New open problems related to old conjectures by Helleseth

Daniel J. Katz · Philippe Langevin

Received: 27 November 2014 / Accepted: 22 April 2015 / Published online: 12 May 2015
© Springer Science+Business Media New York 2015

Abstract Recently, very interesting results have been obtained concerning the Fourier spectra of power permutations over a finite field. In this note we survey the recent ideas of Aubry, Feng, Katz, and Langevin, and we pose new open problems related to old conjectures proposed by Helleseth in the middle of the seventies.

Keywords Finite fields · Weil sums · Exponential sums · Cross-correlation · M-sequence

1 Introduction

Let $L$ be a finite field of characteristic $p$ and order $q$. One defines the Fourier coefficient of a mapping $f : L \rightarrow L$ at a point $a \in L$ as

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

where $\mu : L \rightarrow \mathbb{C}$ is the canonical additive character. Strictly speaking, $\hat{f}(a)$ is the Fourier coefficient of the complex map $\mu \circ f$ at the additive character $\mu_a : x \mapsto \mu(ax)$. The minus sign that appears in the definition of the Fourier coefficient is not usual, but there are several good reasons to adopt it. Above all, one should note that $\mu_a$ will be an eigenvector of eigenvalue $\hat{f}(a)$ for the operator of convolution by $\mu \circ f$ over the mappings from $L$ to $\mathbb{C}$.

Philippe Langevin
langevin@univ-tln.fr
Daniel J. Katz
daniel.katz@csun.edu

1 California State University, Northridge, CA, USA
2 Université de Toulon, La Garde, France
In this paper, we are mainly interested in the Fourier coefficient of the power mapping \( f : x \mapsto x^s \) where \( s \) is a positive integer. In that case, the Fourier coefficient is sometimes called a Weil sum, and we also use the notation

\[
W_{L,s}(a) = \hat{f}(a) = \sum_{x \in L} \mu(x^s - ax).
\]

In the case where the exponent \( s \) is coprime to \( q - 1 \), we say that it is an invertible exponent, and the mapping \( f : x \mapsto x^s \) is called a power permutation, because it is indeed a permutation of \( L \). In this case, the Fourier coefficient at the origin is equal to zero:

\[
W_{L,s}(0) = \hat{f}(0) = \sum_{x \in L} \mu(x^s) = \sum_{x \in L} \mu(x) = 0.
\]

A power permutation \( f \), or its exponent \( s \), is said to be singular if there exists an \( a \in L^\times \) such that \( \hat{f}(a) = 0 \). We now present the first conjecture proposed in 1976 by Helleseth [7].

**Conjecture 1.1 (Helleseth Vanishing Conjecture, 1976)** If \( |L| > 2 \) and \( s \equiv 1 \) (mod \( p - 1 \)), then \( s \) is singular.

The conjecture was based on numerical evidence. The Fourier spectra of all the exponents over the extensions of \( \mathbb{F}_2 \) with degree less than or equal to 25 have been computed in 2007 by Langevin [13], and no counterexample was found. Up to now, very little in the way of partial results has been obtained for this conjecture. This question has every appearance of difficulty. Let us consider the special case when the exponent \( s = q - 2 \) satisfies Conjecture 1.1. Then \( s = q - 2 \equiv -1 \) (mod \( p - 1 \), so the congruential hypothesis of Conjecture 1.1 is satisfied for \( s = q - 2 \) if and only if \( -1 \equiv 1 \) (mod \( p - 1 \), which is true if and only if \( p = 2 \) or \( p = 3 \). For such an exponent, the Fourier coefficient is one plus a Kloosterman sum

\[
W_{L,q-2}(a) = 1 + \sum_{x \in L^\times} \mu \left( \frac{1}{x} - ax \right).
\]

If \( L \) is of characteristic 2, one can use the theory of elliptic curves as in [12] to prove that \( W_{L,q-2}(a) \) assumes all integer values divisible by 4 in the range \([1 - 2\sqrt{q}, 1 + 2\sqrt{q}]\) as \( a \) runs through \( L^\times \), a consequence of Deuring’s work. In particular, the Fourier coefficient \( W_{L,q-2}(a) \) takes the value 0 for some \( a \neq 0 \). In characteristic 3, it was shown (see [10]) that \( W_{L,q-2}(a) \) assumes all integer values divisible by 3 in the range \([1 - 2\sqrt{q}, 1 + 2\sqrt{q}]\) as \( a \) runs through \( L^\times \).

**Problem 1.2** Prove the Helleseth Vanishing Conjecture for \( p \in \{2, 3\} \) and \( s = q - 2 \) without using of the theory of elliptic curves.

**Remark 1.3** In characteristic \( p > 3 \) the exponent \(-1\), i.e., the exponent \( q - 2 \), is not singular. Indeed, for such fields \( W_{L,q-2}(a) \) has been shown to be nonzero when \( a \neq 0 \) in [11].

An exponent \( s \) is said to be \( r \)-valued if the number of distinct Fourier coefficients on \( L^\times \) is \( r \). The following theorem is a consequence of recent results of Feng and Katz.

**Theorem 1.4** If \([L : \mathbb{F}_2]\) is a power of two, then an invertible exponent is not three-valued.
Feng [6] proved the above theorem assuming that at least one of the Fourier coefficients is zero on \( L \). Katz [8] proved that this vanishing always occurs when the exponent \( s \) is three-valued. Katz’s methods work in arbitrary characteristic, but Feng’s work was specific to characteristic 2, so that Theorem 1.4 only concerns fields of characteristic 2. More recently, Katz [9] has shown that one can replace \( \mathbb{F}_2 \) by \( \mathbb{F}_3 \) in Theorem 1.4. The proof of Theorem 1.4 and its analogue in characteristic 3 verify parts of a conjecture by Helleseth, who proposed that the result should hold in arbitrary characteristic.

**Conjecture 1.5** (Helleseth Three-Valued Conjecture, 1976) For any prime \( p \), if \( [L : \mathbb{F}_p] \) is a power of two, then the spectrum of an invertible exponent is not three-valued.

This conjecture remains open for \( p > 3 \).

In this paper, we survey old and recent results dealing with Fourier coefficients of power mappings to conclude with a very interesting open question in the theory of finite fields.

## 2 Fourier coefficients and convolution

The **Fourier coefficient** at a point \( a \in L \) of a complex function \( F \) defined over \( L \) is

\[
\hat{F}(a) = \sum_{x \in L} F(x) \overline{\mu(ax)}.
\]

**Remark 2.1** \( \hat{F}(a) \) is a scalar product. The additive characters of \( L \) form an orthogonal basis of the complex mappings on domain \( L \).

If \( f : L \to L \), then we write \( \widehat{f}(a) \) in place of \( \mu \circ f(a) \) by a common abuse of notation. As mentioned in the Introduction, the Weil sum \( W_{L,s}(a) \) is nothing but the Fourier coefficient \( \hat{f}(a) \) of \( \mu \circ f \) when \( f(x) = x^s \).

If \( f : L \to L \) and \( b \in L \), then we write \( fb \) for the function \( bf \), that is, \( fb(x) = bf(x) \) for \( x \in L \). In certain applications it is important to understand the Fourier transform not only of \( f \), but of all scalar multiples \( fb \) of \( f \). Power permutations are special in this regard: if \( f(x) = x^s \) with \( \gcd(s, q - 1) = 1 \) and \( b \in L \), then

\[
\hat{fb}(a) = \sum_{x \in L} \mu(bx^s - ax) = \sum_{x \in L} \mu \left( (b^{\frac{1}{s}}x)^s - ab^{-\frac{1}{s}}(b^{\frac{1}{s}}x) \right) = \hat{f}(ab^{-\frac{1}{s}}),
\]

where \( 1/s \) is interpreted modulo \( q - 1 \). Also, when \( f(x) = x^s \) is a power permutation, \( \hat{fb}(a) \) is always a real number:

\[
\hat{fb}(a) = \sum_{x \in L} \mu(-bx^s - ax)) = \sum_{x \in L} \mu(b(-x)^s - a(-x)) = \hat{fb}(a),
\]

since the condition \( \gcd(s, q - 1) = 1 \) makes \( s \) odd when the characteristic of the field is odd.

Fourier coefficients satisfy general rules, namely, the inversion formula,

\[
\sum_{a \in L} \hat{F}(a) \mu(ax) = qF(x),
\]

or more generally the Poisson formula over an additive subgroup \( S \) of \( L \),

\[
\sum_{a \perp S} \hat{F}(a) \mu(ax) = \frac{q}{|S|} \sum_{s \in S} F(x + s),
\]
where \( S \) is considered a subspace of the \( \mathbb{F}_p \)-linear space \( L \) equipped with inner product \( (x, y) \mapsto \text{Tr}(xy) \), with \( \text{Tr}: L \to \mathbb{F}_p \) the absolute trace. There is also the Parseval-Plancherel identity,

\[
\sum_{a \in L} |\hat{F}(a)|^2 = q \sum_{x \in L} |F(x)|^2.
\]

In this context, one introduces the convolutional product of two complex mappings \( F \) and \( G \) at \( z \in L \),

\[
F \ast G(z) = \sum_{x+y=z} F(x)G(y).
\]

The \( \mathbb{C} \)-algebra of complex maps equipped with this product is usually denoted by \( \mathbb{C}[L] \). For \( b \in L \), we denote by \( \delta_b \) the Dirac function

\[
\delta_b(x) = \begin{cases} 1 & \text{if } x = b, \\ 0 & \text{otherwise}, \end{cases}
\]

and we refer to the set of functions \( \{\delta_b\}_{b \in L} \) as the Dirac basis, since it is a basis of the \( \mathbb{C} \)-vector space \( \mathbb{C}[L] \). Then \( \mathbb{C}[L] \) has \( \delta_0 \) for its unit element. The \( k \)th power of convolution is

\[
F^{[k]}(z) = \sum_{x_1+\cdots+x_k=z} F(x_1)F(x_2)\cdots F(x_k),
\]

and one has the well known trivialization formulas

\[
\begin{align*}
\hat{F} \ast \hat{G}(a) &= \hat{F}(a)\hat{G}(a), \\
q \hat{F} \hat{G}(a) &= \hat{F} \ast \hat{G}(a). \tag{3}
\end{align*}
\]

**Remark 2.2** The inversion formula and trivialization formulas show that the Fourier transform is a \( \mathbb{C} \)-algebra isomorphism from \( \mathbb{C}[L] \) into \( \mathbb{C}^L \) with

\[
\hat{\delta}_0 = 1, \quad \hat{1} = q \delta_0.
\]

In the Dirac basis \( \{\delta_b\}_{b \in L} \),

\[
\delta_b \ast F(t) = \sum_{y+x=t} \delta_b(y)F(x) = F(t - b),
\]

whence

\[
\delta_b \ast F = \sum_t F(t - b)\delta_t,
\]

and so, since \( \{\mu_a\}_{a \in L} \) is an eigenbasis for convolution by \( F \) in the \( \mathbb{C} \)-linear space \( \mathbb{C}[L] \), with \( \hat{F}(a) \) the eigenvalue for \( \mu_a \), we have

\[
\prod_{a \in L} \hat{F}(a) = \det[F(a - b)]_{a,b \in L}.
\]

Then the Helleseth Vanishing Conjecture (Conjecture 1.1) is equivalent to the following claim.

**Conjecture 2.3** (Helleseth’s 1976 Vanishing Conjecture, restated) *Let \( s \equiv 1 \pmod{p - 1} \) be an integer coprime to \( q - 1 \). The rank of the matrix \([\mu ((x - y)^s)]_{y,x \in L}\) is less than \( q - 1 \).*
For \( f : L \to L \), the product \( D(f) = \prod_{a \in L^\times} \hat{f}(a) \) of the Fourier coefficients on \( L^\times \) appears naturally in two ways. Firstly, by considering the convolution by the mapping \( x \mapsto \mu (f(x)) - 1 \), one can show that

\[-q D(f) = \det [\mu (f(x) - y)]_{x,y \in L}.\]

Secondly, if \( f(x) = x^s \) for an invertible exponent \( s \), the number of solutions in \( L^n \) of

\[
\begin{align*}
\{ & f(x_1) + f(x_2) + \ldots + f(x_n) = 0, \\
& \lambda^1x_1 + \lambda^2x_2 + \cdots + \lambda^n x_n = 0,
\end{align*}
\]

(4)

where \( \lambda \) has order \( q-1 \) in \( L^\times \), can be written as

\[
\frac{1}{q^2} \sum_{a,b} \mu_b \left( \sum_{i=1}^{n} f(x_i) \right) \bar{\mu}_a \left( \sum_{i=1}^{n} \lambda^i x_i \right) = \frac{1}{q^2} \sum_{a,b} \prod_{i=1}^{n} \hat{f}_b(a \lambda^i) = q^{n-2} + \left( \frac{q-1}{q^2} \right) \sum_{j=0}^{q-2} D_{j,n}(f),
\]

where \( D_{j,n}(f) = \prod_{k=j}^{j+n-1} \hat{f}(\lambda^k) \), which equals \( D(f) \) when \( n = q-1 \). In particular, as remarked by Helleseth, the Vanishing Conjecture is equivalent to saying that the number of solutions of the system (4) with \( n = q-1 \) is equal to \( q^{q-3} \).

### 3 Spectrum of a power mapping

Let \( F : L \to \mathbb{C} \). The set of the Fourier coefficients is called the spectrum of \( F \). The set of Fourier coefficients on \( L^\times \) is called the reduced spectrum of \( F \).

The values and the multiplicities of the Weil sums \( W_{L,s}(a) \) of exponent \( s \) do not change if we replace \( s \) by \( ps \) or \( 1/s \) (modulo \( q-1 \)). We write \( s' \sim s \) if there exists \( j \) such that \( s' \equiv pj s \pmod{q-1} \). We say that the exponents \( s' \) and \( s \) are equivalent and write \( s' \approx s \) if \( s' \sim s \) or \( s' \sim 1/s \).

Recall from (1) that if \( f(x) = x^s \) with \( \gcd(s,q-1) = 1 \) and \( b \neq 0 \), then

\[ \hat{f}_b(a) = \hat{f}(ab^{-1/s}), \]

where \( 1/s \) is interpreted modulo \( q-1 \). Thus \( f_b = bf \) has the same spectrum (reduced or not) as \( f \) for all \( b \in L^\times \). Note that a general power mapping does not satisfy this property, with a simple example being \( x \mapsto x^{q-1} \) when \( q > 2 \). For future work, it could be important to know more about the mappings satisfying this spectrum invariance property.

**Problem 3.1** (invariance) Find necessary and sufficient conditions for a map (or permutation) \( f : L \to L \) to have the property that the spectrum of \( f \) is equal to the spectrum of \( bf \) for all \( b \in L^\times \).

Let \( \zeta_p = \exp(2i\pi/p) \). Then let \( \wp = (1 - \zeta_p) \), the prime ideal above \( p \) in \( \mathbb{Z}[\zeta_p] \). For a power permutation \( f \), the \( \wp \)-divisibility of the Fourier coefficient follows from

\[ \hat{f}(a) \equiv \hat{f}(0) \equiv 0 \pmod{\wp}, \]

(5)

since \( 1 = \mu_0(x) = \mu_a(x) \pmod{\wp} \) for every \( x \in L \).
Another important fact satisfied by power permutations is the invariance of the spectrum under the action of the Galois group of $\mathbb{Q}(\zeta_p)$. Indeed, considering the element $\phi_r$ in $\text{Gal}(\mathbb{Q}(\zeta_p))$ that maps $\zeta_p$ to $\zeta_r^p$, one has

$$\phi_r(\hat{f}(a)) = \sum_{x \in L} \mu(rf(x) - arx) = \hat{f}_r(ar) = \hat{f}(ar^{1/s}).$$

**Lemma 3.2** (algebraic degree) The spectrum of a power permutation of exponent $s$ has all values in $\mathbb{Z}$ if and only if $s \equiv 1 \pmod{p-1}$. If $d | p-1$, then the Fourier coefficients reside in the degree $d$ extension of $\mathbb{Q}$ lying within $\mathbb{Q}(\zeta_p)$ if and only if $s \equiv 1 \pmod{(p-1)/d}$.

**Proof** The first part appears in Helleseth’s paper [7, Theorem 4.2], and is a consequence of the second part. Let $d | p-1$, and let $r$ be an element of multiplicative order $(p-1)/d$ in $\mathbb{F}_p^\times$. Then for $f(x) = x^s$, we see that $\phi_r(\hat{f}(a)) = \hat{f}(a)$ for all $a \in L$ if and only if $\hat{f}(ar^{1/s}) = \hat{f}(a)$ for all $a \in L$. By Fourier inversion, the latter is true if and only if $\mu \circ f(r^{1/s}x^s) = \mu \circ f(x)$ for all $x \in L$, which in turn is true if and only if $\mu(r^{1-s}x^s) = \mu(x^s)$ for all $x \in L$, which happens if and only if $r^{1-s} = 1$, i.e., if and only if $(p-1)/d$ divides $1-s$.

Assume that $f(x) = x^s$ with $s$ an $r$-valued exponent with values $A_1, A_2, \ldots, A_r$, and denote by $\sigma_i$ the $i$th signed elementary symmetric function of these values, that is,

$$\sigma_0 = 1, \quad \sigma_1 = -\sum_{i=1}^r A_i, \quad \ldots, \quad \sigma_r = (-1)^r \prod_{i=1}^r A_i.$$  

For all $a$ in $L$, we have

$$\sum_{i=0}^r \sigma_i \hat{f}(a)^{r-i} = \sigma_r \delta_0(a).$$

Denote the $n$th convolutional power of $\mu \circ f$ by

$$f^{[n]}(z) = \sum_{x_1 + \ldots + x_n = z} \mu(f(x_1) + \ldots + f(x_n)).$$

Then for all $z$ in $L$, we have

$$q \sum_{i=0}^r \sigma_i(A_1, \ldots, A_r) f^{[r-i]}(z) = \sigma_r(A_1, \ldots, A_r).$$

In particular, $q$ divides $\prod_{i=1}^r A_i$. Recall from Conjecture 1.1 that this product is actually conjectured to be 0 when $s \equiv 1 \pmod{p-1}$.

For any $f : L \to L$, the number of solutions in $L^n$ of the system

$$x_1 + x_2 + \ldots + x_n = u \\
f(x_1) + f(x_2) + \ldots + f(x_n) = v$$

is given by

$$N(u, v) = \frac{1}{q^2} \sum_{a,b} \sum_{x_1,\ldots,x_n} \mu_b \left( \sum_{i=1}^n f(x_i) - v \right) \bar{\mu}_a \left( \sum_{i=1}^n x_i - u \right) = \frac{1}{q^2} \sum_{a,b} \hat{f}_b(a)^n \mu(au - bv).$$
In [2], Aubry and Langevin used this relation and the little Fermat theorem to obtain the following congruence result.

**Theorem 3.3** (Aubry, Langevin, 2013) *Let $L$ be a finite field of order $q > 2$. If $f$ is a power permutation of $L$ of exponent $s \equiv 1 \pmod{p - 1}$, then there is an $a \in L^\times$ such that $\hat{f}(a) \equiv 0 \pmod{3}$.*

**Problem 3.4** Is it possible to obtain such a divisibility result involving another prime $\ell \neq p$?

The following result [8, Theorems 1.7, 1.9] proved the vanishing of a Fourier coefficient on $L^\times$ that finished the proof of Theorem 1.4.

**Theorem 3.5** (Katz, 2012) *If $x^s$ is a three-valued power permutation, then $s$ is singular, $s \equiv 1 \pmod{p - 1}$, and the spectrum $\{0, A, B\}$ of $x^s$ lies in $\mathbb{Z}$.*

The action of the Galois group of the cyclotomic field is the main ingredient of the proof.

**Problem 3.6** Find an analogue of Theorem 3.5 for four-valued exponents.

When $f(x) = x^s$ is a three-valued power permutation with values 0, $A$, and $B$, the number of solutions in $L^2$ of the system

\begin{align*}
x + y &= 1 \\
x^s + y^s &= 1
\end{align*}

is known (e.g., see [9, Lemma 4.2]) to be

$$V = N(1, 1) = A + B - \frac{AB}{q}. \quad (6)$$

The following relation between the third power moment of the Fourier coefficient and $N(1, 1)$ is equivalent to an observation of Blokhuis and Calderbank [3] about the weight distribution of certain cyclic codes:

\begin{align*}
\sum_{a \in L} \hat{f}(a)^3 &= \sum_{x, y, z \in L} \mu(x^s + y^s + z^s) \sum_{a \in L} \mu_a(x + y + z) \\
&= q \sum_{x + y + z = 0} \mu(x^s + y^s + z^s) \\
&= q \sum_{x + y = 0} \mu(x^s + y^s) + q \sum_{z \neq 0} \sum_{x + y + z = 0} \mu(x^s + y^s + z^s) \\
&= q \sum_{x} \mu(x^s + (-x)^s) + q \sum_{z \neq 0} \sum_{x + y + 1 = 0} \mu((X^s + Y^s + 1)z^s) \\
&= q^2 + q(q - 1)V - q(q - V) \\
&= q^2 V. \quad (7)
\end{align*}

In the penultimate equality, we use the fact that the condition gcd($s, q - 1$) makes $s$ odd when the characteristic of $L$ is odd (and so $N(1, 1) = N(-1, -1)$).
More generally, the product of nonzero spectral values $A_1, A_2, \ldots, A_n$ appears naturally by Fourier analysis. Define the signed elementary symmetric functions

\[ \sigma_0 = 1, \quad \sigma_1 = -\sum_{i=1}^{n} A_i, \quad \ldots, \quad \sigma_n = (-1)^n \prod_{i=1}^{n} A_i. \]

Let us consider the polynomial

\[ P(T) = \prod_{i=1}^{n} (T - A_i) = \sum_{i=0}^{n} \sigma_{n-i} T^i. \]

The rule of trivializations (3) shows that

\[ \sum_{i=0}^{n} \sigma_{n-i} F^{[i]} * F = 0. \]

This means that $\sum_{i=0}^{n} \sigma_{n-i} F^{[i]}$ is in the kernel of convolution by $F$. Recall that the characters $\{\mu_a : a \in L\}$ form an eigenbasis for convolution by $F$ in the $\mathbb{C}$-linear space $\mathbb{C}[L]$, with $\hat{F}(a)$ the eigenvalue for $\mu_a$. If we let $Z = \{a \in L : \hat{F}(a) = 0\}$, then $\{\mu_c : c \in Z\}$ is a basis of the nullspace for convolution by $F$, and we can write

\[ \sum_{i=0}^{n} \sigma_{n-i} F^{[i]} = \sum_{c \in Z} \lambda_c \mu_c, \]

for some coefficients $\lambda_c \in \mathbb{C}$. Taking the Fourier coefficient at $c \in Z$, we obtain with

\[ \lambda_c = \frac{(-1)^n}{q} \prod_{i=1}^{n} A_i. \]

**Problem 3.7 (product)** For which $s$ is the product of non-zero spectral values $\prod_{i=1}^{n} A_i$ of $F(x) = \mu(x^s)$ divisible by $q$?

### 4 $p$-divisibility

For a power permutation $f(x) = x^s$, we define

\[ V_L(s) = \min_{a \in L} \text{val}_p \left( \hat{f}(a) \right). \]

This minimum valuation is deducible from Stickelberger’s Theorem on the $p$-divisibility of the Gauss sum

\[ \tau_L(\chi) = \sum_{a \in L^\times} \mu(a) \chi(a), \]

for $\chi$ a multiplicative character of $L$. One has [1, eq. (3)] the formula

\[ \hat{f}(a) = \frac{q}{q-1} + \frac{1}{q-1} \sum_{\chi \neq 1} \tau_L(\chi) \tau_L(\chi^s) \chi^s(-a), \]

whence [1, Lemma 4.1]

\[ V_L(s) = \min_{1 \neq \chi \in L^\times} \text{val}_p \left( \tau_L(\chi) \tau_L(\chi^s) \right). \]

Using the Hasse-Davenport relation, given an extension $L/K$, we obtain [1, Corollary 4.2]

\[ V_L(s) \leq V_K(s) \times [L : K]. \]

(8)
Recall the Helleseth Three-Valued Conjecture (Conjecture 1.5), which states that if \([L : \mathbb{F}_p]\) is a power of two, then the spectrum of a power permutation is not three-valued. Feng [6, Theorem 2] showed that this conjecture holds in characteristic \(p = 2\) under the additional assumption that at least one Fourier coefficient in the reduced spectrum vanishes. In [8, Corollary 1.10], [9, Theorem 1.7] Katz showed that the conjecture holds in characteristic \(p = 2\) and 3 without additional assumptions.

Feng uses the following proposition [4] to obtain Conjecture 1.5 in even characteristic under the assumption that the exponent is singular.

**Proposition 4.1** (Calderbank, McGuire, Poonen, Rubinstein, 1996) Let \(s \not\approx 1\) be an invertible exponent. If \([L : \mathbb{F}_2]\) is a power of two, then

\[
2 \times V_L(s) \leq [L : \mathbb{F}_2].
\]

**Remark 4.2** In fact, if \(s \not\approx 1\) is an invertible exponent and \([L : \mathbb{F}_p]\) is a power of two, then \(2 \times V_L(s) \leq [L : \mathbb{F}_p]\) still holds for an arbitrary prime \(p\), as we shall show below.

The following result [1, Corollary 4.4] shows what happens when \(L/K\) is a quadratic extension in which \(s \equiv 1 \pmod{|K^\times|}\) but \(s \not\equiv 1 \pmod{|L^\times|}\). The characteristic 2 case was proved by Charpin [5, Theorem 1, Corollary 1].

**Lemma 4.3** (quadratic extension) Let \(L/K\) be a quadratic extension. If \(x^s\) is constant over \(K^\times\) but not over \(L^\times\), then there is an \(a \in L^\times\) such that \(\hat{f}(a) = -|K|\) and \(2 \times V_L(s) = [L : \mathbb{F}_p]\).

Using (8), we now see that if \(1 \not\approx s \equiv 1 \pmod{p - 1}\) and \([L : \mathbb{F}_p] = 2^r\), then \(2 \times V_L(s) \leq [L : \mathbb{F}_p]\), thus validating Remark 4.2.

## 5 Differential multiplicity and the uniformity property

For \(f(x) = x^s\) a power permutation over \(L\), we denote by \(N(u, v)\) the number of solutions in \(L^2\) of the system

\[
x + y = u,
\]

\[
f(x) + f(y) = v.
\]

Since \((-y)^s = -y^s\), \(N(u, v)\) is also the number of solutions of \(x - y = u, f(x) - f(y) = v\). Therefore, the numbers \(N(u, v)\) are called the differential multiplicities of the exponent \(s\).

Recall that \(N(1, 1)\) arose in (6) and was subsequently shown to be connected to the third power moment of the Fourier coefficients of \(f\). Note that if \(u \neq 0\), then \(N(u, v) = N(1, v/u^s)\).

**Definition 5.1** We say that a power permutation \(f\) is \(\Delta\)-uniform over \(L\) if the number of solutions \(N(1, v)\) in \(L^2\) of the system

\[
x + y = 1,
\]

\[
f(x) + f(y) = v,
\]

is equal to 0 or \(\Delta\) for all \(v \neq 1\).
Katz [9, Lemma 4.4, Theorem 4.5, Remark 4.6] proved the following theorem using the group algebra techniques of Feng.

**Theorem 5.2** (Katz) Let \( f(x) = x^s \) be a power permutation over \( L \) with three-valued spectrum \( \{0, A, B\} \), and write \( A = p^a \alpha, B = p^b \beta \) and \( A - B = p^c \gamma \) where \( p \nmid \alpha, \beta, \gamma \). Then \( \alpha \beta \gamma \) divides the differential multiplicities \( N(u, v) \) for all \( v \neq u^s \) and

\[
|\alpha \beta \gamma| \leq -\frac{AB}{q},
\]

leading to the alternative:

(i). \( a, b > \frac{1}{2} \left[ L : \mathbb{F}_p \right] \) (impossible when \( L : \mathbb{F}_p \) is a power of 2), or

(ii). \( a = b = \frac{1}{2} \left[ L : \mathbb{F}_p \right], |\gamma| = 1, \) and \( s \) is a \( |\alpha \beta| \)-uniform exponent.

**Remark 5.3** Note that because of Lemma 4.3, case (i) is impossible when \( L : \mathbb{F}_p \) is a power of 2.

**Corollary 5.4** If \( p = 2 \) or \( p = 3 \) then the Helleseth Three-Valued Conjecture is true.

**Proof** \( N(1, 1) \) is divisible by \( p \) when \( p = 2 \) (see [6, Proof of Theorem 2]) and when \( p = 3 \) (see [9, Lemma 4.2]). If \( f(x) = x^s \) is three-valued, then \( A \) and \( B \) lie in \( \mathbb{Z} \) (by Theorem 3.5), and so they are divisible by \( p \) by (5), and then (6) tells us that \( pq \mid AB \), so that we cannot be in case (ii) of Theorem 5.2. On the other hand, Remark 5.3 shows that case (i) is impossible when \( L : \mathbb{F}_p \) is a power of 2.

We end this section by proving Theorem 5.2 without the language of the group algebra. Let \( f(x) = x^s \) be a power permutation with a three-valued spectrum with values 0, \( A \), and \( B \). In view of (1), for each \( u \in L^\times \), the spectrum of \( f_u \) has the same values 0, \( A \), and \( B \). Write

\[
A = p^a \alpha, \quad B = p^b \beta, \quad A - B = p^c \gamma
\]

with \( \alpha, \beta \) and \( \gamma \) coprime to \( p \).

**Lemma 5.5** The integers \( \alpha, \beta \) and \( \gamma \) are pairwise coprime, \( \alpha \gamma \) divides \( q - B \), and \( \beta \gamma \) divides \( q - A \).

**Proof** From the first and second power moments of the spectrum of \( f \), one may deduce (see [8, Proposition 3.2]) that if \( \hat{f}(x) = A \) for \( N_A \) values of \( x \in L^\times \) and \( \hat{f}(x) = B \) for \( N_B \) values of \( x \in L^\times \), then

\[
N_A = \frac{q(q - B)}{A(A - B)},
\]

\[
N_B = \frac{q(q - A)}{B(B - A)},
\]

from which all of our claims quickly follow. \( \square \)
Now we proceed to a proof of Theorem 5.2. Using a character counting principle, we have

\[ N(u, v) = \frac{1}{q^2} \sum_{y,z} \sum_{w,x \in L} \mu_x(f(y) + f(z) - v) \bar{\mu}_w(y + z - u) \]  

(9)

\[ = \frac{1}{q^2} \sum_{w,x \in L} \hat{f}_x(w)^2 \bar{\mu}_x(v) \mu_w(u). \]

In other words, \( \hat{f}_x(w)^2 \) is a Fourier coefficient of \( N \) over the group \( L \times L \). On the other hand,

\[ \frac{1}{q^2} \sum_{w,x \in L} \hat{f}_x(w) \bar{\mu}_x(v) \mu_w(u) = \frac{1}{q} \sum_{x \in L} \mu_x(f(u)) \bar{\mu}_x(v) \]  

(10)

\[ = \delta_v(f(u)) = \delta_v(u^x). \]

By subtraction of \( A \) times (10) from (9), it follows that \( N(u, v) \) is divisible by \( \beta \gamma \) when \( v \neq u^x \), and similarly, by subtracting \( B \) times (10) from (9), it follows that \( N(u, v) \) is divisible by \( \alpha \gamma \) when \( v \neq u^x \). So when \( v \neq u^x \), Lemma 5.5 shows us that \( \alpha \beta \gamma | N(u, v) \).

Applying the Parseval relation to the mapping \( N \),

\[ \sum_{w,x} \hat{f}_x(w)^4 = q^2 \sum_{u,v} N(u, v)^2, \]  

(11)

where we use \( \hat{f}_x(w)^4 \) in place of \( |\hat{f}_x(w)|^4 \) because (2) shows that \( \hat{f}_x(w) \) is always a real number. For our power permutation \( f \), recall that for any \( x \in L^\times \), the function \( f_x = xf \) has the same spectrum as \( f \), and note that \( \hat{f}(0) = 0 \). On the other hand \( \hat{f}_0 = 0 \) has spectrum \( \hat{f}_0(0) = q \) and \( \hat{f}_0(w) = 0 \) for \( w \in L^\times \). Also note that \( N(u, v) = N(1, v/u^x) \) and \( N(u, 0) = 0 \) when \( u \neq 0 \), while \( N(0, 0) = q \) and \( N(0, v) = 0 \) when \( v \neq 0 \). With these observations, (11) becomes

\[ \sum_{w} \hat{f}(w)^4 = q^2 \sum_{v \neq 0} N(1, v)^2, \]  

(12)

and since the spectrum is three-valued with values 0, \( A \), and \( B \), we have

\[ \sum_{w} \hat{f}(w)^4 = (A + B) \sum_{w} \hat{f}(w)^3 - AB \sum_{w} \hat{f}(w)^2 \]

\[ = (A + B)q^2 V - ABq^2, \]

where we have used the calculation (7) for the third power moment, and the well-known value \( q^2 \) of the second power moment (which can be obtained by a similar, but easier calculation). We substitute the fourth power moment into (12) to obtain

\[ -V^2 + (A + B)V - AB = \sum_{v \neq \{0, 1\}} N(1, v)^2, \]

because \( V \) denotes the same number as \( N(1, 1) \). Then since \( \alpha \beta \gamma \) divides \( N(1, v) \) when \( v \neq 1 \), we have

\[ N(1, v)^2 \geq |\alpha \beta \gamma| N(1, v) \]  

(13)

for all \( v \neq 1 \), and so

\[ -(V - A)(V - B) \geq |\alpha \beta \gamma| \sum_{v \neq \{0, 1\}} N(1, v) \]  

(14)

\[ = |\alpha \beta \gamma|(q - V). \]
since \( \sum_v N(1, v) = q \), inasmuch as it counts the solutions in \( L^2 \) of \( x + y = 1 \), and we have noted that \( N(1, 1) = V \) and \( N(1, 0) = 0 \). We substitute the value of \( V \) from (6) into (14), and simplify to obtain

\[
|\alpha\beta\gamma| \leq \frac{-AB}{q}.
\]

Note that this proves that \( A \) and \( B \) have opposite sign, and then

\[
|\gamma| \leq \frac{p^{a+b}}{q}.
\]

(15)

For the rest, we proceed as in the proof of Theorem 4.5 and Remark 4.6 in [9]. If \( a \neq b \), then we would have \( c = \min\{a, b\} \). Then let \( d = \max\{a, b\} \), and so \( q|A - B| = qp^c|\gamma| \leq p^{a+b+c} = p^{2c+d} \). But since \( A \) and \( B \) have opposite signs, \( |A - B| > \max\{|A|, |B|\} \geq p^d \), so that \( qp^d < q|A - B| \leq p^{2c+d} \), and so \( p^c > \sqrt[q]{q} \), and thus \( a, b > \frac{1}{2}[L : \mathbb{F}_p] \), which is case (i) in the statement of Theorem 5.2.

If \( a = b \), then inequality (15) shows that \( a = b \geq \frac{1}{2}[L : \mathbb{F}_p] \), and if this inequality is strict, we are again in case (i). Otherwise, we have \( a = b = \frac{1}{2}[L : \mathbb{F}_p] \), and then \( |\gamma| = 1 \) and inequality (15) becomes an equality, as do the previous inequalities from which it was deduced, and in particular (13) shows that \( N(1, v) = 0 \) or \( |\alpha\beta\gamma| = |\alpha\beta| \) for all \( v \neq 1 \), that is, \( s \) is \( |\alpha\beta| \)-uniform. This is case (ii) in the statement of Theorem 5.2.

We have already noted why case (i) is impossible when \([L : \mathbb{F}_p] \) is a power of 2 in Remark 5.3. This completes the proof of Theorem 5.2.

### 6 Conjectures on differential uniformity

The previous section shows that the Helleseth Three-Valued Conjecture depends on the nonexistence of uniform exponents in certain cases. We present a numerical experiment [14] which shows that the nonexistence of such exponents could be the key point to obtain a proof of Helleseth’s conjecture.

**Definition 6.1** Let \( s \) be an invertible exponent over the finite field \( L \). We say that \( s \) is a nice exponent over \( L \) if the number \( N(1, v) \) of solutions in \( L^2 \) of

\[
x + y = 1,
\]

\[
x^s + y^s = v,
\]

takes at most 3 values as \( v \) runs through \( L \).

**Remark 6.2** A \( \Delta \)-uniform exponent is nice.

Recall the relation \( \approx \) defined near the beginning of Section 3.

**Remark 6.3** If \( s \) is a nice exponent, then every exponent \( s' \approx s \) equivalent to \( s \) is also nice.

**Remark 6.4** If \( s \approx 1 \) then \( s \) is trivially a nice exponent with two differential multiplicities: 0 and \( q \).

We show two paradigmatic examples of nice exponents in the following propositions.
Proposition 6.5 The exponent $s = 3$ is nice if and only if $q \not\equiv 1 \pmod{3}$, with the following differential multiplicities:

| characteristic | differential multiplicities | respective frequencies |
|----------------|----------------------------|------------------------|
| 2              | 0, 2                       | $q/2, q/2$             |
| 3              | 0, $q$                     | $q - 1, 1$             |
| $p > 3$        | 0, 1, 2                    | $q/2 - 1, 1, q/2 - 1$  |

Proof The congruence condition is necessary and sufficient to make 3 an invertible exponent, and the result for characteristic 3 is trivial, for then $3 \equiv 1$. In other characteristics, $N(1, v)$ is the number of solutions in $L$ of $x^3 + (1 - x)^3 = v$, which is the number of roots of the quadratic $x^2 - x + (v - 1)/3 = 0$. In characteristic 2, the additive Hilbert Theorem 90 shows that this quadratic polynomial has zero or two roots depending on whether the absolute trace of $(v - 1)/3$ is 1 or 0, respectively. In odd characteristic, the quadratic polynomial has zero, one, or two roots depending on whether the discriminant $(7 - 4v)/3$ is a quadratic nonresidue, zero, or a quadratic residue, respectively.

Proposition 6.6 The exponent $s = q - 2$ is nice if and only if $q \not\equiv 1 \pmod{6}$, with the following differential multiplicities:

| order          | differential multiplicities | respective frequencies |
|----------------|-----------------------------|------------------------|
| $q \equiv 2 \pmod{6}$ | 0, 2                       | $q/2, q/2$             |
| $q \equiv 3 \pmod{6}$ | 0, 2, 3                    | $(q + 1)/2, (q - 3)/2, 1$ |
| $q \equiv 4 \pmod{6}$ | 0, 2, 4                    | $q/2 + 1, q/2 - 2, 1$   |
| $q \equiv 5 \pmod{6}$ | 0, 1, 2                    | $(q - 1)/2, 1, (q - 1)/2$ |

Proof The exponent $s$ is always invertible, and odd when $p$ is odd, so that $x^s + y^s = 0$ if and only if $y = -x$, which makes $N(1, 0) = 0$. The pairs $(0, 1)$ and $(1, 0)$ are solutions of $x + y = 1, x^s + y^s = 1$, and for the other contributions, we may assume $vxy \neq 0$, so that

$$x + y = 1, \quad x^s + y^s = v \quad \iff \quad \frac{1}{xy} = v, \quad x + y = 1.$$  

Thus $N(1, 1)$ is two plus the number of roots of $x^2 - x + 1$, and $N(1, v)$ for $v \neq 0, 1$ is the number of roots of $x^2 - x + 1/v$. Since $x^2 - x + 1$ is the sixth cyclotomic polynomial in fields of characteristic $p > 3$ (while it degenerates to the third cyclotomic polynomial in characteristic 2 and to $(x + 1)^2$ in characteristic 3), we see that

$$N(1, 1) = \begin{cases} 
2 & \text{if } q \equiv 2 \pmod{3}, \\
3 & \text{if } q \equiv 0 \pmod{3}, \\
4 & \text{if } q \equiv 1 \pmod{3}.
\end{cases}$$

If $v \neq 0, 1$ and we are in characteristic 2, then the additive Hilbert Theorem 90 shows that $x^2 - x + 1/v$ has zero or two solutions depending on whether the absolute trace of $1/v$ is 1 or 0, respectively. So if $[L : \mathbb{F}_2]$ is odd ($q \equiv 2 \pmod{6}$), we obtain $q/2 - 1$ instances each of the differential multiplicities 0 and 2, while if $[L : \mathbb{F}_2]$ is even ($q \equiv 4 \pmod{6}$) we obtain $q/2$ instances of 0 and $q/2 - 2$ instances of 2.

If $v \neq 0, 1$ and we are in odd characteristic, the quadratic $x^2 - x + 1/v$ has zero, one, or two solutions depending on whether the discriminant $1 - 4/v$ is a quadratic nonresidue, zero, or a quadratic residue, respectively. Our discriminant runs through all values except 1 and $-3$. In characteristic 3 ($q \equiv 3 \pmod{6}$), this produces $(q - 1)/2$ instances differential
multiplicity 0 and \((q - 3)/2\) instances of differential multiplicity 2. When \(-3\) is a quadratic residue (i.e., when \(q \equiv 1 \pmod{6}\)), this produces one instance of differential multiplicity 1, \((q - 1)/2\) instances differential multiplicity 0, and \((q - 5)/2\) instances of differential multiplicity 2. When \(-3\) is a quadratic nonresidue (i.e., when \(q \equiv 5 \pmod{6}\)), this produces one instance of differential multiplicity 1, and \((q - 3)/2\) instances each differential multiplicities 0 and 2. We collate the information about the various \(N(1, v)\) to see that we get a nice exponent if and only if \(q \not\equiv 1 \pmod{6}\).

It is easy to find numerically all of the differential multiplicities for exponents over a small field using the Zech logarithm. Here, we focus on odd characteristic. Let \(\omega\) be a primitive root of the finite field \(L\) of order \(q\). Then for \(k \neq (q - 1)/2\), we define \(\text{Zech}(k)\) to be the unique \(\ell\) such that \(\omega^{\ell} = 1 + \omega^k\). The logarithm of

\[
x^s + (1 - x)^s = x^s \left(1 + \left(\frac{1 - x}{x}\right)^s\right)
\]

for \(x = \omega^k\) is

\[
k \times s + \text{Zech}[s \times (\text{Zech}[n + k] - k)].
\]

where \(n = (q - 1)/2\). In the numerical experiment [14], all nice exponents over fields of characteristic \(2 \leq p \leq 31\) and order \(q \leq 2^{20}\) were found. Nice exponents \(s\) with \(s \not\approx 1\) occur in the majority of these fields. For example, Table 1 shows the nice exponents (\(\not\approx 1\)) up to the equivalence \(\approx\) for the fields of order \(11^m\) with \(m \leq 5\). The sixth line of the table indicates that 241 is nice over \(F_{11^4}\), congruent to 1 modulo 10, with three differential multiplicities 0, 2, and 121. The \(s^\dagger\) indicates that \(s \approx q - 2\).

As one can see in this example, the nice exponents \(s \not\approx 1\) are rare, and all have differential multiplicity 2. Surprisingly, this seems to be a general fact. Indeed, for the characteristics 3 to 31, all the observed nice exponents \(s \not\approx 1\) have 2 as a differential multiplicity.

**Problem 6.7** All nice exponents \(s \not\approx 1\) over the prime fields of characteristic \(p < 5000\) were found in the numerical experiment [14], and they all correspond to the paradigmatic examples of Propositions 6.5 and 6.6. Is this a general property?

We propose some conjectures based on our numerical evidence.

**Conjecture 6.8** (nice exponent) Let \(s \not\approx 1\) be an exponent over a finite field of odd characteristic. If \(s\) is nice, then 2 is a differential multiplicity.

**Table 1** Nice exponents \(s \not\approx 1\) over the fields \(F_{11^m}\)

| degree | \(s\) | \(s \pmod{p-1}\) | differential multiplicities |
|--------|------|-----------------|-----------------------------|
|        |      | frequency [value]|                             |
| 1      | 3    | 3               | 5 [0] 1 [1] 5 [2]           |
|        | 9\dagger | 9               | 5 [0] 1 [1] 5 [2]           |
| 2      | 3    | 3               | 665 [0] 1 [1] 665 [2]       |
|        | 1209\dagger | 9               | 665 [0] 1 [1] 665 [2]       |
| 4      | 241  | 1               | 7380 [0] 7260 [2] 1 [121]   |
| 5      | 3    | 3               | 80525 [0] 1 [1] 80525 [2]   |
|        | 146409\dagger | 9               | 80525 [0] 1 [1] 80525 [2]   |
We can make an even stronger conjecture.

**Conjecture 6.9** (optimist) *Let $s \not\approx 1$ be an exponent over a finite field of odd characteristic. If $s$ is invertible, then 2 is a differential multiplicity.*

Then we claim that we have the following implications among conjectures

$$\text{optimist} \implies \text{nice exponent} \implies \text{Helleseth Three-Valued}.$$

**Remark 6.10** It is interesting to notice that Conjecture 6.8 implies the Helleseth Three-Valued Conjecture. Indeed, let $s$ be an exponent over a field $L$ of characteristic $p > 3$ with $[L: \mathbb{F}_p]$ a power of two, and suppose that $s$ is three-valued with values 0, $A$, and $B$. Write $A = \alpha p^a$, $B = \beta p^b$, and $A - B = \gamma p^c$ with $p \nmid \alpha, \beta, \gamma$. Now assume Conjecture 6.8 holds, so that 2 is a differential multiplicity of $s$. Since we must be in case (ii) of Theorem 5.2, this shows that $|\alpha \beta| = 2$ and $a = b = \frac{1}{2} [L: \mathbb{F}_p]$. Since the nonzero spectral values $A$ and $B$ are opposites in sign (as was seen in our proof of Theorem 5.2), this means that $|A - B| = 3 \sqrt{|L|}$, but since $p > 3$, this contradicts the fact that $|\gamma| = 1$, which also must hold in case (ii) of Theorem 5.2. Thus, if Conjecture 6.8 is true, then Helleseth’s Conjecture will be true in all characteristics $p > 3$. Since Helleseth’s Conjecture is already proved in characteristic 2 and 3 (see Corollary 5.4), it would then be fully established.

**Acknowledgments** The first author was supported in part by a Research, Scholarship, and Creative Activity Award from California State University, Northridge. The first author was also supported in part by the Institut de Mathématiques de Toulon at Université de Toulon as a visiting professor. The authors thank anonymous reviewers for helpful corrections and suggestions.

**References**

1. Aubry, Y., Katz, D.J., Langevin, P.: Cyclotony of Weil sums of binomials (2013). arXiv:1312.3889 [math.NT]
2. Aubry, Y., Langevin, P.: On a conjecture of Helleseth. In: Algebraic informatics, volume 8080 of Lecture Notes in Comput. Sci., pp. 113–118. Springer, Heidelberg (2013)
3. Blokhuis, A., Calderbank, A.R.: Unpublished note
4. Calderbank, A.R., McGuire, G., Poonen, B., Rubinstein, M.: On a conjecture of Helleseth regarding pairs of binary $m$-sequences. IEEE Trans. Inform. Theory 42(3), 988–990 (1996)
5. Charpin, P.: Cyclic codes with few weights and Niho exponents. J. Combin. Theory Ser. A 108(2), 247–259 (2004)
6. Feng, T.: On cyclic codes of length $2^{2r} - 1$ with two zeros whose dual codes have three weights. Des. Codes Cryptogr. 62(3), 253–258 (2012)
7. Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discrete Math. 16(3), 209–232 (1976)
8. Katz, D.J.: Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth. J. Combin. Theory Ser. A 119(8), 1644–1659 (2012)
9. Katz, D.J.: Divisibility of Weil sums of binomials (2014). arXiv:1407.7923 [math.NT]
10. Katz, N., Livně, 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)
11. Kononen, K.P., Rinta-aho, M.J., Vañanen, K.O.: On integer values of Kloosterman sums. IEEE Trans. Inform. Theory 56(8), 4011–4013 (2010)
12. Lachaud, G., Wolfmann, J.: Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. C. R. Acad. Sci. Paris Sér. I Math. 305(20), 881–883 (1987)
13. Langevin, P.: Numerical projects page: spectra of power maps (2007). http://langevin.univ-tln.fr/project/spectrum
14. Langevin, P.: Numerical projects page : nice exponents, 2013 and 2015. http://langevin.univ-tln.fr/project/expo