The History of the Crosscorrelation of m-Sequences: An Overview

Tor Helleseth

Selmer Center
Department of Informatics
University of Bergen
Bergen, Norway

December 1, 2021

Outline

- Basic introduction to m-sequences
- Autocorrelation of m-sequences
- Crosscorrelation of m-sequences
- Gold Sequences and applications
- Overview over more than 50 year history (1968-2021)
- Relations to Bent functions / APN functions/ AB functions
- Conclusions and open problems

Basic introduction to m-sequences

May 25, 2016 Stephen Wolfram states in his blog:

Solomon Golomb (1932 – 2016)

The Most-Used Mathematical Algorithm Idea in History An octillion. A billion billion billion. That's a fairly conservative estimate of the number of times a cellphone or other device somewhere in the world has generated a bit using a maximum–length linear-feedback shift register sequence. It's probably the single most-used mathematical algorithm idea in history. And the main originator of this idea was Solomon Golomb, who died on May 1 - and whom I knew for 35 years.

Generating m-sequences

- Linear recurrence (over $\mathbb{F}_p$)
  - $s_{t+n} + c_{n-1}s_{t+n-1} + \cdots + c_0 s_t = 0$
- Characteristic polynomial
  - $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$
- Select f(x) such that
  - $f(x)$ is irreducible of degree n
  - $f(x)$ divides $x^{p^n-1} - 1$
  - $f(x)$ do not divide $x^r - 1$ for any r, $1 \leq r < p^n - 1$

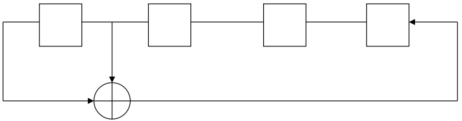
Then $f(x)$ generates an m-sequence $\{s_t\} = s_0, s_1, s_2, \cdots$ of period $p^n - 1$.

Example

The binary m-sequence generated by $s_{t+4} + s_{t+1} + s_t = 0$ is:

$$\{s_t\} = 000100110101111$$

Binary m-sequences



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

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

$\{S_t\} = 000100110101111 \ldots$

- Period $\varepsilon = 2^n - 1$ (if the characteristic polynomial $f(x)$ has degree n)
- Balanced (except for a missing 0)
- Run property
- $s_{t+\tau} - s_t = s_{t+\gamma}$
- If $gcd(d, 2^n - 1) = 1$, then its decimation $\{s_{dt}\}$ is also an m-sequence
- $\{s_{2t}\} = \{s_{t+\mu}\}$ for some μ
- The trace mapping is: $Tr : \mathbb{F}_{2^n} \to \mathbb{F}_2$ where $Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$
- Let $f(\alpha) = 0$ then (after suitable cyclic shift)

$$s_t = Tr(\alpha^t)$$

Correlation of Sequences

Correlation of Sequences

Let $\{a_t\}$ and $\{b_t\}$ be sequences of period ε over the alphabet $\mathbb{F}_p$.

Crosscorrelation

Then crosscorrelation between $\{a_t\}$ and $\{b_t\}$ at shift τ is

$$\theta_{a,b}(\tau) = \sum_{t=0}^{\varepsilon-1} \omega^{a_{t+\tau} - b_t} \quad \text{where } \omega = \exp 2\pi i/p$$

Autocorrelation

Then autocorrelation of $\{a_t\}$ at shift τ is

$$\theta_{a,a}(\tau) = \sum_{t=0}^{\varepsilon-1} \omega^{a_{t+\tau} - a_t} \quad \text{where } \omega = \exp 2\pi i/p$$

Ideal Two-Level Autocorrelation

Theorem

Let $\{s_t\}$ be an m-sequence of period $p^n - 1$. The autocorrelation is

$$C_1(\tau) = \begin{cases} p^n - 1 & \textit{if} \quad \tau = 0 \pmod{p^n - 1} \\ -1 & \textit{if} \quad \tau \neq 0 \pmod{p^n - 1}. \end{cases}$$

Proof.

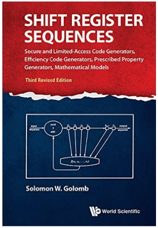
Let $\tau \neq 0 \pmod{p^n - 1}$. Then since m-sequences are balanced:

$$\begin{aligned} C_1(\tau) &= \sum_{t=0}^{p^n-2} \omega^{s_{t+\tau} - s_t} \\ &= \sum_{t=0}^{p^n-2} \omega^{s_{t+\gamma}} \\ &= -1 \end{aligned}$$

□

Golomb's influence on the early applications of m-sequence

Golomb's Influence on m-sequences



Golomb's influence on m-sequences

Applications of m-sequences in the 1960s

- Interplanetary ranging system (1958)
  - Orbit determination of Explorer I
  - Signal sent back from Explorer I was modulated by an m-sequence
- Determining the position of Venus (1961)
  - Bounced signal from Venus and detected return signal.
  - Improved accuracy of location of Venus by a factor of 10^3
- Experiment verifying Einstein General Relativity Theory
  - Experiment designed (1960)
  - Experiment performed using Mars Mariner 9 (1969).

Major Prizes

- Shannon Award 1985
- National Medal of Science 2013
- Franklin Medal 2016

Crosscorrelation of m-sequences

Crossscorrelation of m-sequences

Basic results on crosscorrelation of m-sequences

- Let $\{s_t\}$ be an m-sequence of period $p^n - 1$
- Let $\{s_{dt}\}$ be a decimated m-sequence i.e., $gcd(d, p^n - 1) = 1$
- The crosscorrelation between the two m-sequences is

$$C_d(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_{dt} - s_{t+\tau}} = -1 + \sum_{x \in \mathbb{F}_{p^n}} \omega^{Tr(x^d + ax)}$$

where α is a primitive element in $\mathbb{F}_{p^n}$ and $a = \alpha^\tau$.

- In the case $d = p^i \pmod{p^n - 1}$ then $C_d(\tau)$ is two-valued (autocorrelation)
- In all other cases at least three values occur when $\tau = 0, 1, \cdots, p^n - 2$

Three valued crosscorrelation: Gold sequences

Three-Valued Crosscorrelation: The Gold Cases

Theorem (Gold(1968))

Let $d = 2^k + 1$ *and* $e = gcd(n,k)$ *where* $\frac{n}{gcd(n,k)}$ *is odd.*
Then $C_d(\tau)$ *has three-valued crosscorrelation with distribution:*

$$\begin{array}{ccc} -1+2^{\frac{n+e}{2}} & \textit{occurs} & 2^{n-e-1}+2^{\frac{n-e-2}{2}} & \textit{times} \\ -1 & \textit{occurs} & 2^n-2^{n-e}-1 & \textit{times} \\ -1-2^{\frac{n+e}{2}} & \textit{occurs} & 2^{n-e-1}-2^{\frac{n-e-2}{2}} & \textit{times} \end{array}$$

In particular when $gcd(k,n) = 1$ then the values of $C_d(\tau) + 1$ are

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^d + ax)}$$

belong to $\{0, \pm 2^{\frac{n+1}{2}}\}$.

Applications of sequences to CDMA

CDMA

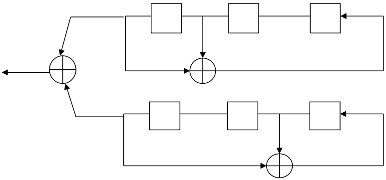
In Code-Division Multiple Access (CDMA) one needs large families $\mathcal{F}$ with good correlation properties

Parameters of sequence families

Parameters of a familiy are denote $(\varepsilon, \mathrm{M}, \theta_{max})$

- ε is the period of the sequences in $\mathcal{F}$
- M is the size of the family ($\#$ of cyclically distinct sequences in $\mathcal{F}$)
- θ_{max} is the maximal (nontrivial) value of the auto- or crosscorrelation of the sequences in $\mathcal{F}$ (except when sequences are the same and shift $\tau = 0$)

Gold sequences (Example m=3)



(s_t)	:	1 0 0 1 0 1 1	
(s_{3t})	:	1 1 1 0 1 0 0	
$(s_t + s_{3t})$	:	0 1 1 1 1 1 1	M=|F|=9
$(s_t + s_{3t+1})$	:	0 1 0 0 0 1 0	θ_{max}=5
……………………………			
$(s_t + s_{3t+6})$	:	1 1 1 0 0 0 1	

The Gold family - Example

The Gold family

The Gold family is used in GPS and in the 3G standard for wireless communication.

Construction of the Gold sequence family

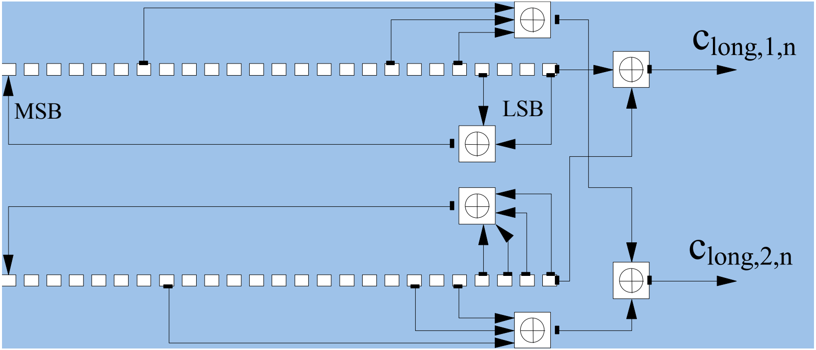
- Let $\{s_t\}$ be a binary m-sequence of period $2^n - 1$ where n is odd, $d = 2^k + 1$ and $\gcd(k, n) = 1$
- $\mathcal{G} = \{s_t\} \cup \{s_{dt}\} \cup \{\{s_{t+\tau} - s_{dt}\} \mid \tau = 0, 1, \cdots, 2^n - 2\}$

The parameters of the Gold family $\mathcal{G}$ is:

- $\varepsilon = 2^n - 1$ is period of the sequences in the family
- $M = 2^n + 1$ is the size of the family $\mathcal{G}$
- $\theta_{max} = 2^{(n+1)/2} + 1$ is the maximal value of the nontrivial auto- or crosscorrelation of the sequences in $\mathcal{G}$

The Gold family is optimal since no other family of sequences of the same length and size can have a lower θ_{max}

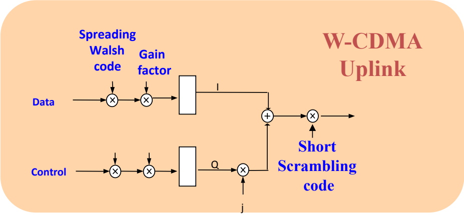
Long Scrambling Code Generator

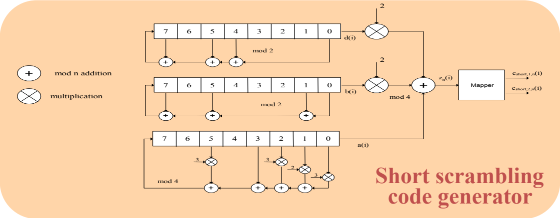


Gold sequence family is based upon on sequences generated by

$$x^{25} + x^3 + 1 \text{ and } x^{25} + x^3 + x^2 + x + 1$$

3G Scrambling Code





P. V. Kumar

T. Helleseth

A. R. Calderbank

A. R. Hammons Jr.,

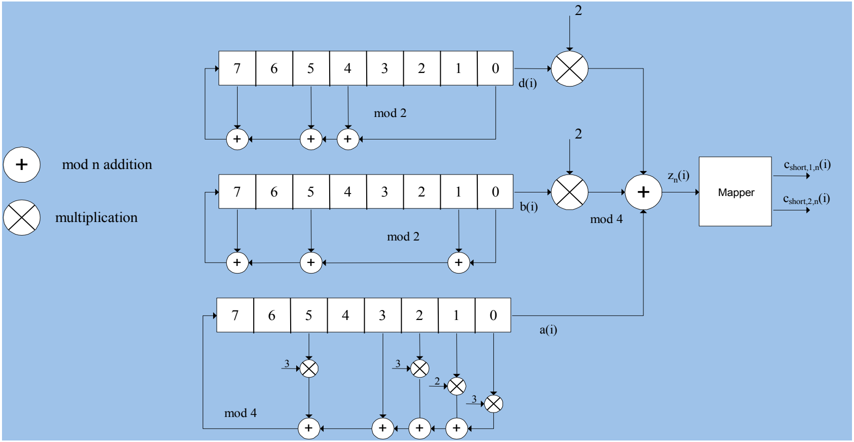
``Large Families of Quaternary Sequences with Low Correlation,"

IEEE Trans. Inform. Theory, March 1996.

Short Scrambling Code Family S(2) used in W-CDMA

Scrambling code design for 3G Wireless Cellular Communication

Short Scrambling Code



Family $S(2)$ of sequences $\pmod 4$

Distribution of the crosscorrelation of m-sequences and open problems

Some Properties of $C_d(\tau)$

Some properties of $C_d(\tau)$

- $C_d(\tau)$ is a real number
- $C_d(\tau)$ and $C_{d'}(\tau)$ have the same distribution when $d \cdot d' = 1 \pmod{p^n - 1}$ or $d' = d \cdot p^i \pmod{p^n - 1}$
- $\sum_\tau (C_d(\tau) + 1) = p^n$
- $\sum_\tau (C_d(\tau) + 1)^2 = p^{2n}$
- $\sum_\tau C_d(\tau)^k = -(p-1)^k + 2(-1)^{k-1} + a_k p^{2n}$ where a_k is the number of nonzero solutions $x_i \in \mathbb{F}_{p^n}$ of

$$\begin{array}{ccccccc} x_1 & + & x_2 & + \cdots + & x_{k-1} & +1 = 0 \\ x_1^d & + & x_2^d & + \cdots + & x_{k-1}^d & +1 = 0 \end{array}$$

When is $C_d(\tau)$ Two-Valued?

Theorem

If $d \notin \{1, p, p^2, \cdots, p^{n-1}\}$ (i.e., when the two m-sequences are cyclically distinct) then $C_d(\tau)$ is at least 3-valued.

Proof.

Suppose $C_d(\tau)$ has two values x and y occurring r and s times respectively. Then

$$\begin{array}{rcccccc} & r & + & s & = & p^n - 1 \\ \sum_\tau C_d(\tau) = & rx & + & sy & = & 1 \\ \sum_\tau C_d(\tau)^2 = & rx^2 & + & sy^2 & = & p^{2n} - p^n - 1 \end{array}$$

This leads to the equation (eliminating r and s)

$$(p^n x - (x+1))(p^n y - (y+1)) = p^{2n}(2 - p^n)$$

For $p = 2$ this is a Diophantine equation with no valid integer solutions.
(Note $\{x, y\} = \{-1, p^n - 1\}$) corresponds to two-weight autocorrelation..
For $p > 2$ the result follows similarly from divisibility properties in $Z[\omega]$. $\square$

Three-valued Crosscorrelation of m-sequences

The crosscorrelation $C_d(\tau)$ is known to be three-valued in the cases:

- (Gold 1968): $d = 2^k + 1$, $\frac{n}{gcd(n,k)}$ odd
- (Kasami 1968), (Welch 1960's): $d = 2^{2k} - 2^k + 1$, $\frac{n}{gcd(n,k)}$ odd
- Welch's conjecture: (Canteaut, Charpin, Dobbertin (2000))
  $d = 2^{\frac{n-1}{2}} + 3$, n odd
- Niho's conjecture: (Hollmann and Xiang (2001), Dobbertin (1999))

$$\begin{aligned} d &= 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} - 1 \text{ when } n = 1 \pmod 4 \\ &= 2^{\frac{n-1}{2}} + 2^{\frac{3n-1}{4}} - 1 \text{ when } n = 3 \pmod 4 \end{aligned}$$

- Cusick and Dobbertin (1996)

$$\begin{aligned} d &= 2^{\frac{n}{2}} + 2^{\frac{n+2}{4}} + 1 \text{ when } n = 2 \pmod 4 \\ &= 2^{\frac{n+2}{2}} + 3 \qquad \text{ when } n = 2 \pmod 4 \end{aligned}$$

The 4-Valued Conjecture

Conjecture (Helleseth 1971, 1976)

Let p be any prime. If $n = 2^i$ then $C_d(\tau)$ takes on at least 4 values.

Theorem (Katz 2012)

The conjecture is true for $p = 2$ *and* $p = 3$.

The case $p > 3$ is still open

The $C_d(\tau) = -1$ conjecture

Conjecture (Helleseth 1971, 1976)

For any $d \equiv 1 \pmod{p-1}$ then $C_d(\tau) = -1$ for some τ

The conjecture is equivalent to proving one of the following two statements:

(1)

$$\sum_x \omega^{Tr(x^d - bx)} = -1$$

for some nonzero b.

(2) The system of equations

$$\begin{array}{ccccccc} x_0 & + & \alpha x_1 & + \cdots + & \alpha^{q-2} x_{q-2} & = 0 \\ x_0^d & + & x_1^d & + \cdots + & x_{q-2}^d & = 0 \end{array}$$

has exactly q^{q-3} solutions $x_i \in \mathbb{F}_{p^n}$ where $q = p^n$.

Correlation Function

Known 3-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{2^n}$

No.	d-Decimation	Condition	Remarks
1	$2^k + 1$	$n/\gcd(n,k)$ odd	Gold, 1968
2	$2^{2k} - 2^k + 1$	$n/\gcd(n,k)$ odd	Kasami, 1971
3	$2^{n/2} - 2^{(n+2)/4} + 1$	$n \equiv 2 \pmod 4$	Cusick et al., 1996
4	$2^{n/2+1} + 3$	$n \equiv 2 \pmod 4$	Cusick et al., 1996
5	$2^{(n-1)/2} + 3$	n odd	Canteaut et al., 2000
6	$2^{(n-1)/2} + 2^{(n-1)/4} - 1$	$n \equiv 1 \pmod 4$	Hollmann et al., 2001
7	$2^{(n-1)/2} + 2^{(3n-1)/4} - 1$	$n \equiv 3 \pmod 4$	Hollmann et al., 2001

Remarks: (1) No. 5 is the Welch's conjecture; (2) Nos. 6 and 7 are the Niho's conjectures

Open Problem

Show that the table contains all decimations with 3-valued correlation function.

Correlation Function

Known 3-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{p^n}$

No.	d-Decimation	Condition	Remarks
1	$(p^{2k}+1)/2$	$n/\gcd(n,k)$ odd	Trachtenberg, 1970
2	$p^{2k}-p^k+1$	$n/\gcd(n,k)$ odd	Trachtenberg, 1970
3	$2\cdot 3^{(n-1)/2}+1$	n odd	Dobbertin et al., 2001
4	$2\cdot 3^{(n-1)/4}+1$	$n\equiv 1 \pmod 4$	Katz and Langevin 2013
5	$2\cdot 3^{(3n-1)/4}+1$	$n\equiv 3 \pmod 4$	Katz and Langevin 2013

Remarks: (1) Nos. 1 and 2 are due to Helleseth for even n; (2) The result obtained by Xia et al. (IEEE IT 60(11), 2014) is covered by No. 1. The 3-valued correlation function in No. 4 and No. 5 was conjectured by Dobbertin et al. in 2001.

Open Problems

- Show that the table contains all decimations with 3-valued correlation function for $p>3$.

Cross Correlation Functions of Niho Exponents

Niho Exponent

Let p be a prime, $n = 2m$ a positive integer and $q = p^m$. Let $\mathbb{F}_q$ denote the finite field with q elements.

Niho Exponent

A positive integer d is called a Niho exponent (with respect to $\mathbb{F}_{q^2}$) if there exists some $0 \leq j \leq n-1$ such that

$$d \equiv p^j \pmod{q-1}$$

- Normalized form: $j = 0$, i.e., $d = (q-1)s + 1$.
- Equivalence class: cyclotomic coset, inverse, etc.

Niho exponents

Niho exponents and solutions of equations

Let $n = 2m$ and $d = 1 \pmod{2^m - 1}$. Then each $x \in \mathbb{F}_{2^n}$ can be uniquely written as $x = yz$ where $y \in \mathbb{F}_{2^m}$ and $z \in U = \{z | z^{2^m+1} = 1\}$.
Then

$$
\begin{aligned}
C_d(\tau) &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{Tr_n(x^d + ax)} \\
&= \sum_{y \in \mathbb{F}_{2^m}^*, z \in U} (-1)^{Tr_n(y(z^d + az))} \\
&= \sum_{y \in \mathbb{F}_{2^m}^*, z \in U} (-1)^{Tr_m(y(z^d + az + z^{-d} + a^{2^m} z^{-1}))} \\
&= (2^m - 1)N + (2^m + 1 - N) - 1 \\
&= -1 + 2^m(N - 1)
\end{aligned}
$$

where $N = |\{z \in U | z^d + az + z^{-d} + a^{2^m} z^{-1} = 0\}|$.

Correlation Function

Known 4-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{2^n}$

No.	d-Decimation	Condition	Remarks
1	$2^{n/2+1}-1$	$n \equiv 0 \pmod 4$	Niho, 1972
2	$(2^{n/2}+1)(2^{n/4}-1)+2$	$n \equiv 0 \pmod 4$	Niho, 1972
3	$\frac{2^{(n/2+1)r}-1}{2^r-1}$	$n \equiv 0 \pmod 4$	Dobbertin, 1998
4	$\frac{2^n+2^{s+1}-2^{n/2+1}-1}{2^s-1}$	$n \equiv 0 \pmod 4$	Helleseth et al., 2005
5	$(2^{n/2}-1)\frac{2^r}{2^r\pm 1}+1$	$n \equiv 0 \pmod 4$	Dobbertin et al., 2006

Remarks: (1) All are the Niho type decimations; (2) No. 5 covers previous four cases.

Conjecture (Dobbertin, Helleseth et al., 2006)

No. 5 covers all 4-valued cross correlation for Niho type decimation.

Note that these 4-valued binary Niho cases are strongly related to the polynomial $x^{2^r+1}+ax^{2^r}+bx+c$ that has $0, 1, 2$ or $2^{gcd(r,n)}+1$ zeros in $\mathbb{F}_{2^n}$.

Correlation Function

Known 4-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{p^n}$

No.	d-Decimation	Condition	Remarks
1	$2 \cdot p^{n/2} - 1$	$p^{n/2} \not\equiv 2 \pmod 3$	Helleseth, 1976
2	$3^k + 1$	$n = 3k, k$ odd	Zhang et al., 2013
3	$3^{2k} + 2$	$n = 3k, k$ odd	Zhang et al., 2013

Remarks: (1) No. 1 is a Niho type decimation; (2) Nos. 2 and 3 are due to Zhang et al. if $\gcd(k, 3) = 1$ and due to Xia et al. if $\gcd(k, 3) = 3$.

Open Problem

Find new 4-valued $C_d(\tau)$ for any prime p.

Correlation Function

Known 5 or 6-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{2^n}$

No.	d-Decimation	Condition	Remarks
1	$2^{n/2}+3$	$n \equiv 0 \pmod 2$	Helleseth, 1976
2	$2^{n/2}-2^{n/4}+1$	$n \equiv 0 \pmod 8$	Helleseth, 1976
3	$\frac{2^n-1}{3}+2^i$	$n \equiv 0 \pmod 2$	Helleseth, 1976
4	$2^{n/2}+2^{n/4}+1$	$n \equiv 0 \pmod 4$	Dobbertin, 1998

Remarks: (1) No. 1 was conjectured by Niho; (2) No. 3 is of Niho type if $n/2$ is odd.

Open Problem (Dobbertin, Helleseth et al., 2006)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (2^{n/2}-1)+1$.

The binary Niho case $d = 3 \cdot (2^m - 1) + 1$

A partial solution.

Theorem (Dobbertin, Felke, Helleseth and Rosendahl (2006))

Let $n = 2m$, m *is even and* $d = 3 \cdot 2^n - 2$. *Then* $C_d(\tau) + 1$ *takes on the following values.*

$$
\begin{array}{rlrl}
-2^m & \textit{occurs} & \frac{1}{30}(11 \cdot 2^n - 24 \cdot 2^m + R) & \textit{times} \\
0 & \textit{occurs} & \frac{1}{24}(9 \cdot 2^n - 22 \cdot 2^m - 3R - 20) & \textit{times} \\
2^m & \textit{occurs} & \frac{1}{6}(9 \cdot 2^n - 2 \cdot 2^m + R - 4) & \textit{times} \\
2 \cdot 2^m & \textit{occurs} & \frac{1}{12}(2^n - R + 12) & \textit{times} \\
3 \cdot 2^m & \textit{occurs} & \frac{1}{3}(2^m - 2) & \textit{times} \\
4 \cdot 2^m & \textit{occurs} & \frac{1}{120}(2^m - 14 \cdot 2^m + R + 20) & \textit{times.}
\end{array}
$$

where

$$R = \sum_{y \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2} \chi_m(1/y) K\left(\frac{1}{y^3 + y}\right)$$

and $K(y) = \sum_{c \in \mathbb{F}_{2^m}} \chi_m(1/x + xy)$ *denotes a Kloosterman sum.*

The exponential sum R was not determined in this paper.

Solving the binary Niho case $d = 3 \cdot (2^n - 1) + 1$

The full solution.

Let k be a positive integer and N_k denote the number of solutions to

$$\begin{aligned} x_1 + x_2 + \cdots + x_k &= 0, \\ x_1^d + x_2^d + \cdots + x_k^d &= 0. \end{aligned}$$

Question: How to determine the values of N_k?

Open Problem (Dobbertin, Helleseth et al., 2006)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (2^{n/2} - 1) + 1$.

Solved! (surprising connection with the Zetterberg code) by Xia, L., Zeng and Helleseth 2016 (IEEE IT, 62(12), 2016)

Correlation Function

Known 5 or 6-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{p^n}$

No.	d-Decimation	Condition	Remarks
1	$(p^n-1)/2+p^i$	$p^n \equiv 1 \pmod 4$	Helleseth, 1976
2	$(p^n-1)/3+p^i$	$p \equiv 2 \pmod 3$	Helleseth, 1976
3	$p^{n/2}-p^{n/4}+1$	$p^{n/4} \not\equiv 2 \pmod 3$	Helleseth, 1976
4	3^k+1	$n=3k, k$ even	Zhang et al., 2013
5	$3^{2k}+2$	$n=3k, k$ even	Zhang et al., 2013

Remarks: (1) No. 1 is of Niho type if $n/2$ is odd; (2) Nos. 4 and 5 are due to Zhang et al. if $\gcd(k,3)=1$ and due to Xia et al. if $\gcd(k,3)=3$.

Open Problem (Dobbertin, Helleseth and Martinsen, 1999)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (3^{n/2}-1)+1$.

The ternary Niho case $d = 3 \cdot (3^{n/2} - 1) + 1$

Open Problem (Dobbertin, Helleseth and Martinsen, 1999)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (3^{n/2} - 1) + 1$.

Solved!

by Xia, Li, Zeng and Helleseth 2017 (IEEE Trans. Inf. Theory 63(11): 7206-7218 (2017)).

Future Work

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (p^{n/2} - 1) + 1$ for $p > 3$.

This case is much more complicated!

The last Niho :conjecture $d = 4 \cdot (2^m - 1) + 1$

Theorem (Helleseth, Katz and Li (2021))

Let $n = 2m$, m is even and $d = 2^{m+2} - 3$. Then $C_d(\tau) + 1$ takes on at most the following five values: $\{-2^m, 0, 2^m, 2 \cdot 2^m, 4 \cdot 2^m\}$.

This is proved by considering the polynomial

$$x^7 + ax^4 + a^{2^m}x^2 + 1$$

and showe the number of zeros in $U = \{\ x \mid x^{2^m+1} = 1\}$ is 0, 1, 2, 3 or 5.

Open Problem

Find the complete crosscorrelation distribution in this case.

Note that in the m odd case the same method shows there are at most 6 correlation values in $\{-2^m, 0, 2^m, 2 \cdot 2^m, 3 \cdot 2^m, 4 \cdot 2^m\}$ (the complete correlation distribution is unknown also in this case).

Bent Functions From Niho Exponents

Bent Functions From Niho Exponents

Bent functions have applications in cryptography and coding theory.

Walsh Transform

Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The Walsh transform of $f(x)$ is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}(\lambda x)}, \lambda \in \mathbb{F}_{2^n}.$$

Bent Function

A function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is called Bent if $|\widehat{f}(\lambda)| = 2^{n/2}$ for any $\lambda \in \mathbb{F}_{2^n}$.

Bent Functions From Niho Exponents

Problem Description

Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by

$$f(x) = \sum_{i=1}^{2^n-2} \mathrm{Tr}(a_i x^i), a_i \in \mathbb{F}_{2^n}.$$

Then how to choose a_i and i such that $f(x)$ is Bent?

Remarks

Known infinite classes of Boolean Bent functions:

1. Monomial Bent: only 5 classes
2. Binomial Bent: only about 6 classes
3. Polynomial form: quadratic form, Dillon type and Niho type

Constructions of Bent Functions of Niho Type

Known Constructions of Niho Bent Functions

Table: Known Niho Bent Functions

No.	Class of Functions	Authors	Year
1	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1})$	–	–
2	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + bx^{(2^m-1)3+1})$	Dobbertin et al.	2006
3	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + bx^{(2^m-1)\frac{1}{4}+1})$	Dobbertin et al.	2006
4	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + bx^{(2^m-1)\frac{1}{6}+1})$	Dobbertin et al.	2006
5	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + \sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1})$	Leander, Kholosha	2006

Remarks: (1) No. 1 is trivial; (2) No. 3 is covered by No. 5

Binomial Bent Functions

A simple family of binomial bent functions which have a quite complex dual bent functions are due to Helleseth and Kholosha (2010).

Theorem (Helleseth and Kholosha (2010))

Let $n = 4k$. Then p-ary function $f(x)$ given by

$$f(x) = \mathrm{Tr}_n\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)$$

is a weakly regular bent function and

$$\hat{f}(y) = -p^{2k}\omega^{\mathrm{Tr}_k(x_0)/4} \quad ,$$

where x_0 is a unique root in $\mathrm{GF}(p^k)$ of the polynomial

$$y^{p^{2k}+1} + (y^2+X)^{(p^{2k}+1)/2} + y^{p^k(p^{2k}+1)} + (y^2+X)^{p^k(p^{2k}+1)/2} \quad .$$

These bent functions led to constructions of some new strongly regular graphs.

APN functions and AB functions

Almost Perfect Nonlinear (APN) Functions

Definition

A function $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if for all $a, b \in \mathbb{F}_{2^n}, a \neq 0$, the equation

$$f(x+a) - f(x) = b$$

has at most two solutions $x \in \mathbb{F}_{2^n}$.

- More generally such an f is called a differentially 2-uniform function
- Optimal resistant against the differential attack

A Simple APN Example $f(x) = x^3$

Theorem

The function $f(x) = x^3$ is APN

Proof.

Let

$$f(x) = x^3$$

be defined over $\mathbb{F}_{2^n}$. Then

$$f(x+a) + f(x) = x^2 a + x a^2 + a^3 = b$$

which has at most two solutions $x \in \mathbb{F}_{2^n}$ for any $a \neq 0$ and $b \in \mathbb{F}_{2^n}$. $\square$

The Walsh Transform

The nonlinearity $NL(F)$ of an (n, m) function F can be expressed by means of the Walsh transform. The Walsh transform of F at $(\alpha, \beta) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is defined by

$$W_F(\alpha, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\beta F(x)) + Tr_1^n(\alpha x)}$$

and the Walsh spectrum of F is the set

$$\{W_F(\alpha, \beta) : \alpha \in \mathbb{F}_{2^n}, \beta \in \mathbb{F}_{2^m}^*\}.$$

The Walsh spectrum of AB functions consists of three values $0, \pm 2^{\frac{n+1}{2}}$. The Walsh spectrum of a bent function is $\{\pm 2^{\frac{n}{2}}\}$.

Theorem (Chabaud and Vaudenay (1994))

Any AB function is APN.

APN Power Functions

Table 1a. Known APN power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	$d^\circ(x^d)$
Gold	2^i+1	$\gcd(i,n)=1$	2
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$
Welch	2^t+3	$n=2t+1$	3
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{3t+1}{2}}-1$, t odd	$n=2t+1$	$(t+2)/2$ $t+1$
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$

AB Power Functions

Table 1b. Known AB power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	$d^\circ(x^d)$
Gold	$2^i + 1$	$\gcd(i,n) = 1$	2
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i,n) = 1$	$i+1$
Welch	$2^t + 3$	$n = 2t+1$	3
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t+1$	$(t+2)/2$ $t+1$

Other Relations to Crosscorrelation Decimations

Sequences and the S-box in AES

Kloosterman sum

The crosscorrelation between m-sequence $\{s_t\}$ and the reverse sequence $\{s_{-t}\}$ corresponds to the famous Kloosterman sum

$$C_{-1}(\tau) = \sum_{x \neq 0} \omega^{Tr(ax + x^{-1})}$$

- Bound for Kloosterman sum is $|C_{-1}(\tau) + 1| \leq 2p^{\frac{n}{2}}$
- The AES S-box is based on $f(x) = x^{-1}$ for $n = 8$.
- The nonlinearity between $Tr(x^{-1})$ and $Tr(ax)$ is $|C_{-1}(\tau)|$
- The S-box for is 4 uniform (not APN), the best possible known for a permutation for $n = 8$
- The S-box is not AB, but uniformity and nonlinearity is the best possible known for $n = 8$

Sequences with Ideal Autocorrelation

Sequences with ideal autocorrelation: Kasami-Exponent

Property of APN power functions

Let $f(x) = x^d$ be a binary APN power mapping of $\mathbb{F}_{2^n}$.
Then $(x+1)^d + x^d = b$ has two solutions for 2^{n-1} values of b and 0 solutions for the 2^{n-1} other values of b.

Theorem (Dillon and Dobbertin (2004))

Let $d = 2^{2k} - 2^k + 1$ *where* $\gcd(k, n) = 1$ *and define the binary sequence* $\{s_t\}$ *such that*

$$s_t = \begin{cases} 1 & \textit{if} \quad (x+1)^d + x^d = b \quad \textit{has 2 solutions} \\ 0 & \textit{if} \quad (x+1)^d + x^d = b \quad \textit{has 0 solutions} \end{cases}$$

The $\{s_t\}$ *is balanced and has two-level ideal autocorrelation.*

Ternary sequences: Ideal Autocorrelation

The Lin sequence

Let $p = 3$ and n odd. Let α be a primitive element of $\mathbb{F}_{p^n}$.
Let $\{s_t\}$ be the ternary m-sequence where $s_t = Tr(\alpha^t)$.
Then the sequence

$$u_t = s_t + s_{(2\cdot 3^{(n-1)/2}+1)t}$$

has two-level autocorrelation.

Remarks

- This result was conjectured by Lin in 1998.
- The result was proved by Gong et al. 2014 and Arasu et al. 2014.
- Note that the decimation $d = 2 \cdot 3^{(n-1)/2} + 1$ gives a three-valued crosscorrelation.

Helleseth-Kumar-Martinsen sequences

Helleseth-Kumar-Martinsen sequences (2001)

- $p = 3$
- $n = 3k$
- $d = 3^{2k} - 3^k + 1$
- α is a primitive element in $GF(3^n)$

Then the ternary sequence $\{s_t\}$ of period $3^n - 1$ defined by

$$s_t = Tr(\alpha^t + \alpha^{dt})$$

has ideal two-level autocorrelation.

Family was further generaliised by Helleseth and Gong (2002).

USC note

Note on a USC Lab at the EE Department

Theory is when you know everything but nothing works.

Practice is when everything works but no one knows why.

In our lab theory and practice are combined nothing works and no one knows why.

Thank You!

Questions? Comments? Suggestions?