Power Permutations, Three-Valued Weil Sums, and Helleseth's Conjecture

Daniel J. Katz
Department of Mathematics
California State University, Northridge

Yet Another Conference on Cryptography
Porquerolles, France
11 June 2014

Power Permutations

- p prime
- $q = p^e$
- $\mathbb{F}_q$ finite field of order q
- d a positive integer with $\gcd(d, q-1) = 1$
- $x \mapsto x^d$ is a permutation of $\mathbb{F}_q$

Example: $q = 5^1$, $d = 3$

$0 \mapsto 0^3 = 0$

$1 \mapsto 1^3 = 1$

$2 \mapsto 2^3 = 3$

$3 \mapsto 3^3 = 2$

$4 \mapsto 4^3 = 4$

p-Ary Functions

- $\mathbb{F}_q = \mathbb{F}_{p^e}$ finite field of characteristic p
- $\gcd(d, q-1) = 1$
- $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ absolute trace:
  $$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{e-1}}$$
- $x \mapsto \mathrm{Tr}(x^d)$ maps from $\mathbb{F}_q$ to $\mathbb{F}_p$

  regarding $\mathbb{F}_q = \mathbb{F}_{p^e}$ as vector space ${\mathbb{F}_p}^e$

  makes $x \mapsto \mathrm{Tr}(x^d)$ a p-ary function on ${\mathbb{F}_p}^e$

E.g., $\mathbb{F}_{5^2} = \mathbb{F}_5 \oplus \mathbb{F}_5\alpha$, $\alpha^2 + \alpha + 2 = 0$, $\binom{u}{v} = u + v\alpha$, $x \mapsto \mathrm{Tr}(x^7)$

$$\left\{\binom{0}{0}, \binom{1}{2}, \binom{2}{4}, \binom{3}{1}, \binom{4}{3}\right\} \mapsto 0$$
$$\left\{\binom{0}{3}, \binom{2}{0}, \binom{2}{2}, \binom{2}{3}, \binom{4}{2}\right\} \mapsto 1$$
$$\left\{\binom{0}{4}, \binom{1}{0}, \binom{1}{1}, \binom{1}{4}, \binom{2}{1}\right\} \mapsto 2$$
$$\left\{\binom{0}{1}, \binom{4}{0}, \binom{4}{4}, \binom{4}{1}, \binom{3}{4}\right\} \mapsto 3$$
$$\left\{\binom{0}{2}, \binom{3}{0}, \binom{3}{3}, \binom{3}{2}, \binom{1}{3}\right\} \mapsto 4$$

Question of Nonlinearity

- $\mathbb{F}_q = \mathbb{F}_{p^e}$ finite field of characteristic p, $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$
- $\gcd(d, q-1) = 1$
- $x \mapsto \mathrm{Tr}(x^d)$ a p-ary function
- How nonlinear is $x \mapsto \mathrm{Tr}(x^d)$?
- Compare with $\mathbb{F}_p$-linear functionals of $\mathbb{F}_q$

  these are $\phi_a(x) = \mathrm{Tr}(ax)$ for $a \in \mathbb{F}_q$

$\mathbb{F}_{5^2} = \mathbb{F}_5(\alpha)$, $\alpha^2 + \alpha + 2 = 0$, $\binom{u}{v} = u + v\alpha$, $x \mapsto \mathrm{Tr}((1+4\alpha)x)$

$$\left\{ \binom{0}{0}, \binom{1}{1}, \binom{2}{2}, \binom{3}{3}, \binom{4}{4} \right\} \mapsto 0$$
$$\left\{ \binom{2}{0}, \binom{3}{1}, \binom{4}{2}, \binom{0}{3}, \binom{1}{4} \right\} \mapsto 1$$
$$\left\{ \binom{4}{0}, \binom{0}{1}, \binom{1}{2}, \binom{2}{3}, \binom{3}{4} \right\} \mapsto 2$$
$$\left\{ \binom{1}{0}, \binom{2}{1}, \binom{3}{2}, \binom{4}{3}, \binom{0}{4} \right\} \mapsto 3$$
$$\left\{ \binom{3}{0}, \binom{4}{1}, \binom{0}{2}, \binom{1}{3}, \binom{2}{4} \right\} \mapsto 4$$

Comparison

How to compare $x \mapsto \mathrm{Tr}(x^7)$

$$\left\{ \binom{0}{0}, \binom{1}{2}, \binom{2}{4}, \binom{3}{1}, \binom{4}{3} \right\} \mapsto 0$$
$$\left\{ \binom{0}{3}, \binom{2}{0}, \binom{2}{2}, \binom{2}{3}, \binom{4}{2} \right\} \mapsto 1$$
$$\left\{ \binom{0}{4}, \binom{1}{0}, \binom{1}{1}, \binom{1}{4}, \binom{2}{1} \right\} \mapsto 2$$
$$\left\{ \binom{0}{1}, \binom{4}{0}, \binom{4}{4}, \binom{4}{1}, \binom{3}{4} \right\} \mapsto 3$$
$$\left\{ \binom{0}{2}, \binom{3}{0}, \binom{3}{3}, \binom{3}{2}, \binom{1}{3} \right\} \mapsto 4$$

with $x \mapsto \mathrm{Tr}((1+4\alpha)x)$

$$\left\{ \binom{0}{0}, \binom{1}{1}, \binom{2}{2}, \binom{3}{3}, \binom{4}{4} \right\} \mapsto 0$$
$$\left\{ \binom{2}{0}, \binom{3}{1}, \binom{4}{2}, \binom{0}{3}, \binom{1}{4} \right\} \mapsto 1$$
$$\left\{ \binom{4}{0}, \binom{0}{1}, \binom{1}{2}, \binom{2}{3}, \binom{3}{4} \right\} \mapsto 2$$
$$\left\{ \binom{1}{0}, \binom{2}{1}, \binom{3}{2}, \binom{4}{3}, \binom{0}{4} \right\} \mapsto 3$$
$$\left\{ \binom{3}{0}, \binom{4}{1}, \binom{0}{2}, \binom{1}{3}, \binom{2}{4} \right\} \mapsto 4$$

Method of Comparison

- binary functions $f, g\colon \mathbb{F}_{2^e} \to \mathbb{F}_2$

  count # of agreements - # of disagreements

  correlation $= \sum_{x \in \mathbb{F}_{2^e}} (-1)^{f(x)-g(x)}$

  note: -1 is the primitive 2nd root of unity

- p-ary functions $f, g\colon \mathbb{F}_{p^e} \to \mathbb{F}_p$

  $\zeta_p = e^{2\pi i/p}$

  correlation $= \sum_{x \in \mathbb{F}_{p^e}} \zeta_p^{f(x)-g(x)}$

$\mathbb{F}_{25}$, $\alpha^2 + \alpha + 2 = 0$, $f(x) = \mathrm{Tr}(x^7)$, $g(x) = \mathrm{Tr}((1+4\alpha)x)$

$$\sum_{x \in \mathbb{F}_{25}} \zeta_5^{\mathrm{Tr}(x^7) - \mathrm{Tr}((1+4\alpha)x)} = 7 \cdot 1 + 7\zeta_5 + 2\zeta_5^2 + 2\zeta_5^3 + 7\zeta_5^4$$

$$= \frac{5\sqrt{5}+5}{2}$$

$$\approx 8.090$$

Walsh Transform

- $\mathbb{F}_q = \mathbb{F}_{p^e}$ finite field of characteristic p, $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$
- $\gcd(d, q-1) = 1$
- comparing $x \mapsto \mathrm{Tr}(x^d)$ to $x \mapsto \mathrm{Tr}(ax)$ for each $a \in \mathbb{F}_q$
- $\zeta_p = e^{2\pi i/p}$

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(x^d) - \mathrm{Tr}(ax)} = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(x^d - ax)}$$

is the Walsh transform of $x \mapsto \mathrm{Tr}(x^d)$

Weil Sums

- $\mathbb{F}_q = \mathbb{F}_{p^e}$ finite field of characteristic p, $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$
- $\gcd(d, q-1) = 1$
- comparing $x \mapsto \mathrm{Tr}(x^d)$ to $x \mapsto \mathrm{Tr}(ax)$ for each $a \in \mathbb{F}_q$
- $\zeta_p = e^{2\pi i/p}$

$\psi(x) = \zeta_p^{\mathrm{Tr}(x)}$, the canonical additive character of $\mathbb{F}_q$ into $\mathbb{C}$

$$W_{q,d}(a) = \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(x^d - ax)} = \sum_{x\in\mathbb{F}_q} \psi(x^d - ax)$$

is a character sum with a polynomial argument (a Weil sum)

ours is a Weil sum of a binomial

Equivalent Sums

One could consider any sum

$$\sum_{x \in \mathbb{F}_q} \psi(bx^m + cx^n)$$

with $\gcd(m, q-1) = \gcd(n, q-1) = 1$

Reparameterize with $y = (b^{1/m}x)^n$ to get

$$\sum_{y \in \mathbb{F}_q} \psi(y^{m/n} + cb^{-n/m}y) = W_{q,m/n}(cb^{-n/m})$$

Value at 0

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi(x^d - ax)$$

If $a = 0$, then

$$\begin{aligned} W_{q,d}(0) &= \sum_{x \in \mathbb{F}_q} \psi(x^d) \\ &= \sum_{y \in \mathbb{F}_q} \psi(y) \\ &= 0 \end{aligned}$$

so $W_{q,d}(0) = 0$ trivially

Spectra

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi(x^d - ax)$$

Fix q and d and investigate the spectrum of values $W_{q,d}(a)$ as a runs through $\mathbb{F}_q^*$, from which one readily obtains:

- Cryptography: Walsh spectrum, measuring nonlinearity of the power permutation $x \mapsto x^d$,
- Sequence Design: Cross-correlation spectrum for a pair of p-ary m-sequences of length $q-1$, where one is the decimation of the other by d,
- Coding Theory: Weight distribution for the dual of cyclic code with two zeroes α, α^d [α primitive in $\mathbb{F}_q$, $d \equiv 1 \pmod{p-1}$],
- Finite Geometry: Sizes of hyperplane sections of certain constructions in $\mathrm{PG}(e-1,2)$ [for $p=2$].

Trivial Bound and Weil Bound

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi(x^d - ax)$$

Trivial bound: summing q elements on the unit circle in $\mathbb{C}$, so

$$|W_{q,d}(a)| \leq q$$

Weil or Weil-Carlitz-Uchiyama bound for generic d

$$|W_{q,d}(a)| \leq (d-1)\sqrt{q}$$

becomes trivial for $d \geq 1 + \sqrt{q}$

Example Spectrum

- $\mathbb{F}_{25} = \mathbb{F}_5 \oplus \mathbb{F}_5\alpha$, $\alpha^2 + \alpha + 2 = 0$, $\binom{u}{v} = u + v\alpha$
- linear functionals: $x \mapsto \mathrm{Tr}(ax)$ for $a \in \mathbb{F}_{25}$
- Now compare $x \mapsto \mathrm{Tr}(x^7)$ with all $\mathbb{F}_5$-linear functionals of $\mathbb{F}_{25}$

$a \in \mathbb{F}_{25}$	$W_{q,d}(a) = \sum_{x\in\mathbb{F}_{25}} \zeta_5^{\mathrm{Tr}(x^7 - ax)}$
$\binom{0}{0}, \binom{0}{2}, \binom{0}{1}, \binom{0}{3}, \binom{0}{4}, \binom{1}{1}, \binom{3}{3}, \binom{2}{2}, \binom{4}{4}$	0
$\binom{1}{2}, \binom{2}{0}, \binom{3}{0}, \binom{4}{3}$	5
$\binom{2}{4}, \binom{3}{1}$	-5
$\binom{1}{4}, \binom{2}{1}$	$\frac{5+\sqrt{5}}{2} \approx 8.090$
$\binom{3}{4}, \binom{4}{1}$	$\frac{5-5\sqrt{5}}{2} \approx -3.090$
$\binom{2}{3}, \binom{4}{2}$	$\frac{-5+5\sqrt{5}}{2} \approx 3.090$
$\binom{1}{3}, \binom{3}{2}$	$\frac{-5-\sqrt{5}}{2} \approx -8.090$
$\binom{1}{0}$	$\frac{15+5\sqrt{5}}{2} \approx 13.090$
$\binom{4}{0}$	$\frac{15-5\sqrt{5}}{2} \approx 1.910$

Initial Observations

all values are algebraic integers

all values are real

$$\overline{W_{q,d}(a)} = \overline{\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(x^d - ax)}} = \sum_{x\in\mathbb{F}_q} \zeta_p^{-\mathrm{Tr}(x^d - ax)}$$

$$= \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}((-x)^d - a(-x))} = W_{q,d}(a)$$

($\gcd(d, q-1) = 1$ makes d odd when p is odd)

Galois conjugates always appear equally often

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ has form $\sigma(\zeta_p) = \zeta_p^j$ with $\gcd(j, p) = 1$

$$\sigma(W_{q,d}(a)) = \sigma\left(\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(x^d - ax)}\right) = \sum_{x\in\mathbb{F}_q} \zeta_p^{j\,\mathrm{Tr}(x^d - ax)}$$

$$= \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}((j^{1/d}x)^d - aj^{1-1/d}(j^{1/d}x))} = W_{q,d}(j^{1-1/d}a)$$

Degenerate d Values

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi(x^d - ax)$$

If $d \equiv p^k \pmod{q-1}$, then

$\mathrm{Tr}(x^d) = \mathrm{Tr}(x)$, so that $\psi(x^d) = \psi(x)$, and so

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi((1-a)x)$$
$$= \begin{cases} q & \text{if } a = 1, \\ 0 & \text{otherwise.} \end{cases}$$

We say that d is degenerate:

$W_{q,d}(a)$ is essentially a Weil sum of a monomial

and takes at most two values as a runs through $\mathbb{F}_q^*$.

Nondegenerate Weil Sums are at Least Three-Valued

For the Weil sum

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi(x^d - ax),$$

we say that $W_{q,d}$ is v-valued if

$$\left|\{W_{q,d}(a) : a \in \mathbb{F}_q^*\}\right| = v.$$

Last slide: $W_{q,d}$ is at most two-valued if d is degenerate (i.e., $d \equiv p^k \pmod{q-1}$ for some k).

On the other hand, if d is nondegenerate, then $W_{q,d}$ is at least three-valued (Helleseth, 1976, using power moments, algebraic number theory)

Our example with $q = 25$, $d = 7$: Weil sum $W_{25,7}$ is nine-valued.

Number of Values Taken

Big Question: When is $W_{q,d}$ **exactly** three-valued?

(if ever)

2-adic valuation, $v_2(a)$ is the largest k such that $2^k \mid a$

$e > 2$ and $0 < i < e$ for all e, i on table

q	d		Values of $W_{q,d}$
$q = 2^e$	$d = 2^i + 1$,	$v_2(i) \geq v_2(e)$	$0, \pm\sqrt{2^{\gcd(e,i)} q}$
$q = p^e$, p odd	$d = (p^{2i} + 1)/2$,	$v_2(i) \geq v_2(e)$	$0, \pm\sqrt{p^{\gcd(e,i)} q}$
$q = 2^e$	$d = 2^{2i} - 2^i + 1$,	$v_2(i) \geq v_2(e)$	$0, \pm\sqrt{2^{\gcd(e,i)} q}$
$q = p^e$, p odd	$d = p^{2i} - p^i + 1$,	$v_2(i) \geq v_2(e)$	$0, \pm\sqrt{p^{\gcd(e,i)} q}$
$q = 2^e$, $v_2(e) = 1$	$d = 2^{e/2} + 2^{(e+2)/4} + 1$		$0, \pm 2\sqrt{q}$
$q = 2^e$, $v_2(e) = 1$	$d = 2^{(e+2)/4} + 3$		$0, \pm 2\sqrt{q}$
$q = 2^e$, e odd	$d = 2^{(e-1)/2} + 3$		$0, \pm\sqrt{2q}$
$q = 3^e$, e odd	$d = 2 \cdot 3^{(e-1)/2} + 1$		$0, \pm\sqrt{3q}$
$q = 2^e$, e odd	$d = 2^{2i} + 2^i - 1$,	$e \mid 4i + 1$	$0, \pm\sqrt{2q}$
$q = 3^e$, e odd	$d = \frac{3^{e+1}-1}{3^i+1} + \frac{3^e-1}{2}$,	$2i \mid e + 1$	$0, \pm\sqrt{3q}$

Thanks to

- Kasami (1966), Kasami-Lin-Peterson (1967), Gold(1968)
- Trachtenberg (1970), Helleseth (1971, 1976)
- Welch, Kasami (1971)
- Trachtenberg (1970), Helleseth (1971, 1976)
- Cusick-Dobbertin (1996)
- Cusick-Dobbertin (1996)
- Canteaut-Charpin-Dobbertin (1999, 2000), Hollmann-Xiang (2001)
- Dobbertin-Helleseth-Kumar-Martinsen (2001)
- Hollmann-Xiang (2001)
- Ding-Gao-Zhou (2013)

General Observations

Concerning the $W_{q,d}$ values:

- 0 always present
- other two values are $\pm A$ for some A
- all values in $\mathbb{Z}$

Concerning the degree e of the field $\mathbb{F}_q = \mathbb{F}_{p^e}$ over $\mathbb{F}_p$:

- e can be anything, except that it is never a power of 2

2-adic valuation, $v_2(a)$ is the largest k such that $2^k \mid a$

$e > 2$ and $0 < i < e$ for all e, i on table

q	d		Values of $W_{q,d}$
$q = 2^e$	$d = 2^i + 1,$	$v_2(i) \geq v_2(e)$	$0, \pm\sqrt{2^{\gcd(e,i)} q}$
$q = p^e$, p odd	$d = (p^{2i} + 1)/2,$	$v_2(i) \geq v_2(e)$	$0, \pm\sqrt{p^{\gcd(e,i)} q}$

Helleseth's Conjecture

Conjecture (Helleseth, 1976)

If $q = p^{2^k}$ for some k, then $W_{q,d}$ is not three-valued.

Assuming $q = 2^{2^k}$ for the rest of this slide...

Theorem (Calderbank-McGuire-Poonen-Rubinstein, 1996)

If $W_{q,d}$ is three-valued, then the values are not of the form $0, \pm A$.

method: McEliece/Stickelberger and tricky additive combinatorics

Helleseth's Conjecture

Conjecture (Helleseth, 1976)

If $q = p^{2^k}$ for some k, then $W_{q,d}$ is not three-valued.

Assuming $q = 2^{2^k}$ for the rest of this slide...

Theorem (Calderbank-McGuire-Poonen-Rubinstein, 1996)

If $W_{q,d}$ is three-valued, then the values are not of the form $0, \pm A$.

Other Interesting Partial Results:

- Calderbank-Blokhuis (unpublished): if $d \equiv -1, -2, -4, -8 \pmod{15}$, and $W_{q,d}$ takes the value 0, then $W_{q,d}$ is not three-valued (computer assisted)
- McGuire (2002): if $W_{q,d}$ is three-valued with one value 0, the cyclic code with zeroes α, α^d has minimum distance 3
- Charpin (2004): conjecture is true in the case where d is a power of 2 modulo $\sqrt{q} - 1$
- Langevin (2007), ÇakÇak-Langevin (2010): conjecture is true for $q = 2^{2^2}, 2^{2^3}, 2^{2^4}, 2^{2^5}$ (computer experiments)

Helleseth's Conjecture

Conjecture (Helleseth, 1976)

If $q = p^{2^k}$ for some k, then $W_{q,d}$ is not three-valued.

Assuming $q = 2^{2^k}$ for the rest of this slide...

Theorem (Calderbank-McGuire-Poonen-Rubinstein, 1996)

If $W_{q,d}$ is three-valued, then the values are not of the form $0, \pm A$.

Theorem (Feng, 2012)

If $W_{q,d}$ is three-valued, then none of the values is 0.

method: group rings, archimedean and p-adic bounds

Helleseth's Conjecture

Conjecture (Helleseth, 1976)

If $q = p^{2^k}$ for some k, then $W_{q,d}$ is not three-valued.

Assuming $q = 2^{2^k}$ for the rest of this slide...

Theorem (Calderbank-McGuire-Poonen-Rubinstein, 1996)

If $W_{q,d}$ is three-valued, then the values are not of the form $0, \pm A$.

Theorem (Feng, 2012)

If $W_{q,d}$ is three-valued, then none of the values is 0.

Theorem (K., 2012)

If $W_{q,d}$ is three-valued, then one of the values is 0.

Corollary (K., 2012)

Helleseth's Conjecture is true in characteristic $p = 2$.

The Full Result

The full result works for any q (not just $q = 2^{2^k}$).

Theorem (K., 2012)

For any q, if $W_{q,d}$ is three-valued, then all three values are in $\mathbb{Z}$, and one of those values is 0.

method: Galois theory, algebraic number theory, archimedean and p-adic bounds

Progress for three-valued Weil sums $W_{q,d}$

Concerning the $W_{q,d}$ values:

- 0 always present   proved
- other two values are $\pm A$ for some A
- all values in $\mathbb{Z}$ proved

Concerning the degree e of the field $\mathbb{F}_q = \mathbb{F}_{p^e}$ over $\mathbb{F}_p$

- e can be anything, except that it is never a power of 2

  proved for $p = 2$

A Key Fact in Feng's Argument

Feng uses power moments in his proof:

$$\sum_{a\in\mathbb{F}_q^*} W_{q,d}(a) = q$$

$$\sum_{a\in\mathbb{F}_q^*} W_{q,d}(a)^2 = q^2$$

$$\sum_{a\in\mathbb{F}_q^*} W_{q,d}(a)^3 = q^2|V|$$

where V is the set of roots of $(1-x)^d + x^d - 1$ in $\mathbb{F}_q$.

He relies critically on the fact that $|V|$ is divisible by 2.

The problem: $|V|$ is not divisible by p in general.

Example: if $p = 5$, $q = 25$, and $d = 13$, then $|V| = 7$, so $p \nmid |V|$.

However, when $p = 3$, we find that $|V|$ is always divisible by 3.

3-Divisibility of $|V|$

Lemma

Let V be the set of roots of $f(x) = (1-x)^d + x^d - 1$ in $\mathbb{F}_q$. If $\mathrm{char}(\mathbb{F}_q) = 3$, then $|V(f)|$ is divisible by 3.

The following involutions act on roots:

$$\sigma(x) = 1 - x \qquad (\text{on } V)$$
$$\tau(x) = \frac{1}{x} \qquad (\text{on } V \setminus \{0\})$$

The group $\Gamma = <\sigma, \tau> \cong S_3$

Generic orbits are of size 6, and the only smaller orbits are $\{0, 1\}$ and $\{2\}$.

Thus $|V| \equiv 3 \pmod 6$.

Consequence

This enables us to adapt the techniques of Feng to characteristic 3 to obtain:

Theorem

If $q = 3^{2^k}$ for some k, and $W_{q,d}$ is three-valued, then none of the values is 0.

Combine with our theorem

Theorem (K., 2012)

For any q, if $W_{q,d}$ is three-valued, then all the values are in $\mathbb{Z}$ and one of the values is 0.

To obtain Helleseth's Conjecture in characteristic 3:

Theorem (K.)

If $q = 3^{2^k}$ for some k, then $W_{q,d}$ is not three-valued.

Symmetric Sums (joint with Y. Aubry and P. Langevin)

A three-valued $W_{q,d}$ with values $-A, 0, A$ is called symmetric

Theorem (Aubry-K.-Langevin, 2013)

If $q = p^{2^k}$ for some k, then $W_{q,d}$ is not symmetric three-valued.

The specialization to $p = 2$ is the result of Calderbank, McGuire, Poonen, Rubinstein (1996)

Their proof uses McEliece/Stickelberger and a tricky calculation in additive number theory

Our proof uses Fourier analysis and the Davenport-Hasse relation

Preferred Weil Sums (joint with Y. Aubry and P. Langevin)

A symmetric three-valued $W_{q,d}$ with values $-A, 0, A$ (with $A > 0$) must have

- $A \geq \sqrt{pq}$ if e is odd
- $A \geq p\sqrt{q}$ if e is even

When these are equalities, $W_{q,d}$ is called preferred

Theorem (Aubry-K.-Langevin, 2013)

If $q = p^{4k}$ for some k, then $W_{q,d}$ is not preferred three-valued.

The specialization to $p = 2$ is the conjecture of Sarwate-Pursley (1980), proved by Calderbank-McGuire (1995)

We again eliminate the use of McEliece/Stickelberger

Niho Exponents (joint with Y. Aubry and P. Langevin)

Theorem (Aubry-K.-Langevin, 2013)
Let $q = p^{2k}$ for some k. If d is degenerate over $\mathbb{F}_{\sqrt{q}}$, i.e., if d is a power of p modulo $p^k - 1$, then $W_{q,d}$ is not three-valued.

Such a d is called a Niho exponent for q

The $p = 2$ case is the result of Charpin (2004)

Methods that work for $p = 2$ don't work in odd characteristic

Open Questions

Conjecture

If $W_{q,d}$ is three-valued, then it is symmetric, that is, the two nonzero values are A and $-A$ for some A.

Conjecture (Helleseth, 1976)

If $q = p^{2^k}$ for some k, then $W_{q,d}$ is not three-valued.
(only settled for $p = 2, 3$)

The first conjecture implies the second, in view of the Aubry-K.-Langevin proof that $W_{q,d}$ cannot be symmetric for $q = p^{2^k}$.

Conjecture (Helleseth, 1976)

If $q > 2$ and $d \equiv 1 \pmod{p-1}$, then $W_{q,d}(a) = 0$ for some $a \in \mathbb{F}_q^*$.