ACTA ARITHMETICA
105.2 (2002)

Poids des duaux des codes BCH de distance prescrite p^{a_0} et sommes exponentielles

par

Eric Férard (Marseille)

1. Introduction. Soient p un nombre premier et n un entier strictement positif. Soit C_n un code BCH sur $\mathbb{F}_p$ de longueur $q-1=p^n-1$ et de distance prescrite δ. On peut supposer que $\delta-1$ n'est pas divisible par p.

Considérons l'application de l'espace vectoriel des polynômes à coefficients dans $\mathbb{F}_q$ sans terme constant de degré au plus $\delta-1$ dans $\mathbb{F}_q^{q-1}$ définie par

$$f \mapsto c_f = (\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(x)))_{x\in\mathbb{F}_q^*}.$$

L'image de cette application est le code dual de C_n (voir Wolfmann [11]). Comme les traces de $\mathbb{F}_q$ sur $\mathbb{F}_p$ de x et x^p sont égales, on peut supposer que f est nul ou bien de degré premier à p.

Soit f un polynôme à coefficients dans $\mathbb{F}_q$ sans terme constant de degré premier à p et strictement inférieur à δ. Soit N_f le nombre de points sur $\mathbb{F}_q$ du modèle projectif de la courbe d'équation affine $y^p-y=f(x)$. Le poids w_f de c_f et N_f sont liés par la relation suivante (voir Wolfmann [11]) :

$$w_f = q - \frac{N_f-1}{p}. \tag{1}$$

Le nombre de points N_f satisfait la borne de Weil :

$$|N_f - q - 1| \le (p-1)(\deg f - 1)\sqrt{q}.$$

Par conséquent, le poids w d'un mot quelconque non nul du dual de C_n vérifie

$$\left| w - q\left(1-\frac{1}{p}\right)\right| \le \frac{(p-1)(\delta-2)\sqrt{q}}{p}.$$

Pour $p=2$, on retrouve la borne de Carlitz–Uchiyama (voir [7]).

Soit ζ une racine primitive p-ième de l'unité. On définit la somme exponentielle $S(f)$ par

2000 *Mathematics Subject Classification*: 11G20, 11T23, 14G50, 11G10.

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

Weil a montré que

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

Dans cet article, on s'intéressera à ces trois bornes quand n est un entier pair. Le théorème suivant donne des familles de codes BCH dont le dual atteint la borne de Carlitz–Uchiyama. Ces résultats sont dus à Wolfmann [12], van der Geer et van der Vlugt [4, 5].

THÉORÈME 1. *Soit n un entier pair, $n \geq 4$. Soient a_0, l deux entiers strictement positifs. Soit C_n un code BCH sur $\mathbb{F}_p$ de longueur $q-1 = p^n - 1$ et de distance prescrite δ. Si l'une des conditions suivantes est vérifiée* :

(i) *l divise $p^{a_0} + 1$ et $p^n - 1$, $2a_0$ divise n et $\delta = l + 1$,*
(ii) *$1 \leq a_0 < n/2$ et $\delta = p^{a_0} + 2$,*

alors il existe un mot dans le dual de C_n de poids w tel que

$$\left| w - q\left(1 - \frac{1}{p}\right)\right| = \frac{(p-1)(\delta-2)\sqrt{q}}{p}.$$

Soit a_0 un entier strictement positif. Nous nous intéresserons aux codes duaux des codes BCH C_n de longueur $q-1 = p^n - 1$ et de distance prescrite $\delta = p^{a_0}$. Dans [3], nous avons étudié la distance minimale de ces codes quand $p = 2$. Les résultats obtenus dans cet article peuvent se généraliser au cas où p est impair.

Dans un premier temps, nous étudierons les sommes exponentielles $S(f)$ lorsque f est un polynôme à coefficients dans $\mathbb{F}_q$ de degré $p^{a_0} - 1$. Nous calculerons ensuite, grâce au théorème de Stickelberger, le début du développement p-adique du nombre de points de la courbe $y^p - y = f(x)$ sur certaines extensions de $\mathbb{F}_q$. Ces résultats et l'étude de la quasi-supersingularité de la Jacobienne (voir la partie 2) de cette courbe nous permettront de montrer que N_f n'atteint pas la borne de Weil. Sous certaines hypothèses, on obtiendra

$$|N_f - q - 1| \leq (p-1)(p^{a_0} - 2)\sqrt{q} - ap^{\mu}$$

où μ est la partie entière de n/a et $a = a_0(p-1)$ (théorème 4). Par conséquent, le poids w d'un mot quelconque non nul du dual d'un code BCH de longueur $q-1$ et de distance prescrite $\delta = p^{a_0}$ vérifie

$$\left| w - q\left(1 - \frac{1}{p}\right)\right| \leq \frac{(p-1)(p^{a_0} - 2)\sqrt{q} - ap^{\mu}}{p}.$$

Nous montrerons aussi que si f est un polynôme de degré $p^{a_0} - 1$, alors $S(f)$ n'atteint pas la borne de Weil (théorème 5).

2. Variétés abéliennes quasi-supersingulières. Soit A une variété abélienne sur $\mathbb{F}_q$ de dimension g. Le polynôme caractéristique h_A de l'endomorphisme de Frobenius sur $\mathbb{F}_q$ est un polynôme unitaire à coefficients dans $\mathbb{Z}$ de degré $2g$ (on l'appellera aussi le polynôme caractéristique de A sur $\mathbb{F}_q$) (voir Waterhouse [10]).

Soient $\omega_1, \overline{\omega}_1, \ldots, \omega_g, \overline{\omega}_g$ les racines de h_A dans $\mathbb{C}$. Le polynôme caractéristique de A sur $\mathbb{F}_{q^l}$ est donné par

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

On dira que A est *quasi-supersingulière* si $h_A^{(l)}(1)$ est premier avec p pour tout entier l strictement positif (cf. Rosen [9] et Xing [13]).

Remarque 1. On dit qu'une variété abélienne A est *supersingulière* si A est isogène sur une extension finie de $\mathbb{F}_q$ à la puissance d'une courbe elliptique supersingulière (voir Oort [6]). Remarquons que si A est supersingulière, alors A est quasi-supersingulière. Pour les variétés abéliennes de dimension 1 et 2, ces deux notions coïncident. Mais si A est une variété abélienne de dimension supérieure à 3, la réciproque n'est plus vraie.

Proposition 1. *Soit A une variété abélienne sur $\mathbb{F}_q$ de dimension g, $g \geq 2$. Soit $h_A(t)$ le polynôme caractéristique de A sur $\mathbb{F}_q$. Soit ω une racine de $h_A(t)$ dans $\mathbb{C}$. Soit v une place de $\mathbb{Q}(\omega)$ au-dessus de p. Si A est quasi-supersingulière, alors*

$$v(\omega)/v(q) \geq g^{-1}.$$

Preuve. Ce résultat a été démontré dans [3].

Remarque 2. Il est bien connu que si A est une courbe elliptique supersingulière (donc quasi-supersingulière) sur $\mathbb{F}_q$, on a

$$v(\omega)/v(q) = 1/2$$

(voir Waterhouse [10]).

3. Sommes exponentielles. Soit ζ une racine primitive p-ième de l'unité. L'extension $\mathbb{Q}(\zeta)$ de $\mathbb{Q}$ est une extension de Galois de degré $p-1$ (voir [2]). Il existe un unique idéal premier $\mathfrak{p}$ dans $\mathbb{Q}(\zeta)$ divisant p. De plus, $\mathfrak{p}$ est totalement ramifié au-dessus de p (l'indice de ramification $e(\mathfrak{p}|p)$ est égal à $p-1$).

La complétion de $\mathbb{Q}(\zeta)$ par rapport à la valuation $v_\mathfrak{p}$ est $\mathbb{Q}_p(\zeta)$. Il existe une unique valuation discrète sur $\mathbb{Q}_p(\zeta)$ prolongeant $v_\mathfrak{p}$. On notera également cette valuation par $v_\mathfrak{p}$. Puisque $\mathfrak{p}$ est totalement ramifié au-dessus de p, l'extension $\mathbb{Q}_p(\zeta)$ de $\mathbb{Q}_p$ est totalement ramifiée. Son corps résiduel est isomorphe à $\mathbb{F}_p$. De plus, $\pi = 1 - \zeta$ est une uniformisante de l'extension $\mathbb{Q}_p(\zeta)$.

3.1. *La relation de congruence de Stickelberger.* Soit Ω une clôture algébrique de $\mathbb{Q}_p$. Soient s un entier et ξ_s une racine primitive de $W^{p^s-1}=1$ dans Ω. Notons $K_s=\mathbb{Q}_p(\xi_s)$ l'unique extension non ramifiée de $\mathbb{Q}_p$ de degré s contenue dans Ω. Soit $T_s=\{0,1,\xi_s,\ldots,\xi_s^{p^s-2}\}$ l'ensemble des représentants de Teichmüller de $\mathbb{F}_{p^s}$ dans K_s. Il y a un isomorphisme entre le groupe multiplicatif de $\mathbb{F}_{p^s}$ et $T_s^*=T_s-\{0\}$.

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

$$t_s(\xi)=\xi+\xi^p+\ldots+\xi^{p^{s-1}}.$$

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

$$B(\xi)=\zeta^{t_{nl}(\xi)}$$

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

$$G_l(i)=\sum_{\xi\in T_{nl}}\xi^{-i}\zeta^{t_{nl}(\xi)}.$$

On peut montrer que $C_l(0)=1, C_l(q^l-1)=-q^l/(q^l-1)$ et que

$$(q^l-1)C_l(i)=G_l(i)$$

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

Si d est un entier dont le développement p-adique est donné par

$$d=\sum d_ip^i,$$

alors on définit le *poids p-adique* $\sigma_p(d)$ de d par

$$\sigma_p(d)=\sum d_i.$$

Théorème 2 (Stickelberger, voir [1]). *Soit i un entier, $i=1,\ldots,q^l-2$. Supposons que le développement p-adique de i soit donné par*

$$i=\sum_j a_jp^j.$$

Alors

$$G_l(i)\equiv-\varphi(i)^{-1}\pi^{\sigma_p(i)}\ (\mathrm{mod}\,\pi^{\sigma_p(i)+1})$$

où $\varphi(i)=\prod(a_j!)$.

On déduit de la congruence de Stickelberger le résultat suivant :

Corollaire 1. *Pour $i=1,\ldots,q^l-1$, on a*

$$v_{\mathfrak{p}}(C_l(i))=\sigma_p(i).$$

3.2. *Une expression de $S(f)$.* Soit $q = p^n$. Soit $f(x) = \sum_{j=1}^{J} \alpha_j x^{d_j}$ un polynôme à coefficients dans $\mathbb{F}_q$ de degré strictement positif et premier à p. On suppose que tous les coefficients α_j de f sont non nuls. Soit a le poids p-adique de f, i.e. le plus grand entier parmi les $\sigma_p(d_j)$. Pour tout entier l strictement positif, on posera

$$S_l = \sum_{x \in \mathbb{F}_{q^l}} \zeta^{\mathrm{Tr}_{\mathbb{F}_{q^l}/\mathbb{F}_p}(f(x))}.$$

Soit X_l l'ensemble des J-uplets (i_j) formés d'entiers non tous nuls vérifiant

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

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

$$\sum \sigma_p(i_j) = \left\lceil \frac{(p-1)ln}{a} \right\rceil + r.$$

Si d et s sont des entiers, on notera $\varrho_s(d)$ 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^l et que son développement p-adique est donné par $i = \sum a_j p^j$. On définit une action de $\mathbb{Z}$ sur l'ensemble des entiers positifs strictement inférieurs à q^l par

$$t \triangleright i = \sum a_j p^{\varrho_{nl}(j+t)}.$$

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

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

où (i_j) appartient à X_l. Pour un élément $\mathbf{u}$ de X_l, on notera $\mathcal{O}_{\mathbf{u}}$ son orbite et $o(\mathbf{u})$ le cardinal de celle-ci.

Pour $j = 1, \ldots, J$, on notera β_j le représentant de Teichmüller de α_j dans K_n. Si $\mathbf{u} = (i_j)$ est un élément de X_l, on définit $\beta^{\mathbf{u}}$ et $C_l(\mathbf{u})$ par

$$\beta^{\mathbf{u}} = \beta_1^{i_1} \ldots \beta_J^{i_J} \quad \text{et} \quad C_l(\mathbf{u}) = C_l(i_1) \ldots C_l(i_J).$$

Posons

$$H_{l,r} = \sum_{\mathbf{u}} t_{o(\mathbf{u})}(\beta^{\mathbf{u}}) C_l(\mathbf{u})$$

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

$$S_l = q^l + (q^l - 1) \sum_{r=0}^{\infty} H_{l,r}. \tag{2}$$

Cette égalité a été prouvée dans [3] pour $p = 2$. La démonstration est identique quand p est impair.

4. Divisibilité de $S(f)$. La somme $S(f)$ s'exprime en fonction des $H_{1,r}$ (voir (2)) et on peut minorer la valuation $\mathfrak{p}$-adique des $H_{1,r}$ (corollaire 1). On retrouve ainsi un résultat de Litsyn, C. Moreno et O. Moreno (voir [8]).

THÉORÈME 3 (Litsyn, Moreno, Moreno). *Soit f un polynôme à coefficients dans $\mathbb{F}_{p^n}$. Alors*

$$v_{\mathfrak{p}}(S(f)) \geq n(p-1)/\sigma_p(f)$$

où $\sigma_p(f)$ est le poids p-adique de f.

Rappelons que l'on a posé $q = p^n$. Soit $f(x)$ un polynôme de degré $p^{a_0} - 1$ à coefficients dans $\mathbb{F}_q$ où a_0 est un entier strictement positif. Le poids p-adique a de f est $(p-1)a_0$. Soit α le coefficient du terme de degré $p^{a_0} - 1$ de f et soit γ le représentant de Teichmüller dans K_n de α.

Si $n = a\mu$ où μ est un entier, on a calculé dans [3] une expression de $H_{l,0}$ quand $p = 2$. On obtient de manière analogue

$$H_{l,0} = t_{a_0}(\gamma^{l(q-1)/(p^{a_0}-1)})C_l((q^l-1)/(p^{a_0}-1)). \tag{3}$$

5. Borne de Weil. Nous allons montrer que le nombre de points N_f de la courbe $y^p - y = f(x)$ peut s'exprimer en fonction de la somme exponentielle $S(f)$.

LEMME 1. *On a*

$$N_f - q - 1 = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(S(f)).$$

Preuve. On a les égalités suivantes :

$$\begin{aligned}\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(S(f)) &= \sum_{x\in\mathbb{F}_q}\sum_{b=0}^{p-1}\zeta^{b\,\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(x))}\\ &= (p-1)\#\{x\in\mathbb{F}_q \mid \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(x)) = 0\}\\ &\quad -(q - \#\{x\in\mathbb{F}_q \mid \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(f(x)) = 0\})\\ &= p(q - w_f) - q.\end{aligned}$$

On déduit de (1) que cette dernière expression est bien égale à $N_f - q - 1$.

On rappelle que l'on a supposé que $f(x)$ est un polynôme de degré $p^{a_0} - 1$ sur $\mathbb{F}_q$ dont le coefficient du terme dominant est α et que γ est le représentant de Teichmüller de α. Le poids p-adique de f est $a = a_0(p-1)$.

Pour tout entier l strictement positif, on notera par N_l le nombre de points sur $\mathbb{F}_{q^l}$ du modèle projectif de la courbe $y^p - y = f(x)$.

LEMME 2. *Soit l un entier strictement positif. Supposons que a soit supérieur ou égal à 2. Si $n = a\mu$ où μ est un entier strictement positif, alors il existe un élément y appartenant à $\mathbb{Q}_p(\zeta)$ de valuation $\mathfrak{p}$-adique strictement supérieure à $l(p-1)\mu$ tel que $(N_l - pq^l - 1)/(q^l - 1)$ soit égal à*

$$t_{a_0}(\gamma^{l(q-1)/(p^{a_0}-1)})((p-1)\pi^{l(p-1)\mu} + y) + \sum_{r\geq 1} \mathrm{Tr}_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}(H_{l,r}).$$

Preuve. Dans cette démonstration, pour simplifier les notations, on posera $i = (q^l - 1)/(p^{a_0} - 1)$ et $N'_l = (N_l - pq^l - 1)/(q^l - 1)$. On désignera aussi par $\mathrm{Tr}(\cdot)$ la trace de $\mathbb{Q}_p(\zeta)$ sur $\mathbb{Q}_p$.

La somme S_l peut s'exprimer en fonction des $H_{l,r}$ (voir (2)) et $H_{l,0}$ est égal à (voir (3))

$$H_{l,0} = t_{a_0}(\gamma^{l(q-1)/(p^{a_0}-1)})C_l(i).$$

Par ailleurs, le théorème de Stickelberger donne le début du développement π-adique de la somme de Gauss $G_l(i) = (q^l - 1)C_l(i)$. Comme q^l est congru à zéro modulo $\pi^{l(p-1)\mu+1}$ $(a \geq 2)$, il existe un élément y_1 appartenant à $\mathbb{Q}_p(\zeta)$ de valuation π-adique strictement supérieure à $l(p-1)\mu$ tel que

$$C_l(i) = \pi^{l(p-1)\mu} + y_1.$$

On conclut que S_l est égal à

$$S_l = q^l + (q^l - 1)\Big[t_{a_0}(\gamma^{l(q-1)/(p^{a_0}-1)})(\pi^{l(p-1)\mu} + y_1) + \sum_{r\geq 1} H_{l,r}\Big].$$

Le nombre de points N_l dépend de la trace de S_l. Il en résulte que

$$N'_l = t_{a_0}(\gamma^{l(q-1)/(p^{a_0}-1)})\,\mathrm{Tr}(\pi^{l(p-1)\mu} + y_1) + \sum_{r\geq 1} \mathrm{Tr}(H_{l,r}).$$

Nous allons montrer que la trace de $\pi^{l(p-1)\mu}$ n'est pas congrue à zéro modulo $\pi^{l(p-1)\mu+1}$. Cette trace peut s'écrire sous la forme

$$\mathrm{Tr}(\pi^{l(p-1)\mu}) = \sum_{\phi} \left(\frac{\phi\pi}{\pi}\right)^{l(p-1)\mu} \pi^{l(p-1)\mu}$$

où ϕ parcourt le groupe de Galois de $\mathbb{Q}_p(\zeta)$ sur $\mathbb{Q}_p$. Le corps résiduel de $\mathbb{Q}_p(\zeta)$ est isomorphe à $\mathbb{F}_p$ et $\phi\pi/\pi$ est un élément inversible de $\mathbb{Q}_p(\zeta)$. Il s'ensuit que

$$(\phi\pi/\pi)^{l(p-1)\mu} \equiv 1 \pmod{\pi}.$$

Finalement, on obtient

$$\sum_{\phi} \phi\pi^{l(p-1)\mu} \equiv (p-1)\pi^{l(p-1)\mu} \pmod{\pi^{l(p-1)\mu+1}}.$$

Par conséquent, il existe un élément y_2 appartenant à $\mathbb{Q}_p(\zeta)$ de valuation π-adique strictement supérieure à $l(p-1)\mu$ tel que N_l' soit égal à

$$t_{a_0}(\gamma^{l(q-1)/(p^{a_0}-1)})[(p-1)\pi^{l(p-1)\mu}+y_2+\mathrm{Tr}(y_1)]+\sum_{r\geq 1}\mathrm{Tr}(H_{l,r}).$$

L'élément y cherché est $y_2+\mathrm{Tr}(y_1)$.

LEMME 3. *On suppose que $n=a\mu$ où μ est un entier strictement positif et que a est supérieur ou égal à 2. Pour tout entier λ assez grand, on a*

$$\mathrm{ord}_p(N_{p^\lambda(p^{a_0}-1)}-q^{p^\lambda(p^{a_0}-1)}-1)=p^\lambda\mu(p^{a_0}-1)+\mathrm{ord}_p\, a_0.$$

Preuve. Dans [3], on a obtenu une relation de congruence pour $H_{2^\lambda j}$. Cette congruence se généralise au cas où p est un nombre premier quelconque. On a

$$H_{p^\lambda j,r}\equiv 0 \pmod{\pi^{(p^\lambda j\mu+\lambda)(p-1)+1}}$$

si r n'est pas nul (la démonstration est identique à celle qui se trouve dans [3]).

Posons $j=p^{a_0}-1$. Le lemme précédent donne une expression de $N_{p^\lambda j}$ en fonction des $H_{p^\lambda j,r}$ $(r>0)$. Comme $H_{p^\lambda j,r}$ et $q^{p^\lambda j}$ sont congrus à zéro modulo $\pi^{(p^\lambda j\mu+\lambda)(p-1)+1}$ si r n'est pas nul, il existe un élément y appartenant à $\mathbb{Q}_p(\zeta)$ de valuation $\mathfrak{p}$-adique strictement supérieure à $p^\lambda j\mu(p-1)$ tel que

$$N_{p^\lambda j}-q^{p^\lambda j}-1\equiv -a_0((p-1)\pi^{p^\lambda j\mu(p-1)}+y) \pmod{\pi^{(p^\lambda j\mu+\lambda)(p-1)+1}}.$$

Ce terme n'est pas congru à zéro si $\lambda(p-1)+1$ est strictement supérieur à $v_\mathfrak{p}(a_0)$. Il s'ensuit que

$$v_\mathfrak{p}(N_{p^\lambda j}-q^{p^\lambda j}-1)=p^\lambda j\mu(p-1)+v_\mathfrak{p}(a_0)$$

si $\lambda(p-1)+1$ est assez grand. Le lemme est démontré.

Nous allons maintenant montrer que le nombre de points sur $\mathbb{F}_q$ de courbe $y^p-y=f(x)$ n'atteint pas la borne de Weil.

Soit J la Jacobienne de cette courbe sur $\mathbb{F}_q$. C'est une variété abélienne de dimension $g=(p-1)(p^{a_0}-2)/2$. Soit $h_J(t)=\sum_{i=0}^{2g}A_it^{2g-i}$ 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 les ω_i ont une valeur absolue égale à $\sqrt{q}$ et que

$$N_l-q^l-1=-\sum_{i=1}^{g}(\omega_i^l+\overline{\omega}_i^l)$$

pour tout entier l strictement positif.

Soit μ la partie entière de n/a. Notons que $p^{\mu l}$ divise N_l-q^l-1 (voir le théorème 3 et le lemme 1). Donc si on applique le raisonnement de Ax (voir

la démonstration du théorème page 256 dans [1]) à la fonction

$$\exp\left(\sum_{l=1}^{\infty}(N_l - q^l - 1)\,\frac{t^l}{l}\right) = \prod_{i=1}^{g}(1-\omega_i t)(1-\overline{\omega}_i t),$$

on voit que $p^{\mu i}$ divise A_i. Par conséquent, ω_i/p^μ et $\overline{\omega}_i/p^\mu$ sont des entiers algébriques et, si μ est strictement positif, la Jacobienne J est quasi-supersingulière (voir [3]).

THÉORÈME 4. *Soit n un entier strictement positif. Posons $q = p^n$. Soit a_0 un entier strictement positif. Soit f un polynôme à coefficients dans $\mathbb{F}_q$ de degré $p^{a_0}-1$. Soit $a = (p-1)a_0$ le poids p-adique de f. Soit μ la partie entière de n/a. On suppose que μ est strictement positif et que a est supérieur ou égal à 3. Si n est pair, alors le nombre de points N_f sur $\mathbb{F}_q$ de la courbe $y^p - y = f(x)$ n'atteint pas la borne de Weil et on a*

$$|N_f - q - 1| \le (p-1)(p^{a_0}-2)\sqrt{q} - ap^\mu.$$

Preuve. Soit K un corps de décomposition de h_J sur $\mathbb{Q}(\zeta)$. Soit $\mathfrak{P}$ un idéal premier de K divisant $\mathfrak{p}$. Soit $e(\mathfrak{P}|\mathfrak{p})$ l'indice de ramification de $\mathfrak{P}$ sur $\mathfrak{p}$. On rappelle que

$$v_{\mathfrak{P}}(x) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(x)$$

pour tout x appartenant à $\mathbb{Q}(\zeta)$.

Soit g_2 le nombre de ω_i appartenant à $\mathbb{Q}(\zeta)$. Posons $g_1 = g - g_2$. Quitte à renuméroter les ω_i, on peut supposer que $\omega_1, \ldots, \omega_{g_1}$ n'appartiennent pas à $\mathbb{Q}(\zeta)$. Comme $\mathfrak{p}$ est l'unique idéal premier de $\mathbb{Q}(\zeta)$ divisant p, on a

$$v_{\mathfrak{P}}(\omega_i) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(\omega_i) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(\phi\omega_i) = v_{\mathfrak{P}}(\phi\omega_i)$$

pour $i = g_1 + 1, \ldots, g$ et pour tout ϕ appartenant au groupe de Galois de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$. En particulier, ω_i et $\overline{\omega}_i$ ont même valuation $\mathfrak{P}$-adique et, puisque $\omega_i\overline{\omega}_i = q$, on a

$$v_{\mathfrak{P}}(\omega_i) = v_{\mathfrak{P}}(\overline{\omega}_i) = v_{\mathfrak{P}}(q)/2$$

pour $i = g_1 + 1, \ldots, g$. Le polynôme caractéristique $h_J(t)$ de la Jacobienne de la courbe $y^p - y = f(x)$ sur $\mathbb{F}_q$ se factorise dans $\mathbb{Z}[t]$ comme le produit de deux polynômes de degré $2g_1$ et $2g_2$:

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

Donc il existe deux variétés abéliennes A et B sur $\mathbb{F}_q$ telles que J soit isogène à AB (voir Waterhouse [10]). 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 $\prod_{i=g_1+1}^{g}(t-\omega_i)(t-\overline{\omega}_i)$ respectivement.

Comme μ est strictement positif, la Jacobienne J est quasi-supersingulière. Donc A et B sont aussi quasi-supersingulières et on déduit de la

proposition 1 et de la remarque 2 que

$$v_{\mathfrak{P}}(\omega_i) \geq \begin{cases} v_{\mathfrak{P}}(q)/g_1 & \text{si } g_1 > 1, \\ v_{\mathfrak{P}}(q)/2 & \text{si } g_1 = 0, 1, \end{cases}$$

pour $i = 1, \ldots, g$. La valuation $\mathfrak{P}$-adique des $\overline{\omega}_i$ vérifie la même inégalité. Il en résulte que

$$v_{\mathfrak{P}}(N_l - q^l - 1) \geq \begin{cases} l v_{\mathfrak{P}}(q)/g_1 & \text{si } g_1 > 1, \\ l v_{\mathfrak{P}}(q)/2 & \text{si } g_1 = 0, 1, \end{cases}$$

pour tout entier l strictement positif. En simplifiant par les indices de ramification, on obtient

$$\operatorname{ord}_p(N_l - q^l - 1) \geq \begin{cases} ln/g_1 & \text{si } g_1 > 1, \\ ln/2 & \text{si } g_1 = 0, 1. \end{cases} \tag{4}$$

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

Considérons tout d'abord le cas où n est un mutiple de a, i.e. $n = a\mu$. D'après le lemme précédent, on a

$$\operatorname{ord}_p(N_{p^\lambda(p^{a_0}-1)} - q^{p^\lambda(p^{a_0}-1)} - 1) = p^\lambda(p^{a_0} - 1)\mu + \operatorname{ord}_p a_0$$

pour tout entier λ suffisamment grand. Comme a est supérieur ou égal à 3, on peut déduire de (4) que g_1 est strictement supérieur à 1 et que

$$p^\lambda(p^{a_0} - 1)\mu + \operatorname{ord}_p a_0 \geq p^\lambda(p^{a_0} - 1)a\mu/g_1.$$

Si on divise cette inégalité par $p^\lambda(p^{a_0}-1)\mu$, puis on fait tendre λ 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.

Nous avons montré qu'il existe au moins $2a$ racines de h_J n'appartenant pas à $\mathbb{Q}(\zeta)$. En particulier, $\omega_1, \ldots, \omega_{g_1}$ sont différents de $\pm\sqrt{q}$. Posons

$$M = 2\sqrt{q}/p^\mu - 1$$

et

$$x_i = M + 1 + (\omega_i + \overline{\omega}_i)/p^\mu$$

pour $i = 1, \ldots, g_1$. Les nombres x_i sont des entiers algébriques totalement positifs. 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

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

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

$$N_f - q - 1 \leq 2g\sqrt{q} - ap^{\mu}.$$

Si on reprend la même démonstration en posant $x_i = M+1-(\omega_i+\overline{\omega}_i)/p^{\mu}$, on obtient

$$N_f - q - 1 \geq -2g\sqrt{q} + ap^{\mu}.$$

COROLLAIRE 2. *Soit s le reste de la division euclidienne de a par p. Si a ne divise pas n et si p ne divise pas a, alors*

$$|N_f - q - 1| \leq (p-1)(p^{a_0} - 2)\sqrt{q} - (a - s + p)p^{\mu}.$$

Preuve. L'entier $N_f - q - 1$ est égal à la trace de $S(f)$ (voir le lemme 1). Le théorème 3 donne une minoration de la valuation $\mathfrak{p}$-adique de $S(f)$. Ces deux résultats impliquent

$$\mathrm{ord}_p(N_f - q - 1) \geq \mu + 1.$$

On en déduit l'inégalité annoncée car $(p-1)(p^{a_0} - 2)\sqrt{q} - (a - s + p)p^{\mu}$ est le plus petit entier inférieur ou égal à $(p-1)(p^{a_0} - 2)\sqrt{q}$ divisible par $p^{\mu+1}$.

REMARQUE 3. Les bornes du théorème et du corollaire précédents restent valables quand $\mu = 0$, i.e. $n < a$. En effet, si on reprend la démonstration de ce théorème en considérant l'extension de degré a de $\mathbb{F}_q$, on voit que ω_i^a et $\overline{\omega}_i^a$ sont différents de $\pm q^{a/2}$. Donc ω_i et $\overline{\omega}_i$ sont différents de $\pm q^{1/2}$ et la méthode utilisée pour améliorer la borne de Weil s'applique.

REMARQUE 4. On utilise les notations de la démonstration du théorème précédent. Si $N_f - q - 1 = (p-1)(p^{a_0} - 2)\sqrt{q} - ap^{\mu}$, alors $a = g_1$, $x_1 = \ldots = x_a = 1$ et $\omega_{a+1} = \ldots = \omega_g = -\sqrt{q}$. Par conséquent, le polynôme caractéristique de J est égal à

$$h_J(t) = (t^2 + (2\sqrt{q} - p^{\mu})t + q)^a (t^2 + 2\sqrt{q}\,t + q)^{g-a}.$$

De plus, la variété abélienne correspondant au facteur $(t^2 + (2\sqrt{q} - p^{\mu})t + q)^a$ est simple.

THÉORÈME 5. *Soit n un entier strictement positif. Posons $q = p^n$. Soit a_0 un entier. Soit f un polynôme à coefficients dans $\mathbb{F}_q$ de degré $p^{a_0} - 1$. Soit $a = (p-1)a_0$ le poids p-adique de f. Soit μ la partie entière de n/a. On suppose que μ est strictement positif et que a est supérieur ou égal à 3. Si n est pair, alors $S(f)$ n'atteint pas la borne de Weil, i.e.*

$$|S(f)| < (p^{a_0} - 2)\sqrt{q}.$$

Preuve. Weil a montré qu'il existe des entiers algébriques $\nu_1, \ldots, \nu_{p^{a_0}-2}$ de valeur absolue $\sqrt{q}$ tels que

$$S_l = -\sum_{i=1}^{p^{a_0}-2} \nu_i^l$$

pour tout entier l strictement positif.

Supposons que $S(f)$ atteint la borne de Weil. Alors, on a $\nu_1 = \ldots = \nu_{p^{a_0}-2}$ et ν_1 appartient à $\mathbb{Q}(\zeta)$.

Le polynôme caractéristique h_J de la Jacobienne de la courbe d'équation $y^p - y = f(x)$ sur $\mathbb{F}_q$ est donné par

$$h_J = \prod_{\phi} (t - \phi(\nu_1))^{p^{a_0}-2}$$

où ϕ parcourt le groupe de Galois de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$. Donc toutes les racines de h_J sont dans $\mathbb{Q}(\zeta)$. Il y a une contradiction car on a vu dans la démonstration du théorème précédent qu'il y a au moins $2a$ racines de h_J qui ne sont pas dans $\mathbb{Q}(\zeta)$.

6. Tables. Les tables suivantes donnent, pour certaines valeurs de p et a_0, la borne de Weil et les résultats obtenus dans la partie précédente. Une étoile indique que la borne est atteinte.

6.1. *Cas où* $p = 2$

Table 1. Degré 7

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^*

Table 2. Degré 15

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

Table 3. Degré 31

n	$30\sqrt{q}$	$\begin{cases} 30\sqrt{q} - 5 \cdot 2^{n/5} & \text{si 5 divise } n \\ 30\sqrt{q} - 6 \cdot 2^{[n/5]} & \text{sinon} \end{cases}$
8	480	468
10	960	940
12	1920	1896
14	3840	3816
16	7680	7632
18	15360	15312
20	30720	30640
22	61440	61344
24	122880	122784

6.2. *Cas où* $p = 3$

Table 4. Degré 8

n	$14\sqrt{q}$	$\begin{cases} 14\sqrt{q} - 4 \cdot 3^{n/4} & \text{si 4 divise } n \\ 14\sqrt{q} - 6 \cdot 3^{[n/4]} & \text{sinon} \end{cases}$
6	378	360
8	1134	1098
10	3402	3348
12	10206	10098
14	30618	30456
16	91854	91530
18	275562	275076

6.3. *Cas où* $p = 5$

Table 5. Degré 24

n	$92\sqrt{q}$	$\begin{cases} 92\sqrt{q} - 8 \cdot 5^{n/8} & \text{si 8 divise } n \\ 92\sqrt{q} - 10 \cdot 5^{[8/4]} & \text{sinon} \end{cases}$
6	11500	11490
8	57500	57460
10	287500	287450
12	1437500	1437450
14	7187500	7187450
16	35937500	35937300

Références

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

[2] B. J. Birch, *Cyclotomic fields and Kummer extensions*, in: Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich (eds.), Academic Press, 1967, 85–93.

[3] E. Férard, *Poids des duaux des codes BCH de distance prescrite* $2^a + 1$ *et sommes exponentielles*, Bull. Soc. Math. France, à paraître.

[4] G. van der Geer and M. van der Vlugt, *Reed–Muller codes and supersingular curves I*, Compositio Math. 84 (1992), 333–367.
[5] —, —, *Fibre products of Artin–Schreier curves and generalized Hamming weights of codes*, J. Combin. Theory Ser. A 70 (1995), 337–348.
[6] K. Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties*, Lecture Notes in Math. 1680, Springer, 1998.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, Amsterdam, 1977.
[8] O. Moreno and C. J. Moreno, *The MacWilliams–Sloane conjecture on the tightness of the Carlitz–Uchiyama bound and the weights of duals of BCH codes*, IEEE Trans. Inform. Theory 40 (1994), 1894–1907.
[9] M. Rosen, *The asymptotic behavior of the class group of a function field over a finite field*, Arch. Math. (Basel) 24 (1973), 287–296.
[10] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. 2 (1969), 521–560.
[11] J. Wolfmann, *New bounds on cyclic codes from algebraic curves*, in: Lecture Notes in Comput. Sci. 388, Springer, 1989, 47–62.
[12] —, *The number of points on certain algebraic curves over finite fields*, Comm. Algebra 17 (1989), 2055–2060.
[13] C. Xing, *The characteristic polynomials of abelian varieties of dimensions three and four over finite fields*, Sci. China Ser. A 37 (1994), 147–150.

IML CNRS UPR 9016
163, Avenue de Luminy
13288 Marseille Cedex 9, France
E-mail: ferard@upf.pf

Reçu le 21.3.2001
et révisé le 26.11.2001 (3999)