TRICKS AND TIPS AROUND WEIL SUMS PART ONE : RECENT RESULTS (DRAFT VERSION)

PAVLE MICHKO

Abstract. Recently, Daniel Katz and Tao Feng proved a important conjecture about the Fourier spectra of power permutations in characteristic two. In this note[1], I report on their nice ideas and all the folklore that I know.

Let L be a finite field of characteristic p and order q. One defines the Fourier coefficient of a polynomial mapping $f \in L[X]$ at a point $a \in L$ by means of the canonical additive character of L by :

$$\widehat{f}(a) = \sum_{x \in L} \mu(f(x) - ax)$$

Remark 1. *The minus sign that appears in the definition of the Fourier coefficient is not usual but there are several good reasons to adopt it.*

Strictely speaking, $\widehat{f}(a)$ is the Fourier coefficient of the complex map $\mu \circ f$ at the additive character $\mu_a \colon x \mapsto \mu(ax)$, the reason why probably certain authors prefer to refer as *Weil sum*. We are mainly interested by the values of Weil sums in the case of monomial. Given a positive integer d, the Fourier coefficient of the power mapping x^d is denoted

$$\mathrm{W}_{L,d}(a) = \sum_{x \in L} \mu(x^d - ax)$$

Remark 2. *In the paper, I use d for any exponent, and s for invertible exponent. In this case, t denotes the inverse of s modulo $q-1$:*

$$st = 1 \pmod{q-1}.$$

The Fourier coefficient at 0 is said in phase, the other are out phase.

Remark 3. *Like for any permutation π, the phase Fourier coefficient of any power permutation is null,*

$$\widehat{\pi}(0) = \sum_{x \in L} \mu(\pi(x)) = \sum_{x \in L} \mu(x) = 0.$$

An exponent s is said r-valued if the number of distinct out-phase Fourier coefficients is r. Daniel Katz and Tao Feng proved recently the Theorem below

Date: start january 2013, last revision September 16, 2014.

Theorem 1. *If $[L:\mathbb{F}_2]$ is a power of two then an invertible exponent is not three valued.*

The proof of this proposition is in two parts coming from complementary papers. Tao Feng [17] proved the above theorem assuming the vanishing of Weil sums. Daniel Katz [7] proved that at least one of the outphase Fourier coefficient is null for a three valued exponent. Most of their ingredients works in odd characteristic but, for $p > 3$, the above theorem is still a conjecture.

Conjecture 1. *If $[L:\mathbb{F}_p]$ is a power of two then the spectrum of an invertible exponent is not three valued.*

This conjecture as a lot of results concerned by by three valued spectra would be an immediate consequence of the following :

Conjecture 2 (symetric)**.** *If the spectrum of an invertible exponent takes 3 values then the nonzero values are opposite.*

Contents

1. Fourier coefficient

The Fourier coefficient at a point $a \in L$ of a complex function F defined over L is

$$\widehat{F}(a) = \sum_{x \in L} F(x)\bar{\mu}(ax)$$

Remark 4. *$\widehat{F}(a)$ is a scalar product. The additive characters of L form an orthogonal basis of the complex mappings of domain L.*

As said the Weil sum $\widehat{f}(a)$ is nothing but the Fourier coefficient of $\mu \circ f$ and they satisfy general rules. Like inversion formula

$$\sum_{a\in L} \widehat{F}(a)\mu(ax) = qF(x)$$

or more generally the Poisson formula over an additive subgroup S of L

$$\sum_{a\perp S} \widehat{F}(a)\mu(ax) = \frac{q}{|S|}\sum_{x\in S} F(x+s)$$

In this context, one introduces the convolutional product of two complex mappings F and G at $z \in L$ is defined by:

$$F * G(z) = \sum_{x+y=z} F(x)G(y)$$

The $\mathbb{C}$-algebra of complex maps equiped with this product is usually denoted by $\mathbb{C}[L]$, it has δ_0 for unit element.

Note that the k-th iteration

$$F^{[k]}(z) = \sum_{x_1+\cdots+x_k=z} F(x_1)F(x_2)\cdots F(x_k)$$

and one has the well known trivialisation formulas

$$\widehat{F * G}(a) = \widehat{F}(a)\widehat{G}(a), \qquad q\widehat{FG}(a) = \widehat{F} * \widehat{G}(a),$$

Remark 5. *The left part says that the Fourier transform is an isomorphism from $\mathbb{C}[L]$ into $\mathbb{C}^L$,*

$$\widehat{\delta_0} = 1, \quad \widehat{1} = q\delta_0.$$

2. Spectrum

Let f be a polynomial. The distribution of the Fourier coefficients is called the spectrum of f. The spectrum of a power permutation f is very particular in the sense that :

$$\widehat{f_b}(a) = \widehat{f}(ab^{-t}), \quad f(x) = x^s, \quad st = 1 \pmod{q-1}.$$

Problem 1. *Characterize the map f such that the spectrum of f is equal to the spectrum of bf for all $b \in L^\times$.*

Note that the values and the multiplicities of the Weil sums of exponent s do not change if we replace s by ps or $1/s$. We say that $s' \sim s$ if there exists j such that $s' = p^j s \pmod{q-1}$, and $s' \approx s$ if $s' \sim s$ or $s' \sim 1/s$.

Assuming a r-valued exponent, denoting by σ_i the symmetric functions of the r-values says $A_1, A_2, \ldots, A_r$ that is

$$\sigma_0 = 1, \quad \sigma_1 = -\sum_{i=1}^{r} A_i, \quad \ldots \quad , \quad \sigma_r = (-1)^r \prod_{i=1}^{r} A_i,$$

for all a in K :

$$\sum_{i=0}^{r} \sigma_i \widehat{f}(a)^{r-i} = \sigma_r \delta_0(a) \tag{1}$$

by inversion, denoting the n-th convolutionnal power of $\mu \circ f$ by

$$f^{[n]}(z) = \sum_{x_1+\ldots+x_n=z} \mu(f(x_1) + \ldots + f(x_n))$$

for all t in K

$$q \sum_{i=0}^{r} \sigma_i(A_1, \ldots, A_r) f^{(r-i)}(z) = \sigma_r(A_1, \ldots, A_r) \tag{2}$$

In particular, q divides $\prod_{i=1}^{r} A_i$.

Conjecture 3 (Helleseth vanishing conjecture)**.** *If $s \equiv 1 \pmod{p-1}$ then one the spectrum vanishes i.e. one of the A_i's is null.*

Aubry and Langevin got a microscopic step in this direction but it is also one of the rare result obtained in this context !

Theorem 2. *Let L be a field of cardinal $q > 2$. If f is a power permutation of L of exponent $s \equiv 1 \mod (p-1)$ then it exists $a \neq 0$ such that $\widehat{f}(a) \equiv 0 \pmod 3$.*

I recently propose the following optimist version :

Conjecture 4. *Let L be a field of cardinal $q > 2$. Let s be coprime with $q-1$, t the inverse of s modulo $q-1$. There exists $a \neq 0$ such that*

$$\sum_{x \in L} \mu_{\mathbb{F}_p}\big(\mathrm{trace}_L(x^s)^t + \mathrm{trace}_L(ax)\big) = 0.$$

This strange idea come naturally by introducing the new additive law

$$x \oplus y = (x^s + y^s)^t$$

Hence, the exponential sums of argument $\mathrm{trace}_L(x^s)^t - \mathrm{trace}_L(ax)$ is nothing but the scalar product of two additive characters of a "bifield". Finaly, it false, the smaller counter exemple has parmeters : $p = 5$, $s = 3$, $q = 5^3$, and the distribution of the sums are:

-30	-20	-15	-10	-5	5	10	15	20
1	3	10	21	21	28	21	10	9

3. Action of the Galois group

The Galois group of $\mathbb{Q}(\zeta_p)$ acts over the Fourier coefficient. Let σ_v be an element of the Galois group of $\mathbb{Q}(\zeta_p)$.

$$\sigma_v(\widehat{f}(a)) = \widehat{f}(av^{1-t}) \tag{3}$$

this shows that the Fourier coefficient are real numbers, and integral when $s \equiv 1 \mod p-1$.

Proposition 1 (Helleseth)**.** *The spectrum of x^s is integral if and only if is congruent to 1 modulo $p-1$.*

Proof. Let v be an element of order $p-1$. Let us denote $w := v^{1-t}$. The order of w is from the rationnality and (3), we deduce

$$\widehat{f}(a) = \sigma_v(\widehat{f}(a)) = \widehat{f}(aw)$$

by inversion we get

$$\begin{aligned} q\mu(x^s) &= \sum_{a\in L} \widehat{f}(a)\mu(ax) \\ &= \sum_{a\in L} \widehat{f}(aw)\mu(ax) \\ &= \sum_{a\in L} \widehat{f}(aw)\mu(awx/w) \\ &= q\mu((x/w)^s) \end{aligned}$$

whence $w^s = 1 = v^{1-t^s} = v^{s-1}$ i.e $s = 1 \pmod{p-1}$. □

The degree of the field generated by the Weil sums is shortly say the degree of s.

Remark 6. *In the case of $p \equiv 3 \pmod 4$ the degree of s is not equal to 2.*

Proposition 2. *The spectrum of x^s is quadratic if and only $p \equiv 1 \pmod 4$ and $(s-1, p-1) = \frac{p-1}{2}$.*

Proof. Let v be an element of order $\frac{p-1}{2}$. Let us denote $w := v^{1-t}$. Like in the previous proof, we get $s \equiv 1 \pmod{\frac{p-1}{2}}$. Since s is invertible, in the case of $p \equiv 3 \pmod 4$, we recover that $s = 1 \pmod{p-1}$. □

4. Action of Frobenius

Let f be a power mapping. The Frobenius of L maps $x \mapsto x^p$ commutes with the trace.

$$\widehat{f}(a^p) = \widehat{f}(a) \tag{4}$$

Let K be a subfield of L. If $[L:K]$ is a power of a prime $\ell \neq p$ then for all $a \in K$,

$$\begin{aligned} \widehat{f_L}(a) &= \sum_{x\in K} \mu_K([L:K]x^s - \mathrm{T}_{L/K}(a)x) + \cdots \\ &\equiv \widehat{f_{[L:K]}}_K(\mathrm{T}_{L/K}(a)) \mod \ell. \end{aligned}$$

Remark 7. *In the case where the spectrum is integral the values over the prime field*

$$\forall a \in \mathbb{F}_p, \quad \widehat{f_L}(a) \equiv p \quad or \quad 0 \pmod{\ell}$$

Now, we establish the analogue result in the quadratic case. We start from the well known quadratic Gauss sums:

$$\sum_{x \in Q} \mu_{\mathbb{F}_p}(ux) = \begin{cases} \kappa, & u \text{ is a square} \\ \frac{p-1}{2}, & u = 0 \\ \bar{\kappa}, & u \text{ is not a square} \end{cases}$$

where Q is the subgroup of squares and $\kappa = \frac{-1+\sqrt{p^*}}{2}$.

Let s having a quadratic spectrum. We know that $s = 1 + k\frac{p-1}{2}$ with k odd.

$$\begin{aligned} \widehat{f_L}(a) &\equiv 1 + \sum_{x \in \mathbb{F}_p{}^\times} \mu(x^s - ax) \pmod{\ell} \\ &\equiv 1 + \sum_{x \in \mathbb{F}_p{}^\times} \mu(x^s - \alpha x) \pmod{\ell} \\ &\equiv 1 + \sum_{x \in Q} \mu((1-\alpha)x) + \sum_{x \in N} \mu(-(1+\alpha)x) \pmod{\ell} \end{aligned}$$

Now, up to conjugaison, this sum takes three values 0, $\kappa + \frac{p+1}{2}$, and $1+2\kappa$. In all, the spectrum takes 5 values modulo ℓ.

5. Two valued spectrum

In the paper, if A denotes a Fourier coefficient then N_A denotes its multiplicity. We will say the spectrum of the exponent s is r-valued, integral, quadratic etc...

Proposition 3. *If the spectrum of s is two valued then s is linear whence one valued.*

Proof.

$$\{ \begin{array}{ccccc} N_A A & + & N_B B & = & q \\ N_A A^2 & + & N_B B^2 & = & q^2 \end{array} \tag{5}$$

$$N_A = q(B-q)/A(B-A) \quad N_B = q(q-A)/B(B-A) \tag{6}$$

case 1. The spectrum is integral. Let A and B the two values, let N_A and N_B their multiplicities of A. We solve the system and

$$q - 1 = N_A + N_B = \frac{q(B^2 - A^2) + q^2(A - B)}{AB(B - A)} = q\frac{A + B - q}{AB}$$

We know that q divides AB. If $s \not\sim 1$ then A and B have absolute value less than $q - p$and the RHS is too small.

case 2. The spectrum is quadratic. In this case, A and B are conjugate, their common mulptiplicity $\frac{q-1}{2}$ impossible except the trivial case $q = 3$. $\square$

6. Power moment of Weil sums

We introduce the moment of Weil sums

$$P_r = \sum_{a \in K} \widehat{f}(a)^r \tag{7}$$

The first values are well known

$$P_1 = q, \quad P_2 = q^2 \tag{8}$$

Assuming a three valued spectrum, we get a recursion formula :

$$P_k = (A + B)\, P_{k-1} - AB\, P_{k-2} \tag{9}$$

In particular,

$$\begin{aligned} P_3 &= (A+B)q^2 - ABq \\ P_4 &= (A+B)P_3 - ABq^2 \end{aligned}$$

The sums P_k are connected by convolution to the character sums :

$$\begin{aligned} P_k &= q \sum_{x_1+x_2+\cdots+x_{k-1}+z=0} \mu(x_1^s + x_2^s + \cdots + x_{k-1}^s + z^s) \\ &= P_{k-1} + q \sum_{z \neq 0} \sum_{x_1+x_2+\cdots+x_{k-1}+z=0} \mu(x_1^s + x_2^s + \cdots + x_{k-1}^s + z^s) \\ &= P_{k-1} + q^2 V_{k-1} - q^{k-1} \end{aligned}$$

where V_k is the number of solutions of

$$\left\{ \begin{array}{ccccccccc} x_1 & + & x_2 & + & \cdots & + & x_k & + & 1 = 0 \\ x_1^s & + & x_2^s & + & \cdots & + & x_k^s & + & 1 = 0 \end{array} \right.$$

In particular, using Daniel's notation $V := V_2$:

$$\begin{aligned} P_3 &= (A+B)q^2 - ABq \\ P_3 &= P_2 + q^2 V_2 - q^2 \\ &= q^2 V \end{aligned}$$

$$V_2 = A + B - \frac{AB}{q} \implies [K : \mathbb{F}_p] + \epsilon(p) \leq a + b$$

where $\epsilon(p) = 1$ if $p = 2$ (immediate) or 3 (more tricky).

7. sum over subfields

Let F be a subfield of L,

$$\begin{aligned}\sum_{a \perp F} \widehat{f_b}(a) &= |F| \sum_{x \in F} \mu_b(x^d) \\ &= q\delta_{F^\perp}(b)\end{aligned}$$

Let G be a subgroup of $L^\times$,

$$\sum_{x \in G} \widehat{f}(ax) = \frac{|G|}{q-1} \sum_{\chi \perp G} F(\chi)\bar{\chi}(a)$$

In particular, if $G = K^\times$ then the Gauss sums are equal to $\sqrt{q}$ and we get

$$\begin{aligned}\sum_{x \in K} \widehat{f}(ax) &= \frac{q}{\sqrt{q}+1} \sum_{\chi \in K^\times} \chi(a) \\ &= q\delta_{K^\times}(a)\end{aligned}$$

8. Partial sums

Since $s \equiv 1(p-1)$, the distribution of $x \mapsto \mathrm{T}_{K/\mathbb{F}_p}(x^s)$ is well balanced over any subspace. Writing

$$n_r(S) = \sharp\{x \in S \mid \mathrm{T}_{K/\mathbb{F}_p}(x^s) = r\}, n_0(S) + (p-1)n_1(S) = p^k$$

$$\begin{aligned}\sum_{x \in S} \mu(x^s) &= \sum_{i=0}^{p-1} n_i(S)\zeta^i = n_0(S) - n_1(S) \\ &= pn_1(S) \\ &= \frac{1}{p^{m-k}} \sum_{s \perp S} \widehat{f}(s)\end{aligned}$$

9. Daniel Katz's result

In his paper [7], Daniel Katz proves that a three valued spectrum is necessary integral. In particular, it must be congruent to 1 modulo $p-1$. From this rather long and hard job, he deduces that one of the outphase Fourier coefficient is equal to zero.

Proposition 4. *An invertible exponent s is three valued is rational and thus congruent to 1 modulo $p-1$.*

Proof. We assume three distincts values A, B and C in the spectrum. The multiplicity of C falls by summing on the $(\widehat{f}(a)-A)(\widehat{f}(a)-B)$:

$$N_C = \frac{q^2-(A+B)q+(q-1)AB}{(C-A)(C-B)}$$

1. Since the Galois group af $\mathbb{Q}(\zeta_p)$ acts over the Fourier coefficients three valued spectrum implies that the degree of the $\mathbb{Q}(A,B,C)$ is less or equal to 3. If the degree of this extension is three then all the values have the same multiplicity $\frac{q-1}{3}$ whence

$$\frac{q-1}{3}(A+B+C) = q$$

which is clearly impossible. If the degree is two, then $p \equiv 1 \pmod 4$, and one of them, say C, is rational and the other are conjugate $A = a+b\sqrt{p}$ and $B = a-\sqrt{b}$, using Parseval relation and (**??**) with $\lambda_1 = 1$ and $\lambda_2 = -1$, we get

$$N_C C^2 + 2N_A(a^2+b^2p) = q^2;$$
$$N_C C^2 + 2N_A(a^2-b^2p) = 0.$$

By adding, we get

$$2N_C C^2 + 4N_A a^2 = q^2$$

that shows that $a \neq 0$. Since p is totaly ramified, or by a direct computation

$$\mathrm{val}_p(A) = \mathrm{val}_p(B) = \begin{cases} \mathrm{val}_p(a), & \mathrm{val}_p(a) \leq \mathrm{val}_p(b); \\ \frac{1}{2} + \mathrm{val}_p(b), & \mathrm{val}_p(a) > \mathrm{val}_p(b); \end{cases}$$

By J-set theory, we know that the p-adic valuation of the Fourier coefficients are not equal. The relation

$$N_A = \frac{q^2-(B+C)+(q-1)BC}{(A-C)(A-B)}$$

proves that $\mathrm{val}_p(C) < \mathrm{val}_p(A)$ and $\mathrm{val}_p(a) > \mathrm{val}_p(b)$. This implies $|a| \geq pb$. By substracting, we get

$$4N_A b^2 = q^2$$

we finally get a contradiction

$$q^2 > 4N_A a^2 \geq 4N_A p^2 b^2 = q^2$$

2. We continue with the arguments of Daniel. Assuming a three valued spectrum, the out-phase Fourier coefficients satisfies :

$$\widehat{f}(a)^3 - (A+B+C)\widehat{f}(a)^2 + (AB+BC+CA)\widehat{f}(a) - ABC = 0 \tag{10}$$

Note that $s = 1 \mod p-1$ is odd.

$$\begin{aligned}\sum_{a\in K}\widehat{f}(a)^3 &= \sum_a\sum_{x,y,z}\mu(x^s+y^s+z^s-a(x+y+z))\\ &= q\sum_{x,y}\mu(x^s+y^s-(x+y)^s)\\ &= q^2+q\sum_{x\neq 0,y}\mu(x^s+y^s-(x+y)^s)\\ &= q^2+q\sum_{x\neq 0,y}\mu_x(1+y^s-(1+y)^s)\\ &= q^2+q\big((q-1)V-(q-V)\big)\\ &= q^2V\end{aligned}$$

where V is the number of roots in K of the polynomial $1+T^s-(1+T)^s$. We get

$$q^2V = (A+B+C)q^2-(AB+BC+CA)q+ABC(q-1) \tag{11}$$

Assuming no Fourier coefficient equal to 0 or q, the term ABC has the minimal p-adic valuation i.e. more than $2v$.

$$\mathrm{val}_p(ABC)\geq 2q \Longrightarrow \mathrm{val}_p(AB)\geq \mathrm{val}_p(q)+1$$

Consequently, the valuation of AB, AC and BC are greater than the valuation of q whence all this products are in absolute value greater than q.

One may assumes that

$$AB<0,\quad |A|\leq B<|C| \tag{12}$$

Let N_C the multiplicity of C

$$\begin{aligned}\sum_{a\in K^\times}(\widehat{f}(a)-A)(\widehat{f}(a)-B) &= q^2-(A+B)q+AB\\ &= N_C(C-A)(C-B)\end{aligned}$$

since $(C-A)(C-B)$ is positive, we get the positivity of $q^2-(A+B)+AB$ implying $AB\geq -2q$ whence a contradiction!

□

10. Tao Feng's trick

From now and on, s is a three valued invertible exponent : it takes three values 0, A, and B over a finite field L of order $q=p^m$, p prime. Recall that s is congruent to 1 modulo $(p-1)$.

$$A = p^a\alpha, \quad B = p^b\beta, \quad A - B = p^c\gamma$$

with α, β and γ coprime with p.

$$\widehat{f_b}(a) = \sum_{x\in K} \mu(bf(x) - ax)$$

Let N_A the multiplicity of A, N_B those of B in the spectrum of f. We solve the system

$$\{ \begin{array}{ccccc} N_A A & + & N_B B & = & q \\ N_A A^2 & + & N_B B^2 & = & q^2 \end{array} \tag{13}$$

$$N_A = q(B-q)/A(B-A) \quad N_B = q(q-A)/B(B-A) \tag{14}$$

and

$$N_A + N_B = \frac{q(B^2 - A^2) + q^2(A-B)}{AB(B-A)} = q\frac{A+B-q}{AB}$$

Let us denote by $N(u,v)$ the number of solutions of the system

$$\{ \begin{array}{ccccc} x & + & y & = u \\ x^s & + & y^s & = v \end{array}$$

We have

$$N(u,v) = \frac{1}{q^2}\sum_{a,b} \widehat{f_b}(a)^2\mu(au+bv)$$

whence

$$q^2 \sum_{u\neq 0,v} N(u,v)^2 = \sum_{a,b\neq 0} \widehat{f_b}(a)^4 \tag{15}$$

When $u^s + v \neq 0$, we also have

$$0 = \sum_{a,b} \widehat{f_b}(a)\mu(au+bv) \tag{16}$$

By the formulas (14) the number $\Delta := \alpha\beta\gamma$ divides $q-A$ and $q-B$, and Feng's trick starts by using the above like identities to get the divisibility of $N(u,v)$ by $\beta\gamma$ and $\alpha\beta$ and finally by Δ.

Considering the map $v \mapsto N(u,v)$, with $u \neq 0$, we see that

$$\sum_v N(u,v) = q$$
$$\sum_v N(u,v)^2 = \sum_v N(1,v)^2$$

Note that also that $N(u,u^d)$ is equal to V. Playing with symmetries

$$q^2 \sum_{0\neq v} N(1,v)^2 = P_4 = (A+B)q^2V - ABq^2$$

$$\begin{aligned}(A+B)V - AB - V^2 &= -(V-A)(V-B)\\ &= -(q-V)AB/q\\ &= q^{-2}P_4 - V^2\\ &= \sum_{v\neq u^d} N(u,v)^2\\ &\geq \Delta \sum_{v\neq u^d} N(u,v)\\ &= \Delta(q-V)\end{aligned}$$

The inequality is in fact an equality

$$-AB/q = \Delta, \quad |A-B| = p^c$$

and very surprisingly,

$$\forall v \neq 1, \quad N(1,v) = 0 \,\text{or}\, \Delta := \alpha\beta. \tag{17}$$

10.1. **the hard case.** Note that

$$|A-B|q \leq p^{a+b+c}$$

A very easy case corresponds to $a \neq b$, for example when p divides V. One gets a contradiction because this assumption implies that $a = c \leq \frac{m}{2}$ and the above inequality leads to $a > \frac{m}{2}$.

The hardest case corresponds to $a = b = \frac{m}{2} =: t$.

$$A = p^t\alpha, \quad B = p^t\beta, \quad |\beta - \alpha| = p^c. \tag{18}$$

The multiplicity of the $N(1,v)$

$$\lambda = \frac{(p^t-\alpha)(p^t-\beta)}{\alpha\beta}$$

10.2. **more about α, β.**

$$f(x) = \frac{\alpha}{p^t} \sum_{a \in A} \mu_a(x) \mod \beta$$

whence

$$1 = \frac{\alpha^2}{q} \sum_{c \in L} N(c) \mu_c(x) \mod \beta$$

where $N(c) = \sharp\{(x,y) \in A \times A \mid y - x = c\}$. We deduce that :

$$\forall c \in L^\times,\ N(c) \equiv 0, \quad N(0) \equiv N_A^2, \quad \alpha N_A = \pm p^t \mod \beta.$$

Note that

$$N_A = \frac{q(B-q)}{A(B-A)} \equiv \frac{q}{\alpha^2}$$

so

$$\alpha N_A \equiv \frac{q}{\alpha} \mod \beta$$

whence

$$\alpha = \pm p^t \mod \beta.$$
$$p^c = \pm p^t \mod \beta.$$

11. Another conjecture

Let us denotes by $M_r(s)$ the number of v having r pre-images by x^s. Actually, I don't know if it is possible to find some exponents s such that $M_2 = 0$ in odd characteristic ! Moreover, I run a program [15] to find all the exponents s satisfying the condition

$$s \equiv 1 \pmod{p-1}, \quad \sharp\{r \mid M_r(s) > 0\} \leq 3, \quad q \leq 2^{32}.$$

In odd charactetistic all the solutions have the same shape : $M_2(s) > 0$. Of course, for such s the spectrum cannot be three-valued.

Conjecture 5 (differentiability)**.** *If f be a power function in odd characteristic such that the number of solutions of the system of equations*

$$x^s + y^s = v, \quad x + y = u.$$

takes 3 values then $M_2(f) > 0$.

Remark 8. *In even characteristic, 4-uniform differentiability is possible. The above conjecture claims (in particular) that uniform differentiability is not possible in odd characteristic. Why that ?*

Actually, one can detail $N(u,v)$ when $v \neq u^s$. Let us denote by $n(v)$ the number of x, y in $K^\times$ such that $x^s + y^s = v$ and $x + y = u$.

Problem 2. *Let $n_s(v)$ be the number of preimages of v by $x \mapsto x^s + (1-x)^s$. We are interested by the exponents s such that $n_s(v)$ takes only two values over $K \setminus \{0,1\}$.*

One has a Jacobi interpretation of these numbers.

$$\begin{aligned} n(u,v) &= \frac{1}{(q-1)^2} \sum_{x+y=u} \sum_{X+Y=v} \sum_{\chi,\psi} \chi(x^s/X)\psi(y^s/Y) \\ &= \frac{1}{(q-1)^2} \sum_{\chi,\psi} \sum_{x+y=u} \sum_{X+Y=v} \chi(x^s)\psi(y^s)\bar{\chi}(X)\bar{\psi}(Y) \\ &= \frac{1}{(q-1)^2} \sum_{\chi,\psi} J(\chi^s,\psi^s)J(\bar{\chi},\bar{\psi})\chi\psi(u^{-s})\chi\psi(v) \end{aligned}$$

References

[1] A. R. Calderbank and Gary McGuire. Proof of a conjecture of sarwate and pursley regarding pairs of binary m-sequences. *IEEE Transactions on Information Theory*, 41(4):1153–1155, 1995.

[2] A. R. Calderbank, Gary McGuire, Bjorn Poonen, and Michael Rubinstein. On a conjecture of Helleseth regarding pairs of binary m-sequences. *IEEE Trans. Inform. Theory*, 42(3):988–990, 1996.

[3] Florent Chabaud and Serge Vaudenay. Links between diffrential and linear cryptanalysis. *Eurocrypt 94*, 950:356–365, 1994.

[4] John F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, Univ. of Maryland, 1974.

[5] Tor Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.

[6] Tor Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.

[7] Daniel J. Katz. Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth. *J. Combin. Theory Ser. A*, 119(8):1644–1659, 2012.

[8] Daniel J. Katz. Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth. *J. Comb. Theory, Ser. A*, 119(8):1644–1659, 2012.

[9] Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.

[10] Selçuk Kavut, Subhamoy Maitra, and Melek D. Yücel. Search for boolean functions with excellent profiles in the rotation symmetric class. *IEEE Transactions on Information Theory*, 53(5):1743–1751, 2007.

[11] Kononen Keijo, Rinta-Aho Marko, and Vaanainen Keijoe. On integer value of Kloosterman sums. *IEEE trans. info. theory*, 2010.

[12] Gilles Lachaud and Jacques Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305:881–883, 1987.

[13] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, 1990.

[14] Philippe Langevin. Numerical projects page: spectra of power maps., 2007. `http://langevin.univ-tln.fr/project/spectrum`.

[15] Philippe Langevin. Numerical projects page : nice exponents., 2013. `http://langevin.univ-tln.fr/project/expo`.

[16] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, 1983.

[17] Feng Tao. On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights. *Designs, Codes and Cryptography*, 62(3), 2012.

E-mail address: pavle.michko@mapix.euphoria.fr