On a Conjecture of Helleseth

Yves Aubry[1,2] and Philippe Langevin[1,⋆]

[1] Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France
[2] Insitut de Mathématiques de Luminy, Université d'Aix-Marseille, France

Abstract. We are concerned 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 $f : L \to L$ 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] the following conjecture on 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 L 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 $s = q - 2 \equiv -1 \pmod{q-1}$, 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]).

In the same paper [3], Helleseth proposed a second conjecture:

⋆ The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve this manuscript.

T. Muntean, D. Poulakis, and R. Rolland (Eds.): CAI 2013, LNCS 8080, pp. 113–118, 2013.

Conjecture 2. If $[L : \mathbb{F}_p]$ is a power of 2 then the spectrum of a power permutation of exponent not a power of p modulo $q-1$ takes at least four values.

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

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 nbz (s) the number of vanishing Fourier coefficients of the power function of exponent s then the numerical experience suggests that:

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

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 $g(x) = \operatorname{Tr}_L(f(x))$ 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

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

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 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 [12]. The next conjecture that appeared in the paper by Pursley and Sarwate (see [11]) is still open

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

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 $\widehat{f}(a)$ 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 :

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

Hence, one of the specifities 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 (APN) 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.

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

$$\mathfrak{D}(f) \equiv 0 \mod 5.$$

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

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

Since the spectrum of f does not depend on λ, it implies that:

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

Assuming $\mathfrak{D}(f) \not\equiv 0 \mod 5$, we get the congruence

$$q - 1 = 2q^3 \pmod 5$$

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

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

By a counting principle using characters, we can state:

Lemma 1. *Let f be a permutation of L. The number $N_n(u,v)$ of solutions in L^n of the system (6) verifies*

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

Proof. For any function $f\colon X \longrightarrow G$ where X is a set and G is a finite abelian group, the number N of solutions in X of $f(x) = y$ for $y \in G$ is

$$N = \frac{1}{\mid G \mid} \sum_{x\in X} \sum_{\chi\in\widehat{G}} \chi(f(x) - y)$$

where $\widehat{G}$ denotes the group of characters of G.

For any $\alpha \in L$, we denote by μ_α the additive character of L defined by $\mu_\alpha(x) = \mu(\alpha x)$, then we have:

$$\begin{aligned} q^2 N_n(u,v) &= \sum_{x_1,x_2,\ldots,x_n} \sum_{\beta\in L} \sum_{\alpha\in L} \bar{\mu}_\beta(v - \sum_{i=1}^{n} f(x_i)) \bar{\mu}_\alpha(u - \sum_{i=1}^{n} x_i) \\ &= \sum_{\beta} \sum_{\alpha} \big(\sum_{y\in L} \mu(\beta f(y) + \alpha y) \big)^n \bar{\mu}(\alpha u + \beta v) \\ &= \sum_{\beta} \sum_{\alpha} \widehat{f_\beta}(\alpha)^n \bar{\mu}(\alpha u + \beta v) \\ &= \sum_{\alpha} \widehat{f_0}(\alpha)^n \bar{\mu}(\alpha u) + \sum_{\beta\neq 0} \sum_{\alpha} \widehat{f_\beta}(\alpha)^n \bar{\mu}(\alpha u + \beta v) \\ &= q^n + \sum_{\alpha\neq 0} \sum_{\beta\neq 0} \widehat{f_\beta}(\alpha)^n \bar{\mu}(\alpha u + \beta v). \end{aligned}$$

Proposition 1. *Assuming the Fourier coefficients of λf, $\lambda \in L$, are integers. Let $\ell \neq p$ 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, by Lemma (1), we have:

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

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

4 Divisibility of Fourier Coefficients

In [3], it is proved that for the exponents $s \equiv 1 \pmod{p-1}$, 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 any permutation f 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

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

Theorem 2. *Let f be a power permutation of $\mathbb{F}_{p^n}$ (with $p^n > 2$) of exponent $s = 1 \mod (p-1)$. Then*

$$\mathfrak{D}(f) \equiv 0 \mod 3.$$

Moreover, if n is a power of a prime ℓ and $p \not\equiv 2 \mod \ell$ then

$$\mathfrak{D}(f) \equiv 0 \mod \ell.$$

Proof. First point. Since p divides $\mathfrak{D}(f)$, we may assume that $p \neq 3$. Suppose that $\mathfrak{D}(f) \not\equiv 0 \mod 3$. Applying Proposition 1 with $\ell = 3$, we get

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

In order to obtain a contradiction, we prove the existence of $v \in L^\times$ such that $N_2(1,v) = 0$. The mapping $x \mapsto (1-x)^s + x^s$ sends x and $1-x$ to the same point. An element v in the image has at least 2 preimages except when $x = 1-x$, which can only happen when p is odd and $x = 1/2$. So this means that if $p = 2$, the cardinality of the image is less or equal to $q/2$ elements, while if p is odd, the image of the map has at most $(q+1)/2$ elements. If $q > 3$ the complementary of the image contains at least two elements whence a nonzero v such that $N(1,v) = 0$.

Second point. Suppose now that n is a power of a prime ℓ and $p \not\equiv 2 \mod \ell$. 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 Proposition 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. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 356–365. Springer, Heidelberg (1995)
2. Dillon, J.F.: Elementary Hadamard Difference Sets. PhD thesis, Univ. of Maryland (1974)
3. Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discrete Math. 16(3), 209–232 (1976)
4. Katz, D.J.: Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth. J. Comb. Theory, Ser. A 119(8), 1644–1659 (2012)
5. Katz, N., Livné, R.: 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. Kavut, S., Maitra, S., Yücel, M.D.: Search for boolean functions with excellent profiles in the rotation symmetric class. IEEE Transactions on Information Theory 53(5), 1743–1751 (2007)
7. Keijo, K., Marko, R.A., Keijoe, V.: On integer value of Kloosterman sums. IEEE Trans. Info. Theory (2010)
8. Lachaud, G., Wolfmann, J.: Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. C. R. Acad. Sci. Paris Sér. I Math. 305, 881–883 (1987)
9. Lang, S.: Cyclotomic fields I and II, 2nd edn. Graduate Texts in Mathematics, vol. 121. Springer, New York (1990), With an appendix by Karl Rubin
10. Langevin, P.: Numerical projects page (2007), `http://langevin.univ-tln.fr/project/spectrum`
11. Pursley, M.B., Sarwate, D.V.: Cross correlation properties of pseudo-random and related sequences. Proc. IEEE 68, 593–619 (1980)
12. Tao, F.: 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)