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 ℓ un entier, on notera $\mathbb{F}_{p^\ell}$ un corps fini à p^ℓ 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 δ un entier impair. Soient a, ℓ deux entiers strictement positifs. Soit C_n un code BCH binaire de longueur $2^n - 1$ et de distance prescrite δ. Si l'une des conditions suivantes est vérifiée*

(i) *$2a$ divise n, ℓ 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 Ω une clôture algébrique de $\mathbb{Q}_p$. On désignera par $\mathrm{ord}_p(\cdot)$ la valuation sur Ω 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 λ et une longueur horizontale ℓ, alors P a exactement ℓ racines (comptées avec multiplicités) dans Ω 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 π_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, π_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 π_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 π_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 ℓ 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.