Three-level cross-correlation of m-sequences and three-weight cyclic codes

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

joint work with

Philippe Langevin
Institut de Mathématiques de Toulon
Université de Toulon, France

Mathematics of Communications: Sequences, Codes and Designs
Banff International Research Station
29 January 2015

About These Slides

These slides were prepared for the talk, but by popular demand, this talk was given with chalkboard.

These slides are posted in hopes they will be useful.

They cover the same topics as the chalkboard talk, but in slightly more detail.

m-Sequences

$\mathbb{F}_q$ finite field of characteristic p and order $q = p^n$

$\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ absolute trace

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$$

$\psi\colon \mathbb{F}_q \to \mathbb{C}$ canonical additive character

$$\psi(x) = e^{2\pi i \,\mathrm{Tr}(x)/p}$$

α primitive element of $\mathbb{F}_q$

m-Sequence (maximal linear sequence, maximal LFSR sequence)

$$s_\alpha = \psi(\alpha^0), \psi(\alpha^1), \ldots, \psi(\alpha^{q-2})$$

Applications: remote sensing, communications networks, scientific instrumentation, acoustic design

Periodic Autocorrelation: inner product of s_α with any nontrivial cyclic shift of itself is -1

Cross-Correlation

$\mathbb{F}_q$ finite field of characteristic p and order $q = p^n$

$\psi : \mathbb{F}_q \to \mathbb{C}$ canonical additive character

α primitive element of $\mathbb{F}_q$

$s_\alpha = \psi(\alpha^0), \psi(\alpha^1), \ldots, \psi(\alpha^{q-2})$ an m-sequence

If $d > 0$ with $\gcd(d, q-1) = 1$, the decimation by d of s_α is

$$s_{\alpha^d} = \psi(\alpha^0), \psi(\alpha^d), \ldots, \psi(\alpha^{(q-2)d}),$$ another m-sequence

If $d \equiv p^k \pmod{q-1}$ for some k, then d is degenerate: $s_{\alpha^d} = s_\alpha$

Cross-Correlation Spectrum: inner products of s_{α^d} with all cyclic shifts of s_α (want them all to be small)

Codes (When $d \equiv 1 \pmod{p-1}$): From the cross-correlation spectrum of s_α and s_{α^d}, one deduces the weight distribution of the dual of the cyclic code of length $q-1$ with zeroes α and α^d

Weil Sums of Binomials

$\mathbb{F}_q$ finite field of characteristic p and order $q = p^n$

$\psi : \mathbb{F}_q \to \mathbb{C}$ canonical additive character

Weil Sum of the binomial $x^d - ax$

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

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 s_α and s_{α^d}
- Coding Theory (When $d \equiv 1 \pmod{p-1}$): Weight distribution for the dual of cyclic code with two zeroes α, α^d

What is Desirable?

Want $|W_{q,d}(a)|$ small for all $a \in \mathbb{F}_q^*$.

Crude upper bound (triangle inequality)

$$|W_{q,d}(a)| \leq \sum_{a \in \mathbb{F}_q} |\psi(x^d - ax)| \leq q \text{ for each } a \in \mathbb{F}_q^*$$

Second Power Moment: $W_{q,d}(a) \in \mathbb{R}$ and we can compute $\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^2 = q^2$

So $|W_{q,d}(a)| > \sqrt{q}$ for some $a \in \mathbb{F}_q^*$, and so

$$\sqrt{q} < \max_{a \in \mathbb{F}_q^*} |W_{q,d}(a)| \leq q$$

You can get close to the lower bound

Number of Distinct Values

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

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

Theorem (Helleseth, 1976)

If d is nondegenerate, then $W_{q,d}$ is at least three-valued

---

Many three-valued $W_{q,d}$ have $\max_{a \in \mathbb{F}_q^*} |W_{q,d}(a)|$ very close to $\sqrt{q}$

$W_{q,d}$ three-valued $\Leftrightarrow$ cross-correlation spectrum three-valued $\Leftrightarrow$ code has three nonzero weights

Number of Values Taken

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

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), Hou (2004)
- Ding-Gao-Zhou (2013)

...and one conjectured family

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	$d = 2 \cdot 3^i + 1$,	$e \mid 4i + 1$	$0, \pm\sqrt{3q}$
$q = 3^e$, e odd	$d = \frac{3^{e+1}-1}{3^i+1} + \frac{3^e-1}{2}$,	$2i \mid e + 1$	$0, \pm\sqrt{3q}$

The Conjecture

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

If $q = 3^n$ with n odd and $n > 1$, and $d = 2 \cdot 3^r + 1$ with $n \mid 4r + 1$, then $W_{q,d}$ is three-valued with $W_{q,d}(a) \in \{0, \pm\sqrt{3q}\}$.

This talk is about our proof of this conjecture.

Proof Strategy

Dobbertin, Helleseth, Kumar, and Martinsen (2001) suggest:

(I). Fourth Power Moment: Show that $\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^4 = 3q^3$

(II). Divisibility: Show $W_{q,d}(a) \in \mathbb{Z}$ with $\sqrt{3q} \mid W_{q,d}(a)$ for $a \in \mathbb{F}_q^*$

They mentioned that they had proved (II), but not (I).

Why would this work?

Second power moment is well known: $\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^2 = q^2$

So (I) implies $\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^2 (W_{q,d}(a)^2 - 3q) = 0$

And (II) implies that every term in the sum is nonnegative

So every term is zero, and $W_{q,d}(a) \in \{0, \pm\sqrt{3q}\}$ for all $a \in \mathbb{F}_q^*$.

Proof of Divisibility

(II). Divisibility: Show $W_{q,d}(a) \in \mathbb{Z}$ with $\sqrt{3q} \mid W_{q,d}(a)$ for $a \in \mathbb{F}_q^*$

$W_{q,d} \in \mathbb{Z}$ for all $a \in \mathbb{F}_q$ by a result of Helleseth (1976)

Stickelberger's Theorem (or McEliece's Theorem): showing $\sqrt{3q} \mid W_{q,d}(a)$ for all $a \in \mathbb{F}_q^*$ is reduced to a problem in additive number theory.

Hollmann-Xiang (2001) method: convert such problems into questions about bounding the cost of cycles in directed graphs with edge costs

Our directed graph has 729 vertices and 2187 edges,
258 strongly connected components:
one of size 471, one of size 2, and the rest of size 1
Check with a computer

Computer-free proof: Seven pages of delicate arguments

Calculation of Fourth Power Moment

Recall our Weil Sum of the Binomial $x^d - ax$

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

Recall $q = 3^n$ (n odd, $n > 1$) and $d = 2 \cdot 3^r + 1$ (with $n \mid 4r + 1$)

(I). Fourth Power Moment: Show that $\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^4 = 3q^3$

Note: $d = 3^r + 3^r + 1$ has three ternary digits

Define a symmetric $\mathbb{F}_p$-trilinear form from $(\mathbb{F}_q^*)^3$ to $\mathbb{F}_p$:

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

If $\epsilon(u) = e^{2\pi i u/p}$, then

$$\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^4 = q \sum_{x,y,z \in \mathbb{F}_q} \epsilon(\langle x, y, x \rangle + \langle x, y, y \rangle + 2\langle x, y, z \rangle)$$

Calculation of Fourth Power Moment, Continued

Recall $\langle \cdot, \cdot, \cdot \rangle : \mathbb{F}_q^3 \to \mathbb{F}_p$, and $\epsilon(u) = e^{2\pi i u/p}$, and

$$\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^4 = q \sum_{x,y,z \in \mathbb{F}_q} \epsilon(\langle x, y, x \rangle + \langle x, y, y \rangle + 2\langle x, y, z \rangle)$$

If $K = \{(x, y) \in \mathbb{F}_q^2 : \langle x, y, z \rangle = 0 \text{ for all } z \in \mathbb{F}_q\}$, then

$$\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^4 = q \sum_{\substack{(x,y) \in K \\ z \in \mathbb{F}_q}} \epsilon(\langle x, y, z \rangle + \langle x, y, y \rangle + 2\langle x, y, z \rangle)$$

$$= q^2 |K|$$

Can show that $K = \{(x, y) \in \mathbb{F}_q : x^{3^{2r}} y^{3^r} + x^{3^r} y^{3^{2r}} + xy = 0\}$

This curve has $3q$ points by a character sum calculation

So $\sum_{a \in \mathbb{F}_q^*} W_{q,d}(a)^4 = 3q^3$, and the conjecture of Dobbertin, Helleseth, Kumar, and Martinsen (2001) is proved.

Eleven Infinite Families

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	$d = 2 \cdot 3^i + 1$,	$e \mid 4i + 1$	$0, \pm\sqrt{3q}$
$q = 3^e$, e odd	$d = \frac{3^{e+1}-1}{3^i+1} + \frac{3^e-1}{2}$,	$2i \mid e + 1$	$0, \pm\sqrt{3q}$