New open questions related to old conjectures by Tor Helleseth

International Workshop on Boolean Functions and Their Application, Rosendal September 2th–7th 2014

Philippe, Langevin

IMATH, université de Toulon

last revision September 3, 2014.

Introduction

In the two/three last years, progress in the direction of two conjectures by Helleseth (1976) regarding the cross-correlation of maximal sequences have been obtained. The goal of this talk is to present several new interesting open questions over finite fields related to these conjectures.

- slides location : `http://langevin.univ-tln.fr/recherche/drafts/openpb.pdf`

Fourier coefficient

Let L be a finite field of characteristic p and order q. The *Fourier coefficient* of a polynomial $f \in L[X]$ at a point $a \in L$ is

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

and more generally, for $b \in K$:

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

where μ is the canonical additive character of K.

Remark

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

Convolution

Let F, G two complex mappings over L.

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

Denoting $F\colon x \mapsto \mu(f(x))$, and $\mu_a\colon x \mapsto \mu(ax)$:

$$\mu_a * F = \widehat{f}(a)\,\mu_a$$

- μ_a is an eigenvector
- $\widehat{f}(a)$ eigenvalue.

Spectrum

For a permutation f of L

$$\mathrm{spec}\,(f) = \{\widehat{f}(a) \mid a \in L^{\times}\}.$$

Definition

The permutation f is said to be r-valued, where $r = \sharp\mathrm{spec}\,(f)$,

$$D(f) = \prod_{a \in L^{\times}} \widehat{f}(a)$$

Power permutation

We are interested by the power permutations:

$$x \mapsto f(x) = x^s, \quad (s, q-1) = 1.$$

[equivalence]

$$s' \sim s \quad \Longleftrightarrow \quad \exists j,\ s' = sp^j \mod q-1$$

Remark

Like for any permutation π, the phase Fourier coefficient of any power permutation is null,

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

Invariance of the Fourier distribution

Note that for a power permutation

$$\forall b \in K^{\times}, \quad \mathrm{spec}\,(f_b) = \mathrm{spec}\,(f)$$

because

$$\widehat{f_b}(a) = \sum_x \mu(bx^s - ax) = \widehat{f}(ab^{-1/s})$$

Problem (invariance by translation)

What are the maps f such that

$$\forall b \in K^{\times}, \quad \mathrm{spec}\,(f_b) = \mathrm{spec}\,(f)?$$

Basic arithmetic facts

Let $\zeta_p = \exp(2i\pi/p)$, $\wp = (1-\zeta_p)$ the prime ideal above p in $\mathbb{Z}[\zeta_p]$, σ_t the Galois automorphism of $\mathbb{Q}[\zeta_p]$ defined by $\sigma_t(\zeta_p) = \zeta_p^t$.
For a power permutation f :

$$\widehat{f}(a) \equiv \widehat{f}(0) \equiv 0 \mod \wp, \quad \sigma_t\big(\widehat{f}(a)\big) = \widehat{f}_t(at)$$

Lemma (action)

If s is invertible then $\mathrm{spec}\,(x^s)$ is invariant by the Galois group of $\mathbb{Q}(\zeta_p)$.

Lemma (integrality)

All the Fourier coefficients of x^s are integral iff $s \equiv 1 \mod p-1$.

Valuation of the Fourier coefficients

For an exponent s, we define

$$\mathrm{V}_K(s) = \min_{a \in K} \mathrm{val}_p\big(\widehat{f}(a)\big)$$

This parameter is connected to Stickelberger congruences on Gauss sum,

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

thus

$$\mathrm{V}_K(s) = \min_{1 \neq \chi \in K^\times} \mathrm{val}_p\big(\tau_K(\chi)\tau_K(\bar{\chi}^s)\big)$$

using Hasse-Davenport, given an extension L/K :

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

Helleseth vanishing conjecture

A permutation f of L is *singular*

$$\exists a \in L^\times, \quad \widehat{f}(a) = 0, \qquad \text{i.e.} \quad D(f) = 0$$

Conjecture (Helleseth conjecture I)

All the power permutations $x \mapsto x^s$ with $s \equiv 1 \mod p-1$ are singular.

Hard ?! May be false ?!

Very difficult to progress on this question.

- A numerical evidence checked for $[L : \mathbb{F}_2] \leq 25$ [PL, 2007].
- If $p = 2$ then 3 divides $D(x^s)$ [Yves Aubry, PL, 2013]
- If $[L : \mathbb{F}_2] = \ell^r$ then $\ell | D(x^s)$
- True for a 3-valued exponent [Daniel Katz, 2012].

Boolean challenges

Problem

find a direct proof for $s = -1$, i.e. Kloostermann sum.

Problem

find an 5-adic analogue of AL result.

Problem

find new general divisibility results.

Problem

find an analogue of Katz result , for 4-valued exponents !

3-valued power permutations

Theorem (Daniel Katz, 2012)

A 3-valued power permutation x^s is singular and

$$s = 1 \mod p-1, \quad \operatorname{spec}(x^s) = \{0, A, B\} \subset \mathbb{Z}.$$

Moreover, the number of solutions of

$$x + y = 1, \quad x^s + y^s = 1$$

is equal to

$$V = A + B - \frac{AB}{q}$$

Folklore Calderbank, Blokuis.

Coefficient of the Minimal polynomial

More generally, the product

$$P(f) = \prod_{0 \neq A \in \mathrm{spec}(f)} A$$

the rationnal number $P(f)/q$ appears naturally by Fourier analysis.

Problem (valuation of coefficients)

It it true that q divides the $P(f)$?

Helleseth 3-valued conjecture

Conjecture (Helleseth conjecture II)

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

- Tao Feng (2012) : $p = 2$ assuming annulation of the spectrum.
- Proved for $p \leq 3$, Daniel Katz (2014).

key point

Tao Feng uses the following proposition to obtain Helleseth conjecture II in even characteristic assuming the singularity of a 3-valued exponents.

Proposition (Calderbank, McGuire, Poonen, Rubinstein, 1996)

Let $s \not\sim 1$ be an invertible exponent. If $[K : \mathbb{F}_2]$ is a power of two then

$$2 \times \mathrm{V}_K(s) \leq [K : \mathbb{F}_2].$$

Remark

In fact the same holds for all p !!!

Lemma (Yves Aubry, Daniel Katz, PL)

Let L/K be a quadratic extension. If x^s is constant over $K^\times$ but not over L then

$$\exists a \in L, \quad \widehat{f}(a) = -|K|, \quad 2 \times \mathrm{V}_L(s) = [L : \mathbb{F}_p]$$

Using Hasse-Davenport relation, we now see by induction that if

$$1 \not\sim s \equiv 1 \mod p-1 \quad \text{and} \quad [L : \mathbb{F}_p] = 2^r$$

then

$$2 \times \mathrm{V}_L(s) \leq [L : \mathbb{F}_p].$$

Notation

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. Note 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.

differential multiplicity

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

$$\left\{ \begin{array}{cccc} x & + & y & = u \\ f(x) & + & f(y) & = v \end{array} \right.$$

By Fourier analysis

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

differential exponent

Definition

Let s be an exponent. We say that s is a Δ-differential exponent over K if the number of solutions of

$$\left\{ \begin{array}{cccl} x & + & y & = 1, \\ x^s & + & y^s & = v, \end{array} \right.$$

is equal to 0 or Δ for all $v \neq 1$.

3-valued exponent

Following the argumentation of Tao Feng

Theorem (Katz)

If s is three valued over L then $\alpha\beta\gamma$ divides the differential multiplicities $N(1, v)$ for all $v \neq 1$ and

$$|\alpha\beta\gamma| \leq -\frac{AB}{q}$$

leading to the alternative

1. $2\mathrm{V}_L(s) > [L : \mathbb{F}_p]$ *(impossible when $[L : \mathbb{F}_p] = 2^r$)*
2. $2\mathrm{V}_L(s) = [L : \mathbb{F}_p]$
   $\gamma = 1$ *and s is $|\alpha\beta|$-differential exponent.*

Corollary

if $p = 2$ or $p = 3$ then Helleseth conjecture II is true.

Nice exponent

Definition

Let s be an exponent. We say that s is a *nice exponent* over K if the number of solutions of

$$\begin{cases} x + y = 1, \\ x^s + y^s = v, \end{cases}$$

takes at most 3 values.

Remark

A Δ-differential exponent is nice.

Numerical result

It is easy to find all the differential distribution of all exponents using Zech logarithm.
Let ω be a primitive root of K :

$$\mathrm{Zech(k) = l,} \quad 1 + \omega^{\mathrm{k}} = \omega^{\mathrm{l}}$$

the logarithm of

$$x^s + (1-x)^s = x^s(1 + (\frac{1-x}{x})^s)$$

for $x = \omega^k$ is

$$k \times s + \mathrm{Zech[(Zech[n+k] - k) \times s],} \quad \mathrm{n} := \frac{\mathrm{q}-1}{2}.$$

http://langevin.univ-tln.fr/project/

sample

```
[pl@microbe ~]$ cat ~/web-docs/project/expo/nice-11.txt
#field is GF(11,2)
#field is GF(11,3)
     3  : 3 : 3 : 664 [ 0]   1 [ 1] 665 [ 2]
   447  : 7 : 3 : 664 [ 0]   1 [ 1] 665 [ 2]
  1209  : 9 : 3 : 664 [ 0]   1 [ 1] 665 [ 2]

#field is GF(11,4)
   241  : 1 : 3 : 7379 [ 0] 7260 [ 2]   1 [121]
  4921  : 1 : 3 : 7379 [ 0] 7260 [ 2]   1 [121]

#field is GF(11,5)
     3  : 3 : 3 : 80524 [ 0]   1 [ 1] 80525 [ 2]
 53687  : 7 : 3 : 80524 [ 0]   1 [ 1] 80525 [ 2]
146409  : 9 : 3 : 80524 [ 0]   1 [ 1] 80525 [ 2]
```

New conjectures ?

Conjecture (nice exponent)

Asuming odd characteristic. Let s be an exponent. If s is nice then 2 is a differential multiplicity.

Conjecture (optimist)

Asuming odd characteristic. Let s be an exponent. If s is invertible then 2 is a differential multiplicity.

$$\text{optimist} \Longrightarrow \text{nice} \Longrightarrow \text{Helleseth 3-valued}$$

Yves Aubry, Daniel J. Katz, and Philippe Langevin.
Cyclotomy of weil sums of binomials.
CoRR, abs/1312.3889, 2013.

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.

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.

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.

Florent Chabaud and Serge Vaudenay.

Links between diffrential and linear cryptanalysis.
Eurocrypt 94, 950:356–365, 1994.

John F. Dillon.
Elementary Hadamard Difference Sets.
PhD thesis, Univ. of Maryland, 1974.

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

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

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.

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.

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.

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.

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

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.

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

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

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

Rudolf Lidl and Harald Niederreiter.

Finite Fields, volume 20 of *Encyclopedia of Mathematics and its Applications*.
Addison-Wesley, 1983.

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.