TRICKS AND TIPS AROUND WEIL SUMS
PART TWO : FOLKLORE
DRAFT

PAVLE MICHKO

ABSTRACT. In this note[1], I report all the basic algebra that can be used in the context of Weil sums.

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. *After several hesitation, I finally adopted the the minus sign in the definition of the Fourier coefficient.*

Strictly speaking, $\widehat{f}(a)$ is the Fourier coefficient of the complex map $\mu \circ f$ at the additive character $\mu_a \colon x \mapsto \mu(ax)$.

CONTENTS

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

1. Weil sum

We are mainly interested by the values of these sums in the case of f is a monomial. The Fourier coefficients falls in Weil sums with binomial argument. Given a positive integer d, the Fourier coefficient of the power mapping x^d is denoted

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

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 $q-1$:*

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

In that case, I also use the notation $f\colon x \mapsto x^s$ and $g\colon x \mapsto x^t$.

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.

2. Characterization

Several conjecture are proposed in the litterature concerning Weil sums with binomial argument. A possible argument resides in the following elementary fact

$$\begin{aligned}\widehat{f_b}(a) &= \sum_{x\in L} \mu(bx^s + ax)\\ &= \sum_{x\in L} \mu(x^s + ab^{1-t}x)\\ &= \widehat{f}(ab^{1-t}\end{aligned}$$

It appears that the spectrum of bf is a permutation of those of f.

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

3. Kernel trick

Assuming a r-valued spectrum,

$$\prod_{i=1}^{r}(\widehat{f}(a)-A_i)\times\widehat{f}(a)=0$$

whence $(f-A_1\delta_0)*\cdots*(f-A_r\delta_0)$ is in the kernel of the convolution by f i.e. the space generated by the μ_z with $z\in Z=\{a\mid\widehat{f}(z)=0\}$.

$$\sum_{i=0}^{r}\sigma_i(A_1,\ldots,A_r)f^{[r-i]}=\sum_{z\in Z}x_z\mu_z \tag{1}$$

Using Fourier transformation

$$\sum_{i=0}^{r}\sigma_i(A_1,\ldots,A_r)\hat{f}(a)^{r-i}=q\sum_{z\in Z}x_z\delta_z(a) \tag{2}$$

one sees that all the coefficient x_a are equal to $\sigma_r(A_1,\ldots,A_r)/q$.

$$\sum_{i=0}^{r}\sigma_i(A_1,\ldots,A_r)f^{[r-i]}=\frac{\sigma_r(A_1,\ldots,A_r)}{q}\sum_{z\in Z}\mu_z \tag{3}$$

It is possible to show that when $r=2$ then x_a is an integer.

Remark 4. *I do not know if the $x_a=\frac{1}{q}\prod_{i=1}^{r}A_i$ is an integer.*

4. Symmetry

Now, we symply check our formulas.

$$\widehat{\widehat{F}}(a)=\sum_{x\in K}\sum_{y\in K}F(y)\bar{\mu}(xy)\bar{\mu}(ax)=q\sum_{a+y=0}F(y)=qF(-a)$$

In odd characteristic disymmetry appears ! Let us denote by Z the indicating function of Z.

First we write (3) as :

$$\sum_{i=0}^{r}\sigma_i(A_1,\ldots,A_r)f^{[r-i]}(a)=\frac{\sigma_r(A_1,\ldots,A_r)}{q}\hat{Z}(-a)$$

Remark 5. *No trouble minus signing here !*

And, we re-apply the Fourier transform again :

$$\begin{aligned}\sum_{i=0}^{r}\sigma_i(A_1,\ldots,A_r)\hat{f}(a)^{r-i}&=\frac{\sigma_r(A_1,\ldots,A_r)}{q}\hat{\hat{Z}}(a)\\&=\sigma_r(A_1,\ldots,A_r)Z(a)\end{aligned}$$

Now, if $\widehat{f}(a) = 0$ then the left-hand side is equal to the product $\sigma_r(A_1, \ldots, A_r)$ and thus :

$$\forall a \in K, \quad Z(a) = Z(a).$$

5. Waring formula

$$A^n + B^n = \sum_{j=0}^{n/2} (-1)^j \frac{n}{n-j} \binom{n-j}{j} (AB)^j (A+B)^{n-2j}$$

In general, denoting by

$$S_k = x_1^k + x_2^k + \cdots + x_n^k$$

then

$$S_k = \sum_{i_1+2i_2+\cdots+ni_n=k} (-1)^{i_2+i_4+\cdots} \times \frac{(i_1+i_2+\cdots+i_n-1)!k}{i_1!i_2!\cdots i_n!} \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$$

This fact can be used to proof that if $f \in K[X]$ has degree d then there exists $d-1$ algebraic numbers ω_i such that for any extension L of degree r of K, one has

$$S(f, L) = \sum_{x \in L} \mu_L(f(x)) = -[\omega_1^r + \omega_2^r + \ldots + \omega_{d-1}^r]$$

In fact these numbers are Weil numbers and they have absolute value $\sqrt{q}$.

6. Kloosterman sum

$$\mathrm{kloos}_L(a) = \sum_{x \in L^\times} \mu(\frac{1}{x} - ax)$$

and one has the Weil bound

$$||\,\mathrm{kloos}_L(a)|| \leq 2\sqrt{q}.$$

It is now known that Kloosterman sum does not vanish in characteristic $p > 3$. At the opposite, according to my knowledge, there is no simple proof of the fact that Kloosterman sums vanish when $p = 2$ or $p = 3$.

Let $f(x) = x^s$ be a pwer mapping and let $h(x) = x^{-d}$

$$\begin{aligned}
\sum_{a \in L} \widehat{f}(ab)\widehat{h}(a)^* &= \sum_a \sum_x \sum_y \mu(x^d - y^{-d})\mu(ax - aby) \\
&= q \sum_y \mu(b^d y^d - y^{-d}) \\
&= q\,\mathrm{kloos}_L(b^d)
\end{aligned}$$

7. Gauss sums

We denote by $\tau_K(\chi)$ the Gauss sum

$$\tau_K(\chi) = \sum_{x \in K^\times} \mu(x)\chi(x)$$

by Fourier inversion, for $x \in K^\times$:

$$\mu(x) = \frac{1}{q-1} \sum_{\chi} \tau_K(\chi)\bar{\chi}(x)$$

By a direct calculation

$$\begin{aligned}
\widehat{f}(a) &= 1 + \frac{1}{(q-1)^2} \sum_x \sum_\chi \tau_K(\chi)\bar{\chi}(x^d) \sum_{\chi'} \bar{\tau}_K(\chi')\chi'(ax) \\
&= 1 + \frac{1}{(q-1)} \sum_{\chi' = \chi^d} \tau_K(\chi)\bar{\tau}_K(\chi')\chi'(a) \\
&= 1 + \frac{1}{(q-1)} \sum_{\chi} \tau_K(\chi)\bar{\tau}_K(\chi^d)\chi^d(a)
\end{aligned}$$

In the case of an invertible exponent s, we continue :

$$\begin{aligned}
\widehat{f}(a) &= 1 + \frac{1}{(q-1)} \sum_{\chi} \tau_K(\chi)\bar{\tau}_K(\chi^s)\chi^s(a) \\
&= \frac{q}{q-1} + \frac{1}{q-1} \sum_{\chi \neq 1} \tau_K(\chi^t)\bar{\tau}_K(\chi)\chi(a) \\
&= \frac{1}{q-1} \sum_{\chi} F(\chi)\chi(a)
\end{aligned}$$

where we use the notation

$$F(\chi) = \begin{cases} q, & \chi = 1; \\ \tau(\chi^t)\bar{\tau}(\chi), & \text{else.} \end{cases}$$

It is well known that flat spectrum implies orthogonality :

$$\begin{aligned}
\sum_{a \in L^\times} \widehat{f}(ab)\widehat{f}(a)^* &= \sum_{x,y \in L^\times} \mu(x^d - y^d + a(bx - y) \\
&= q \sum_{bx = y} \mu(x^d - y^d) \\
&= q^2 \delta_1(b)
\end{aligned}$$

8. Divisibility

By Stickelgerber'scongruence theorem, for any prime $\wp$ above p in the appropriate field, we know the existence of a generator ω of $\widehat{K^\times}$ such that :

$$\tau_K(\bar{\omega}^j) \equiv \frac{(1-\zeta)^{S(j)}}{R(j)} \mod \wp^{(p-1)S(j)+1}$$

where $j = \sum_{k=0}^{m-1} j_k p^k$, $S(j) = \sum_k j_k$ and $R(j) = \prod_k j_k!$.

Let us debote by ν the minimal value :

$$\nu = \frac{1}{p-1} \min_{0<j} S(-jt) + S(j)$$

and define the J-set of s :

$$J(s) = \{0 < j \mid S(-jt) + S(j) = \nu(p-1)\} \tag{4}$$

Indeed,

$$\begin{aligned}
\widehat{f}(a) &= \frac{1}{q-1} \sum_{\chi} F(\chi)\chi(a) \\
&\equiv \frac{1}{q-1} \sum_{\chi \neq 1} \tau(\chi^t)\tau(\chi)\chi(a) \\
&\equiv \frac{1}{q-1} \sum_{j>0} \tau(\omega^{jt})\tau(\bar{\omega}^j)\omega^j(a) \\
&\equiv (1-\zeta)^\nu \sum_{j\in J} \frac{\omega^j(a)}{R(-jt)R(j)} \pmod{(1-\zeta)^{1+\nu}}
\end{aligned}$$

It follows

$$\mathrm{V}_K(s) = \frac{1}{p-1} \min_{0<j<q-1} S(-jt) + S(j)$$

Remark 6. *Using the relation*

$$\mathrm{w}_p(s) + \mathrm{w}_p(-s) = [K : \mathbb{F}_p](p-1)$$

one gets that the weight of s is smaller or equal to $(m-v)(p-1)+1$. That is also the degree of the map $x \mapsto \mathrm{T}_{K/\mathbb{F}_p}(x^s)$.

Remark 7. *If we write*

$$\widehat{f}(a) = \sum_{i=\nu}^{\infty} f_i(a) p^i$$

the degree of f_ν is less or equal to ν.

Lemma 1. *Let K be a subfield of L.*

$$\mathrm{V}_L(s) \leq [L : K] \times \mathrm{V}_K(s)$$

Proof. It is a direct consequence of Hasse-Davenport relation. □

9. J-set connection

Let J be the J-set of s.

$$\mathrm{w}_p(-jt) + \mathrm{w}_p(j) = \mathrm{w}_p(-jt) + \mathrm{w}_p(-(-jt)s)$$

It follows that

$$J(s) \ni j \mapsto -jt \in J(t)$$

This is a manifestation of the Rule

$$\widehat{f}(a) = \sum_{x \in K} \mu(x^s + ax) = \sum_{x \in K} \mu(x + ax^t) = \widehat{g}(a^{-s})$$

Since

$$\sum_{j \in J(s)} \frac{\omega^j(a)}{R(-jt)R(j)} \equiv \sum_{k \in J(t)} \frac{\omega^k(a^{-s})}{R(-ks)R(k)} \equiv \sum_{k \in J(t)} \frac{\omega^{-ks}(a)}{R(-ks)R(k)}$$

The independance of characters concludes.

$$-sJ(t) = J(s), \quad -tJ(s) = J(t).$$

10. Rayleigh quotient

The eigenvalues of the Fourier operator $f \mapsto \widehat{f}$ are $\pm\sqrt{q}$. The Rayleigh quotient of a vector x satisfy

$$-\sqrt{q} \leq R(F, x) = \frac{Ax.\overline{x}}{x.\overline{x}} \leq \sqrt{q}$$

In particular, the Rayleigh quotient of a mapping f is :

$$-q\sqrt{q} \leq \widehat{f} \times f(a) = \sum_{a \in K} \widehat{f}(a)\overline{f(a)} \leq q\sqrt{q}$$

We are interested by the

$$\begin{aligned} \widehat{f} * f(t) &= \sum_{a+b=t} \widehat{f}(a) f(a) \\ &= \sum_{a} f(-a)\widehat{f}(a)\mu(at) \end{aligned}$$

Problem 2. *What is the Rayleigh quotient of a power mapping ?*

For $b \neq 0$, by a direct calculation

$$\begin{aligned}\sum_{a\in L} \widehat{f}(ab)\bar{\mu}(a^s) &= \frac{1}{q-1}\sum_{a\neq 0}\sum_{\chi} F(\chi)\chi(ab)\bar{\mu}(a^s)\\ &= \frac{1}{q-1}\sum_{\chi} F(\chi)\chi(b)\sum_{a\neq 0}\chi(a)\bar{\mu}(a^s)\\ &= \frac{1}{q-1}\sum_{\chi} F(\chi)\chi(b)\tau(\chi^t)\chi^t(-1)\\ &= \frac{-q}{q-1} + \frac{1}{q-1}\sum_{\chi\neq 1}\tau(\bar{\chi})\tau(\chi^t)^2\chi(-b)\end{aligned}$$

The above relation can be interpreted like next. First of all the f_b are orthogonal :

$$f_b.f_c = q\delta_b(c).$$

The decomposition of $\widehat{f}$ in the basis g_b is more simple

$$\widehat{f}(a) = \sum_b \mu(b^t)g_b(a)$$

as we can check very easely

$$\sum_b \mu(b^t + ba^{-s}) = \sum_b \mu(a.b/a + (b/a)^s) = \widehat{f}(a)$$

11. More orthogonality relation

Let f be a power permutation.

$$\sum_{a\in L} \widehat{f}(a+t)\widehat{f}(a)^* = q\delta_0(t).$$

All these orthogonality relation could be make hard the existence of not symmetic small spectrum.

12. Dedekind's determinant

The convolutional endomorphism diagonalizes in the basis of addidive characters of L, the eigenvalues are precisely Fourier coefficients

$$\begin{aligned}\mu_a * F(z) &= \sum_{x+y=z} F(x)\mu(ay)\\ &= \sum_x F(x)\mu(a(z-x)\\ &= \widehat{F}(a)\mu_a(z)\end{aligned}$$

The convolution by F on the Dirac basis

$$\begin{aligned} F * \delta_a(b) &= \sum_{x+y=a} F(x)\delta_a(y) \\ &= F(b-a) \end{aligned}$$

We recover Dedekind's determinant

$$\prod_{a\in L} \widehat{F}(a) = \det[F(b-a))]_{a,b\in L} \tag{5}$$

Remark 8. *Let κ be an arbitrary complex number. Using the map $F+\kappa$, we get*

$$(\widehat{F}(0)+q\kappa) \prod_{a\in L^\times} \widehat{F}(a) = \det[\mu(F(b-a))+\kappa]_{a,b\in L} \tag{6}$$

For example, with $\kappa=-1$ A direct calculation gives

$$\begin{aligned} (\widehat{f}(0)-q) \prod_{a\in L^\times} \widehat{f}(a) &= \sum_{\sigma} \mathrm{sgn}(\sigma) \prod_{a\in L} \big(\mu(f(\sigma(a)-a))-1\big) \\ &= \sum_{\sigma\in\Phi} \mathrm{sgn}(\sigma) P(\sigma) \end{aligned}$$

where

$$\Phi = \{\sigma \mid \forall x\in L,\, \mathrm{trace}_L\big(f(\sigma(x)-x)\big)\neq 0\} \quad \text{and} \quad P(\sigma) = \prod_{a\in L} \big(\mu(f(\sigma(a)-a))-1\big).$$

Remark 9. *If $f(0)=0$ then a permutation of Φ as no fixed point.*

Remark 10. *In the case $p=2$, with $\kappa=-1$ and $f(x)\in L[X]$. A direct calculation gives*

$$\begin{aligned} (\widehat{f}(0)-q) \prod_{a\in L^\times} \widehat{f}(a) &= \sum_{\sigma} \mathrm{sgn}(\sigma) \prod_{a\in L} \big(\mu(f(\sigma(a)-a))-1\big) \\ &= 2^q \sum_{\sigma\in\Phi} \mathrm{sgn}(\sigma) \end{aligned}$$

Remark 11. *One can recover a classical divisibility result using this determinantal approach. Again, with*

$$\Phi = \{\sigma \mid \forall x\in L,\, \mathrm{trace}_L\big(f(\sigma(x)+x)\big)\neq 0\},$$

we get

$$(\widehat{f}(0)-q) \prod_{a\in L^\times} \widehat{f}(a) = \sum_{\sigma\in\Phi} \mathrm{sgn}(\sigma) P(\sigma)$$

where the p-adic valuation of the $P(\sigma)$ is greater than $q/(p-1)$.

Considering (6) as a polynomial in κ, by identification :

$$qD(f) = -\sum_{y}\sum_{\pi}\mathrm{sgn}(\pi)\mu(\sum_{x\neq y} f(\pi(x)-x))$$

As in [13], one can isolate the phase using the space orthogonal to the trivial character. It is generated by $\Delta_a = \delta_a - \delta_0$. $a \in L^\times$.

$$\begin{aligned} F * \Delta_a &= F*\delta_a - F*\delta_0 \\ &= \sum_b F(b-a)\delta_b - \sum_b F(b-0)\delta_b \\ &= \sum_{b\neq 0} \big(F(b-a)-F(b)\big)\Delta_b \end{aligned}$$

In this space

$$\prod_{a\in L^\times} \widehat{F}(a) = \det[F(b-a)-F(a)]_{a,b\in L^\times} \tag{7}$$

13. Moment of Weil sums

We introduce the moment of Weil sums

$$S_r = \sum_{a\in K} \widehat{f}(a)^r$$

The first values are well known

$$S_1 = q, \quad S_2 = q^2$$

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

$$\begin{aligned} S_k &= (A+B)\,S_{k-1} - AB\,S_{k-2} \\ S_3 &= (A+B)q^2 - ABq \\ S_4 &= (A+B)S_3 - ABq^2 \end{aligned}$$

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

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

where N_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 $V := N_2$:

$$\begin{aligned} S_3 &= (A+B)q^2 - ABq \\ S_3 &= S_2 + q^2 N_2 - q^2 \\ &= q^2 V \end{aligned}$$

$$N_2 = A + B - \frac{AB}{q} = V \implies [K : \mathbb{F}_p] + \epsilon(p) \leq a + b$$

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

14. Asymptotic

Let A be the maximal absolute value in the spectrum, and let N'_A be the number of occurences. Recall the relation (**??**)

$$P_k = P_{k-1} + q^2 N_{k-1} - q^{k-1}(q^2 N_{k-1} - q^{k-1}) \sim A^k N'_A$$

one should compare to Deligne bound.

15. Hyperplane section

Let λ_1, λ_2,...,λ_n be n elements of $L^\times$. By convolution, or a direct calculation

$$\begin{aligned} \sum_{a\in L} \prod_{i=1}^{n} \widehat{f_{\lambda_i}}(a) &= \sum_{x_1,x_2,\ldots} \mu(\sum_i x_i^s - a \sum_i \lambda_i x_i) \\ &= q \sum_{\lambda_1 x_1 + \cdots + \lambda_n x_n = 0} \mu(x_1^s + \cdots + x_n^s) \end{aligned}$$

Since s is invertible, the last character sum does not depend on μ, its values S is a non trivial contribution in the character counting of the number of solutions N the hyperplane section of the Fermat hypersurface

$$\left\{\begin{array}{rcccccccc} 0 & = & x_1^s & + & x_2^s & + & \dots & + & x_n^s \\ 0 & = & \lambda_1 x_1 & + & \lambda_2 x_2 & + & \dots & + & \lambda_1 x_n. \end{array}\right.$$

whence $qN = (q-1)S + q^{n-1}$ and

$$q^2 N = (q-1)\sum_{a\in L}\prod_{i=1}^{n}\widehat{f_{\lambda_i}}(a) + q^n \tag{8}$$

Remark 12. *Using (8) with $n = q-1$ and all the λ_i are distincts, the existtence of zero outphase Fourier coefficient is equivalent to say that $N = q^{n-2}$.*

16. Representation

To any f, we introduce the notation

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

and the matrix

$$R(f) := \frac{1}{q}\big(\widehat{f_b}(a)\big)_{b,a}$$

It is easy to check that

$$R(f\circ g) = R(f)\times R(g)$$

In particular, we have a representation of groups, and

$$\chi(f) = \frac{1}{q}\sum_{a\in L}\widehat{f_a}(a) = \frac{1}{q}\sum_{a\in L}\widehat{f}(a^{1-t}) = \mathrm{fix}(f)$$

Note that

$$\begin{aligned}\sum_{a\in L}\big|\widehat{f_a}(a)\big|^2 &= \sum_{a,x,y}\mu_a(f(x)-f(y)+x-y)\\ &= q\,\sharp\{(x,y)\mid f(x)-f(y)=x-y\}\\ &= q(q+N(q-1))\end{aligned}$$

In particular,

$$\sup_{a\in L^\times}\big|\widehat{f_a}\big|^2 \geq Nq$$

Let $\aleph(t)$ the number of preimages of t by $x\mapsto x^s - x$.

$$\aleph(t) = \frac{1}{q}\sum_{a\in L}\widehat{f_a}(a)\bar{\mu}(at)$$

$$q\sum_{t\in L}\aleph(t)^2 = \sum_{a\in L}\widehat{f_a}(a)^2$$

Remark 13. *The set of bijections having an integral spectrum is a group.*

Let G the cyclic group generated by f.
Note the pseudo-cyclic structure of $M(f) = qR(f)$:

$$\begin{array}{cccc} q & 0 & 0 & \dots & 0 \\ 0 & \widehat{f_{\chi^0}}(\gamma^0) & \widehat{f_{\chi^0}}(\gamma^1) & \dots & \widehat{f_{\chi^0}}(\gamma^{q-1}) \\ 0 & \widehat{f_{\gamma^1}}(\gamma^0) & \widehat{f_{\gamma^1}}(\gamma^1) & \dots & \widehat{f_{\gamma^1}}(\gamma^{q-1}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \widehat{f_{\gamma^{q-1}}}(\gamma^0) & \widehat{f_{\gamma^{q-1}}}(\gamma^1) & \dots & \widehat{f_{\gamma^{q-1}}}(\gamma^{q-1}) \end{array}$$

One has the relation

$$M(f)\sum_{g\in G} M(g) = \sum_{g\in G} M(g) =: \Sigma(f)$$

Remark 14. *What is the ring generated by the $M(g)$?*

17. 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

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

18. 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

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

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

19. Open problem

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

$$\left\{\begin{array}{ccccc} N_AA & + & N_BB & = & q\\ N_AA^2 & + & N_BB^2 & = & q^2\end{array}\right. \tag{9}$$

$$N_A = q(B-q)/A(B-A) \quad N_B = q(q-A)/B(B-A) \tag{10}$$

and

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

20. Multiplicities

Let us denotes by $M_r(s)$ the number of v having r pre-images by f. Actually, we don't know if it is possible to find some exponents s such that $M_2 = 0$!

I run a program to find all the exponent s satisfying the condition

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

all of them have the same shape $M_2(s) > 0$. Of course, for such s the spectrum cannot be three-valued.

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 $x + y = u$.

We use

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

Problem 3. *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 $K \setminus \{0,1\}$.*

21. Turyn's result

I recall here charcater sums divisibility results that can be useful in this context.

Proposition 1. *Let S be a cyclic group of order N. Let f be an integral mapping over S. Let χ be acharacter of order b. If $\widehat{f}(\chi) \neq 0$ is divisible by an positive integer m then*

$$m \leq \frac{2^{\mathrm{rad}(b)}N\|f\|_\infty}{b}.$$

Moreover, if f is positive

$$m \leq \frac{2^{\mathrm{rad}(b)}N\|f\|_\infty}{2b}.$$

where $\mathrm{rad}(b)$ *denotes the number of prime divisors of b.*

22. vanishing conjecture

A few words, on the vanishing conjecture :

Conjecture 1 (Helleseth)**.** *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 $\widehat{f}(a) = 0$.*

The congruence modulo $p-1$ is essential. It ensures that the Weil sums are rational integers. Moreover, one knows bu [11] that the Kloostermann sums do not vanish when $p > 3$. Aubry and Langevin got a very small step in this direction

Theorem 1. *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 $\widehat{f}(a) \equiv 0 \pmod 3$.*

Observing this statement I recently propose the following optimist version :

Conjecture 2. *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

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.