Integer Valued Sequences with 2-Level Autocorrelation from Iterative Decimation Hadamard Transform

Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
CANADA
<http://comsec.uwaterloo.ca/∼ggong>

Fields Institute-Carleton Finite Fields Workshop, July 20-23, 2010

Joint work with Honggang Hu

Outline

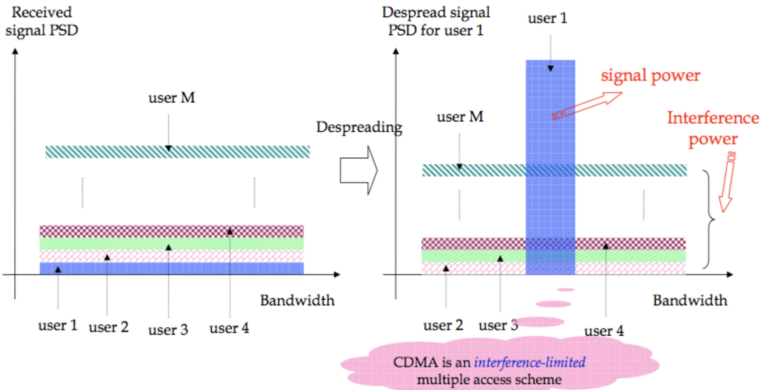
- **Iterative** Decimation Hadamard Transform (DHT)
- **Realizations** from DHT and Known Binary 2-Level Autocorrelation Sequences
- **New Integer** Valued Sequences with 2-Level Autocorrelation Constructed from DHT
- **New Ternary and Quaternary** Sequences with 2-Level Autocorrelation
- **Some Remarks** on Sequences of DHT

Code Division Multiplexing Access (CDMA)

- Multiple users share a common channel simultaneously by using different *codes*
- Narrowband user information is spread into a much wider spectrum by the spreading code
- The signal from other users will be seen as a background noise: Multiple access interference (MAI)
- The limit of the maximum number of users in the system is determined by interference due to multiple access and multipath fading: Adding one user to CDMA system will only cause graceful degradation of quality

Theoretically, no fixed maximum number of users !

Code Division Multiplexing Access (CDMA) (Cont.)



The signal from other users will be seen as a background noise: *Multiple access interference (MAI)*

Spreading Sequences in CDMA Systems

$H_n \times H_n^T = nI_n$

Walsh Codes: Basic spreading codes in CDMA systems

- *n* different Walsh codes: each row of an *nxn* Hadamard matrix
- Mutually orthogonal: inner product of different Walsh codes are zero
- Synchronization of all users are required to maintain the orthogonality: Otherwise, produce multiple access interference (MAI)
- Further, delayed copies received from a multipath fading are not orthogonal any more: Multipath fading interference

MAI and multipath interference are major factors to limit the capacity of CDMA systems !

Basic Concepts and Definitions on Sequences

- p**, a prime**; n, a positive integer; $q = p^n$.
- $f(x)$**, a polynomial** function from $\mathbb{F}_q$ to $\mathbb{F}_p$.
- $Tr(x) = x + x^p + \cdots + x^{p^{n-1}}$, the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$.
- α**, a primitive** element in $\mathbb{F}_q$.
- **A sequence** $\mathbf{a} = \{a_i\}$ where $a_i = f(\alpha^i), i = 0, 1, \cdots$, is a sequence over $\mathbb{F}_p$ with period $q - 1$ or dividing $q - 1$.
- If $f(x) = Tr(x^t)$ where $(t, q - 1) = 1$, then $\mathbf{a}$ is an **m-sequence** over $\mathbb{F}_p$, i.e.,

$$\text{m-sequence} \longleftrightarrow Tr(x^t).$$

Decimation

$$b_i = a_{si}, i = 0, 1, \cdots,$$

is said to be an s-decimation of $\mathbf{a}$, denoted by $\mathbf{a}^{(s)}$.

$$\begin{array}{rcl} \mathbf{a} & \longleftrightarrow & f(x) \\ \mathbf{a}^{(s)} & \longleftrightarrow & f(x^s) \end{array}$$

E.g.,

$$\begin{array}{rcl} \mathbf{a} = 1001011 & \longleftrightarrow & Tr(x) \\ \mathbf{a}^{(3)} = 1110100 & \longleftrightarrow & Tr(x^3) \end{array}$$

Autocorrelation

- **Let** $\omega = e^{2\pi i/p}$, a complex primitive pth root of unity. The canonical additive character χ of F is defined by

$$\chi(x) = \omega^x, x \in \mathbb{F}_p.$$

- The autocorrelation of **a** is defined by

$$C(\tau) = \sum_{i=0}^{N-1} \chi(a_{i+\tau})\overline{\chi(a_i)},\ 0 \le \tau \le N-1 \qquad (1)$$

where $\overline{\chi}$ be the complex conjugate of χ.

2-level Autocorrelation and Orthogonal Functions

- The sequence **a** is said to have a ***2-level autocorrelation function***, if

$$C(\tau) = \begin{cases} N & \textbf{if } \tau \equiv 0 \textbf{ mod } N \\ -1 & \textbf{if } \tau \not\equiv 0 \textbf{ mod } N. \end{cases}$$

- If **a** is also balanced, then we say that **a** has an (ideal) 2-level autocorrelation function.
- **When** $N = q - 1$ and **a** $\leftrightarrow f(x)$, **a** has 2-level autocorrelation if and only if

$$\sum_{x \in \mathbb{F}_q} \chi(f(\lambda x)\overline{\chi(f(x)} = 0, \forall \lambda \in \mathbb{F}_q, \lambda \neq 1.$$

$f(x)$ is called an **orthogonal** function from $\mathbb{F}_q$ to $\mathbb{F}_p$.

Integer Sequences and Complex Valued Sequences

- Let $\mathbb{C}$ be the complex field, $\mathbf{b} = \{b_i\}, b_i \in \mathbb{C}$ with period N. The autocorrelation of $\mathbf{b}$ is defined as

$$C(\tau) = \sum_{i=0}^{N-1} b_{i+\tau}\overline{b_i}, \ 0 \leq \tau \leq N-1. \quad (2)$$

- $\mathbf{b}$ has 2-level autocorrelation if

$$C(\tau) = \begin{cases} N & \textbf{if } \tau \equiv 0 \textbf{ mod } N \\ -1 & \textbf{if } \tau \not\equiv 0 \textbf{ mod } N. \end{cases}$$

Hadamard Transform

- **The Hadamard transform** of $f(x)$ is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_q} \chi(Tr(\lambda x))\overline{\chi(f(x))} = \sum_{x \in \mathbb{F}_q} \omega^{Tr(\lambda x) - f(x)}, \lambda \in \mathbb{F}_q.$$

- **The inverse** formula is given by

$$\chi(f(\lambda)) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi(Tr(\lambda x))\overline{\widehat{f}(x)}, \lambda \in \mathbb{F}_q.$$

- **Parseval Formula**

$$\sum_{x \in \mathbb{F}_q} \chi(f(\lambda x))\overline{\chi(f(x))} = \sum_{x \in \mathbb{F}_q} \widehat{f}(\lambda x)\overline{\widehat{f}(x)}, \lambda \in \mathbb{F}_q.$$

Iterative Decimation Hadamard Transform (DHT) (Gong-Golomb, 2002)

- $h(x)$, orthogonal; v, t, integer $0 < v, t < q-1$, and $\lambda \in \mathbb{F}_q$.
- **The first-order DHT**

$$\begin{aligned} \widehat{f}_h(v)(\lambda) &= \sum_{x \in \mathbb{F}_q} \chi(h(\lambda x))\overline{\chi(f(x^v))} \\ &= \sum_{x \in \mathbb{F}_q} \omega^{h(\lambda x) - f(x^v)}. \end{aligned}$$

- **The second-order DHT**

$$\begin{aligned} \widehat{f}_h(v,t)(\lambda) &= \sum_{y \in \mathbb{F}_q} \chi(h(\lambda y))\overline{\widehat{f}_h(v)(y^t)} \\ &= \sum_{x,y \in \mathbb{F}_q} \omega^{h(\lambda y) - h(y^t x) + f(x^v)}, \lambda \in \mathbb{F}_q \end{aligned}$$

Realizations

- **In general**, for any integer pair (v,t), for $x \in \mathbb{F}_q$, a value of $\widehat{f}_h(v,t)(x)$ may be just a complex number.
- If
$$\widehat{f}_h(v,t)(x) \in \{q\omega^i \mid i = 0, \cdots, p-1\}, \forall x \in \mathbb{F}_q,$$
then we can construct a function, say $g(x)$, from $\mathbb{F}_q$ to $\mathbb{F}_p$, whose elements are given by
$$\chi(g(x)) = \frac{1}{q}\widehat{f}_h(v,t)(x), x \in \mathbb{F}_q.$$
In this case, we say that (v,t) is ***realizable***, and $g(x)$ is a ***realization*** of $f(x)$.
- **Hadamard Equivalence:** If $g(x)$ is realized by $f(x)$, then $g(x)$ and $f(x)$ are Hadamard equivalent respect to $h(x)$.

Important remark

For two functions which are Hadamard equivalent, if one of them has 2-level autocorrelation, so does the other.

Example

- Let $p = 2$, $n = 4$, $h(x) = f(x) = Tr(x)$,
- $\mathbb{F}_{2^4}$ be defined by $t(x) = x^4 + x + 1$, and α a root of $t(x)$ in $\mathbb{F}_{2^4}$. Let

$$f(x) \leftrightarrow \mathbf{a} = 000100110101111.$$

- The first-order DHT of $f(x)$ (or $\mathbf{a}$)

$$\widehat{f_h}(v)(\lambda) = \sum_{x \in \mathbb{F}_{2^4}} (-1)^{Tr(\lambda x) + Tr(x^v)},$$

v	$\{\widehat{f_h}(v)(\alpha^i)\}, i = 0, 1, \cdots, s-1$	$s = \frac{15}{gcd(v,15)}$
3	$8, 0, 0, 0, 0$	5
5	$0, 0, 0$	3
7	$0, 0, 0, 4, 0, 8, 4, -4, 0, 4, 8, -4, 4, -4, -4$	15

Example (cont.)

- **The second-order DHT**, $\widehat{f_h}(7,7)$ and $\widehat{f_h}(7,5)$, are given by

$$\widehat{f_h}(7,t)(\lambda) = \sum_{x,y \in \mathbb{F}_{2^4}} (-1)^{Tr(\lambda y) + Tr(y^t x) + Tr(x^7)}, \ t \in \{5, 7\}$$

and

$$\begin{aligned} \{\widehat{f_h}(7,7)(\alpha^i)\} &= -16, -16, -16, 16, -16, 24, 16, 8, -16, 16, 24, 8, 16, 8, 8 \\ \{\widehat{f_h}(7,5)(\alpha^i)\} &= 16, -16, -16. \end{aligned}$$

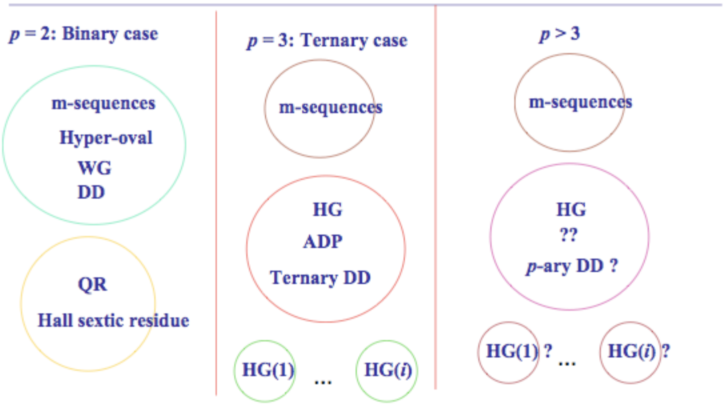
- **Thus,** $(7,7)$ **is not a realizable pair**, while $(7,5)$ is a realizable pair which realizes the sequence 011 of period 3.

Hadamard Equivalent Classes for Known 2-Level Autocorrelation Sequences

- **Experimental** results on the realizations of all the known p-ary sequences with 2-level autocorrelation of period $p^n - 1$ have been done:
  - **Binary case**: for odd $n \leq 17$ (Gong-Golomb, 2002), and even $n \leq 16$ (Yu-Gong, 2005, 2009).
  - **Ternary Case**: for odd $n \leq 15$ (Ludkovski-Gong, 2001, Gong-Helleseth, 2004).
  - ***p*-ary**: $p > 3$, some data.

Hadamard Equivalent Classes for Known 2-Level Autocorrelation Sequences (Cont.)

Experimental Results



New Integer Valued Sequences with 2-Level Autocorrelation Constructed from DHT

New Observation

- Recall

$$\{s_i\} = \{\widehat{f_h}(7,7)(\alpha^i)\}$$
$$= -16, -16, -16, 16, -16, 24, 16, 8, -16, 16, 24, 8, 16, 8, 8$$

- **The sequence** $\{s_i\}$ is not a realization, but it is an integer sequence with 2-level autocorrelation!

Construction of New Integer Valued Sequences

- **For integers** $0 < v, t < q - 1$, we define the sequence $\mathbf{s}'(v, t) = \{s'_i\}$ by

$$s'_i = \widehat{f}_h(v, t)(\alpha^i), \;\; s_i = s'_i/q, i = 0, 1, 2, \cdots .$$

- **Then** $\mathbf{s}'(v, t)$ is an integer valued sequence for $p = 2$ and a complex valued sequence for $p > 2$.
- $\mathbf{s}(v, t)$ **is normalized** from $\mathbf{s}'(v, t)$.

Theorem

If the sequence $\mathbf{a} \leftrightarrow f(x)$ has **two-level autocorrelation**, then the autocorrelation function $C_{\mathbf{s}(v,t)}(\tau)$ of $\mathbf{s}(v,t)$, the normalized version, satisfies

$$\begin{aligned} C_{\mathbf{s}(v,t)}(\tau) &= \sum_{i=0}^{q-2} s_{i+\tau}\overline{s_i} \\ &= \begin{cases} q-1, & \textbf{if } \tau \equiv 0 \textbf{ mod } (q-1); \\ -1, & \textbf{otherwise.} \end{cases} \end{aligned}$$

for any (v,t) which co-prime with $q-1$.

Question: For which (v,t), does the sequence $\mathbf{s}(v,t)$ have “nice" values?

Some Examples

- $p = 2$, $f(x) = h(x) = Tr(x)$.

Table: $n = 5$

(v, t)	$\widehat{Tr}(v, t)(\lambda)/2^n$
(3, 11)	$\{-1, 0, 2\}$
(15, 3)	$\{-1, 0, 2\}$
(3, 7)	$\{-1, 0, 1, 4\}$
(3, 15)	$\{-2, -1/2, 0, 1/2, 1, 3/2\}$
(5, 15)	$\{-7/2, -1, -1/2, 0, 1/2, 3/2\}$
(15, 15)	$\{-1, -3/4, -1/4, 1/2, 3/2, 11/4\}$
maximum magnitude	4

Some Examples (Cont.)

Table: $n = 6$

(v, t)	$\widehat{Tr}(v, t)(\lambda)/2^n$
(5, 13)	$\{-1, 0, 1, 4\}$
(5, 23)	$\{-1, 0, 1, 3\}$
(5, 5)	$\{-2, -1, 0, 1, 2\}$
(5, 31)	$\{-3/2, -1, -1/2, 0, 1/2, 1, 3\}$
(11, 23)	$\{-2, -1, -1/2, 0, 1/2, 1, 2\}$
(31, 31)	$\{-1, -7/8, -5/8, -1/4, 1/4, 7/8, 13/8, 5/2\}$
(11, 31)	$\{-7/2, -5/4, -1, -3/4, -1/2, -1/4, 1/4, 1/2, 1, 5/4, 3/2, 2\}$
maximum magnitude	4

Some Examples (Cont.)

Table: $n = 7$

(v, t)	$\widehat{Tr}(v,t)(\lambda)/2^n$
(3, 43)	$\{-1, 0, 2\}$
(5, 27)	$\{-1, 0, 2\}$
(9, 15)	$\{-1, 0, 2\}$
(3, 19)	$\{-1, 0, 1, 2\}$
(3, 29)	$\{-1, 0, 1, 2\}$
(5, 13)	$\{-1, 0, 1, 2\}$
(5, 21)	$\{-1, 0, 1, 2\}$
(7, 13)	$\{-1, 0, 1, 2\}$
(7, 21)	$\{-1, 0, 1, 2\}$
(9, 9)	$\{-1, 0, 1, 2\}$
(9, 23)	$\{-1, 0, 1, 2\}$
(11, 29)	$\{-1, 0, 1, 2\}$
(3, 23)	$\{-1, 0, 1, 3\}$
(7, 11)	$\{-1, 0, 1, 3\}$
(7, 19)	$\{-1, 0, 2, 6\}$
...	...
maximum magnitude	6

Some Examples (Cont.)

Table: $n = 8$

(v,t)	$\widehat{Tr}(v,t)(\lambda)/2^n$
(11, 47)	$\{-1, 0, 1, 3\}$
(13, 53)	$\{-1, 0, 1, 3\}$
(11, 31)	$\{-1, 0, 1, 2, 3\}$
(23, 43)	$\{-1, 0, 1, 2, 3\}$
(13, 23)	$\{-1, 0, 1, 2, 9\}$
(7, 23)	$\{-1, 0, 1, 2, 3, 5\}$
(7, 31)	$\{-1.5, -1, -0.5, 0, 0.5, 1, 1.5, 4\}$
(11, 61)	$\{-2, -1.5, -1, -0.5, 0, 0.5, 1, 2\}$
(11, 91)	$\{1, 0.5, -2.5, -0.5, 0, -1, 2, 2.5, -2\}$
(13, 31)	$\{1, 0, 0.5, -0.5, -1, 2, -2, -1.5, 1.5\}$
(23, 91)	$\{1, -0.5, 0.5, 1.5, 0, 2.5, -1, -1.5, 2\}$
(7, 19)	$\{5, 0.5, 1.5, -1, 1, -0.5, 0, -1.5, 3, -2\}$
(7, 47)	$\{-3, -0.5, 0, 2, -1, -1.5, 1, 0.5, 1.5, 3\}$
(11, 53)	$\{5, 0, -1.5, 0.5, -0.5, 2, -3, 1.5, 1, -1\}$
(13, 47)	$\{1, 0.5, -1.5, -1, 0, 3, -0.5, 1.5, -2.5, 2.5\}$
...	...
maximum magnitude	9

New Ternary Sequences with 2-Level Autocorrelation

Theorem

1. Let $p = 2$, n be an odd integer, $1 \leq k < n$ with $\gcd(k, n) = 1$, and $f(x) = h(x) = Tr(x)$. Let $v = 2^{n-1} - 1$, and $t = 2^k + 1$. Then $\mathbf{s}(v, t)$ has two-level autocorrelation, and the s_i's take **three distinct values** $-1, 0,$ **or** 2.

2. Let N_η denote the number of η within one period of $\mathbf{s}(v, t)$, where $\eta = -1, 0, \text{or } 2$. Then

$$N_{-1} = (2^n + 1)/3, N_0 = 2^{n-1} - 1, \text{ and} N_2 = (2^{n-1} - 1)/3.$$

How to prove it?

In order to prove

$$\widehat{Tr}(v,t)(\alpha^i)/2^n = -1, 0, \text{or } 2,$$

we need to prove the following lemma:

Lemma

Let n be an odd integer, and $1 \leq k < n$ with $\gcd(k,n) = 1$. Let $v = 2^{n-1} - 1$, and $t = 2^k + 1$. Then for any $\lambda \in \mathbb{F}_{2^n}^*$, we have

$$\sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda y + y^t x + x^v)} = -2^n, 0, \textbf{or } 2^{n+1}.$$

Variable Changes

By changing variables, we have

$$\sum_{x,y\in\mathbb{F}_{2n}}(-1)^{Tr(\lambda y+y^t x+x^v)}=\sum_{x,y\in\mathbb{F}_{2n}}(-1)^{Tr(x^t+y^t+\lambda xy)}.$$

In details,

$$\begin{aligned}\sum_{x,y\in\mathbb{F}_{2n}}(-1)^{Tr(\lambda y+y^t x+x^v)} &= \sum_{x\in\mathbb{F}_{2n}^*,y\in\mathbb{F}_{2n}}(-1)^{Tr(\lambda y+y^t x+x^v)}=\sum_{x\in\mathbb{F}_{2n}^*,y\in\mathbb{F}_{2n}}(-1)^{Tr(\lambda y+y^t x+1/x)}\\ &= \sum_{x\in\mathbb{F}_{2n}^*,y\in\mathbb{F}_{2n}}(-1)^{Tr(\lambda y+y^t/x+x)} \quad (x\leftarrow 1/x)\\ &= \sum_{x_1\in\mathbb{F}_{2n}^*,y\in\mathbb{F}_{2n}}(-1)^{Tr(\lambda y+(y/x_1)^t+x_1^t)} \quad (x_1^t\leftarrow x)\\ &= \sum_{x_1\in\mathbb{F}_{2n}^*,z\in\mathbb{F}_{2n}}(-1)^{Tr(\lambda zx_1+z^t+x_1^t)} \quad (z\leftarrow y/x_1)\\ &= \sum_{x_1,z\in\mathbb{F}_{2n}}(-1)^{Tr(z^t+x_1^t+\lambda zx_1)}.\end{aligned}$$

One New Lemma

Thus, we need to prove the lemma below:

Lemma

Let n be an odd integer, and $1 \leq k < n$ with $\gcd(k, n) = 1$. Then for any $\lambda \in \mathbb{F}_{2^n}^*$, we have

$$\sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{2^k+1} + y^{2^k+1} + \lambda xy)} = -2^n, 0, \textbf{or } 2^{n+1}.$$

Proof Sketch

- Set $L_\lambda(\omega) = \omega^{2^{2k}} + \lambda^{2^k}\omega^{2^k} + \omega + \lambda^{2^{k-1}}$. The we have

$$\sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{Tr(x^{2^k+1}+y^{2^k+1}+\lambda xy)} = 2^n \sum_{\omega : L_\lambda(\omega)=0} (-1)^{Tr(\omega^{2^k+1})}.$$

- Hence we need to study the roots of $L_\lambda(\omega) = 0$.
- Let $z = \omega\sqrt{\lambda}$, and $a = \frac{1}{\lambda^{2^{k-1}+1/2}}$. Then $L_\lambda(\omega) = 0$ if and only if

$$h_a(z) = a^{2^k} z^{2^{2k}} + z^{2^k} + az + 1 = 0.$$

Proof Sketch (Cont.)

The proof can be divided into **two cases**.

Case 1: $a \neq \beta^{2^k+1} + \beta$ for any $\beta \in \mathbb{F}_{2^n}$.

- $h_a(z) = 0$ has precisely one solution $z_0 = R_{k,k'}(1/a)$, where $R_{k,k'}(\cdot)$ is Hans Dobbertin's polynomial. Then $L_\lambda(\omega) = 0$ has precisely one solution $\omega_0 = z_0/\sqrt{\lambda}$.
- We have $Tr(z_0) = 1$ because $x^{2^k+1} + x + a = 0$ has no solution in $\mathbb{F}_{2^n}$.
- According to Hans Dobbertin's result,

$$\omega_0^{2^k+1} = (z_0/\sqrt{\lambda})^{2^k+1} = az_0^{2^k+1} = \sum_{i=1}^{k'} z_0^{2^{ik}} + k' + 1,$$

Proof Sketch (Cont.)

- Thus

$$Tr(\omega_0^{2^k+1}) = Tr\left(\sum_{i=1}^{k'} z_0^{2^{ik}}\right) + k' + 1 = k' \cdot Tr(z_0) + k' + 1 = 1.$$

- It follows that

$$\sum_{\omega : L_\lambda(\omega)=0} (-1)^{Tr(\omega^{2^k+1})} = (-1)^{Tr(\omega_0^{2^k+1})} = -1.$$

Proof Sketch (Cont.)

Case 2: $a = \beta^{2^k+1} + \beta$ for some $\beta \in \mathbb{F}_{2^n}$.

- Set $Q(z) = az^{2^k} + \beta^2 z + \beta$, $\Gamma = \beta^{2^k-1} + 1/\beta$, and $\Delta = \Gamma^{-\frac{1}{2^k-1}}$. Then we have

$$h_a(z) = Q(z)^{2^k} + \Gamma Q(z) = Q(z)(Q(z)^{2^k-1} + \Delta^{-(2^k-1)}).$$

- $h_a(z) = 0$ if and only if $Q(z) = 0$ or $Q(z) + 1/\Delta = 0$.
- We can show that
  - $Q(z) = 0$ has **none or precisely two** solutions, and
  - $Q(z) + 1/\Delta = 0$ has **precisely two** solutions.

Proof Sketch (Cont.)

- If $h_a(z) = 0$ has **four solutions**, then we can show that

$$\begin{aligned}
&\sum_{\omega : L_\lambda(\omega)=0} (-1)^{Tr(\omega^{2^k+1})} \\
&= (-1)^{Tr(\omega_0^{2^k+1})} + (-1)^{Tr(\omega_1^{2^k+1})} + (-1)^{Tr(\omega_2^{2^k+1})} + (-1)^{Tr(\omega_3^{2^k+1})} \\
&= 2.
\end{aligned}$$

- If $h_a(z) = 0$ has **two solutions**, then we show that

$$\sum_{\omega : L_\lambda(\omega)=0} (-1)^{Tr(\omega^{2^k+1})} = (-1)^{Tr(\omega_0^{2^k+1})} + (-1)^{Tr(\omega_1^{2^k+1})} = 0.$$

Element Distribution

Using the following lemma, we can obtain the element distribution of $\mathbf{s}(v, t)$.

Property.

Let $f(x) = h(x) = Tr(x)$, and two integers $0 < v, t < 2^n - 1$ satisfy $\gcd(vt, q-1) = 1$. Then we have

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \widehat{f}(v,t)(\lambda) = 0$$

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \widehat{f}(v,t)(\lambda)^2 = 2^{3n}.$$

New Quaternary Sequences with 2-Level Autocorrelation

- **Construction:** Let n **be an integer**, and $1 \leq k < n$ with $\gcd(k,n) = d$ and n/d **is odd**. Let $f(x) = h(x) = Tr(x)$, $v = 2^{n-1} - 1$, and $t = 2^k + 1$. Then $\mathbf{s}(v,t)$ has ideal two-level autocorrelation, and the s_i's take at most **four distinct values** $-1, 0, 1,$ **or** 2^d.

- **Distribution:**

Element	Frequency
-1	$\frac{2^{(m+1)d}+2^d}{2(2^d+1)}$
0	$2^{(m-1)d} - 1$
1	$\frac{(2^d-2)(2^{md}-1)}{2(2^d-1)}$
2^d	$\frac{2^{(m-1)d}-1}{2^{2d}-1}$

Some Remarks on Sequences of 2nd Order DHT

SIMILARITIES TO THE BINARY CASE

(v, t)	$\widehat{Tr}(v,t)(\lambda)/2^n$	**Conditions**	**Comments**
$(3, 2^k+1)$	$\{-1, 1\}$	$\gcd(k, n) = 1$	Dillon-Dobbertin, 2004
$(-1, 2^k+1)$	$\{-1, 0, 2\}$	$\gcd(k, n) = 1$	Hu-Gong, 2009
$(-1, 2^k+1)$	$\{-1, 0, 1, 2^d\}$	$\gcd(k, n) = d$ n/d odd	Hu-Gong, 2009

Note that $2^{n-1} - 1$ and -1 are in the same coset modulo $2^n - 1$.

New Hadamard Matrices with Entries $-1, 0, 2$

- **The new ternary sequences** yield new Hadamard matrixes with entries $\{-1, 0, 2\}$.
- Using the standard construction from binary 2-level autocorrelation sequences to Hadamard matrices, let

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & s_0 & s_1 & \cdots & s_{q-3} & s_{q-2} \\ 1 & s_1 & s_2 & \cdots & s_{q-2} & s_0 \\ \vdots & & & & & \\ 1 & s_{q-2} & s_0 & \cdots & s_{q-4} & s_{q-3} \end{pmatrix}$$

  Then

$$AA^T = I$$

  where A^T is the transpose of A and I is the identity matrix of q by q ($q = 2^n$).
- **Similarly**, we have new $2^n \times 2^n$ **Hadamard matrixes with entries** $\{-1, 0, 1, 2\}$.

Example

- $n = 5$, $v = 15$, $t = 3$, and

$$
\begin{aligned}
s &= s(15,3) \\
&= \begin{matrix} -1 & 0 & 0 & 2 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 & -1 & -1 & 0 & 2 & 0 & -1 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 & -1 & -1 \\ -1 \end{matrix}
\end{aligned}
$$

- Let L be the left (cyclic) shift operator, and

$$
A = \begin{bmatrix} 1 & 1 \cdots 1 \\ 1 & s \\ 1 & Ls \\ \vdots & \\ 1 & L^{30}s \end{bmatrix} \Longrightarrow AA^T = I_{32}
$$

Reference

- H.G. Hu and G. Gong, New Ternary and Quaternary Sequences with Two-Level Autocorrelation, *the Proceedings of International Symposium of Information Theory (ISIT) 2010*, Austin Texas, June 13-18. Technical Report, CACR 2009-16, 2009, University of Waterloo, Canada.

Open Problems

- How to prove the other **ternary or quaternary** sequences with two-level autocorrelation from the second order DHT of **binary sequences** (shown by experiments)?
- Are **all the binary 2-level** autocorrelation sequences from the second order DHT of binary sequences (at least the experimental results confirm it)?
- How to prove **conjectured ternary** 2-level autocorrelation sequences from the second order DHT of ternary sequences?
- How to determine **analogue classes of p-ary** 2-level autocorrelation sequences for $p > 3$?