On Helleseth conjectures

Yves Aubry Philippe Langevin

Institut de Mathmatiques de Toulon
université du sud Toulon Var.

4 September 2013

5th International Conference on Algebraic Informatics
Porquerolles island

Origine

The mathematical problems of the talk appeared in the 60's when people searched pairs of binary sequences with nice intercorrelation properties : phone, radar etc...

correlation

Given two complex sequences s and s' on unit circle, of period n, the intercorrelation at $t \in \mathbb{Z}$ is

$$s' \times s(t) = \sum_{i=1}^{n} s'_i \overline{s_{i+t}}$$

finding pairs of sequences of root of 1, preferably ternary or binary, with small correlation, ideally 0, is important for applications.

maximal sequence

By the works of people like Gold, Welch, Niho . . . We know it is possible to construct interesting sequences using both the additive and the multiplicative structures of a finite field.

- L be a finite field of characteristic p and order q.
- μ the canonical addidive character of L,

$$L \ni x \mapsto \zeta_p^{\mathrm{Tr}_L(x)}, \quad \zeta_p = \exp(2i\pi/p).$$

- γ a primtive root of L.

$$s_i := \mu(\gamma^i)$$

is $(q-1)$-periodic, it is a *maximal sequence*.

Fourier coefficient

Let s' an other m-sequence.

$$s'_i = \mu(\beta^i) = \mu(\gamma^{si}), \qquad (s, q-1) = 1, \quad \beta = \gamma^s.$$

$$\begin{aligned} s' \times s(t) &= \sum_{i=1}^{q-1} s'_i \overline{s_{i+t}} \\ &= \sum_{i=1}^{q-1} \mu(\gamma^{si}) \bar{\mu}(\gamma^{i+t}) \\ &= \widehat{f}(a) - 1 \end{aligned}$$

where $a = \gamma^t$ and $f(x) = x^s$ (power permutation), and

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

this *Fourier coefficient* is sometimes called a *Weil sum*.

Let $f \colon L \to L$ be any mapping.

- $\widehat{f}(a) \in \mathbb{Q}(\zeta_p)$ is a cyclotomic integer.
- The distribution of the $\widehat{f}(a)'s$ is the spectrum of f.
- We say f (or an exponent s) has a N-valued spectrum, if

$$N = \sharp\left\{\widehat{f}(a) \mid a \in L^\times\right\}$$

- It is convenient to introduce

$$\mathrm{Det}\,(f) := \prod_{a \in L^\times} \widehat{f}(a)$$

Rationality

Theorem (Helleseth)

All the Fourier coefficients of x^s are in $\mathbb{Z}$ iff $s = 1 \pmod{p-1}$.

Proof.

Let t be the inverse of s modulo $p-1$. The automorphism σ_u defined by $\sigma_u(\zeta_p) = \zeta_p^u$ acts like

$$\sigma_u(\widehat{f}(a)) = \sum_{x\in L} \mu(ux^s - uax) = \sum_{x\in L} \mu(x^s - u^{1-t}ax)$$
$$= \widehat{f}(u^{1-t}a)$$

whence by Fourier inversion

$$\forall x \in L, \quad f(x) = f(u^{1-t}x)$$

$$\forall y \in \mathbb{F}_p, \quad y = u^{1-t}y$$

Rationality

Theorem (Helleseth)

All the Fourier coefficients of x^s are in $\mathbb{Z}$ iff $s = 1 \pmod{p-1}$.

Proof.

Let t be the inverse of s modulo $p-1$. The automorphism σ_u defined by $\sigma_u(\zeta_p) = \zeta_p^u$ acts like

$$\begin{aligned}\sigma_u(\widehat{f}(a)) &= \sum_{x\in L} \mu(ux^s - uax) = \sum_{x\in L} \mu(x^s - u^{1-t}ax) \\ &= \widehat{f}(u^{1-t}a)\end{aligned}$$

whence by Fourier inversion

$$\forall x \in L, \quad f(x) = f(u^{1-t}x)$$

$$\forall y \in \mathbb{F}_p, \quad y = u^{1-t}y$$

$\square$

main conjectures

The domain of sequences is full of open questions, problems and conjectures concerning the spectra of power mappings. One of the main conjectures appears in a paper of Sarwate and Pursley (1980).

Conjecture

Assuming $p = 2$. If f is a power permutation of L where $[L : \mathbb{F}_2]$ is even then $\sup_{a \in L} |\widehat{f}(a)| \geq 2\sqrt{q}$.

There is also two conjectures by Helleseth (1976).

Helleseth conjectures

Conjecture (HZ)

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

$$\exists a \in L^{\times}, \quad \widehat{f}(a) = 0.$$

Conjecture (HP)

If $[L : \mathbb{F}_p]$ is a power of 2. If f is a power permutation of L then $\widehat{f}$ takes at least four values.

Recent results

In characteristic 2,

- HZ checked up to dimension 25, numerical project page of PL.
- HP checked up to dimension 32, idem.
- D. Katz proved HZ assuming tri-valued spectrum.
- T. Feng proved HP assuming non trivial zero.
- HP is proved (2012).

In odd characteristic,

- three valued spectrum implies $s = 1 \pmod{p-1}$ (D. Katz)
- D. Katz proved HP in characteristic 3.
- HP checked for $q \leq 2^{20}$, numerical project page of PL.
- HP looks like "almost" proved (2013).

How to progress ?

It appears that the hard conjecture is

Conjecture (HZ)

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

$$\exists a \in L^\times, \quad \widehat{f}(a) = 0.$$

no progress since 40 years !

Kloosterman sum

The case $s = q - 2$ is very interesting

$$f(x) = x^s = x^{-1}, \qquad \widehat{f}(a) = 1 + \sum_{x \in L^\times} \mu(\frac{1}{x} - ax) = 1 + \mathrm{kloos}\,(a)$$

We know HZ is true for the inversion :

- in characteristic 2 (Lachaud-Wolfmann).
- in characteristic 3 (Katz-Livné).
- in characteristic $p > 3$, $sdoma = -1 \pmod{p-1}$. (Kononen-Rinta-Aho-Vaanainen).

Problem

Find a more direct proof !

Problem

What about APN mappings ?

Divisibility

Let f be a permutation of L

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

Definition

We say that HZ is true modulo ℓ if for any power permutation of exponent $s = 1 \pmod{p-1}$,

$$\exists a \in L^\times, \quad \widehat{f}(a) \equiv 0 \pmod{\ell}.$$

Divisibility by p

Proposition

HZ is true modulo p.

$$\widehat{f}(a) = \frac{q}{q-1} + \frac{1}{q-1} \sum_{\chi \neq 1} \tau(\bar{\chi}^t)\tau(\chi)\bar{\chi}(a)$$

where $st = 1 \pmod{q-1}$.
The p-divisiblity is well understand by Stickelberger's congruences on Gauss sums :

$$\tau(\chi) = \sum_{x \in L} \chi(x)\mu(x).$$

The minimal p-adic valuation of $\widehat{f}(a)$ ($a \neq 0$) is

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

where $S(j)$ is the p-ary weight of the residue $\equiv j \bmod (q-1)$.

Divisibility by 3

Theorem

HZ is true modulo 3

primary degree

Theorem

if $[L : \mathbb{F}_p]$ *is a power of a prime* ℓ *then HZ is true modulo* ℓ.

Key point

We consider the number $N_n(u,v)$, of solutions in L^n of the system

$$\begin{cases} x_1 + x_2 + \dots + x_n = u \\ f(x_1) + f(x_2) + \dots + f(x_n) = v. \end{cases} \quad (1)$$

Using characters counting principle :

Lemma

*The number $N_n(u,v)$ of solutions in L^n of the system (**??**) verifies*

$$q^2 N_n(u,v) = q^n + \sum_{\alpha \in L^\times} \sum_{\beta \in L^\times} \widehat{f_\beta}(\alpha)^n \overline{\mu}(\alpha u + \beta v).$$

where $f_\beta(x) = f(\beta x)$.

sketch $\ell = 3$

Suppose that $\mathrm{Det}\,(f) \not\equiv 0 \mod 3$ whence $p \neq 3$

$$q^2 N_2(u,v) = q^2 + \sum_{\alpha \in L^\times} \sum_{\beta \in L^\times} \widehat{f_\beta}(\alpha)^2 \bar{\mu}(\alpha u + \beta v).$$

Assuming $u, v \in L^\times$.
Using little Fermat Theorem, it becomes

$$\begin{aligned} N_2(u,v) &\equiv 1 + \sum_{\alpha \in L^\times} \sum_{\beta \in L^\times} \bar{\mu}(\alpha u + \beta v) \\ &\equiv 1 + \sum_{\alpha \in L^\times} \bar{\mu}(\alpha u) \times \sum_{\beta \in L^\times} \bar{\mu}(\beta v) \\ &\equiv 1 + (-1) \times (-1) \equiv 2 \pmod 3. \end{aligned}$$

$$\forall u \in L^\times, \quad \forall v \in L^\times, \qquad N_2(u,v) \not\equiv 0 \pmod \ell. \tag{2}$$

sketch $\ell = 3$

In order to obtain a contradiction, we exhibit a $v \in L^\times$ such that $N_2(1, v) = 0$. This number is also the number of preimages of v by

$$d \colon x \mapsto x^s + (1-x)^s$$

An element $v \neq 1/2$ in the image has at least two images

$$x, 1-x$$

The image of d contains at most $\frac{q+1}{2}$ elements and there exists a v such that $N_2(1, v) = 0$.

conclusion

still a lot of work !

but up to now, divisibility by 3 (new) and divisibility by p (old) are the only two global results in the direction of the Helleseth conjecture !