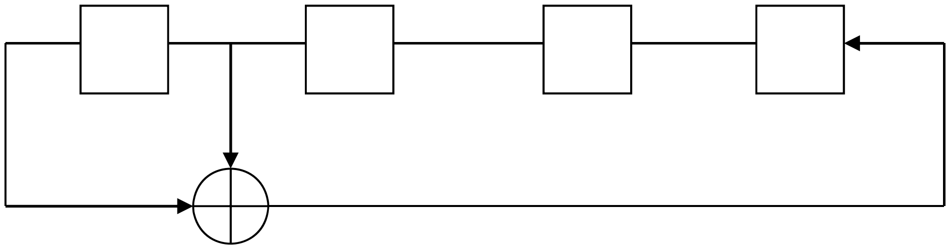
Crosscorrelation of m-Sequences, Exponential sums and Dickson polynomials

Tor Helleseth
University of Bergen
NORWAY
(Joint work with Aina Johansen and Alexander Kholosha)

Outline

- Introduction
  - m-sequences
  - Correlation of sequences
- Properties of m-sequences
  - Two-level ideal autocorrelation
- Survey
  - Three-valued cross correlation
  - Four-valued cross correlation
- New five-valued cross correlations
  - Dickson polynomials
  - Open problems

m-sequence (Example)



(s_t) : 000100110101111…

Linear recursion

$s_{t+4} = s_{t+1} + s_t$

Primitive polynomial

$f(x) = x^4+x+1$

Properties of m-sequences

- Period $\varepsilon = 2^n - 1$,   f(x) primitive polynomial of degree n

Good pseudorandom properties

- Balanced
- Run property
- Two-level autocorrelation
- $s_t - s_{t+\tau} = s_{t+\gamma}$ and $s_{2t} = s_{t+\delta}$
- Decimation by d, $(d,2^n-1)=1$ gives an m-sequence
- Trace representation $s_t = Tr_n(\alpha^t)$, where $f(\alpha)=0$ and Tr: $GF(2^n) \rightarrow GF(2)$ is $Tr_n(x) = \sum_{i=0}^{n-1} x^{2^i}$

Correlation of binary sequences

- Let (a_t) and (b_t) be binary sequences of period ε
- The crosscorrelation between (a_t) and (b_t) at shift τ is

$$\theta_{a,b}(\tau) = \sum_{t=0}^{\varepsilon-1} (-1)^{a_{t+\tau} - b_t}$$

- The autocorrelation of (a_t) at shift τ is

$$\theta_{a,a}(\tau) = \sum_{t=0}^{\varepsilon-1} (-1)^{a_{t+\tau} - a_t}$$

Two-level autocorrelation of m-sequences

- Let (s_t) be an m-sequence of period $\varepsilon=2^n-1$
- Then the autocorrelation of the m-sequence is

$$\theta_{s,s}(\tau) = 2^n-1 \quad \text{if } \tau=0 \pmod{2^n-1}$$
$$= \quad -1 \quad \text{if } \tau\neq 0 \pmod{2^n-1}$$

Proof: Let $\tau\neq 0 \pmod{2^n-1}$. Then

$$\theta_{s,s}(\tau) = \Sigma_t\, (-1)^{s_{t+\tau} - s_t}$$
$$= \Sigma_t\, (-1)^{s_{t+\gamma}}$$
$$= -1 \quad \text{(since m-sequence is balanced)}$$

Cross correlation of m-sequences

- Let (s_t) be an m-sequence
- Let (s_{dt}) be decimated m-sequence i.e., $(d, 2^n - 1) = 1$
- The cross correlation between the two m-sequences is defined by

$$C_d(\tau) = \Sigma_t (-1)^{s_{t+\tau} - s_{dt}}$$

- In the case $d \equiv 2^i \pmod{2^n - 1}$ then $(s_{dt}) = (s_{t+\gamma})$ and $C_d(\tau)$ has only two-values (autocorrelation)
- In all other cases, at least three values occur

Some properties of $C_d(\tau)$

- $C_d(\tau)$ and $C_{d'}(\tau)$ has the same distribution

  when $d \cdot d' \equiv 1 \pmod{2^n - 1}$ or when $d' \equiv d \cdot 2^i \pmod{2^n - 1}$

- $\Sigma_\tau \, (C_d(\tau) + 1) = 2^n$
- $\Sigma_\tau \, (C_d(\tau) + 1)^2 = 2^{2n}$
- $\Sigma_\tau \, C_d(\tau)^k = - (2^n - 1)^{k-1} + 2(-1)^{k-1} + a_k 2^{2n}$

  where a_k is the number of solutions of

$$x_1 + x_2 + \ldots + x_{k-1} + 1 = 0$$

$$x_1^d + x_2^d + \ldots + x_{k-1}^d + 1 = 0$$

  with $x_i \, \varepsilon GF(2^n)^* = GF(2^n)¥\{0\}$

Binary 3-valued cross correlation

- $C_d(\tau)$ has exactly 3 different values in the cases:
  - Gold : $d=2^k+1$ where $n/(n,k)$ is odd
  - Kasami : $d=2^{2k}-2^k+1$ where $n/(n,k)$ is odd
  - Welch's conjecture: (Canteau, Charpin, Dobbertin 2000)

    $d=2^m+3$ where $n=2m+1$ is odd
  - Niho's conjecture: (Dobbertin & Hollman, Xiang)

    $d=2^{(n-1)/2}+2^{(n-1)/4}-1$ when $n\equiv1 \pmod 4$

    $=2^{(n-1)/2}+2^{(3n-1)/4}-1$ when $n\equiv3 \pmod 4$
  - Cusick and Dobbertin

    $d=2^{n/2}+2^{(n+2)/2}+1$ when $n\equiv2 \pmod 4$

    $d=2^{(n+2)/2}+3$ when $n\equiv2 \pmod 4$

Binary 4-valued cross correlation

Theorem (Dobbertin, Felke, Helleseth, Rosendal (2006))

Let $r<k$ be given such that $(2^r-1)^{-1}$ and $(2^r+1)^{-1}$ exist mod 2^k+1. Let $v_2(r)<v_2(k)$ and

$$d = (2^k-1)s+1 \quad \text{with} \quad s = 2^r \cdot (2^r-1)^{-1}$$

$$d' = (2^k-1)s'+1 \quad \text{with} \quad s' = 2^r \cdot (2^r+1)^{-1}$$

Then $C_d(\tau)$ takes on 4 values and distribution is known.

Conjecture:

All 4-valued decimations of the form $d=(2^k-1)s+1$ is covered by the Theorem

Two Conjectures

Conjecture 1 (Helleseth)

If the period is 2^n-1 and $n=2^i$ then $C_d(\tau)$ has at least 4 values

Conjecture 2 (Helleseth)

For any $(d,2^n-1)=1$, then

$$C_d(\tau) = \mathbf{-1} \text{ for some } \tau$$

Remark. The -1 conjecture is equivalent with

$$\Pi_\tau(C_d(\tau)+1)=0$$

Calculations show that the conjecture is equivalent to proving:

The system of equations (α is a primitive element)

$$\begin{aligned} x_0 + \alpha x_1 + \alpha^2 x_2 + \dots + \alpha^{q-2} x_{q-2} &= 0 \\ x_0^d + x_1^d + x_2^d + \dots + x_{q-2}^d &= 0 \end{aligned}$$

has exactly q^{q-3} solutions $x_i \in GF(2^n)$, where $q=2^n$

Decimations $d=(2^l+1)/(2^k+1)$

- $d = (2^{3k} + 1)/(2^k + 1) = 2^{2k} - 2^k + 1$ (Kasami-Welch) 3-Valued
- **Conjecture** (Niho 1972)

  $d=(2^{tk}+1)/(2^k+1)$, $t > 3$ odd, gives at most 5 valued correlation
- **Counterexample** for $t=7$ (Langevin, Leander, McGuire (2007))

- Some cases known with **5-valued** correlation

  - Kasami $d=(2^{5k} + 1)/(2^k + 1)$ $(k,n)=1$, n odd

  - Bracken $d=(2^{5k} + 1)/(2^{3k} + 1)$ $(k,n)=1$, n odd

  Correlation values -1, $-1 \pm 2^{(n+1)/2}$, $-1 \pm 2^{(n+3)/2}$

  Exact correlation distribution is **unknown**

- **Theorem** (Johansen, Helleseth 2008)

  $d=(2^{2k} + 1)/(2^k + 1)$ $k=1$, n odd (i.e., $d=5/3$) gives 5-valued cross correlation and distribution is completely determined

Sketch of proof $d=(2^{2k}+1)/(2^k+1)$, $(k=1, n \text{ odd})$

1. The cross correlation is 5-valued with correlation values

   $$-1,\ -1\pm 2^{(n+1)/2},\ -1\pm 2^{(n+3)/2} \quad (n \text{ odd})$$

2. The distribution depends on the number of solutions of

   $$x^3 + y^3 + 1 = 0$$
   $$x^5 + y^5 + 1 = 0$$

3. The distribution of the correlation values depends on the number of solutions $\mathbf{A_1 = N(1,0,0)}$ of

   $$x + y + u + z = 1 = a$$
   $$x^3 + y^3 + u^3 + z^3 = 0 = b$$
   $$x^5 + x^5 + u^5 + z^5 = 0 = c$$

4. Charpin, Helleseth, Zinoviev (2005) showed that **N(a,b,c)** can be expressed as a function of three exponential sums
5. N(1,0,0) can be determined explicitly

1. The cross correlation is 5-valued

The cross correlation when $d=(2^l+1)/(2^k+1)$ can be expressed by

$$C_d(\tau) = \Sigma_{x\neq 0} (-1)^{Tr(ax + x^d)} = \Sigma_{x\neq 0} (-1)^{Tr(ax^{2^k+1}+x^{2^l+1})}$$

Squaring the correlation

$$(C_d(\tau)+1)^2 = 2^n|K_a| \text{ or } 0$$

where K_a is the zeros in $GF(2^n)$ of

$$L_a(z) = z^{2^{2l}}+a^{2^l}z^{2^{k+l}}+a^{2^{l-k}}z^{2^{l-k}}+z$$

For l=2k

$$L_a(z) = z^{2^{4k}}+a^{2^{3k}}z^{2^k}+a^{2^k}z^{2^k}+z$$

For n odd, the possible number of solutions is

$$1,\ 2^e,\ 2^{2e},\ 2^{3e},\ 2^{4e} \quad \text{for } e = (k,n)$$

Hence, the cross correlation is 5-valued with correlation values

$$-1,\ -1\pm 2^{(n+e)/2},\ -1\pm 2^{(n+3e)/2} \quad (n \text{ odd and } e=(k,n)=1)$$

2. Determination of third powers

Theorem Let $d=(2^l+1)/(2^k+1)$ then $\Sigma_\tau\ (C_d(\tau)+1)^3 = 2^{2n}\ b_3$

where $x, y\ \varepsilon\ GF(2^n)^* = GF(2^n)¥\{0\}$

$$x^{2^k+1} + y^{2^k+1} + 1 = 0$$

$$x^{2^l+1} + y^{2^l+1} + 1 = 0$$

Then $b_3=2^{(k+l,n)} + 2^{(l-k,n)} - 2^{(k+l,l-k,n)} - 2.$

Proof

Eliminating y gives

$$(x^{k+1} + x)(x^{l-k} + x)^{2^k} = 0$$

Corollary

For $l=2k$ then $b_3=2^{(3k,n)} - 2$

3/4. Solutions of equation system

Theorem (Charpin, Helleseth, Zinovev (2005))

Let N(a,b,c) be the number of solutions (x,y,z,u) in $GF(2^n)$ of

$$x + y + u + z = 1 = a$$
$$x^3 + y^3 + u^3 + z^3 = 0 = b$$
$$x^5 + x^5 + u^5 + z^5 = 0 = c$$

If n is odd then N(a,b,c) can be expressed by three exponential sums, especially

$$A_1 = N(1,0,0) = 2^n + 1 + 3G_n - 2K_n - 2C_n$$

where

$$C_n = \Sigma_x (-1)^{Tr_n(x^3 + x)} \quad \text{(Gold sum)}$$
$$K_n = \Sigma_x (-1)^{Tr_n(x + x^{-1})} \quad \text{(Kloosterman sum)}$$
$$G_n = \Sigma_x (-1)^{Tr_n(x^3 + x^{-1})} \quad \text{(“Inverse” Gold sum)}$$

and trace is from $GF(2^n)$ to GF(2)

5. On the number of solutions A_1=N(1,0,0)

- $A_1 = N(1,0,0) = 2^n + 1 + 3G_n - 2K_n - 2C_n$

Finding C_n

- $C_n = \Sigma_{x \varepsilon GF(2^n)} (-1)^{Tr_n(x^3 + x)} = -\eta_1^n - \eta_2^n$
- $C_1 = 2$, $C_2 = 0$ and η_1 , η_2 are zeros of x^2+2x+2 and
- $C_n = (2/n)2^{n+1}$ where (2/n) is the Jacobi symbol

Finding K_n

- $K_n = \Sigma_{x \neq 0} (-1)^{Tr_n(x + x^{-1})} = -\eta_1^n - \eta_2^n$
- $K_1 = 1$, $K_2 = 2$ and η_1 , η_2 are zeros of x^2+x+2

Finding G_n

- $G_n = \Sigma_{x \neq 0} (-1)^{Tr_n(x^3 + x^{-1})} = -\eta_1^n - \eta_2^n - \eta_3^n - \eta_4^n$
- $G_1 = 1$, $G_2 = -1$, $G_3 = 7$ and $G_4 = 7$
- η_1 , η_2, η_3 , η_4 are zeros of x^4+x^3+2x+1

Correlation distribution for d=5/3

Let $A_1 = N(1,0,0) = 2^n + 1 + 3G_n - 2K_n - 2C_n$

Theorem (Distribution of $C_d(\tau)+1$)

- In the case $(3,n)=1$

$\pm 2^{(n+3)/2}$	occurs	$A_1/96$	times
$-2^{(n+1)/2}$	occurs	$(3\cdot 2^{n+1} - 3\cdot 2^{(n+3)/2} - A_1)/24$	times
$+2^{(n+1)/2}$	occurs	$(3\cdot 2^{n+1} + 3\cdot 2^{(n+3)/2} - A_1)/24$	times
0	occurs	$2^{m-1} - 1 + A_1/16$	times

- In the case $(3,n)=3$

$-2^{(n+3)/2}$	occurs	$(-3\cdot 2^{(n+5)/2} + A_1)/96$	times
$+2^{(n+3)/2}$	occurs	$(3\cdot 2^{(n+5)/2} + A_1)/96$	times
$\pm 2^{(n+1)/2}$	occurs	$(3\cdot 2^{n+1} - A_1)/24$	times
0	occurs	$2^{n-1} - 1 + A_1/16$	times

General case $d = (2^{2k}+1)/(2^k+1)$, n odd

- All previous steps work except we need to find A_1
- Consider the number of solutions A_1 of

$$
\begin{aligned}
x + y + z + u &= a\ (=1) \\
x^{2^k+1} + y^{2^k+1} + z^{2^k+1} + u^{2^k+1} &= 0 \\
x^{2^{2k}+1} + y^{2^{2k}+1} + z^{2^{2k}+1} + u^{2^{2k}+1} &= 0
\end{aligned}
$$

- The complete 5-valued correlation distribution can be determined from A_1
- How to find A_1 for general k??

$A_1 = N(1,0,0)$ and exponential sums

Kloosterman sum: $K_n = \Sigma_{x\neq 0} (-1)^{Tr_n(x + x^{-1})}$

Gold sum: $C_n = \Sigma_{x\neq 0} (-1)^{Tr_n(x^{2^k+1} + x)}$

Inverse cubic: $G_n^{(k)} = \Sigma_{x\neq 0} (-1)^{Tr_n(x^{2^k+1} + x^{-1})}$

Gen. sum: $K_n' = \Sigma_{x\neq 0} (-1)^{Tr_n(f(x))}$ where $f(x) = \dfrac{(x^2+x)^{2^k}}{(x^{2^k}+x)^{2^k+1}}$

Theorem Let n be odd and **$(k,n)=1$** then

$$A_1 = 2^n + 1 + 3\,G_n^{(k)} - 2\,C_n - 2\,K_n'$$

Conjecture

For any $(k,n)=1$ then $K_n = K_n'$ and $G_n^{(k)} = G_n^{(1)}$

Introduction to Dickson polynomials

- Dickson polynomial $$D_r(x,u) = \sum_{i=0}^{[\frac{r}{2}]} \frac{r}{r-i}\binom{r}{r-i}(-u)^i x^{r-2i}$$
- $D_r(x_1+x_2, x_1x_2) = x_1^r + x_2^r$
- Let u=1 and $D_r(x)=D_r(x,1)$
- $D_r(x+x^{-1}) = x^r + x^{-r}$
- $D_{2k+1}(x) = x^{2k+1} + x^{2k-1} + x^{2k-3} + \ldots + x$

$D_1(x)=x$	$D_2(x)=x^2$	$D_3(x)=x^3+x$
$D_4(x)=x^4$	$D_5(x)=x^5+x^3+x$	$D_6(x)=x^6+x^2$
$D_7(x)=x^7+x^3+x$	$D_8(x)=x^8$	$D_9(x)=x^9+x^7+x^5+x$

- $D_r(x)$ is a permutation polynomial in $GF(2^n)$ iff $(r,2^{2n}-1)=1$
- If $(r,2^n-1)=1$ and $D_r(x)\neq 0$ then

$$Tr_n(1/x) = Tr_n(1/D_r(x))$$

Dickson and Kloosterman

Let $(r, 2^{2n} - 1) = 1$ then $D_r(x)$ is a permutation polynomial and $Tr_n(D_r(x)^{-1}) = Tr_n(x^{-1})$.

LEMMA

$$\mathrm{K_n} = \sum_{x \neq 0} (-1)^{Tr_n(D_r(x) + x^{-1})}$$

PROOF :

$$K_n = \sum_{x \neq 0} (-1)^{Tr_n(x + x^{-1})}$$

$$= \sum_{x \neq 0} (-1)^{Tr_n(D_r(x) + D_r(x)^{-1})}$$

$$= \sum_{x \neq 0} (-1)^{Tr_n(D_r(x) + x^{-1})}$$

The case l=2k (I)

- Consider the number of solutions A_1 of

$$
\begin{aligned}
x &+ y + z + u = a\ (= 1)\\
x^{2^{k}+1} &+ y^{2^{k}+1} + z^{2^{k}+1} + u^{2^{k}+1} = 0\\
x^{2^{2k}+1} &+ y^{2^{2k}+1} + z^{2^{2k}+1} + u^{2^{2k}+1} = 0
\end{aligned}
$$

- Let

$$x + y = v \quad \text{and } xy = w\ (=v^2 r)\ \text{i.e., } Tr_n(r)=0$$

$$z + u = v+a \ \text{ and }\ zu = (v+a)^2 s \quad \text{i.e., } Tr_n(s)=0$$

- Then system becomes

$$D_{2^{k}+1}(v,v^2 r) + D_{2^{k}+1}(v+a,(v+a)^2 s) = 0$$

$$D_{2^{2k}+1}(v,v^2 r) + D_{2^{2k}+1}(v+a,(v+a)^2 s) = 0$$

or

$$v^{2^{k}+1}(1+r+r^2+\ldots+r^{2^{k-1}}) = (v+1)^{2^{k}+1}(1+r+r^2+\ldots+r^{2^{k-1}})$$

$$v^{2^{2k}+1}(1+r+r^2+\ldots+r^{2^{2k-1}}) = (v+1)^{2^{2k}+1}(1+r+r^2+\ldots+r^{2^{2k-1}})$$

The case l=2k (II)

Let $r = r_1^2 + r_1$ and $s = s_1^2 + s_1$

Then A_1 is the number of solutions of

$$v^{2k+1}(r_1^{2k} + r_1 + 1) = (v+1)^{2k+1}(s_1^{2k} + s_1 + 1)$$

$$v^{22k+1}(r_1^{22k} + r_1 + 1) = (v+1)^{22k+1}(s_1^{22k} + s_1 + 1)$$

and $A_1/4$ is the number of solutions of

$$x_1 = \delta^{2k+1} y_1$$

$$x_1^{2k} + x_1 + 1 = \delta^{22k+1}(y_1^{2k} + y_1 + 1)$$

where $Tr_m(x_1) = Tr_m(y_1) = 1$ and $\delta = (v+1)/v$

Eliminating x_1 leads to the equation

$$\left(\frac{y_1}{u}\right)^{2^k} + \left(\frac{y_1}{u}\right) + C = 0$$

for some u and where

$$C = \frac{(v^{2^{2k}} + v + 1)(v^{2^K} + 1)v^{2k}}{(v^{2^k} + v)^{2^k+1}}$$

A Key Theorem

Theorem

Let A_1 be the number of solutions in $GF(2^m)$ of

$$\begin{aligned} x + y + z + u &= a\ (=1) \\ x^{2^k+1} + y^{2^k+1} + z^{2^k+1} + u^{2^k+1} &= 0 \\ x^{2^{2k}+1} + y^{2^{2k}+1} + z^{2^{2k}+1} + u^{2^{2k}+1} &= 0 \end{aligned}$$

Then $A_1 = 8N$ where N is the number of solutions of

$$Tr_m(f_1(v)) = Tr_m(f_2(v)) = Tr_m(f_3(v) = 0$$

where $v \neq 0,1$ is in $GF(2^m)$ and

$$f_1(v) = \frac{(v^2+v)^{2^k}}{(v^{2^k}+v)^{2^k+1}} + 1,\quad f_2(v) = \frac{(v+1)^{2^k}}{(v^{2^k}+v)^{2^k+1}},\ f_3(v) = \frac{v^{2^k}}{(v^{2^k}+v)^{2^k+1}}$$

Description of $f_i + f_j$'s

$$f_1(v) = \frac{(v^2+v)^{2^k}}{(v^{2^k}+v)^{2^k+1}} + 1 \qquad (= f_1(v+1))$$

$$f_2(v) = \frac{(v+1)^{2^k}}{(v^{2^k}+v)^{2^k+1}} \qquad (= f_3(v+1))$$

$$f_3(v) = \frac{v^{2^k}}{(v^{2^k}+v)^{2^k+1}} \qquad (= f_2(v+1))$$

$$f_1(v) + f_2(v) = \frac{(v+1)^{2^{k+1}}}{(v^{2^k}+v)^{2^k+1}} + 1 \qquad (= f_1(v+1) + f_3(v+1))$$

$$f_1(v) + f_3(v) = \frac{v^{2^{k+1}}}{(v^{2^k}+v)^{2^k+1}} \qquad (= f_1(v+1) + f_2(v+1))$$

$$f_2(v) + f_3(v) = \frac{1}{(v^{2^k}+v)^{2^k+1}}$$

$$f_1(v) + f_2(v) + f_3(v) = \frac{(v^2+v+1)^{2^k}}{(v^{2^k}+v)^{2^k+1}} + 1$$

A_1 and exponential Sums

Let N be the number of solutions of

$$Tr_n(f_1(v)) = Tr_n(f_2(v)) = Tr_n(f_3(v)) = 0$$

Then

$$A_1 = 8N = \sum_{v \neq \{0,1\}} (1+(-1)^{Tr_n(f_1(v))})(1+(-1)^{Tr_n(f_2(v))})(1+(-1)^{Tr_n(f_3(v))})$$

$$= 2^n - 2 + \sum_{v \neq \{0,1\}} (-1)^{Tr_n(f_1(v))} + \sum_{v \neq \{0,1\}} (-1)^{Tr_n(f_2(v))} + \ldots$$

$$+ \sum_{v \neq \{0,1\}} (-1)^{Tr_n(f_1(v)+f_2(v)+f_3(v))}$$

$$= 2^{\mathrm{n}} - 2 + S_1 + S_2 + S_3 + S_{12} + S_{13} + S_{23} + S_{123}$$

$$= 2^{\mathrm{n}} + 1 + 3G_n^{(k)} - 2\mathrm{C}_{\mathrm{n}} - 2K_n^{'}$$

since further calculations give

$$\mathrm{S}_{12} = \mathrm{S}_{13} = -\mathrm{C}_{\mathrm{n}} + 2, \ \ \mathrm{S}_2 = \mathrm{S}_3 = \mathrm{S}_{23} = G_n^{(k)} - 1, \ \ \mathrm{S}_1 = \mathrm{S}_{123} = K_n^{'}$$

$G_n^{(1)} = G_n^{(2)}$ for n odd

LEMMA 1. Let *n* be odd.

$$G_n^{(1)} = -\sum_{xGF(2^m)} (-1)^{Tr_m(x^3+x^{-1})} = -\eta_1^n - \eta_2^n - \eta_3^n - \eta_4^n$$

where η_i^n's are zeros of

$$L_1(z) = z^4 + z^3 + 2z + 4$$

LEMMA 2. Let *n* be odd.

$$G_n^{(2)} = -\sum_{xGF(2^m)} (-1)^{Tr_m(x^5+x^{-1})} = -\omega_1^n - \omega_2^n - \omega_3^n - \omega_4^n - \omega_5^n - \omega_6^n$$

where ω_i^n's are zeros of

$$L_2(z) = z^6 + z^5 + 4z^3 + 4z + 8$$

$$= (z^2 + 2)L_1(z)$$

Hence,

$$G_n^{(2)} = G_n^{(1)} - (i\sqrt{2})^n - (-i\sqrt{2})^n = G_n^{(1)} \text{ for } n \text{ odd}$$

K_n'=K_n for k=2

Let $k=2$

$$f(x)=\frac{(x^2+x)^{2^k}}{(x^{2^k}+x)^{2^k+1}}=\frac{(x^2+x)^4}{(x^4+x)^5}=\frac{z^4}{(z^2+z)^5}=\frac{1}{(z^2+1)^5 z}=\frac{1}{g(z)}$$

where $z=x^2+x$ and

$$g(z)=(z^2+1)^5 z$$

Note

$$D_5(t)+t^{-1}=\frac{1}{g(z)} \quad \text{where} \quad t=\frac{z}{z+1}$$

LEMMA

Let $n=2$ then $K_n'=K_n$

$$\text{Proof}: K_n'=\sum_{x\neq 0}(-1)^{Tr_n(f(x))}=2\sum_{z\neq 0, Tr(z)=0}(-1)^{Tr_n(\frac{1}{g(z)})}$$

$$=\sum_{z\neq 0}(-1)^{Tr_n(\frac{1}{g(z)})}+\sum_{z\neq 0}(-1)^{Tr_n(\frac{1}{g(z)}+z)}$$

$$=K_n+0$$

$$=K_n$$

Connection to Dillon-Dobbertin (DS)

Let $\Delta_k(v) = (v+1)^{2^{2k}-2^k+1} + v^{2^{2k}-2^k+1} + 1$

- $\Delta_k(v) = \Delta_{m-k}(v) = \dfrac{1}{f_1(v)+1} = \dfrac{\left(v^{2^k}+v\right)^{2^k+1}}{\left(v^2+v\right)^{2^k}}$
- $\Delta_k(v)$ is a 2-to-1 map
- $\mathrm{Im}(\Delta_k)$ leads to Dillon - Dobbertin difference sets

Connection: Dickson – Kloostermann

Conjecture. Let k be even and (k,n)=1. Then

$$K_n = \sum_{x \in GF(2^n)^{**}} (-1)^{Tr\left(\frac{1}{D_3(x)^{\frac{1}{2^k+1}}}\right)}$$

Conclusions

- Overview of cross correlation of m-sequences
- Complete correlation distribution for new families with 5-valued correlation if A_1 can be calculated

  $$d=(2^{2k}+1)/(2^k+1)\ , \qquad n \text{ odd}$$

- Complete correlation distribution for $k=1$ and $k=2$
- Conjectured the correlation distribution to be the same for any k whenever $(k,n)=1$
- Two new conjectures on exponential sums
- Connections to Dickson polynomials and Dillon-Dobbertin difference sets

Appendix

- Computing S_{12} and S_{13} $(= - C_n+2)$
- Computing S_2, S_3 and S_{23} $(= - G_n^{(k)}+2)$
- Connection to Dillon-Dobbertin difference sets
- Showing that $S_1 = S_{123}$

Computing S_{12} and S_{13}

LEMMA. Let n be odd and $(k,n)=1$. Then

$$S_{12}=S_{13}=-\sum_{xGF(2^n)}(-1)^{Tr_n(x^{2^k+1}+x)}+2=-C_n+2$$

PROOF: Note that since $f_3(v)=f_2(v+1)$ then $S_{12}=S_{13}$

$$f_1(v)+f_3(v)+1=\frac{(v^2+v)^{2^k}}{(v^{2^k}+v)^{2^k+1}}+\frac{v^{2^k}}{(v^{2^k}+v)^{2^k+1}}=\frac{v^{2^{k+1}}}{(v^{2^k}+v)^{2^k+1}}$$

$$=\frac{v^{2^k-1}}{(v^{2^{k-1}}+1)^{2^k+1}}=\frac{r}{(r+1)^{2^k+1}}=\frac{1}{(r+1)^{2^k+1}}+\frac{1}{(r+1)^{2^k}}$$

$$=x^{2^k+1}+x^{2^k}$$

Hence,

$$S_{12}=S_{13}=\sum_{v\notin\{0,1\}}(-1)^{Tr_n(f_1(v)+f_3(v))}=\sum_{x\notin\{0,1\}}(-1)^{Tr_n(x^{2^k+1}+x+1)}=-C_n+2$$

Computing S_2, S_3 and S_{23}

LEMMA Let n be odd and $(k,n)=1$. Then

$$S_2 = S_3 = S_{23} = \sum_{v \notin \{0,1\}} (-1)^{Tr(x^{2^k+1}+x^{-1})} = G_n^{(k)} - 1$$

PROOF: Let $f_3(v) = \dfrac{v^{2^k}}{(v^{2^k}+v)^{2^k+1}}$ $\quad (= f_2(v+1))$ then $S_2 = S_3$.

Note $f_2(v) + f_3(v) = \dfrac{1}{(v^{2^k}+v)^{2^k+1}}$.

Then $v = t^{2^k+1}$ is one-to-one since $(k,n)=1$ and

$$f_3(v) = \frac{v^{2^k}}{(v^{2^k}+v)^{2^k+1}} = \frac{t^{2^{2k}+2^k}}{(t^{2^{2k}+2^k}+t^{2^k+1})^{2^k+1}} = \left(\frac{t^{2^k}}{t^{2^{2k}+2^k}+t^{2^k+1}}\right)^{2^k+1} = \left(\frac{1}{t^{2^{2k}}+t}\right)^{2^k+1}$$

Hence,

$$S_3 = 2 \sum_{Tr_m(\frac{1}{x})=0,\, x\neq 0} (-1)^{Tr_n(x^{2^k+1})} = \sum_{x\neq 0} (-1)^{Tr_n(x^{2^k+1}+\frac{1}{x})} + \sum_{x \neq 0} (-1)^{Tr_n(x^{2^k+1})}$$

$$= \sum_{x\neq 0} (-1)^{Tr_n(x^{2^k+1}+\frac{1}{x})} = G_n^{(k)} - 1$$

Connection to Dillon-Dobbertin (DS)

Let $\Delta_k(v) = (v+1)^{2^{2k}-2^k+1} + v^{2^{2k}-2^k+1} + 1$.

Then

- $\Delta_k(v) = \Delta_{m-k}(v) = \dfrac{1}{f_1(v)+1} = \dfrac{\left(v^{2^k}+v\right)^{2^k+1}}{\left(v^2+v\right)^{2^k}}$
- $\Delta_k(v)$ is a 2-to-1 map
- $Im(\Delta_k)$ leads to Dillon - Dobbertin difference sets
- Let

$$g(z) = \frac{\left(\sum_{i=0}^{k-1} z^{2^i}\right)^{2^k+1}}{z^{2^k}}$$

- Then g is a 2-to-1 map $Im(g)=Im(\Delta_k)$ and for k even

$$f_1(v) = \frac{1}{g(v^2+v)}+1 \quad \text{and} \quad f_7(v) = \frac{1}{g(v^2+v+1)}+1$$

Showing that $S_1 = S_{123}$

Lemma

Let k be even, n odd and (k,n)=1 then

$$S_1 = S_{123} = -K_n' + 1$$

Proof. Since k is even and g(z) 2-to-1 then $Im(f_1)=Im(f_7)$

$$S_1 + S_{123} = \sum_{v \neq 0,1} (-1)^{Tr(f_1(v))} + \sum_{v \neq 0,1} (-1)^{Tr(f_7(v))}$$

$$= 2 \sum_{z \neq 0,1} (-1)^{Tr(\frac{1}{g(z)}+1)}$$

$$= 2 \sum_{v \neq 0} (-1)^{Tr(f_1(v))}$$

$$= 2S_1$$