New Families of Ideal 2-level Autocorrelation Ternary Sequences From Second Order DHT

Michael Ludkovski and Guang Gong

Department of Electrical and Computer Engineering University of Waterloo
Waterloo, ON N2L 3G1, Canada

Abstract

Following the work of Gong and Golomb on binary sequences, we used the technique of applying Second Order Decimation–Hadamard Transform (DHT) operator to obtain previously unknown ternary (ideal) two-level autocorrelation sequences. This process is referred to as realization. We obtained new multi-term ternary two-level autocorrelation sequences as realization of single 2-term ternary two-level autocorrelation sequence. We conjecture that for \( n = 2m + 1 \) odd, there exist \( m \) or \( m - 1 \) infinite inequivalent families of ternary two-level autocorrelation (AC) sequences which are given by four constructions. We have verified this for \( n = 5, 7, 9 \) and 11. Experimental results are provided.

Key words: 2-level autocorrelation, ternary sequences, Decimation–Hadamard transform, 2-term sequences, cyclic Hadamard difference sets

1 Introduction

Ideal 2-level autocorrelation is one of the principal randomness criteria for periodic sequences. Pseudorandom sequences with good autocorrelation properties have important applications in cryptology and communications.

In the last three years great progress has been made in finding new families of binary 2-level autocorrelation sequences. It is now conjectured [6] that all infinite families of binary 2-level autocorrelation sequences of period \( 2^n - 1 \) having no subfield factorization have been discovered for odd \( n \). As opposed to the binary case, the situation for \( p > 2 \) is largely unknown. Beside the

Email address: ggong@shannon1.uwaterloo.ca (and Guang Gong).
1 Supported by NSERC summer URA grant

Preprint submitted to Elsevier Preprint 4 April 2001
Singer and GMW constructions (or generalized GMW constructions), little else is known about \( p \)-ary two-level autocorrelation sequences. Recently, a few steps have been taken in this direction with investigations into \( p = 3 \), the ternary case. Helleseth et. al. [7] have found one family of 2-term ternary two-level autocorrelation sequences and Lin, in his Ph.D. dissertation [9], has conjectured there is another family of 2-term ternary two-level autocorrelation sequences.

Gong and Golomb found that the Hadamard transform of three-term sequences is determined by one of the \( m \)-sequences [5] (a three term sequence \( \{a_k\} \) is defined by \( a_k = \text{Tr}(\alpha^k + \alpha^{rk} + \alpha^{r^2k}), k = 0, 1, \cdots, r = \frac{2^{(n-1)/2}}{2} + 1 \). It has recently been shown by Dillon and Dobbertin [1] that when \( n \) is odd, all the newly discovered classes of two-level autocorrelation sequences of period \( 2^n - 1 \) have the same Hadamard transform as one of the \( m \)-sequences. Based on this observation, recently, Gong and Golomb developed a new method to study and search for 2-level autocorrelation sequences over a finite field \( GF(p) \) where \( p \) is a prime, which is called by them \( (\text{iterative}) \) decimation-Hadamard transform [6] (the abstract of this work appeared in [4]).

In this paper we followed this recent work of Gong and Golomb [6] by using the second order Decimation-Hadamard Transform (DHT) operator to look for multi-term ternary two-level autocorrelation sequences. Initially, we used \( m \)-sequences for our base, analogous to the binary situation which then gives all the interesting realizations. As it turned out, this attempt wasn’t successful as ternary \( m \)-sequences appear to form a closed equivalence class under DHT (i.e. only \( m \)-sequences could be realized). However, we had success applying the DHT operator to 2-term ternary two-level autocorrelation sequences, obtaining several new multi-term ternary two-level autocorrelation sequences with number of terms from 4 to 89. These latter sequences are computationally infeasible to find if we attempt exhaustive search. Based on our experimental results, we conjecture that for \( n = 2m + 1 \) odd there exist \( m \) or \( m - 1 \) infinite inequivalent families of ternary two-level autocorrelation sequences which are given by four constructions. We have verified this for \( n = 5, 7, 9 \) and 11. All such new ternary two-level autocorrelation sequences are in one-to-one correspondence with cyclic Hadamard difference sets with parameters \( (\frac{3^n-1}{2}, \frac{3^n-1}{2}, \frac{3^n-5}{2}, \frac{3^n-1}{2}) \).

In the first part of this paper, we give a brief theoretical background on two-level autocorrelation sequences along with the definition of the DHT operator and the concepts of realizable pairs and realized sequences. In the second part of the paper (Sections 3 and 4), we present our conjectures followed by a summary of experimental results.
2.1 Preliminaries

Let

- $\mathbb{F} = GF(p)$, $\mathbb{K} = GF(p^n)$, $q = p^n$ power of a prime.
- $\alpha$ a primitive element of $\mathbb{K}$.
- $\omega = e^{2\pi i/p}$ complex primitive $p$-th root of unity.
- $\chi(x) = \omega^x$ the canonical additive character [8] on $\mathbb{F}$.
- $Tr_{m}^{n}(x)$ is the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ where $n = l \cdot m$.

$$Tr_{m}^{n}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{l-1}}, \quad x \in \mathbb{K}.$$ 

We simply write $Tr(x)$ if the context is clear.

- $\Gamma_{q-1}$, the set of cyclotomic coset leaders modulo $p^n - 1$.

Any periodic sequence $\mathbf{a} = \{a_i\}$ over $\mathbb{F}$ with period $v | p^n - 1$ has trace representation. Computationally, to obtain the trace representation of a given $\mathbf{a}$ we use the Discrete Fourier Transform [3]

$$a_i = \frac{1}{q - 1} \sum_{k \in \Gamma_{q-1}} Tr_{m}^{n}(A_k \alpha^{ki})$$

(1)

where $n_k = |C_k|$, and $A_k$ are the discrete Fourier coefficients of $\mathbf{a}$: $A_k = \sum_{i=0}^{q-2} a_i \alpha^{-ki}$. If $r = |\{k \in \Gamma_{q-1}|A_k \neq 0\}|$, then we say that that $\mathbf{a}$ is a $r$-term sequence.

The autocorrelation of a sequence $\mathbf{a}$ is defined by

$$C(\tau) = \sum_{i=0}^{t-1} \chi(a_{i+\tau}) \overline{\chi(a_i)}.$$ 

(2)

where $\tau$ is a phase shift of the sequence $\{a_i\}$ and the indexes are computed modulo $t$, the period of $\mathbf{a}$.

If $t = p^n - 1$ and

$$C_{\mathbf{a}}(\tau) = \begin{cases} 
-1 & \text{if } \tau \neq 0 \mod q - 1 \\
q - 1 & \text{if } \tau \equiv 0 \mod q - 1 
\end{cases}$$

(recall $q = p^n$) then we say that the sequence $\mathbf{a}$ has (ideal) 2-level autocorrelation, or it is an $AC$ sequence for short.
The Decimation-Hadamard Transform is a generalization of usual Hadamard transform where we first decimate \( f \) by \( v \).

**Definition 1** For \( f(x) : \mathbb{K} \to \mathbb{F} \), and an integer \( v \in \Gamma_{q-1} \) define

\[
\hat{f}(\lambda) = \sum_{x \in \mathbb{K}} \chi(Tr(\lambda x))\overline{\chi(f(x^v))}, \quad \lambda \in \mathbb{K}.
\]  

(3)

\( \hat{f}(\lambda) \) is called the first-order decimation-Hadamard transform (DHT) of \( f(x) \) with respect to \( Tr(x) \), the first order DHT for short.

Observe that \( \hat{f}(\lambda) \) is essentially an inner product of \( F(x^v) = \omega^{f(x^v)} \) with a dilation by \( \lambda \) of the trace function. The range of \( \hat{f} \) is in general \( \mathbb{C} \), but in our case it is easy to establish

**Lemma 2** If \( f(-x) = -f(x) \ \forall x \) and \( p = 3 \), then \( \hat{f}(\lambda) \in \mathbb{Z} \) for all \( v, \lambda \).

2.3 Second order DHT

The motivation for the second iteration stems from the inverse formula for Hadamard transform (compare with the classic Fourier expansion):

\[
\omega^{f(\lambda)} = \frac{1}{q} \sum_{x \in \mathbb{K}} \chi(Tr(\lambda x))\overline{\chi(f(x))}, \quad \lambda \in \mathbb{K}
\]  

(4)

Accordingly, with notation as above we define

**Definition 3**

\[
\hat{f}(v,t)(\lambda) = \sum_{y \in \mathbb{K}} \chi(Tr(\lambda y))\overline{\chi(f(v^t y^{\lambda}))), \quad t \in \Gamma_{q-1}, \lambda \in \mathbb{K}
\]  

(5)

\( \hat{f}(v,t)(\lambda) \) is called the second-order decimation-Hadamard transform of \( f(x) \) with respect to \( Tr(x) \), the second-order DHT for short.

Note that for \( p = 3 \), \( \hat{f}(v,t)(\lambda) \) is in \( \mathbb{Z}[\omega] \). From the definitions the following result is immediate

**Lemma 4**

\[
\hat{f}(v,t)(\lambda) = \sum_{x,y \in \mathbb{K}} \omega^{Tr(\lambda y^x) + Tr(y^x) - f(x^v)}. 
\]  

(6)
Remark 5 If \( t = 1 \), then the second order DHT reduces to the inverse Hadamard transform of \( f(x^n) \).

2.4 Realizable pairs

Motivated by the formula for inverse Hadamard transform (4), we are interested in pairs \((v,t)\), such that \( \hat{f}(v,t)(\lambda) \) is a character evaluation of another function.

Definition 6 Let \( \Omega = \{1, \omega, \ldots, \omega^{n-1}\} = \langle \omega \rangle \). If \( \hat{f}(v,t)(\lambda) \in q \cdot \Omega \) for all \( \lambda \), then we call \((v,t)\) a realizable pair and call \( g \) given by

\[
\omega^q(\lambda) = \frac{1}{q} \hat{f}(v,t)(\lambda)
\]

the realization of \( \hat{f}(v,t)(\lambda) \).

The following theorem is proven in [6]

Theorem 7 With the above notation, let \( a_i = f(\alpha^i) \) and \( b_i = g(\alpha^i) \) where \( \alpha \) is a primitive element of \( GF(p^n) \), \( i = 0, 1, \ldots \). Then \( p \)-ary sequence \( \{b_i\} \) has 2-level autocorrelation if and only if \( \{a_i\} \) does.

We wish to have the realization \( g \) to be an entirely new AC sequence, so that the second order DHT gives us a method to generate new sequences.

3 Obtained Realizations

At first, we used the \( m \)-sequence \( \{a_i\} \) where \( a_i = Tr(\alpha^i) \) for our base function \( f \) in the second-order DHT. Unfortunately, only \( m \)-sequences were obtained as realizations. However we had success applying the second-order DHT on 2-term sequence \( \{a_i\} \) where \( a_i = Tr(\alpha^i + \alpha^{id}) \). The experimental results listed in Section 4 suggested the following conjecture.

Let \( n = 2m + 1 \). In his PhD thesis Lin [9] conjectured that the 2-term sequence defined by \( f(x) = Tr(x + x^d) \) where \( d = 2 \cdot 3^m + 1 \) is AC in \( GF(3^n) \) (we verified that \( f(x) \) is AC for all \( n \leq 15 \)). It turns out that this is the most interesting case for applying the second order DHT on ternary sequences.

Conjecture. Let \( n = 2m + 1 \) and \( f(x) = Tr(x + x^d) \) where \( d = 2 \cdot 3^m + 1 \). Then \((1,t)\) is a realizable pair of \( f(x) \) where both \( t \) and the realization \( g(\lambda) \) of \( \hat{f}(1,t)(\lambda) \) are given by the following four constructions where \( g(x) \neq f(x^r) \).
for any \( c \in \Gamma_{q-1} \) with \((c, q - 1) = 1\). In other words, the realization \( g(x) \) of 
\( \hat{f}(1, t)(\lambda) \) produces new ternary AC sequences.

Moreover, all such newly obtained ternary AC sequences are in one-to-one correspondence with cyclic Hadamard difference sets with parameters \((\frac{3^n - 1}{2}, \frac{3^n - 1}{2}, \frac{3^n - 1}{2})\).

This Conjecture has been verified for \( n = 5, 7, 9, \) and \(11\).

**Construction A** Let \( v = \frac{3^n - 1}{2} \) and \( u = \frac{3^m - 1}{2} \). Then we have the following construction

\[
t = \begin{cases} 
v + u & \text{if } n \equiv 1 \mod 4 \\
u & \text{if } n \equiv 3 \mod 4
\end{cases}
\]

The ternary sequence obtained by this realization is a \((m + 1)\)-term AC sequence, whose trace representation \( H_n(x) = Tr(\sum_{j=1}^{m+1} b_j x^j) \) is defined through

\[
b_j = (-1)^j, \quad j = 1, 2, \ldots, m \quad \text{with} \quad b_{m+1} = (-1)^{m+1},
\]

and \( c_j \) are recursively given by

\[
c_1 = 1, \quad c_{j+1} = c_j + 2 \cdot 3^{2j-1}, \quad j = 1, \ldots, m.
\]

This construction has also been verified probabilistically for \( n = 13 \) and \(15 \) (computing several thousand random autocorrelation values).

**Construction B** We also have a conjectured infinite family of 5-term sequences for \( n \) odd. The construction is:

\[
t = 3^m \left( \frac{3^r - 1}{2} \right) - \frac{3^{r-1} - 1}{2} \quad \text{where } n = 4r \pm 1.
\]

The realization gives a 5-term sequence, whose trace representation for \( n = 4r + 1 \) is defined by \( J_n(x) = Tr(-x^{c_1,r} - x^{c_2,r} - x^{c_3,r} + x^{c_4,r} + x^{c_5,r}) \) where

\[
c_{1,r} = 1 \quad c_{3,r} = 3^{r+1} + 2 \\
c_{2,r} = 2 \cdot 3^r + 1 \quad c_{4,r} = 3^{2r+1} + 3^{r+1} + 1^{*} \\
c_{5,r} = 2 \cdot 3^{3r} + 3^{2r} + 3^r + 1
\]

For the case of \( n = 4r - 1 \), we do not know the correct form for \( c_{i,r} \).

* There is a “swinging” anomaly for \( r = 1 \): \( c_{4,1} = 3^{2,1+1} + 3^1 + 1. \)
Construction C We have
\[ t = \frac{3^{2m} + 1}{2} - 2 \cdot 3^{m-1}. \]

Let the sequence given by this realization have \( s_m \) terms. Then \( s_m \) is recursively defined by \( s_{m+1} = 3 \cdot s_m - s_{m-1} \), with \( s_0 = 1, \ s_1 = 2 \).

*Note.* The actual values of \( s_m \), which are 1, 2, 5, 13, 34, 89, correspond to the even Fibonacci numbers \( F_{2m} \). This resembles the hyper-oval construction for binary sequences, however at this point we do not know an appropriate generalization to \( p = 3 \).

Construction D In general, the second component \( t = t_k \) of the realizable pairs \((1, t)\) can be explained by
\[ t_k = 3^m \left( \frac{3^{k+1} - 1}{2} \right) - \frac{3^k - 1}{2} \quad (8) \]

where either \( 1 \leq k \leq m - 1 \) if \( n \not\equiv 0 \mod 3 \) or \( 2 \leq k \leq m - 1 \) if \( n \equiv 0 \mod 3 \). This construction includes Construction B for \( k = 1 \) or \( 2 \) depending on the value of \( n \), and Construction C for \( k = m - 1 \).

**Remark 8** The first order DHT \( \hat{f}(v)(\lambda) \) of \( f(x) \) for \( v = 1 \) is 3-valued, as proven by Helleseth et al. [2]

Last we make a remark on Construction D.

**Remark 9** The ternary AC sequences obtained from the realizable pair \((1, t_k)\) where \( t_k \) is defined by Construction D are analogous to the binary AC sequences obtained from the realizable pairs \((3, \frac{2k+1}{3})\) where \((k, n) = 1\). The realizable pairs \((3, \frac{2k+1}{3})\) give Dobbertin’s Kasami power–function construction sequences [6,1]. Here the 2-term ternary sequences play the same role in the second-order DHT over \( GF(3) \), as the binary m-sequences in the second-order DHT over \( GF(2) \). More precisely, let \( n = 2m + 1 \).

1. For \( p = 2 \) and \( f(x) = Tr(x) \), the function \( g(x) \) defined by
\[ \omega^{g(\lambda)} = \frac{1}{q} \hat{f}(3, \frac{2k+1}{3})(\lambda) \quad (9) \]
gives Dobbertin’s Kasami power–function construction sequences where \( 1 \leq k < m \) and \((k, n) = 1\). If \( k = 2 \), (9) gives the same class as the Segre hyper-oval construction [10].
(2) For $p = 3$ and $f(x) = Tr(x + x^d)$ where $d = 2 \cdot 3^m + 1$, the function defined by

$$\omega^g(\lambda) = \frac{1}{q} \hat{f}(1, t_k)(\lambda)$$

(10)

gives $m - 1$ or $m - 2$ classes of ternary AC sequences where $t_k$ is defined by (8). This has been verified for $n = 5, 7, 9, \text{ and } 11$. For $k = m - 1$, it also has the special form as Construction C. Due to this resemblance, we consider the sequences from Construction C as the Segre hyper-oval sequences over $GF(3)$.

4 Experimental Results

In the following tables, we list all the non-equivalent realizations of 2-term sequences for $n = 5, 7, 9, \text{ and } 11$. All such sequences are new ternary AC sequences which are in one-to-one correspondence with cyclic Hadamard difference sets with parameters $(\frac{3^n-1}{2}, \frac{3^n-1}{2}, \frac{3^n-2-1}{2})$. In each table, the first column lists the realizable pairs $(v, t)$, the second column the number of terms in the realization, the third column the classification according to the conjectures above (for conjecture D, the subscript gives the corresponding value of $k$), and the last column the spectrum obtained using DFT, i.e., the pair $(k; A_k)$ defined in (1). For example, the second row of Table 2 means that if we start with $f(x) = Tr(x + x^{55})$, i.e., 2-term AC sequence, then we get the realizable pair $(1, t) = (1, 107)$. This pair gives the realization $g(x) = Tr(2x + 2x^7 + 2x^{11} + x^{37} + x^{277})$ which is a ternary 5-term AC sequence. This realization can be explained by conjectures B and D (with $k = 1$). We also list the primitive polynomial $h(x)$ of degree $n$ over $GF(3)$ which defines each finite field.

Fig. 1. $n = 5$, $f(x) = Tr(x + x^{19})$, and $h(x) = x^5 + 2x + 1$

<table>
<thead>
<tr>
<th>(1, 125)</th>
<th>3-terms</th>
<th>A</th>
<th>(1, 1) (7, 2) (61, 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, 35)</td>
<td>5-terms</td>
<td>B, C, D_1</td>
<td>(1, 2) (7, 2) (11, 2) (31, 1) (67, 1)</td>
</tr>
</tbody>
</table>

References

Fig. 2. $n = 7$, $f(x) = \text{Tr}(x + x^{55})$, and $h(x) = x^7 + 2x^2 + 1$

| $(1, 13)$ | 4-terms | A | $(1, 1)$ (7, 2) (61, 1) (547, 1) |
| $(1, 107)$ | 5-terms | B, D$^1$ | $(1, 2)$ (7, 2) (11, 2) (37, 1) (277, 1) |
| $(1, 347)$ | 13-terms | C, D$^2$ | $(1, 1)$ (7, 1) (11, 1) (31, 2) (37, 2) (55, 1) (67, 2) (91, 2) (103, 2) (115, 2) (119, 2) (283, 1) (607, 1) |

Fig. 3. $n = 9$, $f(x) = \text{Tr}(x + x^{163})$, and $h(x) = x^9 + 2x^6 + 2x^3 + x + 1$

| $(1, 9881)$ | 5-terms | A | $(1, 1)$ (7, 2) (61, 1) (547, 2) (4921, 2) |
| $(1, 1049)$ | 5-terms | B, D$^2$ | $(1, 2)$ (19, 2) (29, 2) (271, 1) (1549, 1) |
| $(1, 3227)$ | 13-terms | C, D$^3$ | $(1, 1)$ (7, 2) (11, 2) (31, 1) (37, 1) (55, 2) (67, 1) (83, 2) (91, 1) (103, 1) (115, 1) (119, 1) (247, 1) (253, 1) (271, 1) (283, 2) (361, 2) (499, 1) (571, 1) (593, 1) (607, 2) (763, 1) (767, 1) (823, 2) (895, 1) (931, 2) (1003, 2) (1039, 2) (1063, 2) (1075, 2) (1087, 2) (1091, 2) (2551, 1) (5467, 1) |


Fig. 4. $n = 11$, $f(x) = Tr(x + x^{487})$, and $h(x) = x^{11} + 2x^{10} + x^9 + x^8 + 2x^2 + 2x + 1$.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(1, 121) 6-terms</th>
<th>A</th>
<th>(1, 1) (7, 2) (61, 1) (547, 2) (4921, 1) (44287, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, 3155) 5-terms</td>
<td>B, D_2</td>
<td>(1, 2) (19, 2) (29, 2) (271, 1) (6823, 1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1, 9707) 13-terms</td>
<td>D_3</td>
<td>(1, 1) (7, 1) (11, 1) (37, 2) (247, 2) (277, 2) (307, 2) (487, 1) (577, 2) (811, 2) (821, 2) (3007, 1) (22147, 1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1, 971) 34-terms</td>
<td>D_1</td>
<td>(1, 2) (7, 2) (11, 2) (37, 1) (85, 1) (163, 2) (245, 2) (271, 1) (733, 1) (739, 1) (811, 1) (1471, 1) (1549, 1) (1705, 1) (1783, 1) (2221, 1) (2225, 1) (2287, 1) (2299, 2) (2377, 1) (2443, 2) (2459, 1) (2521, 2) (2677, 1) (3001, 2) (7375, 2) (8113, 2) (8347, 2) (8863, 2) (9085, 1) (9565, 2) (16129, 2) (22151, 2) (28039, 1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1, 29363) 89-terms</td>
<td>C, D_4</td>
<td>(1, 1) (7, 1) (11, 1) (31, 2) (37, 2) (55, 1) (67, 2) (83, 1) (91, 2) (103, 2) (115, 2) (119, 2) (247, 2) (253, 2) (271, 2) (283, 1) (325, 2) (361, 1) (487, 1) (499, 2) (571, 2) (595, 2) (607, 1) (739, 2) (751, 2) (763, 2) (767, 2) (811, 2) (823, 1) (895, 2) (919, 2) (931, 1) (979, 2) (983, 2) (1003, 1) (1027, 2) (1039, 1) (1055, 2) (1063, 1) (1075, 1) (1087, 1) (1091, 1) (2215, 2) (2227, 1) (2305, 1) (2443, 1) (2515, 1) (2539, 1) (2551, 2) (2953, 1) (3169, 1) (3277, 2) (4459, 2) (4483, 2) (4495, 1) (5131, 2) (5143, 1) (5359, 1) (5431, 1) (5455, 1) (5467, 2) (6815, 2) (6835, 1) (6871, 1) (6895, 1) (6907, 1) (6919, 1) (6923, 1) (7375, 1) (7411, 2) (8059, 1) (8275, 1) (8347, 1) (8383, 2) (8863, 1) (8867, 1) (9031, 2) (9247, 1) (9355, 2) (9571, 2) (9679, 2) (9751, 2) (9787, 2) (9811, 2) (9823, 2) (9835, 2) (9839, 2) (22963, 1) (49207, 1)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>