The Decimation-Hadamard Transform of Two-Level Autocorrelation Sequences

Guang Gong, *Member, IEEE,* and Solomon W. Golomb, *Fellow, IEEE*

***Abstract*—A new method to study and search for two-level autocorrelation sequences for both binary and nonbinary cases is developed. This method iteratively applies two operations: decimation and the Hadamard transform based on general orthogonal functions, referred to as the *decimation-Hadamard transform (DHT)*. The second iterative DHT can transform one class of such sequences into another inequivalent class of such sequences, a process called *realization*. The existence and counting problems of the second iterative DHT are discussed. Using the second iterative DHT, and starting with a single binary m-sequence (when n is odd), we believe one can obtain all the known two-level autocorrelation sequences of period 2^n-1 which have no subfield factorization. We have verified this for odd $n \leq 17$. Interestingly, no previously unknown examples were found by this process for any odd $n \leq 17$. This is supporting evidence (albeit weak) for the conjecture 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. Experimental results are provided.**

***Index Terms*—Group characters, iterative decimation-Hadamard transform (DHT), orthogonal functions, trace representation, two-level autocorrelation sequences.**

I. Introduction

THE sequences over a finite field GF(p) with (ideal) two-level autocorrelation have important applications in coding, communications, and cryptography. It is well known [5] that a balanced binary sequence $\{a_k\}$ of period 2^n-1 with two-level autocorrelation is constant on cyclotomic cosets, i.e., $\{a_{2k}\}=\{a_{k+r}\}$ for all k and some fixed value of r. Moreover, there is a cyclic shift of the original sequence for which $r=0$. Such binary two-level autocorrelation sequences are in one-to-one correspondence with cyclic Hadamard difference sets with parameters $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$. Perhaps best known among such sequences are the m-sequences, which correspond to Singer difference sets. For any primitive element α in GF(2^n), the set of m-sequences is given by

$$S_r=\{\mathrm{Tr}(\alpha^{rk})\}, \qquad (r, 2^n-1)=1$$

where S_r and $S_{r'}$ are distinct m-sequences iff r and r' belong to different cyclotomic cosets.

In the last three years, the study of binary sequences with two-level autocorrelation has made significant progress. Several new classes of binary sequences with two-level autocorrelation have been discovered. All cyclic difference sets of period 2^n-1 have been determined for all $n \leq 10$ [4]. The authors found that the Hadamard transform of three-term sequences is determined by one of the m-sequences [6] (a three-term sequence $\{a_k\}$ is defined by $a_k=\mathrm{Tr}(\alpha^k+\alpha^{rk}+\alpha^{r^{2k}})$, $k=0, 1, \ldots, r=2^{(n-1)/2}+1$). Dillon first successfully applied the Hadamard transform to a proof that the Welch–Gong transformation sequences, conjectured in [12], have two-level autocorrelation when n is odd by showing that the Hadamard transform of the Welch–Gong transform sequences is equal to the Hadamard transform of one of the m-sequences. A few months later, he and Dobbertin [3] confirmed all the newly conjectured classes of two-level autocorrelation sequences of period 2^n-1 for n odd by also showing that these sequences have the same Hadamard transform as one of the m-sequences. Based on this observation, by extending the above approach we develop a new method to study and search for two-level autocorrelation sequences over a finite field GF(p) where p is a prime. We call this the *(iterative) decimation-Hadamard transform (DHT)*. Using the second-order DHT, and starting with a single binary m-sequence (when n is odd), we believe one can obtain all the known two-level autocorrelation sequences of period 2^n-1 which have no subfield factorization. (We will give the definition for subfield factorization of sequences in Section VII .) We have verified this for odd $n \leq 17$. Interestingly, no previously unknown examples were found by this second-order DHT process for any odd $n \leq 17$. This is supporting evidence (albeit weak) for the conjecture 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.

This paper is organized as follows. In Section II, we give some preliminary concepts about sequences that we frequently use in this paper (for more theory on sequences, the reader is referred to [5], [7]). In Section III, we introduce the concept of iterations of the DHT. We do not restrict ourselves to the original Hadamard transform. Instead, we apply more general group character theory to such cases [10], [16]. In the second-order DHT of sequences, we perform decimation twice so that it is related to an integer pair (v, t). This pair determines whether it can produce other classes of two-level autocorrelation sequences; we call this case *a realizable pair*. In Section IV, we determine a set of special realizable pairs for all two-level autocorrelation sequences over GF(p). In Section V, we prove that the number of realizable pairs for any two-level autocorrelation sequence takes the values $0, 1, 2,$ or 6. In Section VI, we show

Manuscript received August 29, 2000; revised June 12, 2001.

G. Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@calliope.uwaterloo.ca).

S. W. Golomb is with the Communication Sciences Institute, University of Southern California, Los Angeles, CA 90089-2565 USA (e-mail: milly@usc.edu).

Communicated by A. Klapper, Associate Editor for Sequences.

Publisher Item Identifier S 0018-9448(02)01933-8.

some realizable pairs for binary m-sequences. In Section VII, we first introduce the concept of subfield factorization of sequences over GF(p) with period $p^n - 1$. Then we present the experimental results on the second-order DHT of binary m-sequences.

We will continue to investigate odd values of n, to look for analogous results with n even for the binary case, and to explore the nonbinary case. (Note that two-level autocorrelation sequences over GF(p) are in one-to-one correspondence with cyclic Hadamard difference sets with parameters $((p^n-1)/(p-1), (p^{n-1}-1)/(p-1), (p^{n-2}-1)/(p-1))$.)

II. Preliminaries

In this section, we present some preliminary concepts about sequences that we frequently use in this paper. The following notation is used throughout this paper.

- $\mathbb{Z}$ represents the integer ring; $\mathbb{R}$, the real number field; and $\mathbb{C}$, the complex number field.
- p is a prime number, n a positive integer, and $q = p^n$.
- $\mathbb{F}_q = \mathrm{GF}(q)$, the finite field with q elements, $\mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$. We write $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_p$.
- $\mathbb{Z}_m$ is the ring of integers modulo m;
$$\mathbb{Z}_m^* = \{r \in \mathbb{Z}_m | (r, m) = 1\}$$
the unit group of $\mathbb{Z}_m$; and
$$\mathbb{Z}_m^+ = \{r \in \mathbb{Z}_m | r \neq 0\}.$$
- Let $m|n$. The trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is denoted by $\mathrm{Tr}_m^n(x)$, i.e.,
$$\mathrm{Tr}_m^n(x) = x + x^{p^m} + \cdots + x^{p^{m(\frac{n}{m}-1)}}, \qquad x \in \mathbb{F}_{p^n}.$$
If $m = 1$, we simply write $\mathrm{Tr}_1^n(x)$ as $\mathrm{Tr}(x)$.

A. One–to–One Correspondence Between Periodic Sequences and Functions From $\mathbb{K}$ to $\mathbb{F}$

Let $\mathcal{S}$ be the set of all sequences over GF (p) with period $t|(p^n-1)$ and $\mathcal{F}$ be the set of all functions from GF(p^n) to GF(p). Any function $f(x) \in \mathcal{F}$ can be represented as

$$f(x) = \sum_{i=1}^{r} \mathrm{Tr}_1^{n_i}(A_i x^{t_i}),\ A_i \in \mathrm{GF}(p^{n_i}) \tag{1}$$

where t_i is a coset leader of a cyclotomic coset modulo $p^{n_i}-1$, and $n_i|n$ is the size of the cyclotomic coset containing t_i. For any sequence $\underline{\boldsymbol{a}} = \{a_i\} \in \mathcal{S}$, there exists $f(x) \in \mathcal{F}$ such that

$$a_i = f(\alpha^i), \qquad i = 0, 1, \ldots$$

where α is a primitive element of $\mathbb{K}$. $f(x)$ is called *the trace representation* of $\underline{\boldsymbol{a}}$. ($\underline{\boldsymbol{a}}$ is also referred to as an r-term sequence.) If $f(x)$ is any function from $\mathbb{K}$ to $\mathbb{F}$, by evaluating $f(\alpha^i)$, we get a sequence over $\mathbb{F}$ with period dividing $q-1$. Thus,

$$\underline{\boldsymbol{a}} \leftrightarrow f(x)$$

is a one-to-one correspondence between $\mathcal{F}$ and $\mathcal{S}$ through the trace representation (1). Note that in the language of algebraic geometry, $\underline{\boldsymbol{a}}$ is called an *evaluation* of $f(x)$ at α [15]. We adopt this term in this paper. That is, if $f(x)$ is the trace representation of $\underline{\boldsymbol{a}}$, then we also say that $\underline{\boldsymbol{a}}$ is the evaluation of $f(x)$ at α.

If $r = 1$, i.e.,

$$a_i = \mathrm{Tr}_1^n(\beta\alpha^i), \qquad i = 0, 1, \ldots,\ \beta \in \mathbb{F}_{p^n}^*$$

then $\underline{\boldsymbol{a}}$ is an m-sequence over $\mathbb{F}$ of period $q-1$ of degree n. (For a detailed treatment of the trace representation of sequences, see [14], [7].)

B. Decimation of Periodic Sequences

Let $\underline{\boldsymbol{a}}$ be a sequence over $\mathbb{F}$ of period $t|(p^n-1)$ and let $f(x)$ be the trace representation of $\underline{\boldsymbol{a}}$. Let $0 < s < t$. Then a sequence $\underline{\boldsymbol{b}} = \{b_i\}$ whose elements are given by

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

is said to be an s-decimation of $\underline{\boldsymbol{a}}$, denoted by $\underline{\boldsymbol{a}}^{(s)}$. The trace representation of $\underline{\boldsymbol{a}}^{(s)}$ is $f(x^s)$. That is, we have

$$\begin{aligned} \underline{\boldsymbol{a}} &\longleftrightarrow f(x)\\ \underline{\boldsymbol{a}}^{(s)} &\longleftrightarrow f(x^s). \end{aligned}$$

For example

$$\begin{aligned} \underline{\boldsymbol{a}} &= 1\,001\,011 \longleftrightarrow \mathrm{Tr}(x)\\ \underline{\boldsymbol{a}}^{(3)} &= 1\,110\,100 \longleftrightarrow \mathrm{Tr}(x^3). \end{aligned}$$

If $\underline{\boldsymbol{a}}$ is an m-sequence of period p^n-1 and $(s, p^n-1) = 1$, then $\underline{\boldsymbol{a}}^{(s)}$, the s-decimation of $\underline{\boldsymbol{a}}$, is also an m-sequence.

C. Additive Character

Let $\omega = e^{2\pi i/p}$, a complex primitive pth root of unity. The canonical additive character χ of $\mathbb{F}$ is defined by [13]

$$\chi(x) = \omega^x, \qquad x \in \mathbb{F}. \tag{2}$$

D. Autocorrelation

Let $\overline{\chi}$ be the complex conjugate of χ. The autocorrelation of $\underline{\boldsymbol{a}}$ is defined by

$$C_{\underline{\boldsymbol{a}}}(\tau) = \sum_{i=0}^{t-1} \chi(a_{i+\tau})\overline{\chi(a_i)}, \qquad 0 \le \tau \le t-1 \tag{3}$$

where τ is a phase shift of the sequence $\{a_i\}$ and the indexes are computed modulo t, the period of $\underline{\boldsymbol{a}}$. If $\underline{\boldsymbol{a}}$ has period p^n-1 and

$$C_{\underline{\boldsymbol{a}}}(\tau) = \begin{cases} -1, & \text{if } \tau \not\equiv 0 \bmod q-1\\ q-1, & \text{if } \tau \equiv 0 \bmod q-1 \end{cases}$$

(recall $q = p^n$) then we say that the sequence $\underline{\boldsymbol{a}}$ has an *(ideal) two-level autocorrelation function*.

In particular, if $p = 2$ and $\underline{\boldsymbol{a}}$ has two-level autocorrelation over $\mathbb{F}$, according to the result in [8], then the coefficients of the trace representation $f(x)$ of the sequence, defined by (1), satisfy

$$A_i \in \mathbb{F} \quad \text{and} \quad A_i A_{-i} = 0, \qquad \forall i.$$

E. Hadamard Transform and the Inverse Transform

Let $f(x)$ be a polynomial function from $\mathbb{K}$ to $\mathbb{F}$. The Hadamard transform of $f(x)$ is defined by

$$\hat{f}(\lambda)=\sum_{x\in K}\chi(\lambda x)\overline{\chi(f(x))}, \qquad \lambda\in K$$

where $\overline{\chi(f(x))}$ is the complex conjugate of $\chi(f(x))$. The inverse formula is given by

$$\chi(f(\lambda))=\frac{1}{q}\sum_{x\in K}\chi(\lambda x)\overline{\hat{f}(x)}, \qquad \lambda\in K.$$

F. Parseval's Formula

Let $f(x)$ be a function from $\mathbb{K}$ to $\mathbb{F}$. Then

$$\sum_{x\in\mathbb{K}}\chi(f(\lambda x))\overline{\chi(f(x))}=\sum_{x\in\mathbb{K}}\hat{f}(\lambda x)\overline{\hat{f}(x)}, \qquad \lambda\in\mathbb{K}. \quad (4)$$

III. Iterations of the Decimation-Hadamard Transform (DHT)

In this section, we develop a new method to study and search for two-level autocorrelation sequences by applying group character theory [10], [16].

Definition 1: Let $f(x)$ be a function from $\mathbb{K}$ to $\mathbb{F}$ with $f(0)=0$. If

$$\sum_{x\in\mathbb{K}}\chi(f(\lambda x))\overline{\chi(f(x))}=\begin{cases}0, & \text{if } \lambda\neq 1\\ q, & \text{if } \lambda=1\end{cases}$$

for $\lambda\in\mathbb{K}$, then we say that $f(x)$ is *orthogonal over* $\mathbb{F}$.

From the definition, the following result is immediate.

Lemma 1: If $f(x)$ is orthogonal over $\mathbb{F}$, then

$$\sum_{x\in\mathbb{K}}\chi(f(\lambda x))=\begin{cases}0, & \text{if } \lambda\neq 0\\ q, & \text{if } \lambda=0\end{cases}$$

for all $\lambda\in\mathbb{K}$.

Theorem 1: Let $\underline{\boldsymbol{a}}=\{a_i\}$ be a sequence over F of period p^n-1. Let $f(x)$ be the trace representation function of $\underline{\boldsymbol{a}}$. Then $\underline{\boldsymbol{a}}$ has two-level autocorrelation and the balance property if and only if $f(x)$ is orthogonal over $\mathbb{F}$.

We first present the following lemma whose proof comes directly from the definition of the autocorrelation function.

Lemma 2: Let $\underline{\boldsymbol{a}}=\{a_i\}$ be a sequence over F of period p^n-1. Let $f(x)$ be the trace representation function of $\underline{\boldsymbol{a}}$. Let $C_{\underline{\boldsymbol{a}}}(\tau)$ be the autocorrelation of $\underline{\boldsymbol{a}}$ defined by (3). Let

$$\Delta_f(\lambda)=\sum_{x\in\mathbb{K}}\chi(f(\lambda x))\overline{\chi(f(x))}.$$

Then

$$C_{\underline{\boldsymbol{a}}}(\tau)=-1+\Delta_f(\lambda)$$

where $\lambda=\alpha^\tau\in\mathbb{K}^*$.

Proof of Theorem 1: Note that $\lambda=0$ in definition is equivalent to saying that $\underline{\boldsymbol{a}}$ is balanced. Thus, the result is immediate from the definition of orthogonal functions and Lemma 2.

Definition 2: Let $h(x)$ be orthogonal over $\mathbb{F}$ and $f(x)$ be a function from $\mathbb{K}$ to $\mathbb{F}$. For an integer $v\in\mathbb{Z}^+_{q-1}$, we define

$$\hat{f}_h(v)(\lambda)=\sum_{x\in\mathbb{K}}\chi(h(\lambda x))\overline{\chi(f(x^v))}, \qquad \lambda\in\mathbb{K}.$$

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

Remark 1: Let $f(x)$ be the trace representation of the sequence $\underline{\boldsymbol{a}}$. Then $f(x^s)$ is the trace representation of the s-decimation of the sequence. If we take $h(x)=\mathrm{Tr}(x)$, then $\hat{f}_h(v)(\lambda)$, the first-order DHT, is the Hadamard transform of $f(x^v)$. Hence, the computing process $\hat{f}_h(v)(\lambda)$ consists of first applying the decimation operation (corresponding to the sequence), then the Hadamard transform. Note that here, the trace function is replaced by any orthogonal function.

Remark 2: If $h(x)=\mathrm{Tr}(x^s)$ with $(s,q–1)=1$, then $\hat{f}_h(v)(\lambda)$ is the *extended Hadamard transform* introduced in [9] for the analysis of the Data Encryption Standard (DES).

Definition 3: With the above notation, let $t\in\mathbb{Z}^+_{q-1}$. We define

$$\hat{f}_h(v,t)(\lambda)=\sum_{y\in\mathbb{K}}\chi(h(\lambda y))\overline{\hat{f}_h(v)(y^t)}, \qquad \lambda\in\mathbb{K}.$$

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

Remark 3: If $t=1$, then the second-order DHT divided by q is just the inverse Hadamard transform of $f(x^v)$.

For the first-order DHT, we have the following result.

Lemma 3:

1) $\hat{f}_h(v)(\lambda)=\sum_{x\in\mathbb{K}}\omega^{h(\lambda x)-f(x^v)}$.
2) $\hat{f}_h(v)(\lambda)\in\mathbb{R}$. That is, $\hat{f}_h(v)\colon\mathbb{K}\longrightarrow\mathbb{R}$. In particular, for $p=2$, $\hat{f}_h(v)(\lambda)$ is an integer. That is, $\hat{f}_h(v)\colon\mathbb{K}\longrightarrow\mathbb{Z}$.

From the definition and Lemma 3, the following proposition for $\hat{f}_h(v,t)(x)$, the second-order DHT of $f(x)$, is immediate.

Lemma 4:

$$\hat{f}_h(v,t)(\lambda)=\sum_{x,y\in\mathbb{K}}\omega^{h(\lambda y)+h(y^t x)-f(x^v)}. \quad (5)$$

Let $G=\langle\omega\rangle$, i.e., $G=\{\omega^i|i=0,1,\ldots,p-1\}$. Let $\mathbb{Z}[\omega]$ be the set consisting of polynomials over $\mathbb{Z}$ in ω. ($\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$ and $G\subset\mathbb{Z}[\omega]$.) Note that $\omega^p=1$. Thus,

$$\mathbb{Z}[\omega]=\left\{\sum_{i=0}^{p-1}c_i\omega^i|c_i\in\mathbb{Z}\right\}.$$

From Definition 3, the following result is easy to establish.

Proposition 1:

$$\hat{f}_h(v,t)(x)\in\mathbb{Z}[\omega], \qquad \forall\, x\in\mathbb{K}.$$

That is, for the fixed pair

$$(v,\, t) \in \mathbb{Z}_{q-1}^{+} \times \mathbb{Z}_{q-1}^{+}$$

$\hat{f}_h(v,\, t)(x)$ is a map from $\mathbb{K}$ to $\mathbb{Z}[\omega]$.

Proposition 2: For the first- and second-order DHT, we have

$$\sum_{\lambda \in \mathbb{K}} \hat{f}_h(v)(\lambda) = q \quad \text{and} \quad \sum_{\lambda \in \mathbb{K}} \hat{f}_h(v,\, t)(\lambda) = qI_f$$

where

$$I_f = \sum_{\lambda \in \mathbb{K}} \overline{\chi(f(\lambda^v))}.$$

In particular, if $f(x)$ is balanced and $(v,\, q-1) = 1$, then

$$\sum_{\lambda \in \mathbb{K}} \hat{f}_h(v,\, t)(\lambda) = 0.$$

Proof: For the first-order DHT, applying Lemma 3 and then Lemma 1

$$\begin{aligned}\sum_{\lambda \in \mathbb{K}} \hat{f}_h(v)(\lambda) &= \sum_{\lambda} \sum_{x \in \mathbb{K}} \omega^{h(\lambda x) - f(x^v)} \\ &= \sum_{x \in \mathbb{K}} \omega^{-f(x^v)} \sum_{\lambda \in \mathbb{K}} \omega^{h(\lambda x)} \\ &= q\omega^{-f(0)} = q.\end{aligned}$$

Similarly, for the second-order DHT, applying Lemma 4 and then Lemma 1

$$\begin{aligned}\sum_{\lambda \in \mathbb{K}} \hat{f}_h(v,\, t)(\lambda) &= \sum_{\lambda \in \mathbb{K}} \sum_{x,\, y \in \mathbb{K}} \omega^{h(\lambda y) + h(y^t x) - f(x^v)} \\ &= \sum_{x,\, y \in \mathbb{K}} \omega^{h(y^t x) - f(x^v)} \sum_{\lambda \in \mathbb{K}} \omega^{h(\lambda y)} \\ &= q \sum_{x \in \mathbb{K}} \omega^{-f(x^v)} = qI_f.\end{aligned}$$

If $f(x)$ is balanced and $(v,\, q-1) = 1$, then $I_f = 0$, so that

$$\sum_{\lambda \in \mathbb{K}} \hat{f}_h(v,\, t)(\lambda) = 0. \qquad \blacksquare$$

In the following, we introduce a notation on products of two subsets of a ring. Let R be a ring, and D and E be two subsets of R, i.e., $D \subset R$ and $E \subset R$. A product of D and E is defined by

$$DE = \{de | d \in D,\, e \in E\}.$$

If $D = \{d\}$, having only one element, then we write DE as dE.

Definition 4: If

$$\hat{f}_h(v,\, t)(x) \in qG, \qquad \forall x \in \mathbb{K}$$

then we say that $(v,\, t)$ is *realizable*, denoted as realizable-$(v,\, t)$ or R-$(v,\, t)$ for short.

Theorem 2: Let $(v,\, t)$ be realizable with $(v,\, q-1) = 1$ and $(t,\, q-1) = 1$, and let $g(x)$ be defined by

$$\chi(g(x)) = \frac{1}{q}\, \hat{f}_h(v,\, t)(x). \tag{6}$$

Then $g(x)$ is orthogonal if and only if $f(x)$ is orthogonal. Equivalently, let $\underline{\boldsymbol{a}} = \{a_i\}$ and $\underline{\boldsymbol{b}} = \{\underline{\boldsymbol{b}}_i\}$ be the evaluations of $f(x)$ and $g(x)$ at α, respectively. Then $\underline{\boldsymbol{b}}$ has two-level autocorrelation if and only if $\underline{\boldsymbol{a}}$ does.

In order to prove Theorem 2, we need the following lemma.

Lemma 5:

$$\sum_{x \in \mathbb{K}} \chi(h(\lambda x))\overline{\hat{f}_h(v,\, t)(x)} = q\hat{f}_h(v)(\lambda^t), \qquad x \in \mathbb{K}. \tag{7}$$

Proof: Using the orthogonal property of $h(x)$, the left-hand side of (7) can be written as

$$\begin{aligned}\text{Left side } &= \sum_{x \in \mathbb{K}} \chi(h(\lambda x))\overline{\sum_{y \in \mathbb{K}} \chi(h(xy))\hat{f}_h(v)(y^t)} \\ &= \sum_{x \in \mathbb{K}} \chi(h(\lambda x)) \sum_{y \in \mathbb{K}} \overline{\chi(h(xy))}\,\overline{\hat{f}_h(v)(y^t)} \\ &= \sum_{y \in \mathbb{K}} \hat{f}_h(v)(y^t) \sum_{x \in \mathbb{K}} \chi(h(\lambda x))\overline{\chi(h(xy))} \\ &= q\hat{f}_h(v)(\lambda^t).\end{aligned} \qquad \blacksquare$$

Proof of Theorem 2: From Lemma 5 and noticing that $\hat{f}_h(v)(\lambda^t)$ is a real number, we have

$$\hat{f}_h(v)(\lambda^t) = \frac{1}{q} \sum_{x \in \mathbb{K}} \chi(h(\lambda x))\overline{\hat{f}_h(v,\, t)(x)}.$$

Substituting $\chi(g(x)) = \frac{1}{q}\, \hat{f}_h(v,\, t)(x) \in G$ into the above identity, we get

$$\hat{f}_h(v)(\lambda^t) = \sum_{x \in \mathbb{K}} \chi(h(\lambda x))\overline{\chi(g(x))} = \hat{g}(\lambda).$$

According to Parseval's formula (4), since $(v,\, t)$ is realizable, then $g(x)$ is orthogonal if and only if $f(x)$ is orthogonal. □

Corollary 1: Let $f(x)$ be orthogonal. Let $(v,\, t)$ be realizable from $f(x)$ with $(v,\, q-1) = 1$ and $(t,\, q-1) = 1$, and let $g(x)$ be defined by (6). If $g(x) \neq f(x^s)$ for any $s \in Z_{q-1}$ with $(s, q–1) = 1$, then the evaluation of $g(x)$ is a two-level autocorrelation sequence which is shift-distinct from the evaluation of $f(x)$.

This result provides a new method to search for sequences with two-level autocorrelation.

Definition 5: Let $(v,\, t)$ be realizable and let $g(x)$ be defined by (6). Then we say that $g(x)$ or the sequence $\{b_i\}$, the evaluation of $g(x)$, is a *realization* of f under h. We also say that $(v,\, t)$ is a *realizable pair* of $g(x)$ from $f(x)$ (under $h(x)$).

Remark 4: According to Remark 1, we have the following trivial realization:

$$\hat{f}_h(v,\, 1)(x) = \chi(f(x^v)), \qquad x \in \mathbb{K}.$$

So, $(v, 1)$ is realizable for all $v \in \mathbb{Z}_{q-1}^{+}$ and the realization is $f(x^v)$.

Example 1: Let $p = 2$, $n = 5$, and $f(x) = \mathrm{Tr}(x)$. Let α be a primitive element in GF (2^5) with the minimal polynomial $t(x) = x^5 + x^3 + 1$. Then the m-sequence $\underline{\boldsymbol{a}}$ of degree 5, which is the evaluation of $\mathrm{Tr}(x)$ at α, is as follows:

$$\underline{\boldsymbol{a}} = 1000010101110110001111100110100.$$

Case 1: $(v, t) = (3, 3)$. Then the first DHT of $f(x)$ is

$$\widehat{f_h}(3)(\lambda) = \sum_{x \in GF(2^5)} (-1)^{\mathrm{Tr}(\lambda x) + \mathrm{Tr}(x^3)}$$

whose values are listed as

$$\{\widehat{f_h}(3)(\alpha^i) \colon 0 \le i < 30\} = \begin{array}{rrrrrrrrrr} -8 & 0 & 0 & 0 & 0 & -8 & 0 & 8 & 0 & -8 \\ -8 & 8 & 0 & 8 & 8 & 0 & 0 & 0 & -8 & 8 \\ -8 & 8 & 8 & 0 & 0 & 8 & 8 & 0 & 8 & 0 \\ 0. \end{array}$$

The second DHT of $f(x)$ is

$$\widehat{f_h}(3, 3)(\lambda) = \sum_{x, y \in GF(2^5)} (-1)^{\mathrm{Tr}(\lambda y) + \mathrm{Tr}(y^3 x) + \mathrm{Tr}(x^3)}$$

whose values are listed as shown in the first expression at the bottom of the page. Thus, $(3, 3)$ is realizable. The realization is given by

$$g(x) = \mathrm{Tr}(x + x^5 + x^7)$$

or the sequence

$$10010010000011101010001111011011.$$

Case 2: We take $(v, t) = (15, 7)$. Then the values of the first DHT $\hat{f}_h(15)$ are as follows:

$$\{\hat{f}_h(15)(\alpha^i) \colon 0 \le i \le 30\} = \begin{array}{rrrrrrrrrr} 12 & 8 & 8 & -8 & 8 & 4 & -8 & 4 & 8 & 4 \\ 4 & -4 & -8 & -4 & 4 & 0 & 8 & -8 & 4 & 4 \\ 4 & -4 & -4 & 0 & -8 & 4 & -4 & 0 & 4 & 0 \\ 0. \end{array}$$

The values of the second DHT $\hat{f}_h(15, 7)$ are as shown in the second expression at the bottom of the page. According to Definition 5, $(15, 7)$ is not realizable.

In the preceding example, we take $f(x) = h(x) = \mathrm{Tr}(x)$. This is a very interesting case which leads to the following definition.

Definition 6: Let $h(x)$ be orthogonal with $h(0) = 0$ and let the sequence $\underline{\boldsymbol{a}}$ be the evaluation of $h(x)$. Let $f = h$. In this case, we denote $\hat{f}_h(v)(x)$ and $\hat{f}_h(v, t)(x)$ by $\hat{h}(v)(x)$ and $\hat{h}(v, t)(x)$, respectively, and call them the *first- and second-order symmetric decimation-Hadamard transforms (SDHT)* of h, respectively. If (v, t) is realizable, then $g(x)$, defined by (6), becomes

$$\chi(g(x)) = (1/q)\hat{h}(v, t)(x), \qquad x \in \mathbb{K}$$

which is said to be a *realization* of $h(x)$ or the sequence $\underline{\boldsymbol{a}}$, the evaluation of $h(x)$. Moreover, if $g(x) = h(x^s)$, then we say that (v, t) is *self-realizable*.

Lemma 6:

$$\hat{h}(v, t)(\lambda) = \sum_{x, y \in \mathbb{K}} \omega^{h(\lambda y) + h(y^t x) - h(x^v)}, \qquad \lambda \in \mathbb{K}.$$

Note: A self-realizable pair does not give any other class of two-level autocorrelation sequences except for the class given by $h(x)$ itself. But it is still worth determining how many of these there are.

Remark 5: If $h(x) = \mathrm{Tr}(x)$, the case of represented Singer sets or m-sequences, then

$$\widehat{\mathrm{Tr}}(v, t)(\lambda) = \sum_{x, y \in \mathbb{K}} \omega^{\mathrm{Tr}(\lambda y + y^t x - x^v)}, \qquad \lambda \in \mathbb{K}.$$

Remark 6: We can iteratively define the kth-order DHT of $f(x)$ by using Definitions 2 and 3.

With the notation in Definition 3, let $k \ge 2$, $v_i \in \mathbb{Z}_{q-1}^{+}$, $i = 1, \ldots, k$, and $\lambda \in \mathbb{K}$. We define

$$\hat{f}_h(v_1, v_2, \ldots, v_k)(\lambda) = \sum_{y \in \mathbb{K}} \chi(h(\lambda y)) \overline{\hat{f}_h(v_1, v_2, \ldots, v_{k-1})(y^{v_k})}.$$

$\hat{f}_h(v_1, v_2, \ldots, v_k)(\lambda)$ is called the *kth-order DHT of* $f(x)$ (*with respect to* $h(x)$).

However, this transformation only has theoretical interest, so we do not discuss it in this paper.

$$\{\widehat{f_h}(3, 3)(\alpha^i) \colon 0 \le i < 30\} = \begin{array}{rrrrrrrrrr} -32 & 32 & 32 & -32 & 32 & 32 & -32 & 32 & 32 & 32 \\ 32 & -32 & -32 & -32 & 32 & -32 & 32 & -32 & 32 & 32 \\ 32 & -32 & -32 & -32 & -32 & 32 & -32 & -32 & 32 & -32 \\ -32. \end{array}$$

$$\{\hat{f}_h(15, 7)(\alpha^i) \colon 0 \le i \le 30\} = \begin{array}{rrrrrrrrrr} -112 & 0 & 0 & -16 & 0 & -32 & -16 & 16 & 0 & -32 \\ -\ 32 & 0 & -16 & 0 & 16 & 48 & 0 & -16 & -32 & 16 \\ -\ 32 & 0 & 0 & 48 & -16 & 16 & 0 & 48 & 16 & 48 \\ 48. \end{array}$$

In the remainder of the paper, we will discuss the second-order SDHT of h where h is an arbitrary orthogonal function, or equivalently, the evaluation of $h(x)$ is a two-level autocorrelation sequence.

IV. Self-Realizable Pairs

Let $\underline{\boldsymbol{a}}$ be a two-level autocorrelation sequence over $\mathbb{F}$ of period $q-1$ and let $h(x)$ be its trace representation. In this section, we determine a set of self-realizable pairs for $\hat{h}(v, t)$, the second-order SDHT of h or $\underline{\boldsymbol{a}}$. First we introduce a set related to cyclotomic cosets for easier presentation of the result.

Cyclotomic Coset Set

Let

$$C = \{1, p, p^2, \dots, p^{n-1}\}.$$

Then C is a subgroup of Z^*_{q-1} $(q = p^n)$. Hence C establishes an equivalence relation on $\mathbb{Z}^*_{q-1}$, denoted by $\sim$. For $r,\, s \in \mathbb{Z}^*_{q-1}$, $s \sim t$ if and only if $st^{-1} \in C$. In other words, $s \sim t$ if and only if there exists a positive integer j: $0 \le j < n$ such that $s \equiv p^j t \pmod{q-1}$. Let Ω be the set consisting of all equivalence classes of $\sim$. Then

$$\Omega = \{C_s | s \in Z^*_{q-1}\}$$

where

$$C_s = sC = \{s, sp, \dots, sp^{n_s - 1}\} \subset \mathbb{Z}_{q-1}$$

where the subscript s is the smallest integer in C_s, called its *coset leader modulo* $q-1$; C_s, the cyclotomic coset modulo $q-1$; and n_s, the smallest integer such that $s \equiv sp^{n_s} \pmod{q-1}$.

Let $\Omega^* = \{C_s \in \Omega | \gcd(s, q-1) = 1\}$.

Lemma 7: Let $I_p(d)$ be the number of irreducible polynomials over F_p of degree d. Then

$$|\Omega| = \sum_{d|n} I_p(d)$$

and

$$|\Omega^*| = \phi(p^n - 1)/n.$$

Remark 7: From the theory of linear feedback shift register (LFSR) sequences [5], $|\Omega|$ is the number of shift distinct LFSR sequences over $\mathbb{F}_p$ with degree dividing n, and $|\Omega^*|$ is the number of all shift distinct m-sequences over F_p of degree n.

For simplicity, we represent the elements of Ω by coset leaders, i.e.,

$$\Omega = \{r | r \text{ is a coset leader} \bmod q-1\}$$

and

$$\Omega^* = \{r \in \Omega | \gcd(r, q-1) = 1\}.$$

Theorem 3: For $\hat{h}(v, t)(\lambda)$, the second-order SDHT of h, defined in Definition 6, and for each $s \in \Omega^*$, there exists exactly one realizable pair $(v, t) \in \Omega^* \times \Omega^*$ such that

$$\frac{1}{q}\,\hat{h}(v, t)(\lambda) = \chi(h(\lambda^s)), \qquad \lambda \in K.$$

Proof: Let $g(\lambda) = 1/q\hat{h}(v, t)(\lambda)$. From Lemma 2 we have

$$\hat{g}(\lambda) = \hat{h}(v)(\lambda^t). \tag{8}$$

Note that the first-order SDHT of h is given by

$$\hat{h}(v)(\lambda^t) = \sum_{x \in K} \omega^{h(\lambda^t x) - h(x^v)}. \tag{9}$$

For each $s \in \Omega^*$, we make a change of variables by setting

$$\lambda^t x = z^s. \tag{10}$$

Then we get

$$x = \lambda^{-t} z^s \quad \text{and} \quad x^v = \lambda^{-vt} z^{vs}.$$

Let v and t be the solutions of the equations

$$sv = 1 \tag{11}$$

$$-vt = 1 \tag{12}$$

in Ω^*. Then we have $v = s^{-1}$ and $t = -s$.

In the following, we discuss the cases $p = 2$ and $p > 2$ separately.

Case 1: $p = 2$

For fixed $s \in \Omega^*$, after the variable change at (10), we have $(v, t) = (s^{-1}, -s)$ such that (9) can be written as

$$\hat{h}(v)(\lambda^t) = \sum_{z \in \mathbb{K}} (-1)^{h(z^s) + h(\lambda z)} = \hat{h}(s)(\lambda).$$

Combining with (8), we have

$$\hat{g}(\lambda) = \hat{h}(s)(\lambda).$$

Applying the inverse Hadamard transform to the above identity, it follows that

$$(1/q)\hat{h}(v, t)(\lambda) = (-1)^{h(\lambda^s)}$$

where $(v, t) = (s^{-1}, -s)$.

Case 2: $p > 2$

Similarly, we have

$$\hat{h}(v)(\lambda^t) = \sum_{z \in \mathbb{K}} \omega^{h(z^s) - h(\lambda z)} = \overline{\hat{h}(s)(\lambda)}.$$

According to Lemma 3, $\hat{h}(s)(\lambda) \in \mathbb{R}$. Thus, $\overline{\hat{h}(s)(\lambda)} = \hat{h}(s)(\lambda)$. Therefore, we still have

$$\hat{g}(\lambda) = \hat{h}(s)(\lambda).$$

Using the inverse Hadamard transform, we have

$$\frac{1}{q}\,\hat{h}(v, t)(\lambda) = \chi(h(\lambda^s))$$

where $(v, t) = (s^{-1}, -s)$, which completes the proof. ■

Corollary 2: Let $\hat{h}(v, t)(\lambda)$ be as defined in Definition 6. Then for each $s \in \Omega^*$, we have

$$\frac{1}{q}\,\hat{h}(s^{-1}, -s)(\lambda) = \chi(h(\lambda^s)), \qquad \lambda \in K.$$

In other words, every orthogonal function $h(x)$ has all pairs in $\{(s^{-1}, -s) | s \in \Omega^*\}$ as self-realizable pairs.

V. Realizable Pairs for the Binary Case

In this section, we discuss the realizable pairs for binary two-level autocorrelation sequences. Throughout this section, we assume $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$ to be two shift distinct binary two-level autocorrelation sequences and $h(x)$ and $g(x)$ to be the trace representations of $\underline{\boldsymbol{a}}$ and $\underline{\boldsymbol{b}}$, respectively. In this case, we have $g(x) \neq h(x^s),\ \forall\, s \in \Omega^*$. Note that the following computation on integers is carried out in Ω^*.

Theorem 4: With the above notation, assume that (v, t) is a realizable pair of $h(x)$, and the realization is $g(x)$, i.e.,

$$\frac{1}{q}\,\hat{h}(v, t)(\lambda) = (-1)^{g(\lambda)}, \quad \lambda \in \mathbb{K}. \tag{13}$$

Let

$$R_h(g) = \left\{(a, b) \in \Omega^* \times \Omega^* \,\middle|\, (1/q)\hat{h}(a, b)(\lambda) = (-1)^{g(\lambda^s)} \text{ for some } s \in \Omega^* \right\}. \tag{14}$$

If $v = -1$, then $|R_h(g)| = 1$. Otherwise

$$|R_h(g)| = \begin{cases} 6, & \text{if } v \neq t \text{ or } v = t \text{ and } v^3 \neq -1 \\ 2, & \text{if } v = t \text{ and } v^3 = -1, \text{ and } v^2 \neq 1. \end{cases}$$

In other words, either $g(x)$ cannot be realized by $h(x)$, or $g(x)$ can be realized by $h(x)$ with either six or two or one realizable pairs.

Proof: According to the assumption, $(a, b) \in R_h(g)$ if and only if

$$\frac{1}{q}\,\hat{h}(a, b)(\lambda) = (-1)^{g(\lambda^s)}$$

for some $s \in \Omega^*$. By the variable change $\beta = \lambda^s$ and replacing β by λ, the above identity is equivalent to the following identity:

$$\frac{1}{q}\,\hat{h}(a, b)(\lambda^c) = (-1)^{g(\lambda)} \tag{15}$$

where $c = s^{-1}$. Substituting (13) into (15), we have

$$\frac{1}{q}\,\hat{h}(v, t)(\lambda) = \frac{1}{q}\,\hat{h}(a, b)(\lambda^c)$$

or equivalently

$$\sum_{x,\, y \in \mathbb{K}} (-1)^{h(\lambda y) + h(y^t x) + h(x^v)} = \sum_{w,\, z \in \mathbb{K}} (-1)^{h(\lambda^c z) + h(z^b w) + h(w^a)}. \tag{16}$$

Let $L = \{x^v, xy^t, y\lambda\}$ and $T = \{w^a, wz^b, z\lambda^c\}$. Thus, $(a, b) \in R_h(g)$ if and only if there is a variable change from (x, y) to (w, z) such that (16) is true. This is equivalent to there being a permutation from T to L. Since $|L| = |T| = 3$, there are six permutations from T to L, which can be represented by the elements of S_3, the group consisting of the permutations of $\{1, 2, 3\}$ (i.e., the symmetric group on three letters). Thus, $|R_h(g)| \leq 6$. In the following, first we compute all elements $R_h(g)$. Then we determine that $|R_h(g)| = 6$ or $|R_h(g)| = 2$ according to the values of v and t. Note that

$$S_3 = \{(1), (23), (12), (123), (13), (132)\}.$$

We will write $L = \{x_1, x_2, x_3\}$ and $T = \{y_1, y_2, y_3\}$. Then for $\tau \in S_3$, $L = \tau(T)$ means that

$$x_i = \tau(y_i) = y_{\tau(i)}, \qquad i = 1, 2, 3.$$

Since $\tau = (1)$ gives $(a, b, c) = (v, t, 1)$, we start with the second element in S_3 in order to determine the values for a, b, and c.

1) $\tau = (23)$. Then $L = (23)T$ gives

$$x^v = w^a \tag{17}$$
$$xy^t = z\lambda^c \tag{18}$$
$$y\lambda = wz^b. \tag{19}$$

From (17) and (18), we have

$$x = w^{av^{-1}} \tag{20}$$

$$y = x^{-t^{-1}} z^{t^{-1}} \lambda^{ct^{-1}} \overset{(20)}{=} w^{-a(vt)^{-1}} z^{t^{-1}} \lambda^{ct^{-1}}, \text{ i.e.,}$$

$$y = w^{-a(vt)^{-1}} z^{t^{-1}} \lambda^{ct^{-1}}. \tag{21}$$

Substituting (21) into (19), we get

$$w^{-a(vt)^{-1}} z^{t^{-1}} \lambda^{ct^{-1}} \lambda = wz^b.$$

Since $v, t, a, b \in \Omega^*$ and w, z, λ are variables taking values in $\mathbb{K}$, it therefore follows that

$$\begin{aligned} -a(vt)^{-1} &= 1 \implies a = -vt \\ t^{-1} &= b \\ ct^{-1} + 1 &= 0 \implies c = -t. \end{aligned}$$

Thus, for the case of $L = (23)T$, we have

$$(a, b, c) = (-vt, t^{-1}, -t). \tag{22}$$

2) $\tau = (12)$. Then $L = (12)T$ provides that

$$x^v = wz^b \tag{23}$$
$$xy^t = w^a \tag{24}$$
$$y\lambda = z\lambda^c. \tag{25}$$

From (23) and (24), we obtain

$$y = w^{-(vt)^{-1} + at^{-1}} z^{b(vt)^{-1}}.$$

Substituting this into (25)

$$\begin{aligned} & w^{-(vt)^{-1} + at^{-1}} z^{-b(vt)^{-1}} \lambda = z\lambda^c \\ \implies & -(vt)^{-1} + at^{-1} = 0,\ -b(vt)^{-1} = 1 \\ & \text{and } c = 1. \end{aligned}$$

Thus, for $L = (12)T$, we have

$$(a, b, c) = (v^{-1}, -vt, 1). \tag{26}$$

3) $\tau = (123)$. From $L = (123)T$, we have

$$x^v = wz^b \tag{27}$$
$$xy^t = z\lambda^c \tag{28}$$
$$y\lambda = w^a. \tag{29}$$

From (26) and (27), it follows that

$$y = w^{-(vt)^{-1}} z^{-b(vt)^{-1} + t^{-1}} \lambda^{ct^{-1}}.$$

Substituting this into (29), we get

$$\begin{aligned} & w^{-(vt)^{-1}} z^{-b(vt)^{-1} + t^{-1}} \lambda^{ct^{-1}} \lambda = w^a \\ \implies & -(vt)^{-1} = a,\ -b(vt)^{-1} + t^{-1} = 0 \\ & \text{and } ct^{-1} + 1 = 0. \end{aligned}$$

Hence, for $L = (123)T$, we have

$$(a, b, c) = (-(vt)^{-1}, v, -t). \tag{30}$$

4) Similarly, we can derive

$$L = (13)T \longrightarrow (a, b, c) = (t^{-1}, v^{-1}, vt) \tag{31}$$

and

$$L = (132)T \longrightarrow (a, b, c) = (t, -(vt)^{-1}, vt). \tag{32}$$

We now group $(v, t, 1)$, (32), and (30) together as follows:

$$\begin{array}{l}(v, t, 1)\\ (t, -(vt)^{-1}, vt)\\ (-(vt)^{-1}, v, -t)\end{array}$$

which gives the following cycle on the realizable pairs:

$$(v, t) \longrightarrow (t, -(vt)^{-1}) \longrightarrow (-(vt)^{-1}, v). \tag{33}$$

From the group of (31), (26), and (22)

$$\begin{array}{l}(t^{-1}, v^{-1}, vt)\\ (v^{-1}, -vt, 1)\\ (-vt, t^{-1}, -t)\end{array}$$

we get the following cycle:

$$(t^{-1}, v^{-1}) \longrightarrow (v^{-1}, -vt) \longrightarrow (-vt, t^{-1}). \tag{34}$$

Thus, if $v \neq t$, it is immediate that $|R_h(g)| = 6$. If $v = t$ and $v^3 \neq -1$, then $v \neq -v^{-2}$. Again, all six realizable pairs are different. Hence, $|R_h(g)| = 6$. If $v = t$ and $v^3 = -1$, then three realizable pairs in the cycle (33) degenerate to (v, v) and the ones in the cycle (34) degenerate to (v^{-1}, v^{-1}). If $v^2 \neq 1$, then (v, v) and (v^{-1}, v^{-1}) are different pairs, so that $|R_h(g)| = 2$. Otherwise, $|R_h(g)| = 1$. ■

From the proof of Theorem 4, we have the following two corollaries.

Corollary 3: With the notation in Theorem 4, let (v, t) be a realizable pair of $h(x)$ with the realization $g(x)$. Let

$$\hat{S}_3 = \{(v, t), (t, -(vt)^{-1}), (-(vt)^{-1}, v), (t^{-1}, v^{-1}), (v^{-1}, -vt), (-vt, t^{-1})\}. \tag{35}$$

Then, all other realizable pairs of $h(x)$ which realize $g(x)$ belong to $\hat{S}_3$. Precisely,

1) If $v \neq t$ or $v = t$ and $v^3 \neq -1$, then $|\hat{S}_3| = 6$. That is, there are exactly six different realizable pairs of $h(x)$ such that the following identities are true:

$$\frac{1}{q}\,\hat{h}(v, t)(\lambda) = (-1)^{g(\lambda)} \tag{36}$$

$$\frac{1}{q}\,\hat{h}(t, -(vt)^{-1})(\lambda) = (-1)^{g(\lambda^{(vt)^{-1}})} \tag{37}$$

$$\frac{1}{q}\,\hat{h}(-(vt)^{-1}, v)(\lambda) = (-1)^{g(\lambda^{-t^{-1}})} \tag{38}$$

$$\frac{1}{q}\,\hat{h}(t^{-1}, v^{-1})(\lambda) = (-1)^{g(\lambda^{(vt)^{-1}})} \tag{39}$$

$$\frac{1}{q}\,\hat{h}(v^{-1}, -vt)(\lambda) = (-1)^{g(\lambda)} \tag{40}$$

$$\frac{1}{q}\,\hat{h}(-vt, t^{-1})(\lambda) = (-1)^{g(\lambda^{-t^{-1}})}. \tag{41}$$

2) If $v = t$ and $v^3 = -1$, and $v^2 \neq 1$, then $|\hat{S}_3| = 2$. That is, there are two and only two different realizable pairs such that

$$\frac{1}{q}\,\hat{h}(v, v)(\lambda) = (-1)^{g(\lambda)} \tag{42}$$

$$\frac{1}{q}\,\hat{h}(v^{-1}, v^{-1})(\lambda) = (-1)^{g(\lambda^{v^{-2}})}. \tag{43}$$

3) If $v = t$ and $v^3 = -1$, and $v^2 = 1$, then $|\hat{S}_3| = 1$. That is, there is only one realizable pair (v, v) which is given as (15).

Corollary 4: Let $R_h(g)$ be defined by (15). Then

$$|R_h(g)| \in \{0, 1, 2, 6\}.$$

Example 2: Let $n = 5$, $h(x) = \mathrm{Tr}(x)$, and

$$g(x) = T3(x) = \mathrm{Tr}(x + x^5 + x^7).$$

Note that for $n = 5$, the quadratic sequence and the three-term sequence are equal and $T3(x)$ is their trace representation. From Example 1, $(3, 3)$ is a realizable pair of $h(x)$ with the realization $T3(x)$. Here we have $v = 3$ and $t = 3$, so that $v = t$. Note that $v^3 = 27 = -1$ and $v^2 = 9 \neq 1$. According to Corollary 3, we only have two different realizable pairs of $h(x)$. Note that $v^{-1} = 11$. Thus, we have the following two identities:

$$\frac{1}{32}\sum_{x, y \in \mathbb{F}_{2^5}} (-1)^{\mathrm{Tr}(\lambda y + y^3 x + x^3)} = (-1)^{T3(\lambda)}$$

$$\frac{1}{32}\sum_{x, y \in \mathbb{F}_{2^5}} (-1)^{\mathrm{Tr}(\lambda y + y^{11} x + x^{11})} = (-1)^{T3(\lambda)}$$

and $|R_{\mathrm{Tr}}(T3)| = 2$.

Example 3: Let $n = 7$ and $h(x) = \mathrm{Tr}(x)$.

Case 1: Let $g(x) = T3(x) = \mathrm{Tr}(x + x^9 + x^{13})$ which is the trace representation of the three-term sequence. By computation, $(3, 3)$ is a realizable pair of $h(x)$ with the realization $T3(x)$. Thus, we have $v = 3$ and $t = 3$. Here $v = t$. But $v^3 = 27 \neq -1$. According to Corollary 3, we have six different realizable pairs of $\mathrm{Tr}(x)$ with the realization $T3(x)$. Note that we have $v^{-1} = 43$. Thus, we have the following six identities:

$$\frac{1}{128}\sum_{x, y \in \mathbb{F}_{2^7}} (-1)^{\mathrm{Tr}(\lambda y + y^3 x + x^3)} = (-1)^{T3(\lambda)}$$

$$\frac{1}{128}\sum_{x, y \in \mathbb{F}_{2^7}} (-1)^{\mathrm{Tr}(\lambda y + y^7 x + x^3)} = (-1)^{T3(\lambda^9)}$$

$$\frac{1}{128}\sum_{x, y \in \mathbb{F}_{2^7}} (-1)^{\mathrm{Tr}(\lambda y + y^3 x + x^7)} = (-1)^{T3(\lambda^{21})}$$

$$\frac{1}{128}\sum_{x, y \in \mathbb{F}_{2^7}} (-1)^{\mathrm{Tr}(\lambda y + y^{43} x + x^{43})} = (-1)^{T3(\lambda^9)}$$

$$\frac{1}{128}\sum_{x, y \in \mathbb{F}_{2^7}} (-1)^{\mathrm{Tr}(\lambda y + y^{55} x + x^{43})} = (-1)^{T3(\lambda)}$$

$$\frac{1}{128}\sum_{x, y \in \mathbb{F}_{2^7}} (-1)^{\mathrm{Tr}(\lambda y + y^{43} x + x^{55})} = (-1)^{T3(\lambda^{21})}$$

and $|R_{\mathrm{Tr}}(T3)| = 6$.

Case 2: Let $g(x) = H(x) = \mathrm{Tr}(x^9 + x^{11} + x^{21})$, the trace representation of one of the Hall sextic residue sequences. $(5, 5)$

is a realizable pair of $h(x)$ and the realization is $H(x)$. Here we have $v=5$ and $t=5$, so that $v=t$. Note that $v^3=125=-1$. According to Corollary 3, we only have two different realizable pairs of $h(x)$. Note that $v^{-1}=27$ and there are only six of these that are shift distinct among the set of decimations of the Hall sextic residue sequences. Thus, we have the following two identities:

$$\frac{1}{128}\sum_{x,\,y\in\mathbb{F}_{2^7}}(-1)^{\mathrm{Tr}(\lambda y+y^5x+x^5)}=(-1)^{H(\lambda)}$$

$$\frac{1}{128}\sum_{x,\,y\in\mathbb{F}_{2^7}}(-1)^{\mathrm{Tr}(\lambda y+y^{27}x+x^{27})}=(-1)^{H(\lambda)}$$

and $|R_{\mathrm{Tr}}(H)|=2$.

Example 4: Let $n=9$, $h(x)=\mathrm{Tr}(x)$, and

$$g(x)=T3(x)=\mathrm{Tr}(x+x^{17}+x^{25})$$

the trace representation of the three-term sequence. $(3,\,11)$ is a realizable pair of $h(x)$ and the realization is $T3(x)$. Thus, we have $v=3$ and $t=11 \Longrightarrow v^{-1}=171$ and $t^{-1}=93$. Since $v\neq t$, according to Corollary 3 we have the following six identities:

$$\frac{1}{512}\sum_{x,\,y\in\mathbb{F}_{2^9}}(-1)^{\mathrm{Tr}(\lambda y+y^{11}x+x^3)}=(-1)^{T3(\lambda)}$$

$$\frac{1}{512}\sum_{x,\,y\in\mathbb{F}_{2^9}}(-1)^{\mathrm{Tr}(\lambda y+y^{15}x+x^{11})}=(-1)^{T3(\lambda^{31})}$$

$$\frac{1}{512}\sum_{x,\,y\in\mathbb{F}_{2^9}}(-1)^{\mathrm{Tr}(\lambda y+y^{3}x+x^{15})}=(-1)^{T3(\lambda^{45})}$$

$$\frac{1}{512}\sum_{x,\,y\in\mathbb{F}_{2^9}}(-1)^{\mathrm{Tr}(\lambda y+y^{171}x+x^{93})}=(-1)^{T3(\lambda^{31})}$$

$$\frac{1}{512}\sum_{x,\,y\in\mathbb{F}_{2^9}}(-1)^{\mathrm{Tr}(\lambda y+y^{239}x+x^{171})}=(-1)^{T3(\lambda)}$$

$$\frac{1}{512}\sum_{x,\,y\in\mathbb{F}_{2^9}}(-1)^{\mathrm{Tr}(\lambda y+y^{93}x+x^{239})}=(-1)^{T3(\lambda^{45})}$$

and $|R_{\mathrm{Tr}}(T3)|=6$.

Next we define an equivalence relation $\sim$ on $\Omega^*\times\Omega^*$ by

$$(a,\,b)\sim(c,\,d)\Longleftrightarrow\quad\text{both}\quad(a,\,b)\quad\text{and}\quad(c,\,d)\in\hat{S}_3.$$

Under this definition, applying Theorem 4, we have the following result.

Theorem 5: If $g(x)$ can be realized by $h(x)$, then up to the equivalence of $\hat{S}_3$, there is exactly one realizable pair of $h(x)$ whose realization is $g(x)$.

Let $\overline{R}_h(g)$ be the set consisting of realizable pairs of $h(x)$ with realization $g(x)$ up to equivalence of $\hat{S}_3$. According to Theorem 5, $|\overline{R}_h(g)|=0$ if $g(x)$ cannot be realized by $h(x)$, or $|\overline{R}_h(g)|=1$ if $g(x)$ can be realized by $h(x)$.

We define

$$N_h(n)=\sum_g|R_h(g)| \tag{44}$$

and

$$\overline{N}_h(n)=\sum_g|\overline{R}_h(g)| \tag{45}$$

where summation is over all g. Then $\overline{N}_h(n)$ represents the number of different classes of two-level autocorrelation sequences realized from $h(x)$.

TABLE I
DISTRIBUTION OF $N_{\mathrm{Tr}}(n)$

n	5	7	9	11	13	15	17
$N_{Tr}(n)$	2	20	18	42	48	30	60
$\overline{N}_{Tr}(n)$	1	4	3	7	8	5	10

For $h(x)=\mathrm{Tr}(x)$, we computed all $R_{\mathrm{Tr}}(g)$ for $n\le 17$. For n even, we have $R_{\mathrm{Tr}}(g)=\emptyset$, so that $N_{\mathrm{Tr}}(n)=0$ and $\overline{N}_{\mathrm{Tr}}(n)=0$, and for n odd, we have the data listed in Table I.

VI. Realizable Pairs of Binary m-Sequences

In this section, we exhibit realizable pairs of binary m-sequences by applying the recent work of Dobbertin and Dillon [3] and Corollary 3.

We use the following notation to represent the known binary two-level autocorrelation sequences (or Hadamard difference sets).

- WG, the trace representation of the Welch–Gong transformation sequences [12].
- $B=B_k$, the trace representation of Dobbertin's Kasami-power-function construction sequences [3] for $(k,\,n)=1$, where for $k=2^{-1} \bmod n$ it gives the three-term sequences [12] and for $k=3^{-1} \bmod n$, the five-term sequences [12].
- $G=G_i,\ i=1,\,2$ represent the hyperoval sequences of Glynn types I and II [11]. (Note that the Segre hyperoval sequences are sequences in B_2.)
- H, the Hall sextic residue sequences.
- QR, the quadratic residue sequences.

According to [3] (1999) of Dobbertin and Dillon and the definition of the second-order DHT, we directly have the following lemma.

Lemma 8: Let $\underline{\boldsymbol{a}}=\{a_i\}$ be an m-sequence whose elements are given by $a_i=\mathrm{Tr}(\alpha^i)$, $i=0,\,1,\,\ldots,$ where α is a primitive element of $\mathbb{F}_{2^n}$, and let $n=2m+1$ and $\sigma=2^{m+1}$. Then

1) $\frac{1}{q}\widehat{\mathrm{Tr}}(3,\,\frac{2^k+1}{3})(x)=(-1)^{B(x^{2^k+1})}$, for $(k,\,n)=1$.
   In other words, $(3,\,\frac{2^k+1}{3})$ is a realizable pair of $\underline{\boldsymbol{a}}$ and the realization is the (2^k+1)-decimation of the sequence B_k defined in [3].
2) $\frac{1}{q}\widehat{\mathrm{Tr}}(k,\,\frac{k-1}{k})(x)=(-1)^{G(x)}$, where $k=\sigma+\gamma$ where $4\gamma\equiv 1 \bmod n$ for Glynn I and $k=3\sigma+4$ for Glynn II. That is, $(k,\,\frac{k-1}{k})$ is a realizable pair of $\underline{\boldsymbol{a}}$ and the realization is the Glynn I or II sequences.
3) $\frac{1}{q}\widehat{\mathrm{Tr}}(2^k+1,\,d^{-1})(x)=(-1)^{WG(x)}$,
   where $d=2^{2k}-2^k+1$ for $3k\equiv 1 \bmod n$.
   That is, $(2^k+1,\,d^{-1})$ is a realizable pair of $\underline{\boldsymbol{a}}$ and the realization is the Welch–Gong (WG) sequences.

Theorem 6: With the same notation, let

$$\Gamma(n)=\{B_k,G_1,G_2,WG|1<k<n/2\text{ and }(k,n)=1\}. \tag{46}$$

For $n > 5$

$$|R_{\mathrm{Tr}}(g)| = 6, \qquad \forall g \in \Gamma(n).$$

In other words, every sequence in $\Gamma(n)$ can be realized by an m-sequence of period $2^n - 1$, and there are exactly six realizable pairs for each class in Γ.

Proof: According to Lemma 8, we have

$$\left(3, \frac{2^k+1}{3}\right) \in R_{\mathrm{Tr}}(B_k), \qquad (k, n) = 1 \tag{47}$$

$$\left(k, \frac{k-1}{k}\right) \in R_{\mathrm{Tr}}(G_j), \qquad j = 1, 2 \tag{48}$$

$$(2^k + 1, d^{-1}) \in R_{\mathrm{Tr}}(WG). \tag{49}$$

According to Theorem 4, we only need to show that

$$v^3 \not\equiv -1$$

where $v = 3$ in (47), $v = k$ in (48), and $v = 2^k + 1$ in (49).

Case 1: $v = 3$ in (47). Since $v^3 = 27 \not\equiv -1$‘, $\bmod 2^n - 1$ for $n > 5$, applying Theorem 4, $|R_{\mathrm{Tr}}(B_k)| = 6$.

Case 2: $v = k$ in (48). Let r be an integer and let $w(r)$ represent the Hamming weight of r, i.e., the number of nonzero coefficients in the binary representation of r. For G_1, we have

$$k = 2^{m+1} + 2^{il} \begin{cases} \text{where} \quad i = 1 & \text{if} \quad n = 4l - 1 \\ \text{where} \quad i = 3 & \text{if} \quad n = 4l + 1. \end{cases}$$

Thus

$$\begin{aligned} k^3 &= (2^{m+1} + 2^{il})^3 \\ &= 2^{3(m+1)} + 3 \cdot 2^{2(m+1)} 2^{il} + 3 \cdot 2^{m+1} 2^{2il} + 1 \\ &\equiv 2^{m+2} + 3 \cdot 2^{1+il} + 3 \cdot 2^{m+1+2il} + 1 \\ &= r \bmod 2^n - 1. \end{aligned}$$

Thus, $w(r) \le 6$. Since $-1 \equiv 2^{n-1} - 1 (\bmod 2^n - 1)$ and $w(2^{n-1} - 1) = n - 1$, then $r \ne 2^n - 1$ when $n > 7$. Thus, $|R_{\mathrm{Tr}}(G_i)| = 6$, $i = 1, 2$ for $n > 7$. For $n = 7$, the Glynn I and II degenerate to the thrree-term sequence and the five-term sequence, respectively. According to Case 1, the result is true.

Case 3: $v = 2^k + 1$ in (49). Note that k is a solution of $3x \equiv 1 \bmod n$. Then

$$\begin{aligned} v^3 &= (2^k + 1)^3 = 2^{3k} + 3 \cdot 2^{2k} + 3 \cdot 2^k + 1 \\ &\equiv 1 + 3 \cdot 2^{2k} + 3 \cdot 2^k + 1 = r. \end{aligned}$$

Thus, $w(r) = 5$. Since $n > 5$, the smallest integer n that has WG sequences is 7. But $-1 = 2^{n-1} - 1$ and $w(2^{n-1} - 1) = n - 1 > 5$. Thus, $v^3 \not\equiv -1$. According to Theorem 4, we have $|R_{\mathrm{Tr}}(WG)| = 6$. ■

Note: We have

$$|\Gamma(n)| = \left(\frac{\phi(n)}{2} - 1\right) + 2 + \delta \tag{50}$$

where $\phi(x)$ is the Euler function, $\frac{\phi(n)}{2} - 1$ represents the number of equivalence classes of B_k, 2 represents two Glynn types sequences, and $\delta = 0$ if $n \equiv 0 \bmod 3$ and otherwise $\delta = 1$, which represents the class of the WG transformation sequences.

$$\begin{tikzcd} & \mathrm{K} \arrow[dl, "\mathrm{Tr}(x^s)"'] \arrow[dd, "f(x)"] \\ \mathrm{E} \arrow[dr, "d(x)"'] & \\ & \mathrm{F} \end{tikzcd}$$

Fig. 1. Commutative diagram for subfield factorization.

VII. Experimental Results

In this section, we present our experimental results on the realization of m-sequences. First, we give the definition of subfield factorization of the sequences (or functions).

Definition 7 (Subfield Factorization of Functions From $\mathbb{K}$ to $\mathbb{F}$): Let $\underline{\boldsymbol{a}} = \{a_k\}$ be a sequence over $\mathbb{F}$ of period $q - 1$ and $f(x)$ be its trace representation function where $\underline{\boldsymbol{a}}$ is not an m-sequence or, equivalently, there is no $s \in \Omega^*$ such that $f(x) = \mathrm{Tr}(x^s)$. If there is $m > 1$, a proper factor of n, and a function $d(x)$ from $\mathbb{E} = \mathbb{F}_{p^m}$ to $\mathbb{F}$ such that $f(x)$ can be decomposed into a composition of $d(x)$ and the Gordon–Mills–Welch (GMW) function $\mathrm{Tr}_m^n(x^s)$, i.e.,

$$f(x) = d(x) \circ \mathrm{Tr}_m^n(x^s), \tag{51}$$

then we say that $f(x)$ or $\underline{\boldsymbol{a}}$ is *reducible* (with respect to the subfield chain: $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$), (51) is called *a subfield factorization* of $f(x)$ or $\underline{\boldsymbol{a}}$, and $\mathrm{Tr}_m^n(x^s)$ is called a *GMW factor* of $f(x)$ or $\underline{\boldsymbol{a}}$. Otherwise, $f(x)$ or $\underline{\boldsymbol{a}}$ is said to be *irreducible*.

In other words, if the commutative diagram of Fig. 1 exists, where $1 < m < n$, then $f(x)$ or $\underline{\boldsymbol{a}}$ is reducible.

For example, GMW sequences (including cascaded GMW sequences or generalized GMW sequences) are reducible.

Remark 8: All sequences listed in $\Gamma(n)$, defined in (46), are irreducible two-level autocorrelation sequences. (We will give a proof for this result in a separate paper.)

Let $\overline{R}_h(n)$ be the set consisting of all realizable pairs from $h(x)$ up to $\hat{S}_3$. Note that $|\overline{R}_h(n)| = \overline{N}_h(n)$ where $\overline{N}_h(n)$ is defined by (45) in Section V. We did a complete computation of $\widehat{\mathrm{Tr}}(v, t)(x)$, $(v, t) \in \Omega^* \times \Omega^*$ for $n \le 17$. No previously unknown examples were found by the second-order SDHT process for any $n \le 17$. That is, we have the following experimental result:

$$R_{\mathrm{Tr}} = \emptyset, \qquad \text{for all even } n \le 17$$

and

$$\text{Realization of } R_{\mathrm{Tr}} = \Gamma(n), \qquad \text{for all odd } n \le 17.$$

This is supporting evidence (albeit weak) for the conjecture 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.

Remark 9: For the case of $n = 19$, we have now completed only a partial computation of $\widehat{\mathrm{Tr}}(v, t)(x)$. It is expected that the whole computation will be computed in the near future.

TABLE II
ALL REALIZABLE PAIRS FOR $n \leq 13$

n	r	$\lvert\Omega^+\rvert$	$\lvert\Omega^*\rvert$	Defining Polynomial of $\mathbb{F}_{2^n}$	$\overline{N}_{Tr}(n)$	(v,t)	$\frac{1}{q}\widehat{Tr}(v,t)$	Dim	Class
5	31	6	6	x^5+x^3+1	1	(3, 3)	1, 5, 7	3	$T3 = QR$
7	127	18	18	x^7+x+1	4	(3, 3)	1, 9, 13	3	$T3 = G_1$
						(11, 19)	1, 5, 13, 21, 29	5	$T5 = G_2 = B_2$
						(27, 9)	1, 3, 7, 19, 29	5	WG
						(5, 5)	9, 11, 21	3	H
					1	$(3,3)^*_H$	1, 9, 81, 94, 84, 121, 73, 22, 71	9	QR
9	511	58	48	x^9+x^4+1	3	(3, 11)	1, 17 , 25	3	T3
						(3, 43)	1, 5, 7, 9 , 19 , 25, 37, 77, 117	9	B_2
						(5, 25)	1, 5, 9 , 13 , 19, 37 , 43	7	$G_1 = G_2$
11	2047	186	176	$x^{11}+x^2+1$	7	(3, 11)	1, 33, 49	3	T3
						(3, 43)	3, 5, 17, 73, 141,	5	T5
						(7, 17)	21, 23, 29, 35, 37, 41 , 71 , 89, 139, 165, 213, 307, 415	13	WG
						(171, 307)	1 , 5, 13, 21, 53 , 77, 85, 205, 213, 309, 333, 341, 413, 423, 469	15	B_2
						(3, 3)	1, 5, 7, 9 , 19 , 25, 81, 169 , 295	9	B_3
						(9, 25)	1, 5, 9 , 13 , 19 , 37 , 43 , 67 , 69 , 137, 163, 211, 293	13	G_1
						(11, 47)	1, 5, 13, 17, 29, 37, 49, 61, 69, 81, 93, 101, 113, 125, 139, 147, 151, 157, 171, 173, 183	21	G_2
13	8191	630	630	$x^{13}+x^4+x^3+x+1$	8	(3, 43)	1, 65 , 97	3	T3
						(3, 171)	3, 17, 65, 265, 401	5	T5
						(17, 171)	1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 67, 133, 135, 265, 267, 269, 271, 305, 337, 369, 401, 433, 465, 497	29	WG
						(3, 683)	1, 5, 7, 9, 19, 25, 37, 65, 67, 77, 81, 97, 105, 117, 137, 147, 157, 167, 265, 329, 339, 425, 597, 1237, 1877	25	B_2
						(3, 3)	1 , 9, 13, 17, 35, 81, 265, 553, 841	9	B_3
						(11, 1179)	1, 33, 265, 287, 295, 297, 745, 809, 869, 933, 997, 1181, 1189, 1245, 1253	15	B_5
						(9, 113)	11, 19, 21, 33, 39, 41, 65, 81, 89, 101, 105, 133, 135, 137, 149, 155, 197, 269, 273, 327, 423, 465, 1173	23	G_1
						(21, 97)	1 , 5, 9, 17, 21, 33, 37, 41, 49, 51, 53, 67, 75, 83, 133, 137, 145, 149, 163, 171, 229, 231, 233, 309, 393, 397, 401, 423, 489, 553, 569, 591, 661, 665, 749, 943, 1203	37	G_2

TABLE III
ALL REALIZABLE PAIRS FOR $n = 15$

$r = 32767, |\Omega^+| = 2190, |\Omega^*| = 1800, \mathbb{F}_{2^{15}} : x^{15}+x+1$ and $\overline{N}_{Tr}(n) = 5$

(v,t)	$\frac{1}{q}\widehat{Tr}(v,t)$	Dim	Class
(3, 43)	1, 129, 193	3	T3
(3, 2731)	3, 5, 9, 17, 19, 25, 29, 33, 39, 65, 73, 83, 105, 129, 149, 259, 289, 265, 269, 289, 309, 337, 389, 425, 449, 469, 549, 579, 589, 609, 629, 649, 659, 669, 679, 1065, 1353, 1363, 1705, 2389, 4949, 7509	41	B_2
(3, 683)	1, 9, 13, 17, 35, 81, 289, 1169, 2189	9	B_4
(17, 113)	11, 19, 21, 33, 39, 41, 65, 81, 89, 101, 105, 129, 133, 135, 137, 149, 155, 197, 269, 273, 321, 327, 417, 423, 449, 465, 541, 545, 553, 561, 779, 901, 1061, 1093, 1095, 1219, 1315, 1329, 1353, 1637, 1671, 1863, 2189, 2709, 2851	45	G_1
(43, 191)	43, 45, 53, 85, 129, 131, 133, 135, 139, 143, 149, 151, 159, 265, 297, 299, 307, 339, 425, 429, 445, 509, 553, 561, 593, 643, 651, 659, 667, 679, 785, 805, 809, 811, 817, 827, 1065, 1069, 1081, 1101, 1105, 1113, 1145, 1159, 1161, 1169, 1175, 1177, 1187, 1323, 1355, 1443, 1445, 1461, 1525, 1573, 1589, 1781, 1829, 1833, 1845, 2191, 2195, 2203, 2207, 2329, 2339, 2345, 2457, 2461, 2477, 2541, 2699, 2711, 2715, 2853, 2859, 3177, 3225, 3305, 3369, 3371, 3475, 3817, 3881, 5419, 5589, 5845, 6869	89	G_2

In the accompanying three tables, we list the realizations which give irreducible two-level autocorrelation sequences for odd n with $n \leq 17$ where Table II lists the result for $n = 3, 5, 7, 9, 11$, and 13, and Tables III and IV for $n = 15$ and $n = 17$, respectively. We keep the same notations: B_k, G_i, WG, H, and QR as defined in Section V. But here we would like to separate the three-term sequences and the five-term sequences from B_k because of the following special properties that they have. We will denote the trace representations of three-term sequences and five-term sequences by $T3(x)$ and $T5(x)$, respectively. Let $n = 2m+1$.

Proposition 3: We can write

$$T3(x) = \mathrm{Tr}(u(x)), \qquad \text{where } u(x) = x + x^r + x^{r^{-1}}$$

where $u(x) = x + x^r + x^{r^{-1}}$ where $r = 2^{m+1} + 1$ and

$$T5(x) = \mathrm{Tr}(c(x))$$

TABLE IV
ALL REALIZABLE PAIRS FOR $n = 17$
$r = 131071, |\Omega^+| = 7710, |\Omega^*| = 7710, \mathbb{F}_{2^{17}} : x^{17} + x^3 + 1$, and $\overline{N}_{Tr}(n) = 10$

(v, t)	$\frac{1}{q}\widehat{Tr}(v, t)$	Dim	Class
(3, 171)	1 , 257, 385	3	T3
(3, 683)	3, 17, 65, 1057, 2097	5	T5
(31, 65)	93, 479, 503, 527, 551, 913, 1247, 1259, 1319, 1331, 1631, 1637, 1715, 1721, 1823, 1913, 2473, 2973, 3021, 3165, 3213, 3253, 3643, 4315, 4405, 4509, 4533, 4749, 4773, 4777, 5277, 5289, 5521, 5541, 5553, 5661, 5667, 5937, 7003, 7051, 7387, 8979, 8995, 9307, 9319, 9781, 9973, 10539, 11033, 11081, 11609, 12759, 15063, 15831, 19093, 20053, 21203, 21293, 24275, 29647, 31231	61	WG
(3, 10923)	1, 5, 7, 9, 19, 25, 37, 65, 67, 77, 81, 97, 105, 117, 129, 137, 147, 157, 167, 259, 265, 289, 329, 339, 385, 425, 517, 577, 597, 1037, 1041, 1057, 1065, 1077, 1157, 1217, 1237, 1361, 1545, 1557, 1705, 1797, 1857, 1877, 2087, 2197, 2317, 2337, 2357, 2437, 2517, 2597, 2627, 2637, 2657, 2677, 2697, 2707, 2717, 2727, 4265, 5449, 5459, 6825, 9557 19797 30037	67	B_2
(3, 3)	1, 5, 7, 9, 19, 25, 81, 133, 169, 257, 259, 277, 295, 313, 385, 457, 545, 581, 657, 1033, 1171, 1609, 5265, 10825, 18727	25	B_3
(3, 2731)	1, 17, 25, 33, 67, 289, 1089, 4241, 6417	9	B_4
(3, 11)	3, 5, 9, 17, 19, 25, 29, 33, 39, 65, 73, 83, 105, 257, 273, 293, 337, 537, 547, 801, 1041, 1089, 1121, 2085, 2115, 2217, 2593, 3233, 4233, 4243, 4253, 4263, 4329, 4497, 4517, 4761, 4771, 6441, 8741 12965, 21149	41	B_5
(3, 43)	3, 5, 17, 33, 129, 521, 577, 1037, 1065, 1093, 1121, 1553, 2081, 5193, 9321	15	B_7
(17, 481)	1, 5, 13, 17, 29, 33, 45, 49, 61, 67, 71, 75, 77, 81, 85, 87, 145, 163, 177, 201, 225, 259, 265, 267, 271, 337, 385, 405, 433, 457, 529, 547, 553, 565, 571, 643, 651, 655, 661, 773, 835, 841, 931, 1033, 1039, 1041, 1047, 1129, 1177, 1419, 1549, 1611, 1617, 1623, 1713, 1803, 2081, 2085, 2091, 2179, 2185, 2191, 2309, 2357, 2371, 2381, 2575, 2765, 2849, 3101, 3139, 3337, 3343, 3721, 3727, 3907, 4229, 4233, 4281, 4433, 4677, 5769, 8777, 8793, 8873 10797 13465	87	G_1
(85, 385)	1, 5, 9, 17, 21, 33, 37, 41, 65, 69, 73, 81, 85, 129, 133, 137, 145, 149, 161, 165, 169, 193, 195, 197, 201, 203, 209, 211, 213, 259, 267, 275, 291, 299, 323, 331, 339, 517, 521, 529, 533, 545, 549, 553, 577, 581, 585, 593, 597, 643, 651, 659, 675, 683, 901, 903, 905, 913, 917, 919, 929, 933, 935, 937, 1221, 1229, 1237, 1545, 1549, 1553, 1569, 1577, 1581, 1601, 1609, 1613, 1617, 1671, 1687, 1703, 1929, 1945, 1961, 2089, 2121, 2137, 2185, 2201, 2217, 2249, 2255, 2265, 2319, 2351, 2383, 2577, 2581, 2585, 2593, 2597, 2629, 2641, 2645, 2649, 2957, 2961, 2969, 2977, 2989, 3601, 3633, 3665, 3727, 3759, 3989, 3997, 4005, 4241, 4253, 4273, 4305, 4307, 4317, 4371, 4403, 4435, 4649, 4657, 4681, 4755, 4787, 5023, 5033, 5041, 5333, 5657, 5681, 5721, 6693, 6709, 6725, 7069, 7721, 7737, 7753, 7839, 8101, 8741, 8805, 8867, 8891, 9125, 9127, 9445, 9789,, 9895, 10153, 10409, 10473, 10559, 10837, 10853, 12213, 12873, 12905, 13881, 15293, 15945, 16063, 18767, 19405, 20175, 21203	173	G_2

where $c(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}$. (For the values of q_i, see [12]). Then $u(x)$ is an involution, i.e., $u^2(x) = x$ ($u^2(x)$ represents the composition of u and itself), and the five-term sequences and WG sequences are related by $WG(x) = \mathrm{Tr}(c(x+1)+1)$.

The result on $T3$ is proved in [1] and the result on $T5$ in [12]. Note that except for three-term sequences, only m-sequences have the involution property.

In Tables II–IV, in the column under the title $\frac{1}{q}\widehat{\mathrm{Tr}}(v, t)$, we list the set of exponents of all trace terms appearing in the realization $g(x)$. (Note that the set of exponents of all trace terms appearing in $g(x)$ is said to be the *null spectrum* of $g(x)$.) We use Dim to represent the number of terms in $g(x)$. For each class, we only list one realizable pair and the trace representation of the corresponding realization. For the rest of the six pairs (or two pairs) and the trace representations, one can compute these by applying Corollary 3.

For example, in Table I, the third row in the frame for $n = 7$ means that when $n = 7$, then the five-term sequences, $T5$, Glynn type II hyperoval sequences G_2 and Segre hyperoval sequences B_2 are the same, i.e.,

$$g(x) = T_5(x) = G_2(x) = B_2(x) = \mathrm{Tr}(x + x^5 + x^{13} + x^{21} + x^{29})$$

which is obtained by the realizable pair $(11,\,19)$. In other words, we have

$$\frac{1}{128}\,\widehat{\mathrm{Tr}}(11,\,19)(\lambda)=(-1)^{g(\lambda)}$$

or equivalently

$$\frac{1}{128}\sum_{x,\,y\in GF(2^7)}(-1)^{\mathrm{Tr}(\lambda y+y^{19}x+x^{11})} = (-1)^{\mathrm{Tr}(\lambda+\lambda^{5}+\lambda^{13}+\lambda^{21}+\lambda^{29})}.$$

Note: For the case of $n=7$ in Table I, $(3,\,3)_H$ means that it is a realizable pair of $H(x)=\mathrm{Tr}(x+x^{19}+x^{47})$, the trace representation of one sequence in the class of the Hall sextic residue sequences. In other words, we have

$$\frac{1}{128}\,\hat{H}(3,\,3)(\lambda)=(-1)^{QR(\lambda)}.$$

REFERENCES

[1] A. Chang, P. Gaal, S. W. Golomb, G. Gong, T. Helleseth, and P. V. Kumar, “On a conjectured ideal autocorrelation sequence and a related triple error correcting cyclic code,” *IEEE Trans. Inform. Theory*, vol. 46, pp. 680–686, Mar. 2000.

[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,” preprint, Aug. 12, 1999.

[4] P. Gaal and S. W. Golomb, “Exhaustive determination of (1023, 511, 255)-cyclic difference sets,” *Math. Comp.*, vol. 70, no. 233, pp. 357–366, Mar. 2000.

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

[6] G. Gong and S. W. Golomb, “Hadamard transforms of three term sequences,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 2059–2060, Sept. 1999.

[7] G. Gong, *Sequence Analysis*. Waterloo, ON, Canada: Univ. Waterloo, Lecture Notes for Course CO739x, ch. 5. Online. Available: http://www.cacr.math.uwaterloo.ca/~ggong.

[8] G. Gong and S. W. Golomb, “Binary sequences with two-level autocorrelation,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 692–693, Mar. 1999.

[9] ——, “Transform domain analysis of DES,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 2065–2073, Sept. 1999.

[10] I. G. MacDonald, *Symmetric Functions and Hall Polynomials*. Oxford, U.K.: Oxford Sci. Publ., 1995.

[11] A. Maschietti, “Difference sets and hyperovals,” *Des., Codes, Cryptogr.*, vol. 14, pp. 89–98, 1998.

[12] 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.

[13] 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.

[14] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Boston, MA: Kluwer, 1987.

[15] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1991.

[16] R. J. Turyn, “Character sums and difference sets,” *Pacific J. Math.*, vol. 15, no. 1, pp. 319–346, 1965.