# On the Proof of Lin's Conjecture

Tor Helleseth

Department of Informatics
University of Bergen

Joint work with Honggang Hu, Shuai Shao, and Guang Gong

Rosendahl, Norway, Sept. 4, 2014

# Outline

- Ideal two-level autocorrelation sequences (Difference sets)
- Short history
  - Binary sequences
  - Nonbinary sequences
- The Lin conjecture
- Short history of the Lin conjecture
- Ideas behind proof of the Lin conjecture

# Difference Sets

**Definition**

Let $G$ be a group of order $v$. A $(v, k, \lambda)$ difference set

$$D = \{d_1, d_2, \cdots, d_k\}$$

is a $k$-element subset of $G$ such that every $x \neq 0$ can be written as $d_i - d_j = x$ in the same number, $\lambda$, of ways as $d_i$ and $d_j$ run through $D$. The difference set is said to be cyclic if the group $G$ is cyclic.

**Theorem**

*Let $s_t$ be a binary sequence of length $v$ that is the characteristic set of a difference set $Z_v$. The autocorrelation of $s_t$ at shift $\tau$ satisfies*

$$\theta(\tau) = \sum_{i=0}^{v-1} (-1)^{s_{i+\tau} - s_t} = \begin{cases} v - 4(k - \lambda) & \text{if} \quad \tau \neq 0 \pmod{v} \\ v & \text{if} \quad \tau = 0 \pmod{v} \end{cases}$$

If $(v, k, \lambda) = (2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$ then sequence has two-level ideal autocorrelation with an out-of-phase value -1.

# Binary ideal 2-level autocorrelation sequences

Binary ideal 2-level binary sequences before mid 90's

- $m$-sequences: $s_i = Tr(\alpha^i)$, $\alpha$ primitive element in $\mathbb{F}_{2^n}$
- Legendre sequences
- GMW sequences
- Twin-prime sequences
- Hall sextic sequences

Binary ideal 2-level binary sequences after mid 90's

- Conjectures: Gong, Gaal and Golomb (1997)
- Conjectures: No, Golomb, Gong, Lee and Gaal (1998)
- Conjecture: No, Chung and Yun (1998)
- Monomial o-polynomials: Maschietti (1998)
- Proof of conjectures above: Dillon-Dobbertin (2004)

# Two-level Autocorrelation and Walsh Transform

- $s_t = f(\alpha^i)$ binary sequence of period $2^m - 1$
- $F(x) = (-1)^{f(x)}$
- $\hat{F}(y) = \frac{1}{\sqrt{2^m}} \sum_x (-1)^{f(x)+Tr(yx)}$
- $F(x) = \frac{1}{\sqrt{2^m}} \sum_y \hat{F}(y)(-1)^{Tr(xy)}$

Let $gcd(t, 2^m - 1) = 1$ and $a = \alpha^\tau$. The autocorrelation is:

$$
\begin{aligned}
\theta_S(\tau) &= \sum_{i=0}^{2^m-2} (-1)^{f(\alpha^{i+\tau})-f(\alpha^i)} \\
&= -1 + \sum_{x \in GF(2^m)} F(ax)F(x) \\
(Parseval) &= -1 + \sum_{y \in GF(2^m)} \hat{F}(ay)\hat{F}(y) \\
&= -1 + \sum_{y \in GF(2^m)} \hat{F}(ay^t)\hat{F}(y^t) \\
&= -1 \text{ (if sums above are 0)}
\end{aligned}
$$

# Finding two-level autocorrelation sequences

- $S_k(x) = (-1)^{Tr(x^k)}$ where $s_k(x) = Tr(x^k)$ and $gcd(k, 2^m - 1) = 1$

The autocorrelation is

$$\begin{aligned}\theta_S(\tau) + 1 &= \sum_{y \in GF(2^m)} \hat{S}_k(ay^t)\hat{S}_k(y^t) \\ &= \sum_{x \in GF(2^m)} S_k(ax)S_k(x) \\ &= \sum_{x \in GF(2^m)} (-1)^{Tr((a^k-1)x^k)} \\ &= 0\end{aligned}$$

To find a difference set it is sufficient to find a $D$ with characteristic function $f(x)$ such that

$$\hat{F}(y) = \hat{S}_k(y^t)$$

where $gcd(t, 2^m - 1) = 1$.

### Definition

A hyperoval is a set of $2^m + 2$ points no three on a line. Every hyperoval can be represented as

$$D(f) = \{(1, t, f(t)) | t \in GF(2^m)\} \cup \{(0, 1, 0)\} \cup \{(0, 0, 1)\}$$

where $f$ is a permutation polynomial of degree $\leq 2^m - 2$, $f(0) = 0, f(1) = 1$ and

$$f_s(x) = (f(x + s) + f(s))/x, f_s(0) = 0$$

is also a permutation polynomial. If $x^k$ is a monomial then $D(x^k)$ is called a monomial hyperoval

$D(x^k)$ is a hyperoval iff $gcd(k, 2^m - 1) = 1$ and $x^k + x + a = 0$ has 0 or 2 solutions for all for all $a \in GF(2^m)$.

# Monomial hyperovals

- Singer: $k = 2^i$, $gcd(i, m) = 1$
- Segre: $k = 6, m \geq 5$ odd
- Glynn 1a: $k = 2^{\frac{m+1}{2}} + 2^{\frac{3m+1}{4}}$ if $m = 1 \pmod 4, m \geq 7$
- Glynn 1b: $k = 2^{\frac{m+1}{2}} + 2^{\frac{m+1}{4}}$ if $m = 3 \pmod 4, m \geq 7$
- Glynn 2: $k = 3 \cdot 2^{\frac{m+1}{2}} + 4$

# Difference sets from hyperovals

## Theorem

*Let $D(x^k)$ be a monomial hyperoval (i.e., $gcd(k, 2^m - 1) = 1$ and $x^k + x$ a two-to-one map on $GF(2^m)$). Let*

$$D = GF(2^m) \setminus \{x^k + x | x \in GF(2^m)\}.$$

*Then the characteristic sequence of $D$ has ideal two-level autocorrelation.*

## Proof.

(Part 1) Let $F(x) = (-1)^{f(x)}$ where $f(x)$ be characteristic sequence of of $D$. Sufficient to show that

$$\hat{F}(y) = \hat{S}_k(y^t)$$

for some $t$ where $gcd(t, 2^m - 1) = 1$. $\square$

# Difference sets from hyperovals (Proof-Part 2)

**Proof.**

$$
\begin{aligned}
\hat{F}(y) &= \frac{1}{\sqrt{2^m}} \sum_{x \in GF(2^m)} (-1)^{f(x)+Tr(yx)} \\
&= \frac{1}{\sqrt{2^m}} \sum_{x \notin D} (-1)^{Tr(yx)} - \frac{1}{2^m} \sum_{x \in D} (-1)^{Tr(yx)} \\
&= \frac{2}{\sqrt{2^m}} \sum_{x \notin D} (-1)^{Tr(yx)} \\
&= \frac{1}{\sqrt{2^m}} \sum_{x \in GF(2^m)} (-1)^{Tr(y(x^k+x))} \\
&= \frac{1}{\sqrt{2^m}} \sum_{z \in GF(2^m)} (-1)^{Tr(z^k + y^{\frac{k-1}{k}} z)} \\
&= \frac{1}{\sqrt{2^m}} \hat{S}_k(y^{\frac{k-1}{k}}) \text{ for some } t \text{ where } gcd(t, 2^m-1) = 1
\end{aligned}
$$

# Autocorrelation for odd $p$

- $p$ is a prime number
- $S = \{s_i\}$ is a $p$-ary sequence with period $N$
- For any $0 \leq \tau < N$, the autocorrelation of $S$ at shift $\tau$ is defined by

$$C_S(\tau) = \sum_{i=0}^{N-1} \omega_p^{s_{i+\tau} - s_i}, \text{ where } \omega_p = e^{2\pi i/p}$$

- If $C_S(\tau) = -1$ for any $0 < \tau < N$, then $S$ is called an ideal two-level autocorrelation sequence

# Nonbinary ideal 2-level autocorrelation sequences

Recent nonbinary ideal 2-level autocorrelation sequences

- Ternary ($n = 3k$): (Helleseth, Kumar and Martinsen (2001)
  $s_i = Tr(\alpha^i + \alpha^{di})$, $d = 3^{2k} - 3^k + 1$
- $p > 2$: Helleseth and Gong (2002)
- Dillon (2002)
- Arasu, Dillon and Player (2004)
- Conjectures: Ludkowski and Gong (2001)

# Lin's Conjecture

- $n = 2m + 1$
- $\alpha$ is a primitive element in $\mathbb{F}_{3^n}$
- $S = \{s_t\}$ is a ternary sequence defined by

$$s_t = Tr(\alpha^t + \alpha^{(2 \cdot 3^m + 1)t})$$

for $t = 0, 1, 2, \cdots$

**Conjecture (1998, Huashih Alfred Lin)**

$S$ has an ideal two-level autocorrelation.

**Remark**

A proof was claimed by Arasu, Dillon and Player in (2001) but the proof has never been published.

# Lin's conjecture: Components in the proof

- The Second order Decimation-Hadamard transform
- Gauss sums
- Stickelberger's theorem
- Combinatorial arguments

# The Second-Order Decimation-Hadamard Transform I

Let $q = 3^n$, $0 < v, t < q - 1$ and $\gamma \in \mathbb{F}_{3^n}^*$.

- For any integers $0 < v, t < q - 1$, we define

$$\widehat{f}(v,t)(\lambda,\gamma) = \sum_{x,y \in \mathbb{F}_q} \omega_p^{Tr(\lambda y - y^t x + \gamma x^v)}$$

- $\widehat{f}(v,t)(\lambda,\gamma)$ is the second-order decimation-Hadamard (multiplexing) transform (DHT) of $Tr(x)$.

# The Second-Order Decimation-Hadamard Transform II

- Let
$$\widehat{f}(v,t)(\lambda,\gamma) = \sum_{x,y\in\mathbb{F}_q} \omega_p^{Tr(\lambda y - y^t x + \gamma x^v)}$$
- If
$$\widehat{f}(v,t)(\lambda,\gamma) \in \{q\omega_p^i \mid i = 0,1,\cdots,p-1\}, \lambda \in \mathbb{F}_q, \gamma \in \mathbb{F}_q^*$$
then $(v,t)$ is called a realizable pair of $f(x)$.
- Let
$$\omega_p^{g(x,\gamma)} = \frac{1}{q}\widehat{f}(v,t)(x,\gamma), x \in \mathbb{F}_q.$$
$g(x,\gamma)$ is called a realization of $f(x)$ under $(v,t)$ and $\gamma$.

# Gauss Sums over Finite Fields

- $\psi(x) = \omega_p^{Tr(x)}$
- For any multiplicative character $\chi$ over $\mathbb{F}_q$, the Gauss sum $G(\chi)$ over $\mathbb{F}_q$ is defined by

$$G(\chi) = \sum_{x \in F_q} \psi(x)\chi(x)$$

- $G(\overline{\chi}) = \chi(-1)\overline{G(\chi)}$
- $G(\chi^p) = G(\chi)$
- If $\chi$ is trivial, then $G(\chi) = -1$
- if $\chi$ is nontrivial, then $G(\chi)\overline{G(\chi)} = q$

$$\omega_p^{Tr(y)} = \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_{q^*}}} G(\chi)\overline{\chi(y)}$$

# Ideal Two-Level Autocorrelation Sequences

- Let $U = \{x^{vt} | x \in \mathbb{F}_{3^n}^*\}$.
- Let $\Lambda = \{\gamma_0, \gamma_1, \cdots, \gamma_{d-1}\}$ be a set satisfying $\mathbb{F}_{3^n}^* = \gamma_0 U \cup \gamma_1 U \cup \cdots \cup \gamma_{d-1} U$.
- Let $\alpha$ be a primitive element of $\mathbb{F}_{3^n}$.
- For any $0 \leq i < 3^n - 1$, $\alpha^i$ can be written in the form of $\alpha^i = \gamma \lambda^{vt}$, where $\gamma \in \Lambda$ and $\lambda \in \mathbb{F}_{3^n}$.
- We construct a ternary sequence $T = \{t_i\}$ by

$$t_i = g(v, t)(\lambda, \gamma), i = 0, 1, 2, \cdots$$

**Theorem**

*Let $(v, t)$ be a realizable pair. Then the ternary sequence $T = \{t_i\}$ is an ideal two-level autocorrelation sequence.*

# Realizable pairs and Gaussian sums

Using expression for $\omega^{Tr(y)}$ in terms of Gaussian sums.

$$\begin{aligned}\widehat{f}(v,t)(\lambda,\gamma) &= \sum_{x,y\in\mathbb{F}_q} \omega_p^{Tr(\lambda y - y^t x + \gamma x^v)} \\ &= \frac{1}{3^n-1}\Big(\sum_{x\in\mathbb{F}_{3^n}^*} \omega_p^{Tr(\gamma x^v)} + T\Big)\end{aligned}$$

where

$$T = \sum_{\chi^d \neq 1} G(\chi^{vt})G(\overline{\chi}^v)G(\chi)\overline{\chi}^{vt}(\lambda)\overline{\chi}(\gamma)\overline{\chi}^v(-1)$$

- If $wt(jvt) - wt(-jv) + wt(j) > 2n$ for all $jd \neq 0 \pmod{3^n-1}$ then $\widehat{f}(v,t)(\lambda,\gamma) \equiv 0 \pmod{3^n}$.
- Average value of $|\widehat{f}(v,t)(\lambda,\gamma)| = 3^n$
- This leads to $\widehat{f}(v,t)(\lambda,\gamma) = 3^n\omega^i$ for $i = 0,1,2$ i.e., $(v,t)$ realizable.

# Prime Ideal Factorization

$$\begin{tikzcd}
 & \mathbb{Z}[\omega_p, \omega_{q-1}] & \\
\mathbb{Z}[\omega_p] \arrow[ur, "(\pi)=\mathcal{Q}_1\mathcal{Q}_2\cdots\mathcal{Q}_t"] & & \mathbb{Z}[\omega_{q-1}] \arrow[ul, "\mathfrak{p}_i=\mathcal{Q}_i^{p-1}"'] \\
 & \mathbb{Z} \arrow[ul, "(p)=(\pi)^{p-1}"] \arrow[ur, "(p)=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t"'] &
\end{tikzcd}$$

# Prime Ideal Factorization (Cont.)

- $(p)$ is a prime ideal in $\mathbb{Z}$
- Let $\pi = \omega_p - 1$
- $(\pi)$ is a prime ideal in $\mathbb{Z}[\omega_p]$
- $(p) = (\pi)^{p-1}$ in $\mathbb{Z}[\omega_p]$
- $(\pi) = \mathcal{Q}_1 \mathcal{Q}_2 \cdots \mathcal{Q}_t$ in $\mathbb{Z}[\omega_p, \omega_{q-1}]$, where $\mathcal{Q}_i$ are prime ideals in $\mathbb{Z}[\omega_p, \omega_{q-1}]$, and $t = \phi(p^n - 1)/n$
- $(p) = (\mathcal{Q}_1 \mathcal{Q}_2 \cdots \mathcal{Q}_t)^{p-1}$ in $\mathbb{Z}[\omega_p, \omega_{q-1}]$
- $(p) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_t$ in $\mathbb{Z}[\omega_{q-1}]$
- $\mathfrak{p}_i$ is the $(p-1)$-th power of a prime ideal in $\mathbb{Z}[\omega_p, \omega_{q-1}]$

# Teichmüller Character

- For each $\mathcal{Q}$, we have

$$\mathbb{Z}[\omega_p, \omega_{q-1}]/\mathcal{Q} \cong \mathbb{F}_q$$

  because $[\mathbb{Z}[\omega_p, \omega_{q-1}]/\mathcal{Q} : \mathbb{Z}/(p)] = n$.
- There is one special multiplicative character $\chi$ on $\mathbb{F}_q$ satisfying

$$\chi(x) (\text{mod } \mathcal{Q}) = x.$$

- This character is called the Teichmüller character.

# Stickelberger's Theorem

- For any $0 \leq k < q-1$, let $k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}$ be the $p$-adic representation of $k$.
- Let $\mathrm{wt}(k) = k_0 + k_1 + \cdots + k_{n-1}$, and $\sigma(k) = k_0! k_1! \cdots k_{n-1}!$.

**Theorem**

*For any $0 < k < q-1$, we have*

$$G(\chi_{\mathfrak{p}}^{-k}) \equiv -\frac{\pi^{wt(k)}}{\sigma(k)} (mod\, \pi^{wt(k)+p-1}),$$

*where $\chi_{\mathfrak{p}}$ is the Teichmüller character.*

# Main Theorems

- $\mathbb{F}_{3^n}$
- Let $f(x) = Tr(x)$.
- $d = \gcd(v, 3^n - 1) > 1$, and $\gcd(t, 3^n - 1) = 1$.

**Theorem**

*$(v, t)$ is a realizable pair if and only if $wt(jvt) + wt(-jv) + wt(j) > 2n$ for any $0 < j < 3^n - 1$ with $jd \not\equiv 0 (mod\, 3^n - 1)$.*

**Theorem**

*For any $\gamma \in \mathbb{F}_{3^n}^*$, the realization of $f(x)$ under $(v, t)$ and $\gamma$ is given by*

$$g(v, t)(\lambda, \gamma) = \sum_{\substack{wt(jvt) + wt(-jv) + wt(j) \\ = 2n + 1, 0 < j < 3^n - 1}} (-1)^{jv} \sigma(jvt)\sigma(-jv)\sigma(j)(\gamma\lambda^{vt})^j.$$

# The Sequence Conjectured by Lin

- $n = 2m + 1$
- $v = 2(3^{m+1} - 1)$
- $t = (3^n + 1)/4$
- (Then $\gcd(v, 3^m - 1) = 2$ and $\gcd(t, 3^m - 1) = 1$)

**Theorem**

*$wt(jvt) + wt(-jv) + wt(j) > 2n$ for any $0 < j < 3^n - 1$.*

**Theorem**

*$wt(jvt) + wt(-jv) + wt(j) = 2n + 1$ if and only if $j \in \{3^i, (2 \cdot 3^m + 1)3^i \mid i = 0, 1, \cdots, n-1\}$.*

**Theorem**

*Lin's conjecture is true.*

Thanks for your attention!