On a conjecture of Helleseth

Yves Aubry, Philippe Langevin

ON A CONJECTURE OF HELLESETH

YVES AUBRY AND PHILIPPE LANGEVIN

ABSTRACT. We are concern about a conjecture proposed in the middle of the seventies by Hellesseth in the framework of maximal sequences and theirs cross-correlations. The conjecture claims the existence of a zero outphase Fourier coefficient. We give some divisibility properties in this direction.

1. Two conjectures of Helleseth

Let L be a finite field of order $q > 2$ and characteristic p. Let μ be the canonical additive character of L i.e. $\mu(x) = \exp(2i\pi \mathrm{Tr}\,(x)/p)$ where Tr is the trace function with respect to the finite field extension $L/\mathbb{F}_p$. The *Fourier coefficient* of a mapping $f\colon L \to L$ is defined at $a \in L$ by

$$\widehat{f}(a) = \sum_{x \in L} \mu(ax + f(x)). \tag{1}$$

The distribution of these values is called the *Fourier spectrum* of f. Note that when f is a permutation the *phase* Fourier coefficient $\widehat{f}(0)$ is equal to 0.

The mapping $f(x) = x^s$ is called the power function of exponent s, and it is a permutation if and only if $(s, q-1) = 1$. Moreover, if $s \equiv 1 \mod (p-1)$ the Fourier coefficients of f are rational integers. Helleseth made in [3] two "global" conjectures on the spectra of power permutations. The first claims the vanishing of the quantity (related to Dedekind determinant, see [9])

$$\mathfrak{D}(f) = \prod_{a \in L^\times} \widehat{f}(a). \tag{2}$$

Conjecture 1 (Helleseth)**.** *Let L be a field of cardinal $q > 2$. If f is a power permutation of exponent $s \equiv 1 \mod (p-1)$ then $\mathfrak{D}(f) = 0$.*

For $p = 2$, it generalizes Dillon's conjecture (see [2]) which corresponds to the case $s = q-2 \equiv -1 \mod (q-1)$, and known to be true because it is related to the vanishing of Kloosterman sums and the class number h_q of the imaginary quadratic number field $\mathbb{Q}(\sqrt{1-4q})$ (see [5, 8]). Note also that in odd characteristic the Kloosterman sums do not vanish (see [7]) except if $p = 3$ (see [5]).

The second conjecture deals with the number of values in the spectrum of a power permutation.

Conjecture 2. *If $[L : \mathbb{F}_p]$ is a power of 2 then the spectrum of a power function takes at least four values.*

In this note, we prove some results concerning the divisibility properties of the Fourier coefficients of power permutations in connection with Conjecture 1. Our results can be seen as a proof "modulo ℓ" of Conjecture 1 for certain primes ℓ.

Table 1. An example of Walsh spectrum having only one Walsh coefficient equal to zero (see [6]).

Walsh	-48	-44	-40	-36	-32	-28	-24 -	20	-16	-12
mult.	5	30	85	70	115	100	31	62	20	10
Walsh	0	8	16	20	24	28	32	36	40	44
mult.	1	5	25	20	85	90	90	80	50	50

2. Boolean function case

In this section, we assume $p = 2$. In [10], the second author has computed the Fourier spectra of power permutations for all the fields of characteristic 2 with degree less or equal to 25 without finding any counter-example to the above conjectures. More curiously, if we denote by $\mathrm{nbz}\,(s)$ the number of Fourier coefficients of the power function of exponent s equal to zero then the numerical experience suggests that:

$$\mathrm{nbz}\,(s) \geq \mathrm{nbz}\,(-1) = h_q.$$

At this point, it is interesting to notice that Helleseth's conjecture can not be extended to the set of all permutations. Indeed, let m be a positive integer and let $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$ be a Boolean function in m variables. One defines the Walsh coefficient of g at $a \in \mathbb{F}_2^m$ by :

$$g^{\mathcal{W}}(a) = \sum_{x\in\mathbb{F}_2^m} (-1)^{a.x+g(x)}.$$

Identifying L with the $\mathbb{F}_2$-vector space $\mathbb{F}_2^m$, the Boolean function g has a trace representation i.e. there exists a mapping $f\colon L \to L$ such that $g(x) = \mathrm{Tr}_L(f(x))$ for all x in L. Of course, the trace representation is not unique. Moreover, if g is balanced then g can be represented by a permutation of L. In all the cases, the Walsh spectrum of g and the Fourier spectrum of f are identical.

In [6], an example of a ten variables Boolean function with a very atypical Walsh spectrum (see Tab. 1) is given. This Boolean function is balanced and its Walsh coefficients vanish only once. This numerical example, say g, implies the existence of a permutation f of $\mathbb{F}_{1024}$ (not a power permutation) such that

$$g(x) = \mathrm{Tr}_{\mathbb{F}_{1024}} f(x),$$

whence the Fourier spectrum of f is equal to the Walsh spectrum of g, and thus $\sum_{x\in\mathbb{F}_{1024}} \mu(ax + f(x)) \neq 0$ for all $a \in \mathbb{F}_{1024}^\times$.

A possible generalization of the conjecture of Helleseth, proposed by Leander, could be the following one:

Conjecture 3. *If f is a permutation of L then $\prod_{\lambda\in L^\times} \mathfrak{D}(\lambda f) = 0$.*

Note that Conjecture 2 is know to be true in characteristic 2 since recent works of Daniel Katz in [4] and Tao Feng in [11]. In order to complete this short conjecture tour , we recall to the reader the main global conjecture of the domain due to Sarwate and which is still open

Conjecture 4. *If f is a power permutation of L where $[L : \mathbb{F}_2]$ is even then $\sup_{a\in L} \widehat{f}(a) \geq 2\sqrt{q}$.*

In the sequel, if $\lambda \in L$ then we denote by $\widehat{f_\lambda}(a)$ the Fourier coefficient of $x \mapsto \lambda f(x)$. If f is a power permutation of exponent s, denoting by t the inverse of s modulo $q-1$, for all $y \in L^\times$, we have :

$$\widehat{f_\lambda}(a) = \sum_{x\in L} \mu(\lambda x^s + ax) = \sum_{x\in L} \mu(\lambda y^s x^s + axy) = \widehat{f}(a\lambda^{-t}). \tag{3}$$

Hence, one of the specifics of power permutations among the permutations of L is that the spectrum of λf does not depend on $\lambda \in L^\times$.

We conclude this section by giving a divisibility result. Recall that a function f defined over a field L of characteristic 2 is said to be almost perfect nonlinear if for all $u \in L^\times$ 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 L and of $f(x) = x^{-1}$ when $[L : \mathbb{F}_2]$ is odd.

Proposition 1. *Let f be a power permutation over a field L of characteristic two and cardinal $q \not\equiv 2, 4 \mod 5$. If f is almost perfect nonlinear then there exists $a \in L^\times$ such that $\widehat{f}(a) \equiv 0 \mod 5$.*

Proof. It is well-known (see [1]) that an APN function f satisfies

$$\sum_{\lambda\in L^\times} \sum_{a\in L} \widehat{f_\lambda}(a)^4 = 2q^3(q-1). \tag{4}$$

Since the spectrum of λf does not depend on $\lambda \in L^\times$, it implies that:

$$\sum_{a\in L} \widehat{f_\lambda}(a)^4 = 2q^3. \tag{5}$$

Assuming $\mathfrak{D}(f) \not\equiv 0 \mod 5$, we get the congruence $q - 1 \equiv 2q^3 \mod 5$ implying $q \equiv 2, 4 \mod 5$. □

3. HYPERPLANE SECTION

The key point of view of this note is to consider the number, say $N_n(u, v)$, of solutions in L^n of the system

$$\begin{cases} u = x_1 + x_2 + \dots + x_n \\ v = f(x_1) + f(x_2) + \dots + f(x_n). \end{cases} \tag{6}$$

Using characters counting principle, we can write:

$$\begin{aligned} q^2 N_n(u, v) &= \sum_{x_1,x_2,\dots,x_n} \sum_{\beta\in L} \sum_{\alpha\in L} \mu_\beta(\sum_i f(x_i) + v)\mu_\alpha(\sum_i x_i + u) \\ &= \sum_\beta \sum_\alpha \big(\sum_y \mu(\beta f(y) + \alpha y))\big)^n \mu(\alpha u + \beta v) \\ &= \sum_\beta \sum_\alpha \widehat{f_\beta}(\alpha)^n \mu(\alpha u + \beta v) \\ &= \sum_\alpha \widehat{1}(\alpha)^n \mu(\alpha u) + \sum_{\beta\neq 0} \sum_\alpha \widehat{f_\beta}(\alpha)^n \mu(\alpha u + \beta v) \\ &= q^n + \sum_{\alpha\neq 0} \sum_{\beta\neq 0} \widehat{f_\beta}(\alpha)^n \mu(\alpha u + \beta v) \end{aligned}$$

Lemma 1. *Assuming the Fourier coefficients of λf, $\lambda \in L$, are integers. Let ℓ be a prime such that $\prod_{\lambda\in L^\times} \mathfrak{D}(\lambda f) \not\equiv 0 \mod \ell$. 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.

Proof. By the Fermat's little Theorem, we have the congruence

$$\widehat{f_\lambda}(a)^{\ell-1} \equiv 1 - \delta_0(a) \mod \ell.$$

Hence

$$\begin{aligned} q^2 N_{\ell-1}(u,v) &= q^{\ell-1} + \sum_{\alpha\neq 0}\sum_{\beta\neq 0} \widehat{f_\beta}(\alpha)^{\ell-1}\mu(\alpha u + \beta v) \\ &\equiv 1 + \sum_{\alpha\neq 0}\sum_{\beta\neq 0} \mu(\alpha u + \beta v) \mod \ell \end{aligned}$$

and we conclude remarking that $\sum_{\alpha\in L^\times} \mu(\alpha u) = q\delta_0(u) - 1$. □

4. Divisibility of Fourier coefficients

In [3], it is proved that for the exponents $s \equiv 1 \mod (p-1)$, the Fourier coefficients are multiple of p. In this section, we are interested in divisibility properties modulo a prime $\ell \neq p$.

Assuming that the Fourier coefficients of a mapping f, not necessary a power function, are rational integers, we can see that if 3 does not divide $\mathfrak{D}(f)$ then we have necessarily $q \equiv 2 \mod 3$. Indeed, using Parseval relation, we can write

$$1 \equiv q^2 = \sum_{a\in L} |\widehat{f}(a)|^2 = \sum_{a\in L} \widehat{f}(a) \equiv q - 1 \mod 3.$$

Theorem 1. *Let f be the power function of exponent s. If $s = 1 \mod (p-1)$ is coprime with $q-1$ then $\mathfrak{D}(f) \equiv 0 \mod 3$.*

Proof. Suppose that $\mathfrak{D}(f) \not\equiv 0 \mod 3$. Applying Lemma 1 with $\ell = 3$, we get

$$\forall u \in L^\times, \quad \forall v \in L^\times, \qquad N_2(u,v) \not\equiv 0 \mod \ell. \tag{7}$$

To complete the proof we prove the existence of a pair (u,v) of nonzero elements such that $N_2(u,v) = 0$. Let us fix $u = 1$, the v's such that $N_2(1,v) > 0$ are in the image of L by the mapping $x \mapsto (1-x)^s + x^s$, if x is a preimage of v then $1-x$ is an other one except if $p = 2$ and $v = 2(1/2)^s$. Thus, if $q > 3$, there exists $v \in L^\times$ without preimage i.e. $N_2(1,v) = 0$.

□

Proposition 2. *Let f be a power permutation of exponent $s \equiv 1 \mod (p-1)$. If $[L : \mathbb{F}_p]$ is a power of a prime ℓ and $p \not\equiv 2 \mod \ell$ then $\mathfrak{D}(f) \equiv 0 \mod \ell$.*

Proof. The Frobenius automorphism acts on the solutions of the system (6) with $u = 0$, $v = 1$. Since $s \equiv 1 \mod (p-1)$, the system has no $\mathbb{F}_p$-solutions, thus $N_{\ell-1}(0,1) \equiv 0 \mod \ell$. On the other hand, by Lemma 1, if $\mathfrak{D}(f) \not\equiv 0 \mod \ell$ then

$$q^2 N_{\ell-1}(0,1) \equiv 2 - q \equiv 2 - p \mod \ell.$$

□

References

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

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

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

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. With an appendix by Karl Rubin.

[10] Philippe Langevin. Numerical projects page, 2007. `http://langevin.univ-tln.fr/project/spectrum`.

[11] 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.

Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France and Institut de Mathématiques de Luminy, Marseille, France

E-mail address: `yves.aubry@univ-tln.fr`

Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France

E-mail address: `langevin@univ-tln.fr`