*Bull. Soc. math. France*
**130** (2), 2002, p. 211–231

# POIDS DES DUAUX DES CODES BCH DE DISTANCE PRESCRITE $2^a + 1$ ET SOMMES EXPONENTIELLES

PAR ÉRIC FÉRARD

RÉSUMÉ. — Soit $n$ un entier pair. On considère un code BCH binaire $C_n$ de longueur $2^n - 1$ et de distance prescrite $2^a + 1$ avec $a \geq 3$. Le poids d'un mot non nul du dual de $C_n$ peut s'exprimer en fonction d'une somme exponentielle. Nous montrerons que cette somme n'atteint pas la borne de Weil et nous proposerons une amélioration de celle-ci. En conséquence, nous obtiendrons une amélioration de la borne de Carlitz-Uchiyama sur le poids des mots du dual de $C_n$.

ABSTRACT (*Weight of duals of BCH codes of designed distance* $2^a + 1$ *and exponential sums*)

Let $n$ be an even integer. We consider a binary BCH code $C_n$ of length $2^n - 1$ and designed distance $2^a + 1$ with $a \geq 3$. The weight of a nonzero codeword of the dual of $C_n$ is linked to the value of an exponential sum. We will show that this exponential sum does not reach the Weil bound and we will improve this bound. Thus, we obtain an improvement of the Carlitz-Uchiyama bound on the weights of the words of the dual of $C_n$.

## 1. Introduction

Soit $n$ un entier strictement positif. Soit $C_n$ un code BCH binaire de longueur $q - 1 = 2^n - 1$ et de distance prescrite $2t + 1$. Le poids $w$ d'un mot de code non

*Texte reçu le 10 juillet 2000, révisé le 13 décembre 2000, accepté le 5 janvier 2001.*

ÉRIC FÉRARD, Équipe Arithmétique et Théorie de l'Information, I.M.L., C.N.R.S., Luminy case 907, 13288 Marseille Cedex 9 (France) • *E-mail :* `ferard@iml.univ-mrs.fr`

Classification mathématique par sujets (2000). — 11T23, 94B15.

Mots clefs. — Codes BCH, borne de Carlitz-Uchiyama, sommes exponentielles, borne de Weil.

nul du dual de $C_n$ satisfait la borne de Carlitz-Uchiyama :

$$|w - 2^{n-1}| \leq (t-1)2^{n/2}.$$

On s'intéressera au cas où $n$ est pair.

Si $p$ est un nombre premier et $\ell$ un entier, on notera $\mathbb{F}_{p^\ell}$ un corps fini à $p^\ell$ éléments. Si $K$ est un corps et $L$ une extension finie de $K$, on désignera la trace de $L$ sur $K$ par $\mathrm{Tr}_{L/K}$.

Soit $c$ un mot de code du dual de $C_n$. Ce mot peut s'écrire sous la forme

$$c = \big(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(f(\alpha))\big)_{\alpha \in \mathbb{F}_q^\star}$$

où $f$ est un polynôme à coefficients dans $\mathbb{F}_q$ sans terme constant de degré au plus $2t-1$ (voir [9]). Comme $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha^2) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha)$, on peut toujours supposer que $f$ est nul ou bien de degré impair. Le poids $w(c)$ de $c$ est égal à

$$w(c) = \frac{q - S(f)}{2}$$

où $S(f)$ est la somme exponentielle définie par

$$S(f) = \sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(f(x))}.$$

Si le degré de $f$ est impair, la somme exponentielle $S(f)$ vérifie la borne de Weil :

$$\big|S(f)\big| \leq (\deg f - 1)\sqrt{q}.$$

Remarquons que cette borne correspond à la borne de Carlitz-Uchiyama. On pourra aussi noter que le nombre de points $N$ du modèle projectif de la courbe $y^2 + y = f(x)$ sur $\mathbb{F}_q$ est donné par

$$N = q + 1 + S(f).$$

Dans le théorème suivant, nous rappelons quelques résultats.

THÉORÈME 1.1. — *Soit $n$ un entier pair. Soit $\delta$ un entier impair. Soient $a, \ell$ deux entiers strictement positifs. Soit $C_n$ un code BCH binaire de longueur $2^n - 1$ et de distance prescrite $\delta$. Si l'une des conditions suivantes est vérifiée*

(i) *$2a$ divise $n$, $\ell$ divise $2^a + 1$ et $\delta = \ell + 2$ ;*

(ii) *$1 \leq a \leq \frac{1}{2}n$ et $\delta = 2^a + 3$,*

*alors la borne de Carlitz-Uchiyama est atteinte pour le dual de $C_n$ c'est-à-dire il existe un mot dans le dual de $C_n$ de poids $w$ tel que*

$$\big|w - 2^{n-1}\big| = (\delta - 3)2^{n/2-1}.$$

Le premier cas de ce théorème a été montré par Wolfmann [18], puis de manière différente par van der Vlugt [16]. Le deuxième cas a été traité par van der Geer et van der Vlugt (voir [4]). Pour des démonstrations différentes de certains cas particuliers de ce théorème, on pourra voir Stepanov [13] et Bassalygo

et Zinoviev [2]. Ces auteurs ont utilisé différentes méthodes pour donner des familles de polynômes $f$ de degré $\delta - 2$ tels que la somme exponentielle $S(f)$ soit maximale.

Dans cet article, nous étudierons les codes duaux des codes BCH $C_n$ de longueur $q-1 = 2^n - 1$ et de distance prescrite $\delta = 2^a + 1$ quand $a$ est un entier supérieur ou égal à 3. Nous serons amené à étudier les sommes exponentielles $S(f)$ où $f$ est un polynôme à coefficients dans $\mathbb{F}_q$ de degré $2^a - 1$. On montrera que $S(f)$ n'atteint pas la borne de Weil et on obtiendra

$$|S(f)| \leq (2^a - 2)\sqrt{q} - a \cdot 2^{[n/a]}$$

où $[n/a]$ est la partie entière de $n/a$ (voir théorème 8.3). Par conséquent, la borne de Carlitz-Uchiyama n'est pas atteinte pour le dual de $C_n$. Pour un mot $c$ non nul du dual de $C_n$, le poids $w(c)$ de $c$ vérifie

$$\left|w(c) - 2^{n-1}\right| \leq (2^{a-1} - 1)\sqrt{q} - a \cdot 2^{[n/a]-1}.$$

## 2. Polygone de Newton

Soit $p$ un nombre premier. Soit $\mathbb{Q}_p$ le corps des nombres $p$-adiques. Notons $\Omega$ une clôture algébrique de $\mathbb{Q}_p$. On désignera par $\mathrm{ord}_p(\cdot)$ la valuation sur $\Omega$ normalisée par $\mathrm{ord}_p(p) = 1$.

Soit $P = \sum_{i=0}^{2r} B_i t^{2r-i}$ un polynôme à coefficients dans $\mathbb{Q}$ de degré $2r$. Posons

$$b_i = \mathrm{ord}_p B_{2r-i}.$$

Le polygone de Newton de $P$ est l'enveloppe convexe inférieure des points $(i, \mathrm{ord}_p b_i)$ (voir [5]).

PROPOSITION 2.1. — *Si un segment du polygone de Newton de $P$ a une pente $\lambda$ et une longueur horizontale $\ell$, alors $P$ a exactement $\ell$ racines (comptées avec multiplicités) dans $\Omega$ de valution $p$-adique $-\lambda$.*

*Démonstration.* — Voir [5]. □

On dira qu'un point $(i, b_i)$ est le *deuxième* sommet (respectivement *avant-dernier* sommet) de ce polygone si pour tout entier $j$, $0 < j < i$ (respectivement $i < j < 2r$), le point $(j, b_j)$ n'est pas un sommet. Par convexité, le point $(i, b_i)$ est le deuxième sommet si et seulement si

$$\begin{cases} (b_i - b_0)/i < (b_j - b_0)/j & \text{si } j > i, \\ (b_i - b_0)/i \leq (b_j - b_0)/j & \text{si } j < i. \end{cases}$$

De même, le point $(i, b_i)$ est l'avant-dernier sommet si et seulement si

$$\begin{cases} (b_{2r} - b_i)/(2r - i) \geq (b_{2r} - b_j)/(2r - j) & \text{si } j > i, \\ (b_{2r} - b_i)/(2r - i) > (b_{2r} - b_j)/(2r - j) & \text{si } j < i. \end{cases}$$

Considérons maintenant un cas particulier. Supposons que

$$b_i = n(r-i) + b_{2r-i}$$

où $n$ un entier strictement positif et $i = 0, \ldots, 2r$.

LEMME 2.2. — *Supposons que le polynôme $P$ vérifie ces hypothèses. Alors le point $(i, b_i)$ est le deuxième sommet du polygone de Newton de $P$ si et seulement si le point $(2r-i, b_{2r-i})$ en est l'avant-dernier sommet. En particulier, si le polygone de Newton de $P$ a au moins trois sommets, alors son deuxième sommet a une abscisse inférieure ou égale à $r$.*

*Démonstration.* — On a vu que $(i, b_i)$ est le deuxième sommet si et seulement si

$$\begin{cases} (b_i - b_0)/i < (b_j - b_0)/j & \text{si } j > i, \\ (b_i - b_0)/i \leq (b_j - b_0)/j & \text{si } j < i. \end{cases}$$

Grâce à la relation entre les $b_i$, on peut montrer que cette condition est équivalente à

$$\begin{cases} (b_{2r} - b_{2r-i})/i > (b_{2r} - b_{2r-j})/j & \text{si } j > i, \\ (b_{2r} - b_{2r-i})/i \geq (b_{2r} - b_{2r-j})/j & \text{si } j < i. \end{cases}$$

Donc le point $(2r-i, b_{2r-i})$ est l'avant-dernier sommet. □

## 3. Rappels sur les variétés abéliennes

Soient $p$ un nombre premier et $n$ un entier strictement positif. Posons $q = p^n$. Soit $k = \mathbb{F}_q$ un corps fini à $q$ éléments.

On rappelle quelques résultats sur les variétés abéliennes. Le lecteur pourra se référer à Tate [14], [15] et à Waterhouse [17].

Soit $A$ une variété abélienne sur $k$ de dimension $g$. Le polynôme caractéristique $h_A$ de l'endomorphisme de Frobenius $\pi_A$ sur $k$ est un polynôme unitaire à coefficients dans $\mathbb{Z}$ de degré $2g$ (on l'appelera aussi le polynôme caractéristique de $A$ sur $k$). Ce polynôme détermine la classe d'isogénie de $A$ sur $k$.

THÉORÈME 3.1 (Tate). — *Deux variétés abéliennes sont isogènes sur $k$ si et seulement si elles ont mêmes polynômes caractéristiques sur $k$.*

Soit $E = \mathrm{End}_k(A) \otimes \mathbb{Q}$ l'algèbre des endomorphismes de $A$. C'est une algèbre semi-simple de centre $F = \mathbb{Q}[\pi_A]$.

Il existe une unique factorisation de $A$, à isogénie sur $k$ près, en un produit de puissance de variétés abéliennes simples non isogènes sur $k$. Cette factorisation correspond à la décomposition de $E$ en facteurs simples $E_j$ et, par conséquent, à l'écriture de son centre $F$ comme produit de corps $F_j$. Les corps $F_j$ correspondent aux facteurs irréductibles $P_j$ de $h_A$ sur $\mathbb{Q}$. On en déduit à l'aide du théorème précédent le résultat suivant :

THÉORÈME 3.2. — *Soit $h_A = \prod P_j^{m_j}$ la factorisation de $h_A$ dans $\mathbb{Q}$. Pour tout $j$, il existe un entier $e_j$ divisant $m_j$ et une variété abélienne $A_j$ simple sur $k$, dont le polynôme caractéristique de l'endomorphisme de Frobenius sur $k$ est $P^{m_j/e_j}$, tels que $A$ soit isogène sur $k$ à*

$$\prod A_j^{e_j}.$$

Supposons que $A$ soit simple. Alors $F = \mathbb{Q}(\pi_A)$ est un corps. D'après Weil, $\pi_A$ est un entier algébrique tel que pour tout plongement $\phi : \mathbb{Q}(\pi_A) \to \mathbb{C}$, on ait $|\phi(\pi_a)| = q^{1/2}$.

Comme $A$ est simple, le polynôme caractéristique de $\pi_A$ est égal à

$$h_A = P^e$$

où $P$ est un polynôme irréductible sur $\mathbb{Q}$. L'algèbre des endomorphismes $E$ est alors un corps de dimension $e^2$ sur son centre $F = \mathbb{Q}(\pi_A)$.

Soit $v$ une place de $F$. On notera $\mathrm{inv}_v(E)$ l'invariant de $E$ en $v$ (voir [11]). Si $v$ est au-dessus de $p$, on désignera par $\mathrm{ord}_v(\cdot)$ la valuation sur $F$ correspondant à $v$ normalisée par $\mathrm{ord}_v(p) = 1$.

THÉORÈME 3.3 (Tate). — *Soit $A$ une variété abélienne simple sur $k$. Soit $v$ une place de $F$. Soit $F_v$ le complété de $F$ en $v$. L'invariant de $E$ en $v$ est congru, modulo $\mathbb{Z}$, à*

- *0 si $v$ est complexe ou si $v$ est au-dessus de $\ell \neq p$ ;*
- *$\frac{1}{2}$ si $v$ est réel ;*
- *$\mathrm{ord}_v(\pi_A)[F_v : \mathbb{Q}_p]/\mathrm{ord}_v(q)$ si $v$ est au-dessus de $p$.*

PROPOSITION 3.4. — *La somme de tous les invariants de $E$ est congrue à zéro modulo $\mathbb{Z}$. Le plus petit dénominateur commun de tous les invariants de $E$ est $e$.*

On ne suppose plus que $A$ est simple. Soient $\omega_1, \overline{\omega}_1, \ldots, \omega_g, \overline{\omega}_g$ les racines de $h_A$ dans $\mathbb{C}$. Le polynôme caractéristique de $\pi_A$ sur $\mathbb{F}_{q^\ell}$ est donné par

$$h_A^{(\ell)}(t) = \prod_{i=1}^{g} (t - \omega_i^\ell)(t - \overline{\omega}_i^\ell).$$

On dira ici que $A$ est *supersingulière* si $h_A^{(\ell)}(1)$ est premier avec $p$ pour tout entier $\ell$ strictement positif (*cf.* Rosen [10] et Xing [19]).

REMARQUE. — Oort a donné une autre définition de variété abélienne supersingulière : $A$ est supersingulière si $A$ est isogène sur une extension finie de $k$ à la puissance d'une courbe elliptique supersingulière (voir [6]). Pour les variétés abéliennes de dimension 1 et 2, ces deux définitions sont équivalentes. Remarquons que si $A$ est supersingulière au sens de Oort, alors $A$ est supersingulière.

Mais si $A$ est une variété abélienne de dimension supérieure à 3, la réciproque n'est plus vraie.

Nous allons maintenant donner les polynômes caractéristiques de certaines variétés abéliennes.

PROPOSITION 3.5 (Deuring-Waterhouse [17]). — *Les polynômes caractéristiques des courbes elliptiques supersingulières sur $k$ sont*

(i) $t^2 \pm 2\sqrt{q}t + q$ *si $n$ est pair ;*

(ii) $t^2 \pm \sqrt{q}t + q$ *si $n$ est pair et si 3 ne divise pas $p-1$ ;*

(iii) $t^2 \pm p^{(n+1)/2}t + q$ *si $n$ est impair et $p = 2$ ou 3 ;*

(iv) $t^2 + q$ *si $n$ est impair ou si $n$ est pair et 4 ne divise pas $p-1$.*

PROPOSITION 3.6 (Waterhouse [17]). — *Soit $A$ une variété abélienne simple sur $k$. Soit $h_A$ le polynôme caractéristique de $A$ sur $k$. Soit $\pi$ une racine de $h_A$ dans $\mathbb{C}$. Supposons que $\pi$ a un conjugué réel. Si $n$ est pair, alors $A$ est une courbe elliptique de polynôme caractéristique*

$$(t \pm \sqrt{q})^2.$$

*Si $n$ est impair, alors $A$ est une variété abélienne de dimension 2 et de polynôme caractéristique*

$$(t^2 - q)^2.$$

## 4. Variétés abéliennes supersingulières

Le lemme suivant concerne les variétés abéliennes supersingulières.

LEMME 4.1. — *Soient $y_1, \dots, y_{2g}$ des entiers algébriques de $\Omega$. Si pour tout entier $r$ strictement positif, on a*

$$\operatorname{ord}_p\Big(\prod_{i=1}^{2g}(1 - y_i^r)\Big) = 0,$$

*alors*

$$\operatorname{ord}_p(y_i) > 0$$

*pour $i = 1, \dots, 2g$.*

*Démonstration.* — Supposons que $\operatorname{ord}_p(y_1) = 0$. Comme le corps résiduel de $\mathbb{Q}_p(y_1)$ est fini, il existe un entier $r$ tel que

$$\operatorname{ord}_p(1 - y_1^r) > 0.$$

Les $y_i$ sont des entiers algébriques, donc

$$\operatorname{ord}_p\Big(\prod_{i=1}^{2g}(1 - y_i^r)\Big) = \sum_{i=1}^{2g}\operatorname{ord}_p(1 - y_i^r) > 0$$

et le lemme est démontré. □

On rappelle que $k$ est un corps fini à $q = p^n$ éléments.

PROPOSITION 4.2. — *Soit $A$ une variété abélienne sur $k$ de dimension $g$, $g \geq 2$. Soit $h_A(t)$ le polynôme caractéristique de $A$ sur $k$. Soit $\omega$ une racine de $h_A(t)$ dans $\mathbb{C}$. Soit $v$ une place de $\mathbb{Q}(\omega)$ au-dessus de $p$. Si $A$ est supersingulière, alors*

$$\mathrm{ord}_v(\omega) \geq \frac{n}{g}.$$

*Démonstration.* — Soit $A$ une variété abélienne supersingulière sur $k$ de dimension $g$ supérieure ou égale à 2. D'après le théorème 3.2, si $A$ n'est pas simple, alors $h_A$ est le produit de polynômes caractéristiques de variétés abéliennes simples et supersingulières. Si $\omega$ est la racine d'un polynôme caractéristique d'une courbe elliptique supersingulière sur $k$, alors $\mathrm{ord}_v(\omega) \geq \frac{1}{2}n$ (prop. 3.5). Par conséquent, il suffit de considérer le cas où $A$ est simple sur $k$.

Comme $A$ est simple, le polynôme caractéristique $h_A$ de $A$ est égal à

$$h_A = P^e$$

où $P$ est un polynôme de degré $d$ irréductible sur $\mathbb{Q}$ et $e$ un entier strictement positif. Notons l'égalité : $ed = 2g$.

Si $P$ a des racines réelles, alors, d'après la proposition 3.6, $n$ est impair et

$$h_A(t) = (t^2 - q).$$

La proposition est vraie dans ce cas. On peut donc supposer que $h_A(t)$ n'a pas de racines réelles. Par conséquent, l'entier $d = 2r$ est pair.

Posons $E = \mathrm{End}_k(A) \otimes \mathbb{Q}$ et $F = \mathbb{Q}(\omega)$. Soit $P = \prod_{j=1}^{J} P_j$ la factorisation de $P$ dans $\mathbb{Q}_p[t]$. Soit $v_j$ la place de $F$ au-dessus de $p$ correspondant au facteur $P_j (j = 1, \ldots, J)$. D'après le théorème 3.3, l'invariant de $E$ en cette place est congru à

$$i_{v_j} = \frac{\mathrm{ord}_{v_j}(\omega)[F_{v_j} : \mathbb{Q}_p]}{n}$$

modulo $\mathbb{Z}$. Comme $P_j$ est irréductible sur $\mathbb{Q}_p$, toutes ses racines ont même valuation $p$-adique $w_j$. Donc $i_{v_j}$ est égal à

$$i_{v_j} = \frac{w_j \deg P_j}{n}.$$

Puisque $e$ est le plus petit multiple commun des dénominateurs de tous les invariants de $E$ en les places de $F$ (proposition 3.4), il existe un entier positif $b_{v_j}$ tel que

$$i_{v_j} = b_{v_j}/e.$$

D'après le lemme précédent, comme $A$ est supersingulière, on a $w_j > 0$ et $b_{v_j} \geq 1$. On en déduit que

$$w_j \geq \frac{n}{e \deg P_j}.$$

Considérons le polygone de Newton du polynôme $P$. Si ce polygone n'a que deux sommets, alors $w_j = \frac{1}{2}n$ pour tout $j$ et la proposition est démontrée. Supposons que ce ne soit pas le cas. Soit $w_{j_0}$ le plus petit des $w_j$. La pente de la dernière arète du polygone de Newton est donnée par $-w_{j_0}$ (prop. 2.1). D'après le lemme 2.2, on a nécessairement $\deg P_{j_0} \leq r$. Donc $w_{j_0} \geq n/g$ et comme $w_{j_0}$ est minimum, la proposition est démontrée. □

## 5. Poids binaire

Si $d$ est un entier dont le développement dyadique est donné par

$$d = \sum_{i=1}^{s} 2^{d_i},$$

alors on définit le *poids binaire* $\sigma(d)$ de $d$ par

$$\sigma(d) = s.$$

Si $f$ est un polynôme à coefficients dans un corps fini, on définit le *poids binaire* $\sigma(f)$ de $f$ comme étant le maximum du poids binaire des exposants de $f$.

LEMME 5.1. — *Soient $a$ et $b$ deux entiers positifs. Alors*

(i) $\sigma(a+b) \leq \sigma(a) + \sigma(b)$,

(ii) $\sigma(ab) \leq \sigma(a)\sigma(b)$.

*Démonstration.* — La preuve de la première assertion se trouve dans [3], lemme 15.575. Supposons que le développement dyadique de $b$ soit donné par

$$b = \sum b_i 2^i$$

où $b_i$ est égal à 0 ou 1. On déduit de $(i)$ que

$$\sigma(ab) = \sigma\Big(\sum a_i b\, 2^i\Big) \leq \sigma(b) \sum a_i = \sigma(a)\sigma(b). \qquad \square$$

Nous aurons besoin d'une minoration du poids binaire des multiples de $2^m - 1$. Ce sera l'objet du lemme suivant.

LEMME 5.2. — *Soient $m$ et $c$ deux entiers strictement positifs. Le poids binaire de $c(2^m - 1)$ est supérieur ou égal à $m$.*

*Démonstration.* — On peut supposer que $c$ est impair. L'entier $c$ peut s'écrire $c = c_1 + c_2$ avec $1 \leq c_1 < 2^m$ et $2^m$ divise $c_2$. On déduit du lemme 5.1 que

$$\begin{aligned}\sigma\big(c(2^m-1)\big) &= \sigma\big((c-1)2^m - c_2\big) + \sigma(2^m - c_1)\\ &\geq \sigma(c-1) - \sigma(c_2) + m - \sigma(c_1 - 1) = m.\end{aligned}$$

□

## 6. Sommes exponentielles

À partir de maintenant, on ne considérera plus que le cas où $p = 2$. Soit $q = 2^n$. Soit $f(x) = \sum_{j=1}^{J} \alpha_j x^{d_j}$ un polynôme à coefficients dans $\mathbb{F}_q$ de degré strictement positif. On suppose que $d_j < d_{j+1}$ pour $j = 1, \ldots, J-1$ et que tous les coefficients $\alpha_j$ de $f$ sont non nuls. Pour tout entier $\ell$ strictement positif, on posera

$$S_\ell = \sum_{x \in \mathbb{F}_{q^\ell}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_2}(f(x))}.$$

Notre but est de donner une relation de congruence pour les sommes $S_{2^\lambda j}$. Nous utiliserons essentiellement un théorème de Stickelberger.

**6.1. La relation de congruence de Stickelberger.** — Soit $s$ un entier. Soit $\xi_s$ une racine primitive de $W^{2^s-1} = 1$ dans $\Omega$. Notons $K_s = \mathbb{Q}_2(\xi_s)$ l'unique extension non ramifiée de $\mathbb{Q}_2$ de degré $s$ contenue dans $\Omega$. Soit $T_s = \{0, 1, \xi_s, \ldots, \xi_s^{2^s-2}\}$ l'ensemble des représentants de Teichmüller de $\mathbb{F}_{2^s}$ dans $K_s$. Il y a un isomorphisme entre le groupe multiplicatif de $\mathbb{F}_{2^s}$ et $T_s^\star = T_s - \{0\}$. Pour tout élément $x$ de $\mathbb{F}_{2^s}$, on notera $\xi_x$ son unique représentant dans $T_s$.

On désignera par $t_s$ la trace de $K_s$ sur $\mathbb{Q}_2$. Pour tout élément $\xi$ de $T_s$, on a

$$t_s(\xi) = \xi + \xi^2 + \cdots + \xi^{2^{s-1}}.$$

Notons $\mathbb{Z}_2$ l'anneau des entiers de $\mathbb{Q}_2$. En identifiant $\mathbb{Z}_2/2\mathbb{Z}_2$ et $\mathbb{F}_2$, on a la relation

$$\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}(x) \equiv t_s(\xi_x) \pmod{2\mathbb{Z}_2}. \tag{1}$$

Soit $\ell$ un entier strictement positif. Soit $B(U) = \sum_{i=0}^{q^\ell - 1} C_\ell(i) U^i$ l'unique polynôme à coefficients dans $K_{nl}$ de degré $q^\ell - 1$ tel que

$$B(\xi) = (-1)^{t_{nl}(\xi)} \tag{2}$$

pour tout $\xi$ appartenant à $T_{nl}$. D'autre part, pour tout entier $i$, $0 \leq i < q^\ell - 1$, on définit la somme de Gauss $G_\ell(i)$ par

$$G_\ell(i) = \sum_{\xi \in T_{nl}} \xi^{-i} (-1)^{t_{nl}(\xi)}.$$

Cette somme appartient à $\mathbb{Q}_2$ car elle est stable sous l'action du groupe de Galois de $K_{n\ell}$ sur $\mathbb{Q}_2$. On peut montrer que $C_\ell(0) = 1, C_\ell(q^\ell - 1) = -q^\ell/(q^\ell - 1)$ et que

$$(q^\ell - 1)C_\ell(i) = G_\ell(i)$$

pour $i = 1, \ldots, q^\ell - 2$ (voir [1]).

THÉORÈME 6.1 (Stickelberger [1]). — *Pour $i = 1, \ldots, q^\ell - 2$, on a*

$$G_\ell(i) \equiv 2^{\sigma(i)} \pmod{2^{\sigma(i)+1}}.$$

On déduit de la congruence de Stickelberger le résultat suivant :

COROLLAIRE 6.2. — *Pour $i = 1, \ldots, q^\ell - 1$, on a*

$$\operatorname{ord}_2\big(C_\ell(i)\big) = \sigma(i).$$

**6.2. Une expression de $S_\ell$.** — Soit $a$ le poids binaire de $f$. Soit $X_\ell$ l'ensemble des $J$-uplets $(i_j)$ formés d'entiers non tous nuls vérifiant

$$\sum_{j=1}^{J} d_j i_j \equiv 0 \pmod{q^\ell - 1} \quad \text{et} \quad 0 \le i_j \le q^\ell - 1.$$

Si $y$ est un nombre réel, on notera $\lceil y \rceil$ sa partie entière supérieure. Pour un entier positif $r$, on notera $X_{\ell,r}$ le sous-ensemble de $X_\ell$ formé des $J$-uplets $(i_j)$ satisfaisant

$$\sum \sigma(i_j) = \left\lceil \frac{\ell n}{a} \right\rceil + r.$$

Pour $j = 1, \ldots, J$, on notera $\beta_j$ le représentant de Teichmüller de $\alpha_j$ dans $K_n$. Pour tout élément $\mathbf{u} = (i_j)$ de $X_\ell$, on définit les éléments $\beta^{\mathbf{u}}$ et $C_\ell(\mathbf{u})$ de $K_n$ par

$$\beta^{\mathbf{u}} = \beta_1^{i_1} \cdots \beta_J^{i_J} \quad \text{et} \quad C_\ell(\mathbf{u}) = C_\ell(i_1) \cdots C_\ell(i_J).$$

Dans [8], C. Moreno et O. Moreno ont montré, à l'aide de (1) et (2), que si $f$ est un polynôme de degré 7, alors $S_\ell$ pouvait s'exprimer en fonction des $\beta_j$ et des $C_\ell(i)$. Ce résultat se généralise immédiatement ; on obtient

$$S_\ell = q^\ell + (q^\ell - 1) \sum_{\mathbf{u} \in X_\ell} \beta^{\mathbf{u}} C_\ell(\mathbf{u}).$$

D'après les lemmes 5.1 et 5.2, si $(i_j)$ est un élément de $X_\ell$, on a

$$\sum \sigma(d_j)\sigma(i_j) \ge n\ell.$$

Comme $\sigma(d_j)$ est inférieur ou égal à $a$ pour $j = 1, \ldots, J$, on a

$$\sum \sigma(i_j) \ge \left\lceil \frac{n\ell}{a} \right\rceil.$$

Donc la somme $S_\ell$ est égale à

$$S_\ell = q^\ell + (q^\ell - 1)\sum_{r=0}^{\infty} \sum_{\mathbf{u}\in X_{\ell,r}} \beta^{\mathbf{u}} C_\ell(\mathbf{u}).$$

Comme $X_\ell$ est fini, toutes les sommes sont finies.

Si $d$ et $s$ sont des entiers, on notera $\rho_s(d)$ le reste de la division euclidienne de $d$ par $s$.

Soient $t$ et $i$ deux entiers positifs. On suppose que $i$ est strictement inférieur à $q^\ell$ et que son développement dyadique est donné par

$$i = 2^{a_1} + \cdots + 2^{a_r}.$$

On définit une action de $\mathbb{Z}$ sur l'ensemble $I$ des entiers positifs strictement inférieurs à $q^\ell$ par

$$t \triangleright i = 2^{\rho_{n\ell}(a_1+t)} + \cdots + 2^{\rho_{n\ell}(a_r+t)}.$$

Par passage au quotient, on obtient une action de $\mathbb{Z}/nl\mathbb{Z}$ sur $I$. L'orbite de 0 sous cette action est $\{0\}$. L'ensemble $I - \{0\}$ est isomorphe à $\mathbb{Z}/(q^\ell - 1)\mathbb{Z}$. L'action de $\mathbb{Z}/n\ell\mathbb{Z}$ sur $\mathbb{Z}/(q^\ell - 1)\mathbb{Z}$ correspondant à cet isomorphisme est donnée par

$$t \triangleright i = 2^t i.$$

En d'autres termes, si $i$ est strictement positif, l'entier $t \triangleright i$ est l'unique entier congru à $2^t i$ modulo $q^\ell - 1$ qui est strictement compris entre 0 et $q^\ell$.

On définit maintenant une action de $\mathbb{Z}$ sur $X_\ell$ par

$$t \triangleright (i_j) = (t \triangleright i_j)$$

où $(i_j)$ appartient à $X_\ell$. Pour tout entier $r$ positif, $X_{\ell,r}$ est invariant sous l'action de $\mathbb{Z}$. Pour un élément $\mathbf{u}$ de $X_\ell$, on notera $\mathcal{O}_{\mathbf{u}}$ son orbite et $o(\mathbf{u})$ le cardinal de celle-ci.

Soit $\mathbf{u} = (i_j)$ un élément de $X_\ell$. Remarquons que le cardinal $s$ de l'orbite de $\mathbf{u}$ divise $n\ell$. L'orbite de $\mathbf{u}$ est égale à

$$\mathcal{O}_{\mathbf{u}} = \big\{\mathbf{u}, 1 \triangleright \mathbf{u}, \ldots, (s-1) \triangleright \mathbf{u}\big\}.$$

D'autre part, si on pose $d = n\ell/s$ et $\mathbf{w} = (\rho_{2^s}(i_j))_{j=1,\ldots,J}$, le $J$-uplet $\mathbf{u}$ peut se mettre sous la forme

$$\mathbf{u} = \sum_{b=0}^{d-1} 2^{bs}\mathbf{w}.$$

Donc si $\mathbf{u}$ appartient à $X_{\ell,r}$, alors

$$\sum \sigma(i_j) \equiv 0 \pmod{\ell n/o(\mathbf{u})}. \tag{3}$$

La somme $S_\ell$ peut se réécrire

$$S_\ell = q^\ell + (q^\ell - 1)\sum_{r=0}^{\infty} \sum_{\mathbf{u}\in X_{\ell,r}} \frac{1}{o(\mathbf{u})} \sum_{t=0}^{o(\mathbf{u})-1} \beta^{t\triangleright\mathbf{u}} C_\ell(t\triangleright\mathbf{u}).$$

On a $\beta^{t\triangleright\mathbf{u}} = (\beta^{\mathbf{u}})^{2^t}$. Par conséquent, $\beta^{\mathbf{u}}$ appartient à $T_s$. D'autre part, on a $C_\ell(\mathbf{u}) = C_\ell(t\triangleright\mathbf{u})$. On en déduit que

$$\sum_{t=0}^{s-1} \beta^{t\triangleright\mathbf{u}} C_\ell(t\triangleright\mathbf{u}) = t_s(\beta^{\mathbf{u}}) C_\ell(\mathbf{u}).$$

Si on pose

$$H_{\ell,r} = \sum_{\mathbf{u}\in X_{\ell,r}} \frac{1}{o(\mathbf{u})} t_{o(\mathbf{u})}(\beta^{\mathbf{u}}) C_\ell(\mathbf{u}),$$

on obtient le résultat suivant :

PROPOSITION 6.3. — *La somme $S_\ell$ est égale à*

$$S_\ell = q^\ell + (q^\ell - 1)\sum_{r=0}^{\infty} H_{\ell,r}.$$

### 6.3. Une relation de congruence pour $S_{2^\lambda j}$

LEMME 6.4. — *Soit $\ell$ un entier strictement positif. Soit $\mathbf{u}$ un élément de $X_\ell$. Soit $s$ le cardinal de l'orbite de $\mathbf{u}$ sous l'action de $\mathbb{Z}$ sur $X_\ell$. Alors*

$$\mathrm{ord}_2 t_s(\beta^{\mathbf{u}}) \geq \mathrm{ord}_2 \ell - \mathrm{ord}_2(\ell n/s).$$

*Démonstration.* — La racine de l'unité $\beta^{\mathbf{u}}$ appartient à $T_n$. Comme $s$ est le cardinal de l'orbite de $\mathbf{u}$ sous l'action de $\mathbb{Z}$, elle appartient aussi à $T_s$. Soit $h$ le pgcd de $n$ et $s$. L'intersection $T_n \cap T_s$ est égale à $T_h$ car $2^h - 1$ est le pgcd de $2^n - 1$ et $2^s - 1$ (voir [12], th. 10). Grâce à la transitivité de la trace, on obtient

$$t_s(\beta^{\mathbf{u}}) = \frac{s}{h} t_h(\beta^{\mathbf{u}}).$$

Donc l'ordre en 2 de cette trace est supérieur ou égal à celui de $s/h$. Comme $n/h$ est un entier, on a

$$\mathrm{ord}_2 \frac{s}{h} = \mathrm{ord}_2 \frac{s}{n} + \mathrm{ord}_2 \frac{n}{s} \geq \mathrm{ord}_2 \frac{s}{n} = \mathrm{ord}_2 \ell - \mathrm{ord}_2 \frac{\ell n}{s}.$$

Le lemme est démontré. □

Supposons que $a$ divise $n$ et posons $\mu = n/a$. Ce lemme et la proposition précédente vont nous permettre d'obtenir une relation de congruence pour $S_{2^\lambda j}$. Un élément $\mathbf{u} = (i_j)$ de $X_\ell$ appartient à $X_{\ell,r}$ si et seulement si

$$\sum \sigma(i_j) = \mu\ell + r.$$

Si c'est le cas, alors $\ell n/o(\mathbf{u})$ divise $\mu\ell + r$ (voir (3)).

PROPOSITION 6.5. — *Soit $\lambda$ un entier positif (ou nul). Soit $j$ un entier strictement positif. On suppose que $n = a\mu$ où $\mu$ est un entier strictement positif. Si $a$ est supérieur ou égal à 2, alors*

$$S_{2^\lambda j} \equiv -H_{2^\lambda j,0} \pmod{2^{2^\lambda j\mu+\lambda+1}}.$$

*Démonstration.* — Soit $\ell$ un entier strictement positif. Nous allons montrer que

$$S_\ell \equiv -H_{\ell,0} \pmod{2^{\ell\mu+\mathrm{ord}_2\ell+1}}. \tag{4}$$

La proposition se déduit immédiatement de cette congruence.

Comme $a$ est supérieur ou égal à 2, $q^\ell$ est congru à zéro modulo $2^{\ell\mu+\mathrm{ord}_2\ell+1}$. La proposition 6.3 donne une expression de $S_\ell$ en fonction des $H_{\ell,r}$. On en déduit la congruence suivante :

$$S_\ell \equiv -\sum_{r=0}^{\infty} H_{\ell,r} \pmod{2^{\ell\mu+\mathrm{ord}_2\ell+1}}.$$

On rappelle que la somme $H_{\ell,r}$ est égale à

$$\sum_{\mathbf{u}} t_{o(\mathbf{u})}(\beta^{\mathbf{u}})C_\ell(\mathbf{u})$$

où $\mathbf{u}$ parcourt un système de représentants des orbites de $X_{\ell,r}$.

Soit $r$ un entier strictement positif. Soit $\mathbf{u}$ un élément de $X_{\ell,r}$. Pour montrer la congruence (4), il suffit de prouver que

$$\mathrm{ord}_2 t_{o(\mathbf{u})}(\beta^{\mathbf{u}})C_\ell(\mathbf{u}) \geq \ell\mu + \mathrm{ord}_2\ell + 1.$$

D'après le théorème de Stickelberger, l'ordre en 2 de $t_{o(\mathbf{u})}(\beta^{\mathbf{u}})C_\ell(\mathbf{u})$ est supérieur ou égal à $\ell\mu + r$. Par conséquent, on peut supposer que $r$ est inférieur ou égal à l'ordre en 2 de $\ell$.

Posons $d = \ell\mu/o(\mathbf{u})$.Le lemme précédent donne la minoration suivante :

$$\mathrm{ord}_2 t_{o(\mathbf{u})}(\beta^{\mathbf{u}})C_\ell(\mathbf{u}) \geq \ell\mu + \mathrm{ord}_2\ell + r - \mathrm{ord}_2 d.$$

Nous allons montrer que $r$ est strictement supérieur à $\mathrm{ord}_2 d$.

Par hypothèse, $\mathbf{u}$ appartient à $X_{\ell,r}$, donc, d'après (3), $d$ divise $\ell\mu + r$. Par conséquent, l'ordre en 2 de $d$ est inférieur ou égal à celui de $\ell\mu + r$. Puisque $r$ est inférieur ou égal à l'ordre de $\ell$ en 2, on a

$$\mathrm{ord}_2 d \leq \mathrm{ord}_2(\ell\mu + r) = \mathrm{ord}_2 r.$$

On en déduit que $r$ est bien strictement supérieur à $\mathrm{ord}_2 d$. La relation de congruence (4) est donc vraie et la proposition est démontrée. □

## 7. Divisibilité de $S(f)$

La proposition 6.3 donne une expression de $S(f)$ en fonction de $H_{1,0}$, élément de $\mathbb{Q}_2$ dont on sait minorer l'ordre en 2 (voir corollaire 6.2). On retrouve ainsi un résultat de Litsyn, C. Moreno et O. Moreno (voir [7] et [8]).

THÉORÈME 7.1 (Litsyn, Moreno, Moreno). — *Soit $q = 2^n$. Soit $f$ un polynôme à coefficients dans $\mathbb{F}_q$. Alors*

$$\operatorname{ord}_2 S(f) \geq \frac{n}{\sigma(f)}.$$

Soit $f(x)$ un polynôme de degré $2^a - 1$ à coefficients dans $\mathbb{F}_q$ où $a$ est un entier, $a \geq 2$. On peut noter que le poids binaire de $f$ est $a$. Soit $\alpha$ le coefficient du terme de degré $2^a - 1$ de $f$ et soit $\gamma$ le représentant de Teichmüller dans $K_n$ de $\alpha$.

Dans la partie 7, on supposera que $n = a\mu$ où $\mu$ est un entier strictement positif.

Si $f$ est un polynôme de degré 7 ($a = 3$), alors l'ordre de $S(f)$ en 2 est supérieur à $\mu$. C. Moreno et O. Moreno ont prouvé qu'il est égal à $\mu$ si et seulement si la trace $\operatorname{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha^{(q-1)/7})$ est égale à 1. Nous allons généraliser ce résultat.

PROPOSITION 7.2. — *La somme $H_{1,0}$ est égale à*

$$H_{1,0} = t_a\big(\gamma^{(q-1)/(2^a-1)}\big) C_1\big((q-1)/(2^a-1)\big).$$

*Démonstration.* — Le polynôme $f$ peut s'écrire

$$f(x) = \sum_{j=1}^{J} \alpha_j x^{d_j}$$

avec $\alpha_J = \alpha$, $d_J = 2^a - 1$, $\alpha_j \neq 0$, $d_j < d_{j+1}$ pour $j = 1, \ldots, J-1$. Par définition, pour calculer $H_{1,0}$, il suffit d'expliciter l'ensemble $X_{1,0}$, c'est-à-dire de résoudre le système suivant :

$$\begin{cases} \sum_{j=1}^{J} d_j i_j \equiv 0 \pmod{q-1}, \ \sum_{j=1}^{J} \sigma(i_j) = \mu, \\ 0 \leq i_j \leq q-1, \qquad\qquad (i_j)_{j=1,\ldots,J} \neq (0,\ldots,0). \end{cases}$$

Soit $(i_j)$ une solution de ce système. Il existe un entier $c$ strictement positif tel que

$$\sum d_j i_j = c(q-1).$$

D'après les lemmes 5.1 et 5.2, on a

$$a\mu \leq \sigma\left(\sum d_j i_j\right) \leq \sum \sigma(d_j)\sigma(i_j).$$

Il s'ensuit que

$$\sum \big[a - \sigma(d_j)\big]\sigma(i_j) + a\mu \leq a \sum \sigma(i_j).$$

Puisque $\sigma(d_j) < a$ pour $j = 1, \dots, J-1$ et $\sigma(d_J) = a$, le $J$-uplet $(i_j)$ appartient à $X_{1,0}$ si et seulement si $i_j$ est nul pour $j = 1, \dots, J-1$ et $i_J$ est une solution du système suivant :

$$(\star) \quad \begin{cases} (2^a - 1)i \equiv 0 \pmod{q-1}, \\ 0 < i \leq q-1, \\ \sigma(i) = \mu. \end{cases}$$

Les entiers $i$ vérifiant les deux premières conditions de ce système sont

$$i = c(q-1)/(2^a - 1) = c(1 + 2^a + \cdots + 2^{a(\mu-1)})$$

pour $c = 1, \dots, 2^a - 1$. Comme $c < 2^a$, le poids binaire de $i$ vaut $\sigma(c)\mu$. Par conséquent, $i = c(q-1)/(2^a-1)$ est une solution du système $(\star)$ si et seulement si $c = 2^\kappa$ pour un entier $\kappa$, $0 \leq \kappa \leq a-1$. En conclusion, $(i_j)$ appartient $X_{1,0}$ si et seulement si $i_j$ est nul pour $j = 1, \dots, J-1$ et $i_J = 2^\kappa(q-1)/(2^a-1)$ avec $0 \leq \kappa \leq a-1$. Donc la somme $H_{1,0}$ est égale à

$$H_{1,0} = t_a\big(\gamma^{(q-1)/(2^a-1)}\big) C_1\big((q-1)/(2^a-1)\big). \qquad \square$$

Corollaire 7.3. — *Pour tout entier $\ell$ strictement positif, on a*

$$H_{\ell,0} = t_a\big(\gamma^{\ell(q-1)/(2^a-1)}\big) C_\ell\big((q^\ell-1)/(2^a-1)\big).$$

*Démonstration.* — D'après la proposition précédente, on a

$$H_{\ell,0} = t_a\big(\gamma^{(q^\ell-1)/(2^a-1)}\big) C_\ell\big((q^\ell-1)/(2^a-1)\big).$$

Comme $\gamma \in T_n$, on a

$$\gamma^{(q^\ell-1)/(2^a-1)} = \gamma^{(q^{\ell-1}+\cdots+1)(q-1)/(2^a-1)} = \gamma^{\ell(q-1)/(2^a-1)}.$$

Le corollaire est démontré. $\square$

Théorème 7.4. — *Soit $a$ un entier, $a \geq 2$. Soit $\mu$ un entier strictement positif. Posons $n = a\mu$ et $q = 2^n$. Soit $f$ un polynôme sur $\mathbb{F}_q$ de degré $2^a - 1$ dont le coefficient du terme dominant est $\alpha$. L'ordre de $S(f)$ en 2 est supérieur à $\mu$. L'égalité a lieu si et seulement si*

$$\mathrm{Tr}_{\mathbb{F}_{2^a}/\mathbb{F}_2}\big(\alpha^{(q-1)/(2^a-1)}\big) = 1.$$

*Démonstration.* — La somme exponentielle $S(f)$ est congrue à $-H_{1,0}$ modulo $2^{\mu+1}$ (prop. 6.5). On vient de montrer que $H_{1,0}$ dépend d'une somme de Gauss et le théorème de Stickelberger donne le début du développement dyadique de cette somme. On en déduit que

$$S(f) \equiv t_a\big(\gamma^{(q-1)/(2^a-1)}\big) 2^\mu \pmod{2^{\mu+1}}.$$

D'après la relation (1), l'ordre en 2 de $S(f)$ est $\mu$ si et seulement si

$$\mathrm{Tr}_{\mathbb{F}_{2^a}/\mathbb{F}_2}\big(\alpha^{(q-1)/(2^a-1)}\big) = 1. \qquad \square$$

COROLLAIRE 7.5. — *Pour tout entier $\ell$ strictement positif, on a*

$$\mathrm{ord}_2 S_\ell = \ell\mu \Longleftrightarrow \mathrm{Tr}_{\mathbb{F}_{2^a}/\mathbb{F}_2}\big(\alpha^{\ell(q-1)/(2^a-1)}\big) = 1.$$

## 8. Borne de Weil

On a posé $q = 2^n$. On rappelle que $f(x)$ est un polynôme de degré $2^a - 1$ sur $\mathbb{F}_q$ dont le coefficient du terme dominant est $\alpha$. On supposera que $a$ est supérieur ou égal 3. Nous allons montrer que $S(f)$ n'atteint pas la borne de Weil.

Soit $J$ la jacobienne de la courbe $y^2 + y = f(x)$ sur $\mathbb{F}_q$. C'est une variété abélienne de dimension $g = 2^{a-1} - 1$. Soit $h_J(t) = \sum_{i=0}^{2g} A_i t^{2g-i}$ le polynôme caractéristique de $J$. Soient $\omega_1, \overline{\omega}_1, \ldots, \omega_g, \overline{\omega}_g$ les racines de $h_J$ dans $\mathbb{C}$. Weil a montré que

$$S_\ell = -\sum_{i=1}^{g} (\omega_i^\ell + \overline{\omega}_i^\ell)$$

pour tout entier $\ell$ strictement positif.

Soit $\mu$ la partie entière de $n/a$. On supposera que $\mu$ est strictement positif.

LEMME 8.1. — *Pour $i = 1, \ldots, 2g$, $2^{\mu i}$ divise $A_i$.*

*Démonstration.* — Dans [1], Ax donne une minoration de la valuation $p$-adique des zéros et des pôles de la fonction zêta d'une hypersurface (*cf.* th., p. 256). Si on applique le même raisonnement à la fonction

$$\exp\Big(\sum_{\ell=1}^{\infty} S_\ell t^\ell/\ell\Big) = \prod_{i=1}^{g} (1 - \omega_i t)(1 - \overline{\omega}_i t),$$

on obtient le résultat cherché. □

PROPOSITION 8.2. — *La jacobienne de la courbe d'équation $y^2 + y = f(x)$ sur $\mathbb{F}_q$ est supersingulière.*

*Démonstration.* — Soit $\ell$ un entier strictement positif. Supposons que le polynôme caractéristique de la jacobienne de cette courbe sur $\mathbb{F}_{q^\ell}$ s'écrive sous la forme

$$h_J^{(\ell)}(t) = \sum_{i=0}^{2g} A_i^{(\ell)} t^{2g-i}.$$

D'après le lemme précédent, $2^{\ell\mu i}$ divise $A_i^{(\ell)}$ pour $i = 1, \ldots, 2g$. Comme $h_J^{(\ell)}$ est unitaire et $\mu$ est strictement positif, $h_\ell(1)$ est impair. Donc cette jacobienne est supersingulière. □

THÉORÈME 8.3. — *Soit $n$ un entier strictement positif. Posons $q = 2^n$. Soit $a$ un entier, $a \geq 3$. Soit $\mu$ la partie entière de $n/a$. On suppose que $\mu$ est strictement positif. Soit $f$ un polynôme à coefficients dans $\mathbb{F}_q$ de degré $2^a - 1$. Si $n$ est pair, alors $S(f)$ n'atteint pas la borne de Weil :*

$$\big|S(f)\big| \leq (2^a - 2)\sqrt{q} - a \cdot 2^\mu.$$

*Démonstration.* — Soit $g_+$ (resp. $g_-$) le nombre de $\omega_i$ égaux à $+\sqrt{q}$ (resp. $-\sqrt{q}$). Posons

$$g_1 = g - g_+ - g_-.$$

Quitte à renuméroter les $\omega_i$, on peut supposer que $\omega_1, \ldots, \omega_{g_1}$ sont différents de $\pm\sqrt{q}$. Le polynôme caractéristique $h_J(t)$ de la jacobienne de la courbe $y^2 + y = f(x)$ sur $\mathbb{F}_q$ est égal à

$$h_J(t) = (t - \sqrt{q})^{2g_+}(t + \sqrt{q})^{2g_-} \prod_{i=1}^{g_1}(t - \omega_i)(t - \overline{\omega}_i).$$

D'après le théorème 3.2, il existe deux variétés abéliennes $A$ et $B$ sur $\mathbb{F}_q$ telles que $J$ soit isogène à $AB$. Comme $J$ est supersingulière (prop. 8.2), $A$ et $B$ le sont aussi. De plus, les polynômes caractéristiques de $A$ et $B$ sur $\mathbb{F}_q$ sont $\prod_{i=1}^{g_1}(t - \omega_i)(t - \overline{\omega}_i)$ et $(t - \sqrt{q})^{2g_+}(t + \sqrt{q})^{2g_-}$ respectivement.

Soit $K$ un corps de décomposition de $h_J$ sur $\mathbb{Q}$. Soit $v$ une place de $K$ au-dessus de $p$. Comme $A$ est supersingulière, d'après la proposition 4.2, on a

$$\mathrm{ord}_v(\omega_i) \geq \begin{cases} n/g_1 & \text{si } g_1 > 1, \\ n/2 & \text{si } g_1 = 0, 1 \end{cases}$$

pour $i = 1, \ldots, g$. Le même résultat est valable pour $\mathrm{ord}_v(\overline{\omega}_i)$. Il en résulte que

$$\mathrm{ord}_2 S_\ell = \mathrm{ord}_v S_\ell \geq \begin{cases} \ell n/g_1 & \text{si } g_1 > 1, \\ \ell n/2 & \text{si } g_1 = 0, 1 \end{cases} \tag{5}$$

pour tout entier $\ell$ strictement positif.

Nous allons montrer que $g_1$ est supérieur ou égal à $a$.

Considérons tout d'abord le cas où $n$ est un multiple de $a$. Nous allons calculer l'ordre en 2 de la somme exponentielle $S_{2^\lambda(2^a-1)}$ pour un entier $\lambda$ assez grand. Dans la proposition 6.5, on a obtenu la congruence suivante :

$$S_{2^\lambda(2^a-1)} \equiv -H_{2^\lambda(2^a-1),0} \pmod{2^{2^\lambda(2^a-1)\mu+\lambda+1}}.$$

On a déterminé une expression de $H_{2^\lambda(2^a-1),0}$ (cor. 7.3) et, comme $\gamma$ est une racine $(q-1)$-ième de l'unité, on en déduit que

$$H_{2^\lambda(2^a-1),0} = aC_{2^\lambda(2^a-1)}\big((q^{2^\lambda(2^a-1)} - 1)/(2^a - 1)\big).$$

Grâce au théorème de Stickelberger, on peut calculer l'ordre de $H_{2^\lambda(2^a-1),0}$ en 2 :

$$\mathrm{ord}_2 H_{2^\lambda(2^a-1),0} = \mathrm{ord}_2 a + 2^\lambda(2^a - 1)\mu.$$

Donc, d'après la congruence précédente entre $S_{2^\lambda(2^a-1),0}$ et $H_{2^\lambda(2^a-1),0}$, on a

$$\mathrm{ord}_2 S_{2^\lambda(2^a-1)} = \mathrm{ord}_2 a + 2^\lambda(2^a-1)\mu$$

si $\lambda \geq \mathrm{ord}_2 a$. En comparant ce résultat avec la minoration (5) on remarque que, puisque $a$ est supérieur à 3, $g_1$ doit être strictement supérieur à 1. Par conséquent, pour $\lambda$ assez grand, on a

$$\frac{a}{g_1} \leq 1 + \frac{\mathrm{ord}_2 a}{2^\lambda(2^a-1)\mu}\cdot$$

En faisant tendre $\lambda$ vers l'infini, on voit que $g_1$ est supérieur ou égal à $a$.

Si $n$ n'est pas un multiple de $a$, il suffit de considérer les extensions de $\mathbb{F}_q$ dont le degré est divisible par $a$. On déduit du cas précédent que l'ordre en 2 de $S_{2^\lambda(2^a-1)a}$ vaut $\mathrm{ord}_2 a + 2^\lambda(2^a-1)n$ pour $\lambda$ assez grand. On montre à l'aide de (5) que $g_1$ est supérieur ou égal à $a$.

Rappelons que $\omega_1, \ldots, \omega_{g_1}$ sont différents de $\pm\sqrt{q}$. Posons

$$M = \frac{2\sqrt{q}}{2^\mu} - 1 \quad \text{et} \quad x_i = M + 1 + \frac{\omega_i + \overline{\omega}_i}{2^\mu} \quad \text{pour } i = 1, \ldots, g_1.$$

Les nombres $x_i$ sont des entiers algébriques totalement positifs (lemme 8.1). Comme la famille $x_1, \ldots, x_{g_1}$ est stable par conjugaison sur $\mathbb{Q}$, $\prod x_i$ est un entier strictement positif. D'après l'inégalité de la moyenne, on a

$$\frac{\sum x_i}{g_1} \geq \Big(\prod x_i\Big)^{1/g_1} \geq 1.$$

Il en résulte que

$$-\sum_{i=1}^{g_1}(\omega_i + \overline{\omega}_i) \leq g_1 \cdot 2^\mu M = 2g_1\sqrt{q} - g_1 \cdot 2^\mu$$

et, comme $S(f) = -\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i)$ et $g_1 \geq a$, on a

$$S(f) \leq (2^a - 2)\sqrt{q} - a \cdot 2^\mu.$$

Il reste à montrer que $S(f) \geq -(2^a-2)\sqrt{q} + a \cdot 2^\mu$. Remarquons que si $\delta$ est un élément de $\mathbb{F}_q$ dont la trace sur $\mathbb{F}_2$ vaut 1, alors $S(f+\delta) = -S(f)$. Le théorème est démontré. □

Le résultat suivant se déduit immédiatement des théorèmes 7.1 et 8.3.

COROLLAIRE 8.4. — *Supposons que $a$ soit impair et ne divise pas $n$. Si $n$ est pair, alors*

$$\big|S(f)\big| \leq (2^a - 2)\sqrt{q} - (a+1) \cdot 2^\mu.$$

## 9. Tables

Les tables suivantes donnent la borne de Weil et les résultats obtenus dans la partie précédente (théorème 8.3 et corollaire 8.4) pour des polynômes de degré 7, 15 et 31. Une étoile indique que la borne est atteinte.

| $n$ | $6\sqrt{q}$ | $\begin{cases} 6\sqrt{q} - 3 \cdot 2^{n/3} & \text{si 3 divise } n \\ 6\sqrt{q} - 4 \cdot 2^{[n/3]} & \text{sinon} \end{cases}$ |
|---|---|---|
| 6 | 48 | 36* |
| 8 | 96 | 80 |
| 10 | 192 | 160 |
| 12 | 384 | 336 |
| 14 | 768 | 704 |
| 16 | 1536 | 1408 |
| 18 | 3072 | 2880 |
| 20 | 6144 | 5888 |
| 22 | 12288 | 11776 |
| 24 | 24576 | 23808* |
| 26 | 49152 | 48128 |
| 28 | 98304 | 96256 |
| 30 | 196608 | 193536 |

Table 1 : Degré 7

| $n$ | $14\sqrt{q}$ | $14\sqrt{q} - 4 \cdot 2^{[n/4]}$ |
|---|---|---|
| 8 | 224 | 208 |
| 10 | 448 | 432 |
| 12 | 896 | 864 |
| 14 | 1792 | 1760 |
| 16 | 3584 | 3520 |
| 18 | 7168 | 7104 |
| 20 | 14336 | 14208 |
| 22 | 28672 | 28544 |
| 24 | 57344 | 57088 |
| 26 | 114688 | 114432 |
| 28 | 229376 | 228864 |
| 30 | 458752 | 458240 |

Table 2 : Degré 15

| $n$ | $30\sqrt{q}$ | $\begin{cases} 30\sqrt{q} - 5 \cdot 2^{n/5} & \text{si 5 divise } n \\ 30\sqrt{q} - 6 \cdot 2^{[n/5]} & \text{sinon} \end{cases}$ |
|---|---|---|
| 10 | 960 | 940 |
| 12 | 1920 | 1896 |
| 14 | 3840 | 3816 |
| 16 | 7680 | 7632 |
| 18 | 15360 | 15312 |
| 20 | 30720 | 30640 |
| 22 | 61440 | 61344 |
| 24 | 122880 | 122784 |
| 26 | 245760 | 245568 |
| 28 | 491520 | 491328 |
| 30 | 983040 | 982720 |

Table 3 : Degré 31

## BIBLIOGRAPHIE


[1] Ax (J.) – *Zeroes of polynomials over finite fields*, Amer. J. Math., t. **86** (1964), pp. 255–261.

[2] Bassalygo (L. A.) & Zinoviev (V. A.) – *Polynomials of a special form over a finite field with a maximum modulus of a trigonometric sum*, Uspekhi Mat. Nauk, t. **52** (1997), no. 2 (314), pp. 31–44.

[3] Berlekamp (E. R.) – *Algebraic coding theory*, McGraw-Hill Book Co., New York, 1968.

[4] van der Geer (G.) & van der Vlugt (M.) – *Reed-Muller codes and supersingular curves. I*, Compositio Math., t. **84** (1992), no. 3, pp. 333–367.

[5] Koblitz (N.) – *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Springer-Verlag, New York, 1984.

[6] Li (K.-Z.) & Oort (F.) – *Moduli of supersingular abelian varieties*, Springer-Verlag, Berlin, 1998.

[7] Litsyn (S.), Moreno (C. J.) & Moreno (O.) – *Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables*, Appl. Algebra Engrg. Comm. Comput., t. **5** (1994), no. 2, pp. 105–116.

[8] Moreno (O.) & Moreno (C. J.) – *The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes*, IEEE Trans. Inform. Theory, t. **40** (1994), no. 6, pp. 1894–1907.

[9] Rodier (F.) – *Minoration de certaines sommes exponentielles binaires*, in *Coding theory and algebraic geometry (Luminy, 1991)*, Springer, Berlin, 1992, pp. 199–209.

[10] Rosen (M.) – *The asymptotic behavior of the class group of a function field over a finite field*, Arch. Math. (Basel), t. **24** (1973), pp. 287–296.

[11] Serre (J.-P.) – *Local class field theory*, in *Algebraic Number Theory, Proc. Instructional Conf., Brighton, 1965*, Thompson, Washington, D.C., 1967, pp. 128–161.

[12] Shanks (D.) – *Solved and unsolved problems in number theory*, third ed., Chelsea Publishing Co., New York, 1985.

[13] Stepanov (S. A.) – *Lower bounds on character sums over finite fields*, Discrete. Math. Appl, t. **2** (1992), no. 5, pp. 523–532.

[14] Tate (J.) – *Endomorphisms of abelian varieties over finite fields*, Invent. Math., t. **2** (1966), pp. 134–144.

[15] ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T.Honda)*, in *Séminaire Bourbaki*, Lecture Notes in Math., Springer-Verlag, 1968/1969, exposé n° 352.

[16] van der Vlugt (M.) – *Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes*, J. Number Theory, t. **55** (1995), no. 2, pp. 145–159.

[17] Waterhouse (W. C.) – *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup., t. **2** (1969), no. 4, pp. 521–560.

[18] Wolfmann (J.) – *The number of points on certain algebraic curves over finite fields*, Comm. Algebra, t. **17** (1989), no. 8, pp. 2055–2060.

[19] Xing (C.) – *The characteristic polynomials of abelian varieties of dimensions three and four over finite fields*, Sci. China Ser. A, t. **37** (1994), no. 2, pp. 147–150.