Proof of a Conjectured Three-Valued Family of Weil Sums of Binomials

Workshop on Coding and Cryptography,
Paris,
April 13th–17th 2015.

Philippe Langevin

IMATH, université de Toulon

last revision April 22, 2015.

A joint work with Daniel Katz.

Weil sum

$$\begin{aligned}\mathrm{W}_s(a) &= \sum_{x\in L} \mu(x^s - ax) && \text{(Fourier coefficient)}\\ &= 1 + \sum_{x\in L^\star} \mu(x^s)\bar{\mu}(ax) && \text{(cross-correlation)}\end{aligned}$$

- L a finite field of characteristic p and order q;
- s a positive integer, $\gcd(s, q-1) = 1$;
- $\mu\colon t \mapsto \exp\left(\frac{2i\pi}{p}\,\mathrm{trace}_L(t)\right)$.

Remark

$\mathrm{W}_s(a)$ *is a real number, all rational iff* $s \equiv 1 \pmod{p-1}$.

r-valued exponent

since s is coprime with $q-1$

$$\begin{aligned} \mathrm{W}_s(0) &= \sum_{x\in L} \mu(x^s - 0x) \\ &= \sum_{x\in L} \mu(x^s) \\ &= 0 \end{aligned}$$

We say that s is a r-valued exponent when

$$\mathrm{spec}(s) := \{ \quad \mathrm{W}_s(a) \mid a \in L^\star \quad \}$$

has cardinality r.

Two valued exponents

The exponent 1 is two-valued

$$\mathrm{W}_1(a) = \sum_{x \in L} \mu(x^1 - ax) = \sum_{x \in L} \mu((1-a)x) = \begin{cases} q, & a = 1; \\ 0, & \text{else.} \end{cases}$$

Theorem (Helleseth)

if s is two-valued then s is equivalent to 1.

$$s \mapsto ps, \quad s \mapsto s^{-1}.$$

The two-valued exponents are not very interesting !

Three-Valued exponents

One knows a short list of ten families of 3-valued exponents : Kasami (1966), Kasami-Lin-Peterson, Gold, Trachtenberg, Helleseth, Welch, Cusick-Dobbertin, Canteaut-Charpin-Dobbertin, Hollmann-Xiang (2001), Hou, Dobbertin-Helleseth-Kumar-Martinsen (2001) .

Theorem (Katz, 2012)

If s is three valued then

$$0 \in \mathrm{spec}(s) \subset \mathbb{Z}.$$

Conjecture (Dobbertin-Helleseth-Kumar-Martinsen, 2001)

If L is a finite field of order $q = 3^n$ with n odd and $n > 1$, and $s = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then s is three-valued exponent with

$$\mathrm{W}_s(a) = 0, \quad \pm\sqrt{3q}.$$

Remark

$4r \equiv 1 \pmod{n}$ *makes* $s = 3^r + 2$ *coprime to* $q - 1 = 3^n - 1$.

proof strategy

As in DHKM paper !

Proposition (moments)

If F is a finite field of order $q = 3^n$ with n odd, and $s = 3^r + 2$ with $\gcd(s, q-1) = \gcd(r, n) = 1$, then

$$\sum_{a \in F^\star} \mathrm{W}_s(a)^4 = 3q^3.$$

Proposition (divisibility)

If F is a finite field of order $q = 3^n$ with n odd, and $d = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then $\mathrm{W}_s(a)$ is a rational integer divisible by $\sqrt{3q}$ for each $a \in F$.

A new three valued exponent

Theorem

If F is a finite field of order $q = 3^n$ with n odd $n > 1$, and $d = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then $W_{F,d}$ is three-valued with

$$W_{F,d} = \begin{cases} 0 & \text{for } q - q/3 - 1 \text{ values of } a \in F^\star, \\ +\sqrt{3q} & \text{for } (q + \sqrt{3q})/6 \text{ values of } a \in F^\star, \text{ and} \\ -\sqrt{3q} & \text{for } (q - \sqrt{3q})/6 \text{ values of } a \in F^\star. \end{cases}$$

Proof.

A direct consequence of the above statements by means of Parseval-Plancherel identity. □

Moments of order 4

Proposition (fourth moment)

If F is a finite field of order $q = 3^n$ with n odd, and $s = 3^r + 2$ with $\gcd(d, q-1) = \gcd(r, n) = 1$, then

$$\sum_{a \in F^\star} \mathrm{W}_s(a)^4 = 3q^3.$$

Moments of order 4

Proposition (fourth moment)

If F is a finite field of order $q = 3^n$ with n odd, and $s = 3^r + 2$ with $\gcd(d, q-1) = \gcd(r, n) = 1$, then

$$\sum_{a \in F^\star} \mathrm{W}_s(a)^4 = 3q^3.$$

$$\sum_{a \in F^\star} \mathrm{W}_s(a)^4 = q \sum_{x+y+z+t=0} \mu(x^s + y^s + z^s + t^s) \quad (\textit{convolution})$$

Moments of order 4

Proposition (fourth moment)

If F is a finite field of order $q = 3^n$ with n odd, and $s = 3^r + 2$ with $\gcd(d, q-1) = \gcd(r, n) = 1$, then

$$\sum_{a \in F^\star} \mathrm{W}_s(a)^4 = 3q^3.$$

$$\sum_{a \in F^\star} \mathrm{W}_s(a)^4 = q \sum_{x+y+z+t=0} \mu(x^s + y^s + z^s + t^s) \quad (\textit{convolution})$$

Remark

$\mathrm{wt}(\ s\ ) = 1 + 2 = 3$

Moments sketch

The map

$$L \simeq \mathbb{F}_3^n \ni x \mapsto \mathrm{trace}_L(x^s) \in \mathbb{F}_3$$

is a cubic. One introduces the trilinear form :

$$\langle x, y, z \rangle = \mathrm{trace}_L(x^{3^r} yz + xy^{3^r} z + xyz^{3^r}),$$

and its kernel :

$$K := \{(x, y) \in L^2 \quad | \quad \forall z \in L \quad \langle x, y, z \rangle = 0\}$$

Moments sketch

The map

$$L \simeq \mathbb{F}_3^n \ni x \mapsto \mathrm{trace}_L(x^s) \in \mathbb{F}_3$$

is a cubic. One introduces the trilinear form :

$$\langle x, y, z\rangle = \mathrm{trace}_L(x^{3^r}yz + xy^{3^r}z + xyz^{3^r}),$$

and its kernel :

$$K := \{(x, y) \in L^2 \quad | \quad \forall z \in L \quad \langle x, y, z\rangle = 0\}$$

$$\sum_{a \in F^\star} \mathrm{W}_s(a)^4 = q^2|K|$$

It remains to prove $|K| = 2q$.

divisibility

Proposition

If F is a finite field of order $q = 3^n$ with n odd, and $s = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then $\mathrm{W}_s(a)$ is a rational integer divisible by $\sqrt{3q}$ for each $a \in F$.

Proof.

We use Stickelberger, and the add-carry modular method introduced by Xiang & Holmann (2001).

- a short computer assisted proof.
- a rather long proof by hand.

□

Valuation

Proposition

Let F be of characteristic p and order p^n, and let

$$m = (p-1)n + \min_{\substack{j \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ j \neq 0}} w_{p,n}(dj) - w_{p,n}(j).$$

Then $v_p(\mathrm{W}_d(a)) \geq m/(p-1)$ for all $a \in F$, with equality for some $a \in F$.

Proof.

Gauss sums, Stickelberger's conguences. □

weight question

To complete the proof,

$$n + \mathrm{wt}(sx) - \mathrm{wt}(x) > 0,$$

for all nonzero $x \in \mathbb{Z}/(3^n - 1)\mathbb{Z}$.

Under the conditions

- n is odd;
- $s = 2 + 3^r$;
- $4r \equiv 1 \pmod{n}$.

modular add-and-carry $s = 3^r + 2$

Let us consider the 3-adic decompositions:

$$x = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} x_i 3^i, \quad sx = y = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} y_i 3^i$$

with $x_i, y_i \in \{0, 1, 2\} \subseteq \mathbb{Z}$,

	c_{n-2}	c_{n-3}	$\dots$	c_i	c_{i-1}	$\dots$	c_{n-1}
x	x_{n-1}	x_{n-2}	$\dots$	$\dots$	x_i	$\dots$	x_0
x	x_{n-1}	x_{n-2}	$\dots$	$\dots$	x_i	$\dots$	x_0
$3^r x$	x_{n-1-r}	x_{n-2-r}	$\dots$	$\dots$	x_{i-r}	$\dots$	x_{-r}
sx	y_{n-1}	y_{n-2}	$\dots$	$\dots$	y_i	$\dots$	y_0

The vectors x, y and c are the solutions of the problem :

$$y_i + 3c_i = 2x_i + x_{i-r} + c_{i-1}, \quad 0 \leq c_i \leq 2$$

for every $i \in \mathbb{Z}/n\mathbb{Z}$.

weight question

$$n + \mathrm{wt}(sx) - \mathrm{wt}(x) > 0,$$

$$y_i + 3c_i = 2x_i + x_{i-r} + c_{i-1},$$

$$\mathrm{wt}(sx) - \mathrm{wt}(x) = 2\mathrm{wt}(x) - 2\mathrm{wt}(c),$$

$$n + 2\mathrm{wt}(x) - 2\mathrm{wt}(c) > 0.$$

$$0 < \sum_{i=0}^{n-1} (1 + 2x_i - 2c_i).$$

reparametrization

We now set

$$X_i = x_{ri}, \quad Y_i = y_{ri}, \quad C_i = c_{ri}$$

Using the fact that $4r \equiv 1 \pmod{n}$, by the change of variables $i = rj$ we obtain:

$$Y_j + 3C_j = 2X_j + X_{j-1} + C_{j-4}. \tag{1}$$

Remark

does not depend on r !!!

Reformulation

$$Y_j + 3C_j = 2X_j + X_{j-1} + C_{j-4}, \quad C_j = \frac{2X_j + X_{j-1} + C_{j-4}}{3}$$

The sequence of states (T_j) :

$$T_j := (X_{j-1}, X_j, C_{j-4}, C_{j-3}, C_{j-2}, C_{j-1})$$
$$T_{j+1} := (X_j, X_{j+1}, C_{j-3}, C_{j-2}, C_{j-1}, C_j)$$

describes a circuit of length n in the directed 3-graph of order 3^6 :

$$(\xi, \xi', \gamma_4, \gamma_3, \gamma_2, \gamma_1) \rightsquigarrow (\xi', *, \gamma_2, \gamma_3, \gamma_4, \gamma') \quad \gamma' := \frac{2\xi + \xi' + \gamma_1}{3}$$

cost function:

$$1 + 2(\xi' - \gamma')$$

no absorbent circuit

Lemma

The directed graph has no circuit with negative cost.

The cost on a circuit of length n,

$$0 \leq n + 2\sum_i (x_i - c_i)$$

that implies the divisibility property.

Conclusion

order of K	d (nondegenerate)	values of $W_{K,d}$	reference
$q = 2^e$	$d = 2^i + 1$ $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{2^{\gcd(e,i)} q}$	K (1966), K-L-P, G
$q = p^e$ p odd	$d = \frac{1}{2}(p^{2i} + 1)$ $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{p^{\gcd(e,i)} q}$	T-1970 (e odd) H (1971) (e even)
$q = 2^e$	$d = 2^{2i} - 2^i + 1$, $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{2^{\gcd(e,i)} q}$	W,K (1971)
$q = p^e$ p odd	$d = p^{2i} - p^i + 1$ $\mathrm{val}_2(i) \geq \mathrm{val}_2(e)$	$0, \pm\sqrt{p^{\gcd(e,i)} q}$	T (1971) (e odd) H (1971)(e even)
$q = 2^e$ $\mathrm{val}_2(e) = 1$	$d = 2^{e/2} + 2^{(e+2)/4} + 1$	$0, \pm 2\sqrt{q}$	C-D (1996)
$q = 2^e$ $\mathrm{val}_2(e) = 1$	$d = 2^{(e+2)/4} + 3$	$0, \pm 2\sqrt{q}$	C-D (1996)
$q = 2^e$ e odd	$d = 2^{(e-1)/2} + 3$	$0, \pm\sqrt{2q}$	C-C-D (1999),H-X (2001)
$q = 3^e$ e odd	$d = 2 \cdot 3^{(e-1)/2} + 1$	$0, \pm\sqrt{3q}$	D-H-K-M (2001)
$q = 2^e$ e odd	$d = 2^{2i} + 2^i - 1$ $e \mid 4i + 1$	$0, \pm\sqrt{2q}$	H-X (2001),Hou (2004)
$q = 3^e$ e odd	$d = 2 \cdot 3^i + 1$ $e \mid 4i + 1$	$0, \pm\sqrt{3q}$	K-L (2015)