C. R. Acad. Sci. Paris, Ser. I 352 (2014) 373–376

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Théorie des nombres

Cyclotomie des sommes de Weil binomiales

Cyclotomy of Weil sums of binomials

Yves Aubry [a,b], Daniel J. Katz [c], Philippe Langevin [a]

[a] *Institut de mathématiques de Toulon, Université de Toulon, France*
[b] *Institut de mathématiques de Marseille, Aix-Marseille Université – CNRS, France*
[c] *Department of Mathematics, California State University, Northridge, United States*

I N F O A R T I C L E

Historique de l'article :
Reçu le 6 février 2014
Accepté le 5 mars 2014
Disponible sur Internet le 3 avril 2014

Présenté par Jean-Pierre Serre

R É S U M É

Les sommes de Weil de la forme $W_{K,d}(a) = \sum_{x\in K} \psi(x^d + ax)$, où K est un corps fini, ψ un caractère additif de K, d un entier premier à $|K^\times|$ et $a \in K^\times$, apparaissent naturellement en théorie des nombres ainsi qu'en géométrie finie, en cryptographie, dans l'étude de la corrélation des suites et en théorie des codes. Nous nous intéressons ici au cas où $W_{K,d}(a)$ ne prend que trois valeurs distinctes lorsque a varie dans $K^\times$. Via une approche galoisienne, nous donnons plusieurs résultats concernant ces sommes de Weil à trois valeurs, généralisant notamment à toute caractéristique non nulle des résultats de Calderbank–McGuire–Poonen–Rubinstein, de Calderbank–McGuire et de Charpin établis en caractéristique 2.

A B S T R A C T

Weil sums of the form $W_{K,d}(a) = \sum_{x\in K} \psi(x^d + ax)$, where K is a finite field, ψ is an additive character of K, d is coprime to $|K^\times|$, and $a \in K^\times$, arise often in number theory, as well as in finite geometry, in cryptography, in the study of the correlation of sequences, and in coding theory. Here we are interested in the case where $W_{K,d}(a)$ takes only three distinct values as a runs through $K^\times$. Via a Galois-theoretic approach, we give several results concerning three-valued Weil sums, and, in particular, we generalize to any nonzero characteristic some results of Calderbank–McGuire–Poonen–Rubinstein, of Calderbank–McGuire and of Charpin proved in characteristic 2.

1. Introduction

Dans tout ce qui suit, K est un corps fini à q éléments de caractéristique p, $\mathrm{Tr}_{K/\mathbb{F}_p}$ est la trace relative à l'extension $K/\mathbb{F}_p$, et ψ_K est le caractère additif de K défini pour tout $x \in K$ par :

$$\psi_K(x) = \exp\bigl(2i\pi\, \mathrm{Tr}_{K/\mathbb{F}_p}(x)/p\bigr).$$

Adresses e-mail : yves.aubry@univ-tln.fr (Y. Aubry), daniel.katz@csun.edu (D.J. Katz), langevin@univ-tln.fr (P. Langevin).

http://dx.doi.org/10.1016/j.crma.2014.03.001
1631-073X/

Les sommes de Weil binomiales sont les sommes de caractères de la forme $\sum_{x\in K}\psi_K(bx^j+cx^k)$, où b et c appartiennent à K et j et k sont des entiers naturels.

On s'intéresse ici à de telles sommes avec j et k premiers à $q-1$; après une reparamétrisation, il s'agit finalement de sommes de la forme

$$\mathrm{W}_{K,d}(a)=\sum_{x\in K}\psi_K\left(x^d+ax\right) \tag{1}$$

avec d et q premiers entre eux et $a\in K$.

Le cas $d\equiv -1 \pmod{q-1}$ correspond aux sommes de Kloosterman, dont la distribution est étudiée dans [9] et [10].

Les sommes $\mathrm{W}_{K,d}(a)$ sont des entiers algébriques totalement réels (voir [7, Théorème 3.1(a)]) ; ils appartiennent à $\mathbb{Z}$ si et seulement si $d\equiv 1 \pmod{p-1}$ (voir [7, Théorème 4.2]). On a $\mathrm{W}_{K,d}(0)=0$.

Pour K et d fixés, on considère l'ensemble $\mathcal{W}_{K,d}$ des valeurs prises par $\mathrm{W}_{K,d}(a)$ lorsque a décrit $K^\times$:

$$\mathcal{W}_{K,d}=\left\{\mathrm{W}_{K,d}(a),\ a\in K^\times\right\}.$$

Si $d\equiv p^j \pmod{q-1}$ pour un certain entier j, on dit que d est *dégénéré sur* K. On montre aisément que dans ce cas, $\mathrm{W}_{K,d}(a)$ vaut q si $a=-1$, et 0 sinon.

Si d est non dégénéré sur K, alors Helleseth a démontré dans [7, Théorème 4.1] que $\mathrm{W}_{K,d}(a)$ prend au moins trois valeurs lorsque a varie dans $K^\times$, i.e. $|\mathcal{W}_{K,d}|\geqslant 3$.

De plus, Katz a démontré dans [8, Théorèmes 1.7, 1.9] que si $|\mathcal{W}_{K,d}|=3$ alors $d\equiv 1 \pmod{p-1}$ et les valeurs sont nécessairement des entiers relatifs dont l'une est zéro.

Enfin, l'étude des moments d'ordre 2 montre que si $|\mathcal{W}_{K,d}|=3$, les deux valeurs non nulles sont de signes opposés. Bien qu'il ait été observé sur tous les exemples connus que dans ce cas, les valeurs non nulles sont opposées (on parle alors d'ensemble de valeurs *symétrique*), on ne sait pas le démontrer.

2. Les résultats auxiliaires

L'étude de l'action des groupes de Galois des extensions intermédiaires du corps fini K permet de montrer :

Proposition 2.1. *Si $\sigma\in \mathrm{Gal}(K/\mathbb{F}_p)$, alors $\mathrm{W}_{K,d}(\sigma(a))=\mathrm{W}_{K,d}(a)$ et $\mathrm{W}_{K,d}(a)=\mathrm{W}_{K,p^jd}(a)$ pour tout $a\in K$ et $j\in\mathbb{Z}$.*

De plus, soit L une extension de K avec $[L:K]$ une puissance d'un nombre premier ℓ distinct de p. Alors, pour tout $a\in K$, on a :

$$\mathrm{W}_{L,d}(a)\equiv \mathrm{W}_{K,d}\left([L:K]^{1-1/d}a\right) \pmod{\ell},$$

où $1/d$ représente l'inverse de d modulo $p-1$.

La transformée de Fourier des sommes de Weil peut se décrire en termes de sommes de Gauss, ce qui nous permet d'obtenir des critères de p-divisibilité des sommes de Weil.

Pour tout caractère multiplicatif $\chi\in\widehat{K^\times}=\mathrm{Hom}(K^\times,\mathbb{C}^\times)$, on considère la somme de Gauss :

$$\tau_K(\chi)=\sum_{a\in K^\times}\chi(a)\psi_K(a).$$

Par transformation de Fourier inverse, si $a\in K^\times$, on obtient $\psi_K(a)=\frac{1}{q-1}\sum_{\chi\in\widehat{K^\times}}\tau_K(\chi)\bar{\chi}(a)$.

Considérons la valuation p-adique val_p sur $\mathbb{Z}$ que nous étendons à $\mathbb{Q}$ et même au corps de nombres $\mathbb{Q}(\zeta_p,\zeta_{q-1})$ (où ζ_r désigne une racine primitive r-ième de l'unité dans $\mathbb{C}$) dans lequel se trouvent les sommes de Gauss.

On pose :

$$\mathrm{Val}_{K,d}=\min_{a\in K^\times}\mathrm{val}_p\left(\mathrm{W}_{K,d}(a)\right).$$

On commence par montrer que, si d est premier à $q-1$, alors $\mathrm{Val}_{K,d}=\min_{\chi\in\widehat{K^\times}}\mathrm{val}_p(\tau_K(\chi)\tau_K(\bar{\chi}^d))$.

Si L est une extension de degré fini de K, la relation de Hasse–Davenport (voir [5, p. 153, Formule 08]) entraîne que : $\mathrm{Val}_{L,d}\leqslant[L:K].\mathrm{Val}_{K,d}$.

Lorsque l'extension L/K est quadratique, on démontre :

Proposition 2.2. *Soit L une extension quadratique de K. Supposons que d soit dégénéré sur K, mais pas sur L. Alors $\mathrm{Val}_{L,d}=[K:\mathbb{F}_p]$ et de plus $\mathrm{W}_{L,d}(a)=-q$ pour un certain $a\in L^\times$.*

Décrivons à présent l'action des groupes de Galois des extensions cyclotomiques. Soit ζ_p une racine primitive p-ième de l'unité dans $\mathbb{C}$. Si K est de caractéristique p, alors les sommes de Weil $\mathrm{W}_{K,d}(a)$ appartiennent à $\mathbb{Q}(\zeta_p)$.

Lemme 2.3. *Si σ est l'élément de* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ *tel que* $\sigma(\zeta_p) = \zeta_p^j$, *alors* $\sigma(\mathrm{W}_{K,d}(a)) = \mathrm{W}_{K,d}(j^{1-(1/d)}a)$, *où* $1/d$ *désigne l'inverse de* d *modulo* $p-1$.

Corollaire 2.4. *Soient A et B des valeurs prises par* $\mathrm{W}_{K,d}$. *Si A et B sont conjuguées sous* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ *alors le nombre de* $a \in K^\times$ *tel que* $\mathrm{W}_{K,d}(a) = A$ *est égal au nombre de* $a \in K^\times$ *tel que* $\mathrm{W}_{K,d}(a) = B$.

Les sommes de Weil appartiennent souvent à des sous-corps propres de $\mathbb{Q}(\zeta_p)$. Voici un critère pour que cela se produise :

Proposition 2.5. *Soit K un corps fini de caractéristique p. Soit E l'extension de $\mathbb{Q}$ engendrée par les valeurs de* $\mathrm{W}_{K,d}(a)$ *pour* $a \in K^\times$. *Soit m le plus petit diviseur de $p-1$ tel que* $d \equiv 1 \pmod{(p-1)/m}$. *Alors E est l'unique sous-corps de* $\mathbb{Q}(\zeta_p)$ *tel que* $[E:\mathbb{Q}] = m$.

Enfin, si σ est un élément non trivial de $\mathrm{Gal}(E/\mathbb{Q})$, *alors*

$$\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)\sigma\big(\mathrm{W}_{K,d}(a)\big) = 0.$$

3. Les résultats principaux

En étudiant les valuations p-adiques des sommes de Weil, on donne une condition suffisante sur le corps K pour que l'ensemble des valeurs prises par $\mathrm{W}_{K,d}(a)$ lorsque a décrit $K^\times$ ne soit pas symétrique :

Théorème 3.1. *Supposons que I et J soient des sous-corps de K avec $I \subset J$ et $[J:I] = 2$, où d est dégénéré sur I mais pas sur J. Alors $\mathcal{W}_{K,d}$ n'est de la forme $\{-A, 0, +A\}$ pour aucun $A \in \mathbb{Z}$, $A > 0$.*

On obtient en particulier :

Corollaire 3.2. *Soit K un corps fini de caractéristique p, et supposons que $[K:\mathbb{F}_p]$ soit une puissance de 2. Alors $\mathcal{W}_{K,d}$ n'est de la forme $\{-A, 0, +A\}$ pour aucun $A \in \mathbb{Z}$, $A > 0$.*

Si l'on pose $p = 2$ dans le corollaire précédent, on retrouve un résultat de Calderbank–McGuire–Poonen–Rubinstein [3, Théorème 3].

Il est en fait conjecturé depuis 1976 par Helleseth [7, Conjecture 5.2] que, sous l'hypothèse du corollaire précédent, on a nécessairement $|\mathcal{W}_{K,d}| \neq 3$. Cette conjecture est prouvée pour $p = 2$ en combinant les résultats de Feng [6, Théorème 2] et de Katz [8, Théorème 1.9].

L'étude des moments des sommes de Weil nous permet de montrer que, si $\mathcal{W}_{K,d} = \{-A, 0, +A\}$, avec $A \in \mathbb{Z}$, $A > 0$, alors $A = p^k$ pour un certain entier positif k, avec $\sqrt{q} < p^k < q$.

Cela nous conduit à définir les sommes de Weil (symétriques à trois valeurs) *préférées* comme étant celles dont la valeur positive est minimale relativement à l'encadrement ci-dessus, à savoir lorsque les valeurs non nulles sont $\pm\sqrt{pq}$ quand q est une puissance impaire de p, ou lorsqu'elles valent $\pm p\sqrt{q}$ quand q est un carré.

Notre deuxième résultat principal est une borne inférieure sur la valeur positive d'une somme de Weil symétrique à trois valeurs :

Théorème 3.3. *Soit s la valuation dyadique de $[K:\mathbb{F}_p]$. Si $\mathcal{W}_{K,d}$ est de la forme $\{-A, 0, +A\}$ avec $A \in \mathbb{Z}$, $A > 0$, alors $A \geqslant p^{2^{s-1}}\sqrt{q}$.*

En particulier, si le degré de K sur $\mathbb{F}_p$ est un multiple de 4, alors $\mathrm{W}_{K,d}$ n'est pas préférée. Autrement dit :

Corollaire 3.4. *Si* $[K:\mathbb{F}_p] \equiv 0 \pmod 4$ *alors $\mathcal{W}_{K,d}$ n'est pas de la forme* $\{0, \pm p\sqrt{q}\}$.

Le cas $p = 2$ dans ce dernier corollaire est une conjecture de Sarwate–Pursley [12, p. 603] qui avait été démontrée par Calderbank et McGuire [2].

Les deux résultats ci-dessus donnent des restrictions sur les corps finis K sur lesquels nous considérons des sommes de Weil pour que celles-ci soient symétriques ou préférées. Notre troisième résultat principal porte sur une obstruction sur l'exposant d du polynôme intervenant dans la somme de Weil pour qu'elle soit à trois valeurs.

Théorème 3.5. *Supposons que q soit un carré. Si d est une puissance de p modulo $\sqrt{q}-1$, alors on a $|\mathcal{W}_{K,d}| \neq 3$.*

En d'autres termes, on a $|\mathcal{W}_{K,d}| \neq 3$ si K est une extension quadratique d'un corps dans lequel d est dégénéré. Un tel exposant d est appelé un *exposant de Niho* (voir [11]). Le théorème ci-dessus généralise le résultat de Charpin [4, Théorème 2], qui a démontré le cas $p = 2$.

Les démonstrations des résultats ci-dessus se trouvent dans [1].

Références

[1] Y. Aubry, D.J. Katz, P. Langevin, Cyclotomy of Weil sums of binomials, arXiv:1312.3889v2 [math.NT], 2014.
[2] A.R. Calderbank, G. McGuire, Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences, IEEE Trans. Inf. Theory 41 (4) (1995) 1153–1155.
[3] A.R. Calderbank, G. McGuire, B. Poonen, M. Rubinstein, On a conjecture of Helleseth regarding pairs of binary m-sequences, IEEE Trans. Inf. Theory 42 (3) (1996) 988–990.
[4] P. Charpin, Cyclic codes with few weights and Niho exponents, J. Comb. Theory, Ser. A 108 (2) (2004) 247–259.
[5] H. Davenport, H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math. 172 (1935) 151–182.
[6] T. Feng, On cyclic codes of length 2^{2^r} with two zeros whose dual codes have three weights, Des. Codes Cryptogr. 62 (3) (2012) 253–258.
[7] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. 16 (3) (1976) 209–232.
[8] D.J. Katz, Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth, J. Comb. Theory, Ser. A 119 (8) (2012) 1644–1659.
[9] N. Katz, R. Livné, Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3, C. R. Acad. Sci. Paris, Ser. I 309 (11) (1989) 723–726.
[10] G. Lachaud, J. Wolfmann, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2, C. R. Acad. Sci. Paris, Ser. I 305 (20) (1987) 881–883.
[11] Y. Niho, Multi-valued cross-correlation function between two maximal linear recursive sequences, PhD thesis, University of Southern California, Los Angeles, USA, 1972.
[12] D.V. Sarwate, M.B. Pursley, Cross correlation properties of pseudorandom and related sequences, IEEE Trans. Inf. Theory 68 (5) (1980) 593–619, Correction dans IEEE Trans. Inf. Theory 68 (12) (1980) 1554.