New Ternary and Quaternary Sequences with Two-Level Autocorrelation

Honggang Hu
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
Email. h7hu@uwaterloo.ca

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
Email. ggong@calliope.uwaterloo.ca

Abstract

Pseudorandom sequences with good correlation properties are widely used in communications and cryptography. The search of new sequences with two-level autocorrelation has been a very interesting problem for decades. In 2002, Gong and Golomb proposed the iterative decimation-Hadamard transform (DHT) which is an useful tool to study two-level autocorrelation sequences. They showed that for all odd $n \leq 17$, using the second-order decimation-Hadamard transform, and starting with a single binary m-sequence, all known two-level autocorrelation sequences of period $2^n - 1$ which have no subfield factorization can be obtained. In this paper, we find many new ternary or quaternary sequences with two-level autocorrelation using the second-order decimation-Hadamard transform. The period of such sequences is $2^n - 1$.

Index Terms. Pseudorandom sequence, ternary sequence, quaternary sequence, two-level autocorrelation, iterative decimation-Hadamard transform (DHT), Dobbertin's polynomial.

1 Introduction

Pseudorandom sequences with good correlation properties have been widely used in modern communication systems and cryptography, such as radar, global positioning systems, CDMA communication systems, and stream cipher cryptosystems [6, 7, 20]. The search for new sequences with two-level autocorrelation has been an interesting research topic in application areas for some decades [7, 13, 14, 19].

In recent some years, significant progress has been made in finding new sequences with two-level autocorrelation. Several new classes of sequences with two-level autocorrelation have been discovered

which are summarized in [7] or in the literature [2, 3, 10, 11, 14, 17, 18, 19]. In 2002, motivated by the idea of Dillon and Dobbertin in [2, 3], Gong and Golomb proposed the iterative decimation-Hadamard transform (DHT) [9]. For search of new sequences with two-level autocorrelation, they showed that for all odd $n \leq 17$, using the second-order DHT (which will be defined later), and starting with a single binary m-sequence, all the known binary two-level autocorrelation sequences of period 2^n-1 which have no subfield factorization can be obtained. They also conjectured that all families of cyclic Hadamard difference sets of period $2^n - 1$ having no subfield factorization are now known, at least for odd n. Yu and Gong generalized the second-order DHT to two-level autocorrelation sequences with subfield factorization (i.e., generalized GMW sequences) [21], and to the case of n even which is referred to as the multiplexing DHT. They showed that experimentally satrting with a single m-sequence with period $2^n - 1$, n even and $n \leq 16$, all known binary two-level autocorrelation sequences can be realized by the second-order multiplexing DHT. Thus, using the second-order DHT, any known binary two-level autocorrelation sequence can be realized by either the DHT or the multiplexing DHT. However, there is no binary two-level autocorrelation sequence which has been foung by this method. In [16], applying the second-order DHT to ternary sequences over $\mathbb{F}_3$ with period $3^n - 1$, some new classes of ternary sequences of period $3^n - 1$ with two-level autocorrelation have been found experimentally. However, their proof has not been appeared in the literature yet.

In this paper, we revisit the second-order DHT of m-sequences. We observe that if we allow the sequence element could be taken from an enlarged alphabetic set, then under certain conditions, the second-order DHT of m-sequences of period 2^n-1 produces new sequences with two-level autocorrelation whose elements are from the rational field. In some cases, we prove that these sequences are ternary or quaternary using Dobbertin's method. Based on such sequences, new Hadamard matrixes with entries in $\{-1, 0, 2\}$ or $\{-1, 0, 1, 2^d\}$ can be constructed, where d will be defined later.

This paper is organized as follows. In Section 2, we provide some notation and background which will be used. In Section 3, the new construction is given. In Section 4, we present new ternary and quaternary sequences with two-level autocorrelation of period $2^n - 1$. Finally, Section 5 concludes this paper.

2 Preliminaries

2.1 Two-Level Sequence

Let $\mathbf{s} = \{s_i\}$ be a complex-valued sequences with period N. Then the autocorrelation $C_{\mathbf{s}}(\tau)$ of $\mathbf{s}$ at shift τ is defined by

$$C_{\mathbf{s}}(\tau) = \sum_{i=0}^{N-1} s_{i+\tau}\overline{s_i},\ 0 \leq \tau < N,$$

where $\overline{s_i}$ is the complex conjugate of s_i.

Definition 1 ([7]) *A sequence* $\mathbf{s} = \{s_i\}$ *with period* N *is called a two-level sequence if* $C_{\mathbf{s}}(\tau) = -1$ *for any* $0 < \tau < N$.

2.2 The Decimation-Hadamard Transform

Let $\mathbb{F}_q$ denote the finite field of order q, where q is the power of a prime number p, and $Tr(\cdot)$ denote the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. Let $\omega = e^{2\pi i/p}$, a complex primitive pth root of unity. The canonical additive character χ of $\mathbb{F}_p$ is defined by [15]

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

Definition 2 *Let* $h(x)$ *be a function from* $\mathbb{F}_q$ *to* $\mathbb{F}_p$ *with* $h(0) = 0$. $h(x)$ *is called orthogonal if and only if*

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

Let $f(x)$ be a polynomial from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then the Hadamard transform of $f(x)$ is defined by

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

and the inverse transform is given by

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

Definition 3 ([9]) *Let* $h(x)$ *be orthogonal over* $\mathbb{F}_q$, *and* $f(x)$ *be a polynomial from* $\mathbb{F}_q$ *to* $\mathbb{F}_p$. *For any integer* $0 < v < q - 1$, *we define*

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

$\widehat{f_h}(v)(\lambda)$ *is called the first-order decimation-Hadamard transform (DHT) of* $f(x)$ *with respect to* $h(x)$, *and we call it the first-order DHT for short.*

Remark 1 *If* $h(x) = Tr(x)$, *and* $v = 1$, *then* $\widehat{f_h}(v)(\lambda)$ *is just the Hadamard transform of* $f(x)$. *If* $h(x) = Tr(x^s)$ *with* $\gcd(s, q-1) = 1$, *then* $\widehat{f_h}(v)(\lambda)$ *is the extended Hadamard transform introduced in [8] for the analysis of the Data Encryption Standard (DES).*

Definition 4 ([9]) *With the notation as above, for any integer $0 < t < q-1$, we define*

$$\widehat{f_h}(v,t)(\lambda) = \sum_{y \in \mathbb{F}_q} \chi(h(\lambda y))\overline{\widehat{f_h}(v)(y^t)}, \lambda \in \mathbb{F}_q.$$

$\widehat{f_h}(v,t)(\lambda)$ is called the second-order decimation-Hadamard transform (DHT) of $f(x)$ with respect to $h(x)$, and we call it the second-order DHT for short.

Remark 2 *If $h(x) = Tr(x)$, and $t = 1$, then $\widehat{f_h}(v,t)(\lambda)/q$ is just the inverse Hadamard transform of $f(x^v)$.*

Henceforth we take $h(x) = Tr(x)$. For simplicity, we denote $\widehat{f_h}(v)(\lambda)$ and $\widehat{f_h}(v,t)(\lambda)$ by $\widehat{f}(v)(\lambda)$ and $\widehat{f}(v,t)(\lambda)$ respectively.

2.3 Dobbertin's Polynomial

Let n be an integer, and $1 \leq k < n$ with $\gcd(k,n) = 1$. Let $1 \leq k^{'} < n$ be the multiplicative inverse of k modulo n, i.e., $k^{'}k \equiv 1 \bmod n$. We introduce the following sequences of polynomials over $\mathbb{F}_{2^n}$:

$$\begin{aligned}
A_1(x) &= x, \\
A_2(x) &= x^{2^k+1}, \\
A_{i+2}(x) &= x^{2^{(i+1)k}} A_{i+1}(x) + x^{2^{(i+1)k}-2^{ik}} A_i(x), i \geq 1, \\
B_1(x) &= 0, \\
B_2(x) &= x^{2^k-1}, \\
B_{i+2}(x) &= x^{2^{(i+1)k}} B_{i+1}(x) + x^{2^{(i+1)k}-2^{ik}} B_i(x), i \geq 1.
\end{aligned}$$

They are used to define the polynomial

$$R_{k,k'}(x) = \sum_{i=1}^{k^{'}} A_i(x) + B_{k'}(x). \tag{1}$$

Note that the exponents occurring in A_j (resp. in B_j) are precisely those of the form

$$e = \sum_{i=0}^{j-1} (-1)^{\varepsilon_i} 2^{ik},$$

where $\varepsilon_i \in \{0,1\}$ satisfy $\varepsilon_{j-1} = 0, \varepsilon_0 = 0$ (resp. $\varepsilon_0 = 1$), $(\varepsilon_i, \varepsilon_{i-1}) \neq (1,1)$.

In [5], Dobbertin proved that the polynomial

$$S_{k,k'}(x) = \frac{\sum_{i=1}^{k'} x^{2^{ik}} + k' + 1}{x^{2^k+1}}$$

is a permutation polynomial over $\mathbb{F}_{2^n}^*$. (Strictly speaking, we obtain a polynomial $S_{k,k'}(x)$ if $1/x^{2^k+1}$ is replaced by $x^{2^n-1-(2^k+1)}$.) Moreover, for any $x \in \mathbb{F}_{2^n}^*$, he proved that

$$R_{k,k'}((S_{k,k'}(x))^{-1}) = x.$$

3 New Constructions

For any polynomial $f(x)$ from $\mathbb{F}_q$ to $\mathbb{F}_p$, and any integers $0 < v, t < q-1$, we define the sequence $\mathbf{s} = \{s_i\}$ by

$$s_i = \widehat{f}(v,t)(\alpha^i)/q, \ i = 0, 1, 2, ... \tag{2}$$

For the convenience of notation, we denote this sequence by $\mathbf{s}(v,t)$.

Theorem 1 *With the notation as above, let* $\mathbf{s}(v,t)$ *be defined by (2) with* $\gcd(vt, q-1) = 1$. *If the sequence* $\{\omega^{f(\alpha^i)}\}$ *given by* $f(x)$ *has two-level autocorrelation, then the autocorrelation function* $C_{\mathbf{s}(v,t)}(\tau)$ *of* $\mathbf{s}(v,t)$ *satisfies*

$$C_{\mathbf{s}(v,t)}(\tau) = \begin{cases} q-1, & \text{if } \tau \equiv 0 \ mod \ (q-1); \\ -1, & \text{otherwise.} \end{cases}$$

Proof. For any $\lambda \in \mathbb{F}_{2^n}$,

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

Thus, for any τ, we have

$$\begin{aligned} C_{\mathbf{s}(v,t)}(\tau) &= \sum_{i=0}^{q-2} s_{i+\tau} s_i^* \\ &= \sum_{i=0}^{q-2} \sum_{x_1, y_1 \in \mathbb{F}_q} \omega^{Tr(\alpha^{i+\tau} x_1) - Tr(x_1^t y_1) + f(y_1^v)} \sum_{x_2, y_2 \in \mathbb{F}_q} \omega^{-Tr(\alpha^i x_2) + Tr(x_2^t y_2) - f(y_2^v)} / q^2. \end{aligned}$$

Thus, we compute

$$\begin{aligned} q^2 \cdot C_{\mathbf{s}(v,t)}(\tau) &= (q-1) \sum_{\alpha^\tau x_1 = x_2, y_1, y_2 \in \mathbb{F}_q} \omega^{-Tr(x_1^t y_1) + f(y_1^v) + Tr(x_2^t y_2) - f(y_2^v)} \\ &\quad - \sum_{\alpha^\tau x_1 \neq x_2, y_1, y_2 \in \mathbb{F}_q} \omega^{-Tr(x_1^t y_1) + f(y_1^v) + Tr(x_2^t y_2) - f(y_2^v)} \\ &= q \sum_{x_1, y_1, y_2 \in \mathbb{F}_q} \omega^{-Tr(x_1^t y_1) + Tr(\alpha^{t\tau} x_1^t y_2) + f(y_1^v) - f(y_2^v)} \\ &\quad - \sum_{x_1, x_2, y_1, y_2 \in \mathbb{F}_q} \omega^{-Tr(x_1^t y_1) + f(y_1^v) + Tr(x_2^t y_2) - f(y_2^v)} \\ &= q^2 \sum_{y_1 \in \mathbb{F}_q} \omega^{f(y_1^v) - f(\alpha^{-tv\tau} y_1^v)} - q^2. \end{aligned}$$

If $\tau \not\equiv 0 \bmod (q-1)$, then $\sum_{y_1 \in \mathbb{F}_q} \omega^{f(y_1^v) - f(\alpha^{-tv\tau} y_1^v)} = 0$ since the sequence $\{\omega^{f(\alpha^i)}\}$ has two-level autocorrelation and $\gcd(vt, q-1) = 1$. Otherwise, $\sum_{y_1 \in \mathbb{F}_q} \omega^{f(y_1^v) - f(\alpha^{-tv\tau} y_1^v)} = q$. So the result follows. □

Remark 3 *If $p = 2$, then the elements of $\mathbf{s}(v,t)$ are from the rational field $\mathbb{Q}$. In some cases, they are from the integer ring $\mathbb{Z}$.*

4 The Case of New Ternary and Quaternary Sequences

In this section we consider the case of $p = 2$, $f(x) = Tr(x)$, $v = 2^{n-1} - 1$, and $t = 2^k + 1$. The following theorem is the main result.

Theorem 2 *Let n be an integer, and $1 \leq k < n$ with $\gcd(k, n) = d$ and n/d is odd. Let $f(x) = Tr(x)$, and $\mathbf{s}(v,t) = \{s_i\}$ be defined by (2) with $v = 2^{n-1} - 1$ and $t = 2^k + 1$. Then $\mathbf{s}(v,t)$ has two-level autocorrelation, and the s_i's take at most four distinct values $-1, 0, 1,$ or 2^d. Let N_η denote the number of η within one period of $\mathbf{s}(v,t)$, where $\eta = -1, 0, 1,$ or 2^d. Then we have*

$$N_{-1} = \frac{2^{(m+1)d} + 2^d}{2(2^d + 1)}, N_0 = 2^{(m-1)d} - 1, N_1 = \frac{(2^d - 2)(2^{md} - 1)}{2(2^d - 1)}, N_{2^d} = \frac{2^{(m-1)d} - 1}{2^{2d} - 1}.$$

Corollary 1 *With the same notation as in Theorem 2, if n is odd, and $\gcd(k, n) = 1$, then*

$$N_{-1} = \frac{2^n + 1}{3}, N_0 = 2^{n-1} - 1, N_1 = 0, N_2 = \frac{2^{n-1} - 1}{3}.$$

Thus, in this case, we obtain two-level ternary sequences with elements taken from $\{-1, 0, 2\}$.

Corollary 2 *With the same notation as in Theorem 2, if $n = 2m$ with m odd, and $\gcd(k, n) = 2$, then*

$$N_{-1} = \frac{2^{n+1}+2}{5}, N_0 = 2^{n-2} - 1, N_1 = \frac{2^n - 1}{3}, N_4 = \frac{2^{n-2}-1}{15}.$$

Thus, in this case, we obtain two-level quaternary sequences with elements taken from $\{-1, 0, 1, 4\}$.

For the case of $n = 5$ or 6, we list the data below.

Table 1: $n = 5$

(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)	$\{-1, -3/4, -1/4, 1/2, 3/2, 11/4\}$

Table 2: $n = 6$

(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)	$\{-7/2, -5/4, -1, -3/4, -1/2, -1/4, 1/4, 1/2, 1, 5/4, 3/2, 2\}$

In order to prove Theorem 2, we need some lemmas.

Lemma 1 ([1]) *Let n be an integer, and k be an integer with $\gcd(k, n) = d$. For any $a \in \mathbb{F}_{2^n}^*$, the equation $x^{2^k+1} + x + a = 0$ has $0, 1, 2$, or $2^d + 1$ roots in $\mathbb{F}_{2^n}$. For $i \in \{0, 1, 2, 2^d + 1\}$, let N_i denote the number of $a \in \mathbb{F}_{2^n}^*$ such that $x^{2^k+1} + x + a = 0$ has exactly i roots in $\mathbb{F}_{2^n}$. Set $m = n/d$. If m is odd, then*

$$N_0 = \frac{2^{(m+1)d} + 2^d}{2(2^d+1)}, N_1 = 2^{(m-1)d} - 1, N_2 = \frac{(2^d-2)(2^{md}-1)}{2(2^d-1)}, N_{2^d+1} = \frac{2^{(m-1)d}-1}{2^{2d}-1}.$$

If m is even, then

$$N_0 = \frac{2^{(m+1)d} - 2^d}{2(2^d+1)}, N_1 = 2^{(m-1)d}, N_2 = \frac{(2^d-2)(2^{md}-1)}{2(2^d-1)}, N_{2^d+1} = \frac{2^{(m-1)d} - 2^d}{2^{2d}-1}.$$

Lemma 2 ([12]) *Let n be an integer, and $1 \leq k < n$ with $\gcd(k,n) = 1$. Let $1 \leq k' < n$ be the multiplicative inverse of k modulo n, i.e., $k'k \equiv 1 \bmod n$. Then for any $a \in \mathbb{F}_{2^n}^*$, $x^{2^k+1} + x + a = 0$ has only one solution in $\mathbb{F}_{2^n}$ if and only if $Tr(R_{k,k'}(1/a)) = Tr(1) + 1$, where $R_{k,k'}(\cdot)$ is defined by (1).*

Lemma 3 ([4, 5]) *With the notation as in Lemma 2, for any $a \in \mathbb{F}_{2^n}^*$, $R_{k,k'}(1/a)$ is a zero of*

$$ax^{2^k+1} + \sum_{i=1}^{k'} x^{2^{ik}} + k' + 1 = 0 \tag{3}$$

and

$$a^{2^k} x^{2^{2k}} + x^{2^k} + ax + 1 = 0$$

in $\mathbb{F}_{2^n}^*$.

Lemma 4 *Let n be an integer, and $1 \leq k < n$ with $\gcd(k,n) = d$. For any $a \in \mathbb{F}_{2^n}^*$, if $x^{2^k+1} + x + a = 0$ has only one solution β, then $ax^{2^k} + \beta^2 x + \beta = 0$ has no solution in $\mathbb{F}_{2^n}$.*

Proof. Because $x^{2^k+1} + x + a = 0$ has only one solution β, $(\beta + x)^{2^k+1} + \beta + x + a = 0$ has no solution. Hence $\beta x^{2^k} + \beta^2 x^{2^k-1} + a = 0$ has no solution. It follows that $ax^{2^k} + \beta^2 x + \beta = 0$ has no solution. □

Lemma 5 *Let n be an integer, and $1 \leq k < n$ with $\gcd(k,n) = d$. For any $a \in \mathbb{F}_{2^n}^*$, if $x^{2^k+1} + x + a = 0$ has two solutions, and β is one of the solutions, then $ax^{2^k} + \beta^2 x + \beta = 0$ has one solution in $\mathbb{F}_{2^n}$. Moreover, $x^{2^k-1} + \beta^{2^k-1} + 1/\beta = 0$ has no solution.*

Proof. By the same proof as in Lemma 4, we have $ax^{2^k} + \beta^2 x + \beta = 0$ has one solution. If $x^{2^k-1} + \beta^{2^k-1} + 1/\beta = 0$ has one solution, then this solution is nonzero. Hence $ax^{2^k} + \beta^2 x = 0$ has one nonzero solution, and $ax^{2^k} + \beta^2 x + \beta = 0$ has two solutions. It is a contradiction. Hence $x^{2^k-1} + \beta^{2^k-1} + 1/\beta = 0$ has no solution. □

Lemma 6 *Let n be an integer, and $1 \leq k < n$ with $\gcd(k,n) = d$. For any $a \in \mathbb{F}_{2^n}^*$, if $x^{2^k+1} + x + a = 0$ has $2^d + 1$ solutions, and β is one of the solutions, then $ax^{2^k} + \beta^2 x + \beta = 0$ has 2^d solutions in $\mathbb{F}_{2^n}$. Moreover, $x^{2^k-1} + \beta^{2^k-1} + 1/\beta = 0$ has $2^d - 1$ solutions.*

Proof. By the same proof as in Lemma 4, we have $ax^{2^k} + \beta^2 x + \beta = 0$ has 2^d solutions. Hence $ax^{2^k} + \beta^2 x = 0$ has 2^d solutions. It follows that $x^{2^k-1} + \beta^{2^k-1} + 1/\beta = 0$ has $2^d - 1$ solutions. □

Lemma 7 *Let n be an integer, and $1 \le k < n$ with $\gcd(k, n) = d$ and n/d is odd. For any $\lambda \in \mathbb{F}_{2^n}^*$, set*

$$L_\lambda(\omega) = \omega^{2^{2k}} + \lambda^{2^k}\omega^{2^k} + \omega + \lambda^{2^{k-1}},$$

and

$$P_\lambda(\omega) = \omega^{2^k+1} + \omega + \frac{1}{\lambda^{2^{k-1}+\frac{1}{2}}}.$$

Then we have the following 4 cases:

- *if $P_\lambda(\omega) = 0$ has no solution in $\mathbb{F}_{2^n}$, then $L_\lambda(\omega) = 0$ has at most one solution in $\mathbb{F}_{2^n}$. In particular, if n is odd, and $\gcd(n, k) = 1$, then $L_\lambda(\omega) = 0$ has precisely one solution $\omega_0 = R_{k,k'}(\lambda^{2^{k-1}+\frac{1}{2}})/\sqrt{\lambda}$, and $Tr(\omega_0^{2^k+1}) = 1$.*
- *if $P_\lambda(\omega) = 0$ has one solution in $\mathbb{F}_{2^n}$, then $L_\lambda(\omega) = 0$ has 0 or 2^d solutions in $\mathbb{F}_{2^n}$, and $\sum_{\omega: L_\lambda(\omega)=0}(-1)^{Tr(\omega^{2^k+1})} = 0$. In particular, if n is odd, and $\gcd(n, k) = 1$, then $L_\lambda(\omega) = 0$ has precisely two solutions.*
- *if $P_\lambda(\omega) = 0$ has two solutions in $\mathbb{F}_{2^n}$, then $L_\lambda(\omega) = 0$ has one solution ω_0 in $\mathbb{F}_{2^n}$, and $Tr(\omega_0^{2^k+1}) = 0$.*
- *if $P_\lambda(\omega) = 0$ has $2^d + 1$ solutions in $\mathbb{F}_{2^n}$, then $L_\lambda(\omega) = 0$ has 2^{2d} solutions in $\mathbb{F}_{2^n}$, and $\sum_{\omega: L_\lambda(\omega)=0}(-1)^{Tr(\omega^{2^k+1})} = 2^d$.*

Proof. Let $x = \omega\sqrt{\lambda}$, and $a = \frac{1}{\lambda^{2^{k-1}+1/2}}$. Then $L_\lambda(\omega) = 0$ if and only if

$$H_a(x) = a^{2^k} x^{2^{2k}} + x^{2^k} + ax + 1 = 0. \tag{4}$$

Let $f(x) = (ax^{2^k-1})^{2^{n-1}}$. Then we have

$$H_a(x) + 1 = \frac{(f(x)^{2^k+1} + f(x) + a)^2 x}{a}. \tag{5}$$

By Lemma 1, there are 4 cases for the solutions of $P_\lambda(\omega) = 0$ in $\mathbb{F}_{2^n}$.

Case 1: $P_\lambda(\omega) = 0$ has no solution in $\mathbb{F}_{2^n}$. Then $a \neq \beta^{2^k+1} + \beta$ for any $\beta \in \mathbb{F}_{2^n}$. By (5), $H_a(x)+1 = 0$ has one solution. Hence (4) has 0 or 1 solution. In particular, if n is odd, and $\gcd(n, k) = 1$, by Lemma 3, (4) has precisely one solution $x_0 = R_{k,k'}(1/a)$. It follows that $L_\lambda(\omega) = 0$ has precisely one solution

$\omega_0 = R_{k,k'}(1/a)/\sqrt{\lambda}$. By Lemma 2, $Tr(R_{k,k'}(1/a)) = 1$ because $x^{2^k+1} + x + a = 0$ has no solution in $\mathbb{F}_{2^n}$. Hence, we have

$$\omega_0^{2^k+1} = (x_0/\sqrt{\lambda})^{2^k+1} = ax_0^{2^k+1} = \sum_{i=1}^{k'} x_0^{2^{ik}} + k' + 1.$$

It follows that

$$Tr(\omega_0^{2^k+1}) = Tr\left(\sum_{i=1}^{k'} x_0^{2^{ik}}\right) + k' + 1 = k' \cdot Tr(x_0) + k' + 1 = 1.$$

Case 2: $P_\lambda(\omega) = 0$ has one solution in $\mathbb{F}_{2^n}$. Then there is one $\beta \in \mathbb{F}_{2^n}$ such that $a = \beta^{2^k+1} + \beta$. Set $Q(x) = ax^{2^k} + \beta^2 x + \beta$, $\Gamma = \beta^{2^k-1} + 1/\beta$. Then we have

$$H_a(x) = Q(x)^{2^k} + \Gamma Q(x) = Q(x)(Q(x)^{2^k-1} + \Gamma).$$

By Lemma 4, $Q(x) = 0$ has no solution. If $x^{2^k-1} + \beta^{2^k-1} + 1/\beta = 0$ has no solution, then $H_a(x) = 0$ has no solution. If $x^{2^k-1} + \beta^{2^k-1} + 1/\beta = 0$ has $2^d - 1$ solutions, then $(ax^{2^k-1})^{2^{n-1}} = \beta$ has $2^d - 1$ solutions. By (5), $H_a(x) + 1 = 0$ has 2^d solutions. Thus, $H_a(x) = 0$ has 0 or 2^d solutions. If $H_a(x) = 0$ has 2^d solutions, then there is one and only one Δ satisfying $\Delta^{2^k-1} = 1/\Gamma$ such that $Q(x) + 1/\Delta = 0$ has 2^d solutions. Multiplying the equation $Q(x) + 1/\Delta = 0$ with $\mu = (\beta^2\Delta)^{-1}$ gives

$$\mu(ax^{2^k} + \beta^2 x + \beta + 1/\Delta) = (x/\Delta)^{2^k} + x/\Delta + \beta\mu + (\beta\mu)^2 = 0.$$

Let x_0 be one solution of $Q(x) + 1/\Delta = 0$. Then any solution of $Q(x) + 1/\Delta = 0$ can be written as $x_0 + \Delta\theta$, where $\theta \in \mathbb{F}_{2^d}$. We denote $x_0 + \Delta\theta$ by x_θ, and the solution of $L_\lambda(\omega) = 0$ associated with x_θ by ω_θ. It follows that

$$\begin{aligned} Tr(\omega_0^{2^k+1} + \omega_\theta^{2^k+1}) &= Tr(ax_0^{2^k+1} + ax_\theta^{2^k+1}) = Tr(\beta^2 x_0^2 + \beta x_0 + x_0/\Delta + \beta^2 x_\theta^2 + \beta x_\theta + x_\theta/\Delta) \\ &= Tr(\theta) = \frac{n}{d} \cdot Tr_1^d(\theta) = Tr_1^d(\theta). \end{aligned}$$

Hence we have

$$\sum_{x_\theta : Q(x_\theta)+1/\Delta=0} (-1)^{Tr(\omega_\theta^{2^k+1})} = 0$$

which means that

$$\sum_{x_\theta : H_a(x_\theta)=0} (-1)^{Tr(\omega_\theta^{2^k+1})} = 0.$$

In particular, if n is odd, and $\gcd(n,k)=1$, by Lemma 3, $R_{k,k'}(1/a)$ is a zero of (4). Hence, two solutions of $Q(x)+1/\Delta=0$ are precisely $R_{k,k'}(1/a)$ and $R_{k,k'}(1/a)+\Delta$. It follows that $R_{k,k'}(1/a)/\sqrt{\lambda}$ and $(R_{k,k'}(1/a)+\Delta)/\sqrt{\lambda}$ are precisely two solutions of $L_\lambda(\omega)=0$.

Case 3: $P_\lambda(\omega)=0$ has two solutions in $\mathbb{F}_{2^n}$. Let β be one of the solutions. Set $Q(x)=ax^{2^k}+\beta^2x+\beta$, $\Gamma=\beta^{2^k-1}+1/\beta$. Then we have

$$H_a(x)=Q(x)^{2^k}+\Gamma Q(x)=Q(x)(Q(x)^{2^k-1}+\Gamma).$$

By Lemma 5, $Q(x)=0$ has one solution, and $Q(x)^{2^k-1}+\Gamma=0$ has no solution. Let x_0 be the only solution of $H_a(x)=0$. Then $\omega_0=x_0/\sqrt{\lambda}$ is the only solution of $L_\lambda(\omega)=0$. We have

$$Tr(\omega_0^{2^k+1})=Tr(ax_0^{2^k+1})=Tr(\beta^2x_0^2+\beta x_0)=0.$$

Hence

$$\sum_{x_0:H_a(x_0)=0}(-1)^{Tr(\omega_0^{2^k+1})}=1.$$

Case 4: $P_\lambda(\omega)=0$ has 2^d+1 solutions in $\mathbb{F}_{2^n}$. By Lemma 6, for any β satisfying $\beta^{2^k+1}+\beta+a=0$, $x^{2^k-1}+\beta^{2^k-1}+1/\beta=0$ has 2^d-1 solutions. Hence, $(ax^{2^k-1})^{2^{n-1}}=\beta$ has 2^d-1 solutions. By (5), $H_a(x)+1=0$ has 2^{2d} solutions. Thus, (4) has 0 or 2^{2d} solutions. Set $Q(x)=ax^{2^k}+\beta^2x+\beta$, $\Gamma=\beta^{2^k-1}+1/\beta$. Similarly, we have

$$H_a(x)=Q(x)^{2^k}+\Gamma Q(x)=Q(x)(Q(x)^{2^k-1}+\Gamma).$$

By Lemma 6, $Q(x)=0$ has 2^d solutions. So (4) has 2^{2d} solutions, and for any Δ satisfying $\Delta^{2^k-1}=1/\Gamma$, $Q(x)+1/\Delta=0$ has 2^d solutions. Let x_0 be one solution of $Q(x)=0$, and ω_0 be the corresponding solution of $L_\lambda(\omega)=0$. We have

$$Tr(\omega_0^{2^k+1})=Tr(ax_0^{2^k+1})=Tr(\beta^2x_0^2+\beta x_0)=0.$$

By the same method as in Case 2, for any Δ, we have

$$\sum_{x_0:Q(x_0)+1/\Delta=0}(-1)^{Tr(\omega_0^{2^k+1})}=0.$$

Hence

$$\begin{aligned}\sum_{\omega:L_\lambda(\omega)=0}(-1)^{Tr(\omega^{2^k+1})} &= \sum_{x_0:H_a(x_0)=0}(-1)^{Tr(\omega_0^{2^k+1})}\\ &= \sum_{x_0:Q(x_0)=0}(-1)^{Tr(\omega_0^{2^k+1})}+\sum_{\Delta:\Delta^{2^k-1}=1/\Gamma}\sum_{x_0:Q(x_0)+1/\Delta=0}(-1)^{Tr(\omega_0^{2^k+1})}\\ &= 2^d.\end{aligned}$$

□

Lemma 8 *Let $f(x)=Tr(x)$, and two integers $0<v,t<2^n-1$ satisfy $\gcd(vt,q-1)=1$. Then we have*

$$\sum_{\lambda\in\mathbb{F}_{2^n}}\widehat{f}(v,t)(\lambda)=0 \text{ and } \sum_{\lambda\in\mathbb{F}_{2^n}}\widehat{f}(v,t)(\lambda)^2=2^{3n}.$$

Proof. We compute

$$\begin{aligned}\sum_{\lambda\in\mathbb{F}_{2^n}}\widehat{f}(v,t)(\lambda) &= \sum_{\lambda\in\mathbb{F}_{2^n}}\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda y+y^tx+x^v)}=\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{Tr(y^tx+x^v)}\sum_{\lambda\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda y)}\\ &= 2^n\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(x^v)}=0\end{aligned}$$

and

$$\begin{aligned}\sum_{\lambda\in\mathbb{F}_{2^n}}\widehat{f}(v,t)(\lambda)^2 &= \sum_{\lambda\in\mathbb{F}_{2^n}}\sum_{x_1,y_1\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda y_1+y_1^tx_1+x_1^v)}\sum_{x_1,y_2\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda y_2+y_2^tx_2+x_2^v)}\\ &= \sum_{x_1,x_2,y_1,y_2\in\mathbb{F}_{2^n}}(-1)^{Tr(y_1^tx_1+x_1^v+y_2^tx_2+x_2^v)}\sum_{\lambda\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda y_1+\lambda y_2)}\\ &= 2^n\sum_{x_1,x_2,y_1\in\mathbb{F}_{2^n}}(-1)^{Tr(y_1^tx_1+y_1^tx_2+x_1^v+x_2^v)}=2^{3n}.\end{aligned}$$

□

Lemma 9 *Let n be an integer, and $1\le k<n$ with $\gcd(k,n)=d$. Then*

$$\gcd(2^n-1,2^k+1)=\begin{cases}1, & \text{if } n/d \text{ is odd},\\ 2^d+1, & \text{otherwise.}\end{cases}$$

Proof. One can check the result easily. So we omit the detail here. □

Lemma 10 *Let n be an integer, and $1 \leq k < n$ with $\gcd(k,n) = d$ and n/d is odd. Let $v = 2^{n-1} - 1$, and $t = 2^k + 1$. Then for any $\lambda \in \mathbb{F}_{2^n}^*$, we have*

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

Proof. By Lemma 9, $\gcd(2^n - 1, 2^k + 1) = 1$. Hence we have

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

Set $y = x + \omega$. Then we have

$$\begin{aligned}
\sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{2^k+1} + y^{2^k+1} + \lambda x y)} &= \sum_{x,\omega \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{2^k+1} + (x+\omega)^{2^k+1} + \lambda x(x+\omega))} \\
&= \sum_{x,\omega \in \mathbb{F}_{2^n}} (-1)^{Tr(\omega^{2^k+1} + \omega^{2^k} x + \omega x^{2^k} + \lambda x^2 + \lambda \omega x)} \\
&= \sum_{x,\omega \in \mathbb{F}_{2^n}} (-1)^{Tr(\omega^{2^k+1} + (\omega^{2^{2k}} + \lambda^{2^k} \omega^{2^k} + \omega + \lambda^{2^{k-1}}) x^{2^k})}.
\end{aligned}$$

Set $L_\lambda(\omega) = \omega^{2^{2k}} + \lambda^{2^k} \omega^{2^k} + \omega + \lambda^{2^{k-1}}$. It follows that

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

By Lemma 7, the result follows. □

Lemma 11 *Let n be an integer, and $1 \leq k < n$ with $\gcd(k,n) = d$ and n/d is odd. Let $f(x) = Tr(x)$, $v = 2^{n-1} - 1$, and $t = 2^k + 1$. For any $\eta \in \{-1, 0, 1, 2^d\}$, let N_η denote the number of η taken by*

$\widehat{f}(v,t)(\lambda)/2^n$ *with* $\lambda \in \mathbb{F}_{2^n}^*$. *Set* $m = n/d$. *Then we have*

$$N_{-1} = \frac{2^{(m+1)d} + 2^d}{2(2^d+1)}, N_0 = 2^{(m-1)d} - 1, N_1 = \frac{(2^d-2)(2^{md}-1)}{2(2^d-1)}, N_{2^d} = \frac{2^{(m-1)d}-1}{2^{2d}-1}.$$

Proof. If $d = 1$, then the result follows from Lemmas 1, 7 and 10 directly. So we only need to prove the case of $d > 1$.

Let $P_\lambda(\omega)$ and $L_\lambda(\omega)$ be defined as in Lemma 7. By Lemmas 1, 7 and 10, $N_{2^d} = \frac{2^{(m-1)d}-1}{2^{2d}-1}$. Let $M_{0,0}$ denote the number of $\lambda \in \mathbb{F}_{2^n}^*$ such that $P_\lambda(\omega) = 0$ has no solution, and $L_\lambda(\omega) = 0$ has no solution. For any $\sigma \in \{-1, 1\}$, let $M_{0,\sigma}$ denote the number of $\lambda \in \mathbb{F}_{2^n}^*$ such that $P_\lambda(\omega) = 0$ has no solution, and $L_\lambda(\omega) = 0$ has one solution ω_0 satisfying $(-1)^{Tr(\omega_0^{2^k+1})} = \sigma$. By Lemmas 1, 7 and 10, we have

$$\begin{aligned} M_{0,-1} + M_{0,0} + M_{0,1} &= \frac{2^{(m+1)d} + 2^d}{2(2^d+1)}, \\ M_{0,-1} &= N_{-1}, \\ M_{0,0} + 2^{(m-1)d} - 1 &= N_0, \\ M_{0,1} + \frac{(2^d-2)(2^{md}-1)}{2(2^d-1)} &= N_1. \end{aligned}$$

Because $\widehat{f}(v,t)(0) = 2^n$, by Lemma 8, we have

$$-M_{0,-1} + M_{0,1} + \frac{(2^d-2)(2^{md}-1)}{2(2^d-1)} + 2^d \cdot \frac{2^{(m-1)d}-1}{2^{2d}-1} = -1.$$

Hence

$$M_{0,-1} - M_{0,1} = \frac{2^{(m+1)d} + 2^d}{2(2^d+1)}$$

which means that $M_{0,0} + 2M_{0,1} = 0$. Thus, $M_{0,0} = 0$, and $M_{0,1} = 0$. It follows that

$$N_{-1} = \frac{2^{(m+1)d} + 2^d}{2(2^d+1)}, N_0 = 2^{(m-1)d} - 1, N_1 = \frac{(2^d-2)(2^{md}-1)}{2(2^d-1)}.$$

□

Remark 4 *With the same notation as in Lemma 7, we obtain better result in Lemma 11 implicitly compared with that in Lemma 7, namely,*

- *if* $P_\lambda(\omega) = 0$ *has no solution in* $\mathbb{F}_{2^n}$, *then* $L_\lambda(\omega) = 0$ *has precisely one solution* ω_0 *in* $\mathbb{F}_{2^n}$, *and* $Tr(\omega_0^{2^k+1}) = 1$.

Proof of Theorem 2. By Theorem 1 and Lemma 11, the result follows. □

Compared with the binary case proved by Dillon and Dobbertin in 2004, we have Table 3 below. Note that $2^{n-1}-1$ and -1 are in the same coset modulo 2^n-1.

Table 3: 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 and Dobbertin [3]
$(-1, 2^k+1)$	$\{-1,0,2\}$	$\gcd(k,n)=1$, n odd	Theorem 2
$(-1, 2^k+1)$	$\{-1,0,1,2^d\}$	$\gcd(k,n)=d$, n/d odd	Theorem 2

The new ternary or quaternary sequences yield new Hadamard matrixes with entries in $\{-1,0,2\}$ or $\{-1,0,1,2^d\}$. For any binary sequence $\{s_i\}$ with two-level autocorrelation of period 2^n-1, using the standard construction from binary two-level autocorrelation sequences to Hadamard matrices, let

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

Then

$$AA^T = 2^n \cdot I_{2^n},$$

where A^T is the transpose of A and I_{2^n} is the identity matrix of $2^n \times 2^n$. Similarly, we have new $2^n \times 2^n$ Hadamard matrixes with entries in $\{-1,0,2\}$ or $\{-1,0,1,2^d\}$.

Example. Let $n=5$, $v=15$, and $t=3$. Then one sequence $\mathbf{s}$ of period 31 defined by (2) with $f(x)=Tr(x)$ is

$$-1,0,0,2,0,0,2,-1,0,0,0,0,2,0,-1,-1,0,2,0,-1,0,0,0,-1,2,-1,0,-1,-1,-1,-1,\cdots.$$

Let L be the left cyclic shift operator, and

$$A=\begin{pmatrix} 1 & 1\cdots 1 \\ 1 & \mathbf{s} \\ 1 & L\mathbf{s} \\ \vdots & \vdots \\ 1 & L^{30}\mathbf{s} \end{pmatrix}.$$

Then we have

$$AA^T = 32 \cdot I_{32}.$$

5 Conclusion

Pseudorandom sequences with two-level autocorrelation are very useful in communications and cryptography. The search of new sequences with two-level autocorrelation is a very interesting problem. The transform techniques are very important for sequence study. Using the Hadamard transform, Dillon and Dobbertin proved five conjectured classes of binary sequences with two-level autocorrelation. In this paper, some new ternary or quaternary sequences with two-level autocorrelation are found using the decimation-Hadamard transform and Dobbertin's method. Based on such sequences, new Hadamard matrixes with entries in $\{-1, 0, 2\}$ or $\{-1, 0, 1, 2^d\}$ can be constructed. More nice results via the transform technique are desirable.

References

[1] A. W. Bluher, On $x^{q+1} + ax + b$, *Finite Fields and Their Applic.*, vol. 10, no. 3, pp. 285-305, Jul. 2004.

[2] J. F. Dillon, Multiplicative difference sets via additive characters, *Des., Codes, Cryptogr.*, vol. 17, pp. 225-236, Sept. 1999.

[3] J. F. Dillon and H. Dobbertin, New cyclic difference sets with Singer parameters, *Finite Fields and Their Applications* 10 (2004), 342-389.

[4] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): The Welch case, *IEEE Trans. Inform. Theory*, vol. 45, pp. 1271-1275, May 1999.

[5] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, in *Difference Sets, Sequences and their Correlation Properties*, ser. NATO Science Series, Series C: Mathematical and Physical Sciences, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds. Dordrecht, The Netherlands: Kluwer Academic, 1999, vol. 542, pp. 133-158.

[6] S. Golomb, *Shift Register Sequences*, Oakland, CA: Holden-Day, 1967. Revised edition: Laguna Hills, CA: Aegean Park Press, 1982.

[7] S. W. Golomb and G. Gong, *Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications*, Cambridge, U.K.: Cambridge University Press, 2005.

[8] G. Gong and S. W. Golomb, Transform domain analysis of DES, *IEEE Trans. Inform. Theory*, vol. 45, pp. 2065-2073, Sept. 1999.

[9] G. Gong and S.W. Golomb, The decimation-Hadamard transform of two-level autocorrelation sequences, *IEEE Trans. on Inform. Theory*, vol. 48, No. 4, April 2002, pp. 853-865.

[10] G. Gong and A. M. Youssef, Cryptographic Properties of the Welch-Gong Transformation Sequence Generators, *IEEE Trans. Inform. Theory*, vol. 48, no. 11, pp. 2837-2846, Nov. 2002.

[11] T. Helleseth and G. Gong, New nonbinary sequences with ideal two-level autocorrelation functions, *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2868-2872, Nov. 2002.

[12] T. Helleseth, A. Kholosha, and G. J. Ness, Characterization of m-sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued crosscorrelation, *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2236-2245, Jun. 2007.

[13] T. Helleseth and P. V. Kumar, Sequences with low correlation, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, pp. 1765-1853.

[14] T. Helleseth, P. V. Kumar, and H. Martinsen, A new family of ternary sequences with ideal two-level autocorrelation function, *Des., Codes Cryptogr.*, vol. 23, pp. 157-166, 2001.

[15] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison- Wesley, 1983, vol. 20, Encyclopedia of Mathematics and its Applications, Theorem 3.35, pp. 97-98.

[16] M. Ludkovski and G. Gong, New families of ideal 2-level autocorrelation ternary sequences from second order DHT, *Proceedings of the second International Workshop on Coding and Cryptography*, January 8-12, 2001, Paris, France, pp. 345-354.

[17] A. Maschietti, Difference sets and hyperovals, *Des., Codes, Cryptogr.*, vol. 14, pp. 89-98, 1998.

[18] J. S. No, H. Chung, and M. S. Yun, Binary pseudorandom sequences of period 2^m-1 with ideal autocorrelation generated by the polynomial $z^d+(z+1)^d$, *IEEE Trans. Inform. Theory*, vol. 44, pp. 1278-1282, May 1998.

[19] J. S. No, S. W. Golomb, G. Gong, H. K. Lee, and P. Gaal, New binary pseudo-random sequences of period 2^n-1 with ideal autocorrelation, *IEEE Trans. Inform. Theory*, vol. 44, pp. 814-817, Mar. 1998.

[20] M. K. Simon, J. K. Omura, R. A. Sholtz, and B. K. Levitt, *Spread Spectrum Communications*, Rockville, MD: Computer Sci., 1985, vol. 1.

[21] N. Y. Yu and G. Gong, Realization of decimation-Hadamard transform for binary generalized GMW sequences, *Proceedings of Workshop on Coding and Cryptography (WCC2005)*, pp. 127-136, Bergen, Norway, March 14-18. 2005.

[22] N. Y. Yu and G. Gong, Multiplexing realizations of the decimation-Hadamard transform of two-level autocorrelation sequences, invited speaker, *the Proceedings of International Workshop on Coding and Cryptography*, Zhangjiajie, Hunan, China, June 1-5, 2009, the proceedings will be published by Springer in LNCS.