été mises en évidence, notamment en ce qui concerne l'arithmétique additive.

En 1926, H.D.Kloosterman [2] s'est intéressé à l'étude de la représentation d'un entier positif n comme somme:

$$n = ax^2 + by^2 + cz^2 + dt^2$$

avec a, b, c, d des entiers positifs fixés.

En 1996, M.Car [1] a étudié un problème analogue sur l'anneau $\mathbb{F}_q[T]$. Plus précisément, elle a donné une estimation du nombre de représentations d'un polynôme M de $\mathbb{F}_q[T]$ comme somme:

$$A_1M_1^2 + A_2M_2^2 + A_3M_3^2 + A_4M_4^2 \tag{I.1}$$

où M_1, \dots, M_4 sont des polynômes vérifiant les conditions de degré les plus restrictives possibles, à savoir

$$\deg M_i \leq m_i, \tag{I.2}$$

les entiers m_1, \dots, m_4 étant déterminés par la condition

$$\deg M \in \{2m_i + \deg A_i - 1, 2m_i + \deg A_i\} \tag{I.3}$$

et ce, dans les deux cas suivants:

- (i) A_1, A_2, A_3, A_4 sont des polynômes premiers entre eux deux à deux,
- (ii) $A_1 = A_2 = 1; A_3 = A_4 = D$, D étant un polynôme sans facteur carré.

Dans ce travail nous nous intéressons au cas $A_1 = A_2 = D_1; A_3 = A_4 = D_2$ où D_1 et D_2 sont deux polynômes sans facteurs carrés premiers entre eux. Ce cas est intéressant car, si -1 n'est pas carré dans le corps \mathbb{F}_q , tout $M \in \mathbb{F}_q[T]$ s'écrivant comme somme (I.1) où M_i vérifient les conditions de degré (I.2) et (I.3), M admet alors une représentation

$$M = D_1N_1 + D_2N_2,$$

où N_1 et N_2 sont des normes dans l'extension $\mathbb{F}_{q^2}(T)$ de $\mathbb{F}_q(T)$ de polynômes de $\mathbb{F}_{q^2}[T]$.

Notons ici que, de façon triviale, si -1 est carré dans le corps \mathbb{F}_q , tout polynôme $M \in \mathbb{F}_q[T]$ s'écrit comme somme (I.1) sans toutefois que les conditions de degré (I.2) et (I.3) soient assurées.

En utilisant la méthode du cercle, nous établissons essentiellement le théorème suivant:

Théorème Soient D_1 et D_2 deux polynômes sans facteurs carrés et premiers entre eux. Alors,

(i) tout polynôme $M \in \mathbb{F}_q[T]$ premier à D_1D_2 et de degré assez grand admet une représentation de la forme :

$$M = D_1(M_1^2 + M_2^2) + D_2(M_3^2 + M_4^2)$$

où les polynômes M_1, \dots, M_4 vérifient les conditions de degré (I.2) et (I.3).

De plus, si $R(M)$ désigne le nombre de ces représentations, on a:

$$R(M) \gg \frac{q^{\deg M}}{\log(\deg M)},$$

la constante intervenant dans le symbole \gg ne dépendant que de q, D_1, D_2 .

(ii) Le même résultat reste valable pour tout polynôme M tel que -1 soit un carré modulo tout polynôme irréductible P divisant le pgcd de D_1D_2 et M .

Concernant le cas $A_1 = D_1, A_2 = A_3 = A_4 = D_2$ où D_1, D_2 des polynômes premiers entre eux sans facteurs carrés, on montre que si M est divisible par D_2 , alors M est représentable comme somme (I.1) où les polynômes M_i vérifient les conditions de degré (I.2) et (I.3). De plus, la minoration asymptotique ci-dessus reste encore vraie.

II Notations et conventions

Dans cet article, les polynômes considérés sont ceux de l'anneau $\mathbb{F}_q[T]$. On désigne par \mathbb{M} l'ensemble des polynômes unitaires, par I l'ensemble des polynômes irréductibles unitaires.

Pour A et B deux polynômes de $\mathbb{F}_q[T]$, on note (A, B) leur *pgcd*.

Soit H un polynôme non nul de $\mathbb{F}_q[T]$. On note $\deg H$ son degré, \mathcal{C}_H l'ensemble des polynômes de degré strictement inférieur au degré de H identifié à l'ensemble des classes de congruence modulo H . Le groupe multiplicatif des classes inversibles modulo H sera noté \mathcal{C}_H^* , l'ordre de ce groupe sera noté $\Phi(H)$. La fonction ainsi définie a les mêmes propriétés que la fonction d'Euler classique. On définit le symbole de Legendre sur $\mathbb{F}_q[T]$ comme suit:

si P est un polynôme irréductible et A un polynôme premier à P ,

$$\left(\frac{A}{P}\right) = \begin{cases} 1 & \text{si } A \text{ est un carré modulo } P, \\ -1 & \text{sinon.} \end{cases}$$

Le symbole $(\frac{A}{P})$ a les mêmes propriétés que le symbole de Legendre classique et vérifie la loi de réciprocité quadratique [4]. Ce symbole s'étend à tout couple de polynômes premiers entre eux par multiplicativité.

Sur le corps $\mathbb{K} = \mathbb{F}_q(T)$ des fractions rationnelles, on définit une valuation v par :

$$v\left(\frac{A}{B}\right) = \deg B - \deg A$$

si A et B sont des polynômes non nuls. Le complété \mathbb{K}_∞ de \mathbb{K} pour cette valuation s'identifie au corps $\mathbb{F}_q((T^{-1}))$ des séries de Laurent en $\frac{1}{T}$ sur le corps \mathbb{F}_q , la valuation v se prolongeant aux éléments non nuls de \mathbb{K}_∞ , par:

$$v\left(\sum_{s=-\infty}^{+\infty} a_s T^s\right) = -\sup\{s \in \mathbb{Z}; a_s \neq 0\}.$$

On associe à cette valuation, la valeur absolue $|\cdot|_\infty$ définie par:

$$|\alpha|_\infty = \begin{cases} q^{-v(\alpha)} & \text{si } \alpha \neq 0 \\ 0 & \text{si } \alpha = 0 \end{cases}$$

Nous noterons simplement $|\cdot|$ cette valeur absolue car le contexte nous permet de la distinguer de la valeur absolue classique sur le corps \mathbb{R} des nombres réels ou le corps \mathbb{C} des nombres complexes qu'on va utiliser.

H. AÏSSA

Soit $u \in \mathbb{K}_\infty$, si $u = \sum_{s=-\infty}^{+\infty} u_s T^s$, on pose $Res(u) = u_{-1}$.

De plus, si $u \neq 0$, on définit l'application sgn de \mathbb{K}_∞ dans \mathbb{F}_q en posant $sgn(u) = u_{-v(u)}$.

Soit Ψ le caractère additif défini sur \mathbb{F}_q par:

$$\Psi(x) = \exp\left(\frac{2i\pi tr(x)}{p}\right)$$

où tr est l'application trace de \mathbb{F}_q dans \mathbb{F}_p .

Au caractère non trivial Ψ , on associe le caractère additif non trivial E de \mathbb{K}_∞ défini par:

$$E(u) = \Psi(Res(u)).$$

III Les séries singulières

L'estimation de $R(M)$ fait apparaître une série que l'on va étudier dans ce paragraphe.

On pose pour tout polynôme unitaire H et pour $G \in \mathcal{C}_H^*$,

$$S(H, G) = \sum_{R \in \mathcal{C}_H} E\left(\frac{GR^2}{H}\right) \quad (III.1)$$

$$T(H, G) = S^2(H, GD_1)S^2(H, GD_2) \quad (III.2)$$

Soit $M \in \mathbb{F}_q[T]$. Pour tout polynôme unitaire H , on pose:

$$A(H, M) = |H|^{-4} \sum_{G \in \mathcal{C}_H^*} T(H, G)E\left(-M\frac{G}{H}\right). \quad (III.3)$$

On rappelle ici quelques résultats déjà démontrés dans [1].

Proposition III.1 *Soit P un polynôme irréductible. Soit G un polynôme premier à P . Alors, pour tout entier k on a :*

$$S(P^{2k}, G) = |P|^k,$$

$$S(P^{2k+1}, G) = |P|^k \left(\frac{G}{P}\right) S(P, 1).$$

FORMES QUADRATIQUES SUR $\mathbb{F}_q[T]$

Proposition III.2 *Si H_1, H_2 sont deux polynômes unitaires premiers entre eux, pour tout polynôme M on a :*

$$A(H_1H_2, M) = A(H_1, M)A(H_2, M).$$

Proposition III.3 *Soit P un polynôme irréductible, M un polynôme quelconque et k un entier. Alors,*

$$A(P^k, M) = 0 \quad \text{si } k > 1 + v_P(M).$$

On définit alors, pour tout polynôme irréductible P

$$\Psi(P, M) = 1 + \sum_{k=1}^{\infty} A(P^k, M), \quad (III.4)$$

et

$$\mathfrak{S}(M) = \sum_{H \in \mathbb{M}} A(H, M). \quad (III.5)$$

$\mathfrak{S}(M)$ se développe en produit eulérien absolument convergent

$$\mathfrak{S}(M) = \prod_{P \in \mathcal{I}} \Psi(P, M). \quad (III.6)$$

Proposition III.4 *Soit P un polynôme irréductible premier à D_1D_2 . Alors pour tout polynôme M on a :*

$$\Psi(P, M) = (1 - |P|^{-2}) \left(\sum_{k=0}^{v_P(M)} |P|^{-k} \right) \quad (III.7)$$

Démonstration

C'est un cas particulier de la proposition V.3 de [1].

Proposition III.5 *Le produit*

$$\Lambda = \prod_{P \in \mathcal{I}, P \nmid D_1D_2} (1 - |P|^{-2}) \quad (III.8)$$

est absolument convergent et positif.

Démonstration

C'est la proposition V.4 de [1].

Proposition III.6 *Soit P un polynôme irréductible divisant D_1 , respectivement D_2 . Alors pour tout polynôme M on a :*

$$\Psi(P, M) = 1 + \left(\frac{-1}{P}\right)(1 - |P|^{-v_P(M)} - |P|^{-v_P(M)-1}) \quad (III.9)$$

Démonstration

D'après la proposition III.3, on a

$$\begin{aligned} \Psi(P, M) &= 1 + \sum_{k=1}^{v_P(M)+1} A(P^k, M) \\ &= 1 + \sum_{k=1}^{v_P(M)+1} |P|^{-4k} \sum_{G \in \mathcal{C}_{P^k}^*} S^2(P^k, D_1 G) S^2(P^k, D_2 G) E\left(-M \frac{G}{P^k}\right). \end{aligned}$$

Supposons que $v_P(M) = 0$.

Alors, avec la proposition III.1 et la proposition IV.4 de [1], on a

$$\Psi(P, M) = 1 - \left(\frac{-1}{P}\right).$$

Supposons que $v_P(M) \neq 0$.

- Si $v_P(M) \equiv 0 \pmod{2}$, posons $v_P(M) = 2w$.

Alors,

$$\begin{aligned} \Psi(M) &= 1 + \sum_{j=0}^w |P|^{-8j-4} \sum_{G \in \mathcal{C}_{P^{2j+1}}^*} S^2(P^{2j+1}, D_1 G) S^2(P^{2j+1}, D_2 G) E\left(-M \frac{G}{P^{2j+1}}\right) \\ &\quad + \sum_{j=0}^w |P|^{-8j} \sum_{G \in \mathcal{C}_{P^{2j}}^*} S^2(P^{2j}, D_1 G) S^2(P^{2j}, D_2 G) E\left(-M \frac{G}{P^{2j}}\right). \end{aligned}$$

A l'aide de la proposition III.1 et la proposition IV.4 de [1], on obtient

$$\Psi(P, M) = \left(\frac{-1}{P}\right) \left(1 - |P|^{-v_P(M)} - |P|^{-v_P(M)-1}\right).$$

FORMES QUADRATIQUES SUR $\mathbb{F}_q[T]$

- Si $v_P(M) \equiv 1 \pmod{2}$,

avec des calculs analogues à ceux faits précédemment, on montre le résultat annoncé.

Proposition III.7 *Pour tout polynôme M premier à D_1D_2 , on a :*

$$\Lambda \frac{\Phi(D_1D_2)\Phi(M)}{|D_1D_2||M|} \leq \mathfrak{S}(M) \leq \Lambda \frac{|D_1D_2||M|}{\Phi(D_1D_2)\Phi(M)} \quad (III.10)$$

et, pour tout polynôme M tel que -1 soit un carré modulo tout polynôme irréductible P divisant (D_1D_2, M) , on a :

$$\Lambda \frac{\Phi(D_1D_2)\Phi(M)}{|D_1D_2||M|} \leq \mathfrak{S}(M) \leq 2^{\omega(D_1D_2)} \Lambda \frac{|M|}{\Phi(M)}. \quad (III.11)$$

où $\omega(D_1D_2)$ est le nombre de facteurs irréductibles unitaires de D_1D_2 .

Démonstration

On a

$$\begin{aligned} \mathfrak{S}(M) &= \prod_{P \in I} \Psi(P, M) \\ &= \prod_{P \in I, P \nmid D_1D_2} \Psi(P, M) \prod_{P \in I, P \mid D_1D_2} \Psi(P, M) \end{aligned}$$

Or, d'après (III.7) on a :

$$\prod_{P \in I, P \nmid D_1D_2} \Psi(P, M) = \Lambda \Gamma(M) \quad (1)$$

où

$$\Lambda = \prod_{P \in I, P \nmid D_1D_2} (1 - |P|^{-2}) < \infty$$

et

$$\begin{aligned} \Gamma(M) &= \prod_{P \in I, P \nmid D_1D_2} \left(\sum_{k=0}^{v_P(M)} |P|^{-k} \right) \\ &= \prod_{P \in I, P \nmid D_1D_2, P \mid M} \left(\sum_{k=0}^{v_P(M)} |P|^{-k} \right) \end{aligned}$$

H. AÏSSA

$$\begin{aligned}
&= \prod_{P \in I, P \nmid D_1 D_2, P \mid M} \left(\frac{1 - |P|^{-v_P(M)-1}}{1 - |P|^{-1}} \right) \\
&= \prod_{P \in I, P \nmid D_1 D_2, P \mid M} \left(\frac{|P| - |P|^{-v_P(M)}}{|P| - 1} \right).
\end{aligned}$$

D'où,

$$\prod_{P \in I, P \mid M} \left(\frac{|P| - 1}{|P|} \right) \leq \Gamma(M) \leq \prod_{P \in I, P \mid M} \left(\frac{|P|}{|P| - 1} \right). \quad (2)$$

Supposons M premier à $D_1 D_2$. D'après la proposition précédente,

$$\prod_{P \in I, P \mid D_1 D_2} \Psi(P, M) = \prod_{P \in I, P \mid D_1 D_2} \left(1 - \left(\frac{-1}{P} \right) |P|^{-1} \right).$$

Par suite

$$\prod_{P \in I, P \mid D_1 D_2} \frac{|P| - 1}{|P|} \leq \prod_{P \in I, P \mid D_1 D_2} \Psi(P, M) \leq \prod_{P \in I, P \mid D_1 D_2} \frac{|P|}{|P| - 1}. \quad (3)$$

La relation (III.10) se déduit alors de (1), (2) et (3).

Supposons que $(D_1 D_2, M) \neq 1$ et que -1 soit un carré modulo tout polynôme irréductible P divisant $(D_1 D_2, M)$.

• Si $P \mid (D_1 D_2, M)$, alors $\Psi(P, M) = 2 - |P|^{-v_P(M)} - |P|^{-v_P(M)-1}$.

D'où,

$$2 \frac{|P| - 1}{|P|} \leq \Psi(P, M) \leq 2.$$

et par suite

$$\prod_{P \in I, P \mid (D_1 D_2, M)} \frac{|P| - 1}{|P|} \leq \prod_{P \in I, P \mid (D_1 D_2, M)} \Psi(P, M) \leq 2^{\omega(D_1 D_2)}.$$

• Si $P \nmid D_1 D_2$ et $P \nmid M$, alors, d'après la proposition précédente, on a:

$$\Psi(P, M) = 1 - \left(\frac{-1}{P} \right) |P|^{-1},$$

d'où

$$1 - \frac{1}{|P|} \leq \Psi(P, M) \leq 1 + \frac{1}{|P|} \leq 2.$$

FORMES QUADRATIQUES SUR $\mathbb{F}_q[T]$

Par suite,

$$\prod_{P \in I, P|D_1 D_2} \frac{|P| - 1}{|P|} \leq \prod_{P \in I, P|D_1 D_2} \Psi(P, M) \leq 2^{\omega(D_1 D_2)}. \quad (4)$$

Avec (1), (2) et (4), on aura

$$\Lambda \frac{\Phi(D_1 D_2) \Phi(M)}{|D_1 D_2| |M|} \leq \mathfrak{S}(M) \leq 2^{\omega(D_1 D_2)} \Lambda \frac{|M|}{\Phi(M)}.$$

IV Estimation de $R(M)$

On reprend ici des notations introduites dans [1].
Soient A_1, \dots, A_4 des polynômes premiers entre eux, l'un d'entre eux au moins étant non constant.

Pour $i = 1, \dots, 4$, on pose

$$\text{sgn}(A_i) = \alpha_i$$

$$\deg M - \deg A_i = \begin{cases} 2m_i & \text{si } \deg M - \deg A_i \text{ est pair} \\ 2m_i - 1 & \text{si } \deg M - \deg A_i \text{ est impair} \end{cases}$$

$$u(M) = \{i \in \{1, \dots, 4\}; \deg M \equiv \deg A_i \pmod{2}\},$$

$$v(M) = \{i \in \{1, \dots, 4\}; \deg M \not\equiv \deg A_i \pmod{2}\}.$$

Pour tout x dans \mathbb{F}_q , on note $r(\alpha_1, \dots, \alpha_4; x)$ le nombre de solutions (x_1, \dots, x_4) dans $(\mathbb{F}_q)^4$ de l'équation :

$$x = \sum_{i=1}^4 \alpha_i x_i^2.$$

On rappelle la proposition VIII.1 de [1] :

Proposition IV.1 *Soit ε un nombre réel positif. Alors, il existe une constante $c_1 = c_1(\varepsilon, A_1, \dots, A_4)$ telle que pour tout polynôme M de degré supérieur ou égal à $\max\{\deg A_1, \dots, \deg A_4\}$, on ait :*

$$|R(M) - q^{m_1 + \dots + m_4} |M|^{-1} \mathfrak{S}_4(M) \Theta(M)| \leq c_1 |M|^{\frac{3}{4} + \varepsilon} \quad (IV.1)$$

où

$$\Theta(M) = \begin{cases} r_{\{1,\dots,4\}}(\text{sgn}(M)) & \text{si } \deg M \equiv \deg A_i \pmod{2} \ \forall i \in \{1, \dots, 4\} \\ q^{\#u(M)-1} r_{v(M)}(0) + r_{u(M)}(\text{sgn}(M)) - q^{\#u(M)-1} & \text{sinon,} \end{cases} \quad (IV.2)$$

$$\mathfrak{S}_4(M) = \sum_{H \in \mathbb{M}} |H|^{-4} \sum_{G \in \mathcal{C}_H^*} \prod_{i=1}^4 S(H, GA_i) E\left(-M \frac{G}{H}\right)$$

et pour tout $\alpha \in \mathbb{F}_q$,

$$r_{\{1,\dots,4\}}(\alpha) = r(\alpha_1, \dots, \alpha_4; \alpha).$$

Donnons maintenant la démonstration du théorème:

Démonstration du théorème

(i) Si M est premier à $D_1 D_2$, d'après la relation (III.10) on a:

$$\mathfrak{S}(M) \geq \Lambda \frac{\Phi(D_1 D_2) \Phi(M)}{|D_1 D_2| |M|} > 0$$

Par une démonstration analogue à celle du théorème 5.1 chapitre I de [3], on montre qu'il existe une constante c_2 , ne dépendant que de q , telle que pour tout polynôme M de degré strictement supérieur à 1, on ait :

$$\frac{\Phi(M)}{|M|} \geq c_2 (\log(\deg M))^{-1}$$

alors

$$\mathfrak{S}(M) \geq \Lambda c_2 \frac{\Phi(D_1 D_2)}{|D_1 D_2|} (\log(\deg M))^{-1}$$

D'après la démonstration du [corollaire VII.4, [1]] on déduit qu'il existe une constante $c_3 > 0$, ne dépendant que de q telle que

$$\Theta(M) \geq c_3.$$

D'après la relation (IV.1) de la proposition précédente, on déduit que : pour $\deg M$ assez grand et pour $\varepsilon \in]0, \frac{1}{4}[$,

$$\begin{aligned} R(M) &\geq q^{m_1 + \dots + m_4} |M|^{-1} \mathfrak{S}(M) \Theta(M) - c_1 |M|^{\frac{3}{4} + \varepsilon} \\ &\geq \frac{1}{2} q^{m_1 + \dots + m_4} |M|^{-1} \mathfrak{S}(M) \Theta(M) \\ &\geq \frac{1}{2} c_3 |D_1 D_2|^{-1} \Lambda c_2 \frac{\Phi(D_1 D_2)}{|D_1 D_2|} \frac{|M|}{\log(\deg M)} \\ &\geq c_4(q, D_1, D_2) \frac{|M|}{\log(\deg M)} \end{aligned}$$

FORMES QUADRATIQUES SUR $\mathbb{F}_q[T]$

D'où la minoration annoncée.

(ii) Si le polynôme M n'est pas premier à D_1D_2 et si -1 est un carré modulo tout polynôme irréductible P divisant (D_1D_2, M) , la démonstration se fait de la même manière en utilisant la relation (III.11).

Remarque

Choisissons maintenant $A_1 = D_1$, $A_2 = A_3 = A_4 = D_2$ où D_1, D_2 des polynômes premiers entre eux sans facteurs carrés.

Soit M un polynôme divisible par D_2 , alors $M = ND_2$. Si de plus M vérifie:

$$M = D_1X^2 + D_2(Y_1^2 + Y_2^2 + Y_3^2), \quad (**)$$

alors D_2 divise X^2 . Comme D_2 est sans facteur carré, D_2 divise X .

Posons $X = D_2Z$, (***) devient donc:

$$N = D_1D_2Z^2 + Y_1^2 + Y_2^2 + Y_3^2.$$

Le résultat établi en [1] s'applique ici en prenant $A_1 = D_1D_2$, $A_2 = A_3 = A_4 = 1$. On a donc

$$R(N) \gg \frac{|N|}{\log(\deg N)}$$

Alors

$$R(M) \gg \frac{|M|}{\log(\deg M)}.$$

Remerciement

Je remercie le rapporteur pour ses critiques constructives des différentes versions de ce manuscrit.

Références

- [1] M. Car. Quadratic forms on $\varphi_q[t]$. *Journal of Number Theory*. 61 p. 145-180, 1996.
- [2] H.D. Kloosterman. On the representations of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.* 49 p. 407-464, 1926.
- [3] K. Prachar. *Primzahlverteilung*. Springer-Verlag, Berlin, 1957.
- [4] J-P. Serre. *Corps locaux*. 2nd ed. Hermann, Paris, 1968.

H. Aïssa

HOUDA AÏSSA
FACULTÉ DES SCIENCES DE TUNIS.
DÉPARTEMENT DE MATHÉMATIQUES

1060, TUNIS
TUNISIE