On three-valued Weil Sums

International Conference
on
Algebraic Geometry and Coding Theory
Indian Institute of Technology
Mumbai, India

2nd-6th december 2013

Yves Aubry [1 2]
joint work with Daniel Katz[3] and Philippe Langevin[1]

[1]Institut de Mathématiques de Toulon, France

[2]Institut de Mathématiques de Luminy, France

[3]California State University, USA

December 6, 2013

Weil sums

Weil sums of binomials

Let K be a finite field of characteristic p.

Let ψ_K be the canonical additive character of K:

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

We are concerned with character sums of the form

$$\sum_{y \in K} \psi_K(by^m + cy^n) \tag{1}$$

with $\gcd(m, |K| - 1) = \gcd(n, |K| - 1) = 1$ and $b, c \in K^\times$.

Weil sums II

If we reparametrize the sum by setting $y = b^{-1/m}x^{1/n}$ (where inversion is taken modulo $|K| - 1$), then we obtain

$$\sum_{x \in K^\times} \psi_K(x^{m/n} + cb^{-n/m}x) \tag{2}$$

Weil sums III

Hence, we consider character sums

$$\mathrm{W}_{K,d}(a) = \sum_{x \in K} \psi_K(x^d + ax) \tag{3}$$

with $\gcd(d, |K| - 1) = 1$ and $a \in K$, called *Weil sums*.

Rational integers

The sums $\mathrm{W}_{K,d}(a)$ are always algebraic integers.

Furthermore, they are rational integers if and only if $d \equiv 1 \pmod{p-1}$ (Helleseth, 1976).

The value set

Since $x \mapsto x^d$ is a permutation of K, we always have $\mathrm{W}_{K,d}(0) = 0$.

For a fixed K and d, we consider $\mathrm{W}_{K,d}(a)$ as a function of $a \in K^\times$, and are interested in how many different values it assumes as a runs through $K^\times$.

We call

$$\{\mathrm{W}_{K,d}(a) : a \in K^\times\}$$

the *value set* of $\mathrm{W}_{K,d}$, and say that $\mathrm{W}_{K,d}$ is *v-valued* over K to mean that this set is of cardinality v.

Applications

The problem of determining $\{\mathrm{W}_{K,d}(a) : a \in K^\times\}$ is equivalent to problems of interest in information theory, cryptography, and finite geometry:
(i) determination of the Fourier (or Walsh) spectrum of a power permutation,
(ii) the determination of the cross-correlation values for a pair of maximal linear recursive sequences over a finite field,
(iii) in the case where $d \equiv 1 \pmod{p-1}$ the problem of determining the weights of words in certain p-ary cyclic codes,
(iv) in the case where $p = 2$, the problem of determining the sizes of intersections of certain subsets of the finite projective space with the hyperplanes.

Vanishing Helleseth conjecture

A conjecture of Helleseth

In 1976, Helleseth made the following conjecture:

Conjecture

If $|K| > 2$ *and* $d \equiv 1 \pmod{p-1}$ *then* $\mathrm{W}_{K,d}(a) = 0$ *for some* $a \in K^{\times}$.

Fourier coefficient

Recall that the *Fourier coefficient* of a mapping $f\colon K \to K$ is defined at $a \in K$ by

$$\widehat{f}(a) = \sum_{x \in K} \psi_K(ax + f(x)). \tag{4}$$

Then the Weil sum $\mathrm{W}_{K,d}(a) = \sum_{x \in K} \psi_K(x^d + ax)$ can be interpreted as the Fourier coefficient $\widehat{f}(a)$ of the map $f : x \longmapsto x^d$ from K to K at $a \in K$.

A divisibility result for APN functions

Recall that a function f defined over a field K of characteristic 2 is said to be almost perfect nonlinear (APN) if for all $u \in K^\times$ the derivative $x \mapsto f(x+u) + f(x)$ is two-to-one.

It is for example the case of $f(x) = x^3$ over any field K and of $f(x) = x^{-1}$ when $[K : \mathbb{F}_2]$ is odd.

Theorem (Y. A. and P. Langevin, 2013)

Let f be a power permutation over a field K of even characteristic of cardinal $q \not\equiv 2, 4 \mod 5$. If f is almost perfect nonlinear then there exists $a \in K^\times$ such that $\mathrm{W}_{K,d}(a) \equiv 0 \mod 5$.

Hyperplane section

Consider the number $N_n(u, v)$ of solutions in K^n of the system

$$\begin{cases} x_1 + x_2 + \dots + x_n = u \\ f(x_1) + f(x_2) + \dots + f(x_n) = v. \end{cases} \tag{5}$$

$N_n(u, v)$ can be expressed as character sums.

Link with the Helleseth conjecture

Proposition

Assuming the Fourier coefficients of λf, $\lambda \in K$, are integers. Let $\ell \neq p$ be a prime such that $\prod_{\lambda \in K^\times} \prod_{a \in K^\times} \widehat{\lambda f}(a) \not\equiv 0 \mod \ell$. Then

$$q^2 N_{\ell-1}(u,v) \equiv 1 + (q\delta_0(u) - 1)(q\delta_0(v) - 1) \mod \ell$$

where $\delta_a(b)$ is equal to 1 if $b = a$ and 0 otherwise.

A proof modulo ℓ of the Helleseth conjecture

Theorem (Y. A. and P. Langevin, 2013)

Let f be a power permutation of $K = \mathbb{F}_{p^n}$ (with $p^n > 2$) of exponent $d = 1 \mod (p-1)$. Then there exists $a \in K^\times$ such that $\mathrm{W}_{K,d}(a) \equiv 0 \mod 3$.
Moreover, if n is a power of a prime ℓ and $p \not\equiv 2 \mod \ell$ then there exists $a \in K^\times$ such that $\mathrm{W}_{K,d}(a) \equiv 0 \mod \ell$.

Three-valued Weil sums

Degenerate exponents

If

$$d \equiv p^j \pmod{|K| - 1}$$

for some j, we say that d is *degenerate over* K, because $\mathrm{Tr}_{K/\mathbb{F}_p}(x^d + ax) = \mathrm{Tr}_{K/\mathbb{F}_p}((1+a)x)$, and so the binomial effectively becomes zero (if $a = -1$) or a nonvanishing linear form (if $a \neq -1$).

Thus if d is degenerate over K, then

$$\mathrm{W}_{K,d}(a) = \begin{cases} |K| & \text{if } a = -1, \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Helleseth's theorem

Helleseth shows that one always obtains a richer value set than in the nondegenerate case:

Theorem (Helleseth, 1976)

If d is nondegenerate over K, then $\mathrm{W}_{K,d}(a)$ takes at least three values as a runs through $K^\times$.

Our purpose

Here we want to know when Weil sums of this form can be three-valued, and if so, what are the three values they may take.

Katz's theorem

Theorem (Katz, 2012)

Let K be a finite field of characteristic p. If $\mathrm{W}_{K,d}$ is three-valued for some exponent d, then $d \equiv 1 \pmod{p-1}$, and the values must be rational integers, one of which is zero.

Symmetrical three-valued Weil sum

Concerning the two nonzero values of a three-valued Weil sum, one must be positive and the other negative, since it is known that $\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)^2 = \left(\sum_{a\in K^\times} \mathrm{W}_{K,d}(a)\right)^2$.

However, it has not been proved that these values must have the same magnitude, although this is always what has been observed.

We say that a three-valued Weil $\mathrm{W}_{K,d}$ sum is *symmetrical* when the two nonzero values are opposites of each other.

If we assume that a three-valued Weil sum is symmetrical, we can make further conclusions about the possible values.

Our results

An intermediate result

Proposition (A-K-L, 2013)

If K is the finite field of characteristic p and order q, and if $\mathrm{W}_{K,d}(a)$ is three-valued with values 0 and $\pm A$, then $d \equiv 1 \pmod{p-1}$ and $|A| = p^k$ for some positive integer k with $\sqrt{q} < p^k < q$.

First main result

Our first main result shows that if a field is obtained by a tower of quadratic extensions over the prime field, then it cannot support a symmetrical three-valued Weil sum:

Theorem (A-K-L, 2013)

Let K be a finite field of characteristic p. If $[K : \mathbb{F}_p]$ is a power of 2, then the set of values assumed by $\mathrm{W}_{K,d}(a)$ as a runs through $K^\times$ is not of the form $\{-A, 0, +A\}$ for any A.

Generalization to any characteristic

This generalizes a result of Calderbank-McGuire-Poonen-Rubinstein (IEEE, 1996) (the $p = 2$ case).

Our proof is quite different from that of Calderbank et al., who used McEliece's Theorem from coding theory (a relative of Stickelberger's Theorem on the p-divisibility of Gauss sums) and a complicated calculation in additive number theory to obtain the result for $p = 2$.

At least four-valued Helleseth conjecture

Helleseth conjectured that the conditions of the previous theorem make it impossible for the Weil sum to be three-valued at all.

Conjecture (Helleseth, 1976)

Let K be a finite field of characteristic p. If $[K : \mathbb{F}_p]$ is a power of 2, then $\mathrm{W}_{K,d}$ is not three-valued.

Conjecture proved in even characteristic

If it were proved that three-valued Weil sums must be symmetrical, this would follow from the previous theorem.

The $p = 2$ case of this conjecture has been proved.

First, Feng (2012) showed that if $p = 2$, one could strengthen the conclusion of the previous theorem to say that the value set is not only non-symmetric, but entirely lacks the value 0.

Then when Katz (2012) proved that a three-valued Weil sum must take the value 0, the Conjecture was established for $p = 2$.

Preferred Weil sum

A symmetrical three-valued Weil sum is called *preferred* if the magnitude of the nonzero values is as small as possible, that is, if the nonzero values are $\pm\sqrt{pq}$ when q is an odd power of p, or if the nonzero values are $\pm p\sqrt{q}$ when q is an even power of p.

This terminology originates from digital sequence design, wherein smaller magnitude Weil sums of binomials correspond to smaller cross-correlation between a pair of maximal linear recursive sequences, which is desirable.

Second main result

Our second main result shows that it is impossible for $\mathrm{W}_{K,d}$ to be preferred if K is an extension of a quartic extension:

Theorem (A-K-L, 2013)

Let K be the finite field of characteristic p and order q. If $[K:\mathbb{F}_p] \equiv 0 \pmod 4$, then the set of values assumed by $\mathrm{W}_{K,d}$ as a runs through $K^\times$ is not of the form $\{0, \pm p\sqrt{q}\}$.

Generalization to any characteristic

This generalizes Calderbank-McGuire's proof (1995) of a conjecture of Sarwate and Pursley (1980), which is the special case of the previous theorem where $p = 2$.

Again, our proof technique is much simpler than the original, as it obviates the need for McEliece's Theorem or Stickelberger's Theorem.

Special exponents

Our first two results give restrictions on the types of fields that support symmetrical and preferred Weil sums.

Our third result shows that certain exponents d of the polynomial in the Weil sum prevent the Weil sum from being three-valued at all.

Third main result

Theorem (A-K-L, 2013)

Let K be a finite field of characteristic p with $[K : \mathbb{F}_p]$ even. If d is a power of p modulo $\sqrt{|K|} - 1$, then $\mathrm{W}_{K,d}$ is not three-valued.

In other words, it is impossible for $\mathrm{W}_{K,d}$ to be three-valued if K is the quadratic extension of a field F in which d is degenerate.

Such an exponent d is called a *Niho exponent*, since they were first studied by Niho in 1972.

The previous theorem generalizes the result of Charpin (2004), who proved the $p = 2$ case.

Some steps of Charpin's proof for characteristic two do not hold in odd characteristic, so new arguments are devised.

Intermediate results

Power moments

The mth *power moment* of the Weil sum $\mathrm{W}_{K,d}$ is the sum

$$\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)^m.$$

The first few power moments can be calculated as straightforward character sums.

Lemma

Let K be a finite field. Then

(i). $\sum_{a \in K^\times} \mathrm{W}_{K,d}(a) = |K|$,

(ii). $\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)^2 = |K|^2$, *and*

(iii). $\sum_{a \in K^\times} \mathrm{W}_{K,d}(a)^3 = |K|^2 \cdot |V|$,

where V is the set of roots of the polynomial $(x+1)^d - x^d - 1$ in K.

Power moments analysis

Proposition

If K is a finite field, and d is nondegenerate over K, then $|\mathrm{W}_{K,d}(a)| < |K|$ for all $a \in K^\times$. Furthermore, $\mathrm{W}_{K,d}$ assumes at least one positive value and at least one negative value.

Proposition

If K is the finite field of characteristic p and order q, and if $\mathrm{W}_{K,d}(a)$ is three-valued with values 0 and $\pm A$, then $d \equiv 1 \pmod{p-1}$ and $|A| = p^k$ for some positive integer k. If V denotes the set of roots of $(x+1)^d - x^d - 1$ in K, then $\sqrt{q} < \sqrt{|V|\,q} = |A| < q$.

Action of Galois Groups of finite fields

Proposition

Let K be a finite field of characteristic p. If $\sigma \in \mathrm{Gal}(K/\mathbb{F}_p)$, then $\mathrm{W}_{K,d}(\sigma(a)) = \mathrm{W}_{K,d}(a)$.
We also have $\mathrm{W}_{K,d}(a) = \mathrm{W}_{K,p^j d}$ for any $a \in K$ and $j \in \mathbb{Z}$.
Moreover, let L be an extension of K with $[L : K]$ a power of a prime ℓ distinct from p. Then for any $a \in K$, we have

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

where $1/d$ indicates the multiplicative inverse of d modulo $p - 1$.

We explore the Fourier transform of the value set of the Weil sum, which is expressible in terms of Gauss sums.

This will enable us to prove some criteria about the p-divisibility of Weil sum values.

Gauss sums

For any multiplicative character $\chi \in \widehat{K^\times}$, we consider the Gauss sum

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

By Fourier inversion, if $a \in K^\times$, we find that

$$\psi_K(a) = \frac{1}{q-1} \sum_{\chi \in \widehat{K^\times}} \tau_K(\chi)\bar{\chi}(a).$$

Character sum calculus

Thus for $a \in K^\times$,

$$\begin{aligned} \mathrm{W}_{K,d}(a) &= 1 + \frac{1}{(q-1)^2} \sum_{b \in K^\times} \sum_{\chi,\varphi \in \widehat{K^\times}} \tau_K(\chi)\tau_K(\varphi)\bar{\chi}^d(b)\bar{\varphi}(ab) \\ &= 1 + \frac{1}{q-1} \sum_{\substack{\chi,\varphi \in \widehat{K^\times} \\ \varphi = \bar{\chi}^d}} \tau_K(\chi)\tau_K(\varphi)\bar{\varphi}(a) \\ &= \frac{q}{q-1} + \frac{1}{q-1} \sum_{\chi \neq 1} \tau_K(\chi)\tau_K(\bar{\chi}^d)\chi^d(a). \end{aligned} \tag{7}$$

Gauss sums

If we denote by t the inverse of $-d$ modulo $q-1$, the above formula shows that q and the $\tau_K(\chi)\tau_K(\bar{\chi}^d)$ are the Fourier coefficients of the mapping $a \mapsto \mathrm{W}_{K,d}(a^t)$ from $K^\times$ to $\mathbb{C}$, whence by Fourier inversion

$$\sum_{a \in K^\times} \mathrm{W}_{K,d}(a^t)\chi(a) = \begin{cases} \mathrm{q} & \text{if } \chi = 1, \\ \tau_K(\chi)\tau_K(\bar{\chi}^d) & \text{otherwise.} \end{cases} \tag{8}$$

p-adic Valuation

Recall that for any nonzero integer n, the *p-adic valuation* $\mathrm{val}_p(n)$ of n is the largest k such that p^k divides n, and we set $\mathrm{val}_p(0) = \infty$.

Then $\mathrm{val}_p(ab) = \mathrm{val}_p(a) + \mathrm{val}_p(b)$ and $\mathrm{val}_p(a+b) \geq \min\{\mathrm{val}_p(a), \mathrm{val}_p(b)\}$, which becomes an equality whenever $\mathrm{val}_p(a) \neq \mathrm{val}_p(b)$.

We can extend the definition to $\mathbb{Q}$, wherein $\mathrm{val}_p(a/b) = \mathrm{val}_p(a) - \mathrm{val}_p(b)$.

If ζ_p and ζ_{q-1} are, respectively, primitive pth and $(q-1)$th roots of unity in $\mathbb{C}$, we can further extend val_p to the field $\mathbb{Q}(\zeta_p, \zeta_{q-1})$ where the Gauss sums reside.

In this last field, elements can have fractional valuations: for instance $\mathrm{val}_p(1-\zeta_p) = 1/(p-1)$.

Minimum p-adic Valuation

We introduce the useful notation

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

Lemma

For K a finite field of order q and d an integer coprime to $q-1$, we have

$$\mathrm{V}_{K,d} = \min_{\chi \in \widehat{K^\times}} \mathrm{val}_p(\tau_K(\chi)\tau_K(\bar{\chi}^d)).$$

Valuation

Proposition

Let K be a finite field, and let L be the quadratic extension of K. Let d be degenerate over K, but not over L. Then

$$\mathrm{V}_{L,d} = [K : \mathbb{F}_p],$$

and furthermore, $\mathrm{W}_{L,d}(a) = -|K|$ for some $a \in L^\times$.

Action of Galois Groups of Cyclotomic Fields

Let ζ_p denotes a primitive pth root of unity in $\mathbb{C}$. If K is a field of characteristic p, then the Weil sum values $\mathrm{W}_{K,d}(a)$ reside in $\mathbb{Q}(\zeta_p)$. First we see how Galois automorphisms permute the Weil sum values. Recall that we always have d invertible modulo $|K|-1$ whenever we write the sum $\mathrm{W}_{K,d}$.

Lemma

Let K be a finite field of characteristic p. If σ is the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $\sigma(\zeta_p)=\zeta_p^j$, then $\sigma(\mathrm{W}_{K,d}(a))=\mathrm{W}_{K,d}(j^{1-(1/d)}a)$, where $1/d$ indicates the multiplicative inverse of d modulo $p-1$.

Number of occurence

This shows that if two Weil sum values are Galois conjugates over $\mathbb{Q}$, then they occur equally often.

Corollary

Let K be a finite field, and let A and B be values assumed by $\mathrm{W}_{K,d}$. If A and B are Galois conjugates over $\mathbb{Q}$, then the number of $a \in K^\times$ such that $\mathrm{W}_{K,d}(a) = A$ is equal to the number of $a \in K^\times$ such that $\mathrm{W}_{K,d}(a) = B$.

Proof.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $\sigma(A) = B$, and let $j \in \mathbb{F}_p^\times$ such that $\sigma(\zeta_p) = \zeta_p^j$. By the previous Lemma, $\mathrm{W}_{K,d}(a) = A$ precisely when $\mathrm{W}_{K,d}(j^{1-1/d}a) = B$. $\square$

Cyclotomy

Often the Weil sums lie in a proper subfield of $\mathbb{Q}(\zeta_p)$. We give a criterion for determining when this happens.

Proposition

Let K be a finite field of characteristic p. Let E be the extension of $\mathbb{Q}$ generated by all the values of $\mathrm{W}_{K,d}(a)$ for $a \in K^\times$.

Let m be the smallest divisor of $p-1$ such that $d \equiv 1 \pmod{(p-1)/m}$. Then E is the unique subfield of $\mathbb{Q}(\zeta_p)$ with $[E:\mathbb{Q}] = m$.

If σ is a nontrivial element of $\mathrm{Gal}(E/\mathbb{Q})$, then

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

New proof of the rationality of Three-Valued Weil Sums

Rationality

We suppose that $\mathrm{W}_{K,d}$ is three-valued, and we want to show that those three values lie in $\mathbb{Z}$.

Remark that the conclusion that $d \equiv 1 \pmod{p-1}$ will then follow immediately.

The proof of rationality given here is considerably easier than the original, given by Katz in 2012.

Rationality

Let p and q be respectively the characteristic and order of K, and so $\gcd(d, q-1) = 1$.

Let ζ_p be a primitive pth root of unity over $\mathbb{Q}$.

Let $\mathrm{W}_{K,d}(a)$ take the three distinct values A, B, and C, respectively, for N_A, N_B, and N_C values of $a \in K^\times$.

By a previous Lemma, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ permutes A, B, and C.

The field $\mathbb{Q}(A, B, C)$ is a cyclic Galois extension of $\mathbb{Q}$ since it is contained in the cyclic extension $\mathbb{Q}(\zeta_p)$ of $\mathbb{Q}$.

Rationality

Let σ be a generator of $\mathrm{Gal}(\mathbb{Q}(A, B, C)/\mathbb{Q})$.

There are three possible actions of σ upon $\{A, B, C\}$: (i) σ is the identity permutation, (ii) σ acts transitively, or (iii) σ permutes a pair of these elements, and fixes the third.

As A, B, and C are algebraic integers, they lie in $\mathbb{Z}$ if and only if they lie in $\mathbb{Q}$, and this occurs precisely in Case (i), it suffices to show that Cases (ii) and (iii) are impossible

Rationality

In Case (ii), an intermediate result tells us that $N_A = N_B = N_C$, so they all equal $(q-1)/3$.

Then a previous Lemma shows that $N_A A + N_B B + N_C C = q$, so that $A + B + C = 3 + \frac{3}{q-1}$.

As $A + B + C$ is fixed by σ, it lies in $\mathbb{Q}$, and is at the same time an algebraic integer, so it lies in $\mathbb{Z}$.

This means that $q - 1 \mid 3$, which forces $p = 2$, in which case $\zeta_p = -1$, and so the values of $\mathrm{W}_{K,d}$ lie in $\mathbb{Z}$, contradicting our supposition that σ permutes them nontrivially.

So Case (ii) is impossible.

The end

Thank you for your attention