Realizations of Decimation Hadamard Transform for Special Classes of Binary Sequences with Two-level Autocorrelation

Nam Yul Yu and Guang Gong

Abstract

In an effort to search for a new binary two-level autocorrelation sequence, the decimation-Hadamard transform (DHT) based on special classes of known binary sequences with two-level autocorrelation is investigated. It is theoretically proved that some realizations of a binary generalized Gordon-Mills-Welch (GMW) sequence can be predicted from the structure of subfield factorization and the realization in its subfield. Furthermore, it is shown that the realization of any binary two-level autocorrelation sequence with respect to a quadratic residue (QR) sequence is either a QR sequence or the sequence itself.

I. Introduction

Recently, Gong and Golomb developed a new method to study and search for two-level autocorrelation sequences for both binary and non-binary cases [1]. This method is iteratively to apply two operations: decimation and the Hadamard transform based on general orthogonal functions, referred to as the *decimation-Hadamard transform (DHT)*. Basically, it was inspired from Dillon and Dobbertin's work [2] where the Hadamard transform was firstly used for the analysis of a new two-level autocorrelation sequence. The r-th order iterative DHT can transform one class of such sequences into another inequivalent class of such sequences, a process called *realization*. Using the second order iterative DHT and starting with a single binary m-sequence, Gong and Golomb verified that one can obtain all the known two-level autocorrelation sequences of period $2^n - 1$ which have no subfield factorization for odd $n \leq 17$ [1]. Applying the second order iterative DHT to ternary two-level autocorrelation sequences, Ludkovski and Gong discovered several new classes of ternary two-level autocorrelation sequences [3]. In [4], Gong, Dai and Golomb further investigated higher order DHT, and showed that realizations only occur for even order of DHT. They also presented an example of realizations of the GMW sequences.

In this paper, realizations of binary generalized GMW sequences and quadratic residue sequences are investigated. At first, the second order DHT of the binary generalized Gordon-Mills-Welch (GMW) sequences of period $2^n - 1$ and the relation between the subfield factorization and the realization by the second order DHT are investigated. Consequently, it is theoretically shown that some realizations of a binary generalized GMW sequence corresponding to an orthogonal function in a finite field can be predicted by the realization of its subfield component function in its subfield.

In addition, results on the second order DHT of quadratic residue (QR) sequences are provided. Using special properties of a QR sequence, the realization of any binary two-level autocorrelation sequence with respect to a QR sequence by the second order DHT is discussed. It is shown that a valid realization of any binary two-level autocorrelation sequence with respect to a QR sequence is either a self-realization or a QR sequence.

This paper is organized as follows. In Section II, we give some preliminary reviews of concepts and notations on sequences that we will use in this paper. In Section III, realizations of the binary generalized GMW sequences by the second order DHT are investigated. Mathematical proofs and experimental results are provided. In Section IV, realizations of any binary two-level autocorrelation sequence based on a QR sequence are investigated. In Section V, concluding remarks are given.

II. PRELIMINARIES

In this section, we present some preliminary reviews on concepts and notations about sequences that we will frequently use in this paper. The following notation will be used throughout this paper.

- $\mathbb{Z}$ represents the integer ring.
- n is a positive integer and $q = 2^n$.
- $\mathbb{F}_Q = GF(Q)$, the finite field with Q elements, $\mathbb{F}_Q^*$, the multiplication group of $\mathbb{F}_Q$.
- $\mathbb{Z}_m$ is the ring of integers modulo m and $\mathbb{Z}_m^* = \{r \in \mathbb{Z}_m | r \neq 0\}$.
- Let $m|n$. The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is denoted by $Tr_m^n(x)$, i.e.,

$$Tr_m^n(x) = x + x^{2^m} + \cdots + x^{2^{m(\frac{n}{m}-1)}}, x \in \mathbb{F}_{2^n},$$

  or simlply as $Tr(x)$ if $m = 1$ and context is clear.

A. Correspondence between Periodic Sequences and Functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

Let $\mathcal{S}$ be the set of all binary sequences with period $t|(2^n-1)$ and $\mathcal{F}$ be the set of all functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For any function $f(x) \in \mathcal{F}$, $f(x)$ can be represented as

$$f(x) = \sum_{i=1}^{r} Tr_1^{n_i}(A_i x^{t_i}), \quad A_i \in \mathbb{F}(2^{n_i}) \tag{1}$$

where t_i is a coset leader of a cyclotomic coset modulo $2^{n_i}-1$, and $n_i|n$ is the size of the cyclotomic coset containing t_i. For any sequence $\underline{\mathbf{a}} = \{a_i\} \in \mathcal{S}$, there exists $f(x) \in \mathcal{F}$ such that

$$a_i = f(\alpha^i), \quad i = 0, 1, \cdots,$$

where α is a primitive element of $\mathbb{F}_{2^n}$. Then, $f(x)$ is called a *trace representation* of $\underline{\mathbf{a}}$. ($\underline{\mathbf{a}}$ is also referred to as an r-term sequence.) If $f(x)$ is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, by evaluating $f(\alpha^i)$, we get a binary sequence with period dividing 2^n-1. We use the notation:

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

to represent the one-to-one correspondence between $\mathcal{F}$ and $\mathcal{S}$ through the trace representation (1).

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

$$a_i = Tr_1^n(\beta\alpha^i), \quad i = 0, 1, \cdots, \beta \in \mathbb{F}_{2^n}^*,$$

then $\underline{\mathbf{a}}$ is a binary m-sequence of period 2^n-1 of degree n. (For a detailed treatment of the trace representation of sequences, see [5] and [6].)

B. Decimation of Periodic Sequences

Let $\underline{\mathbf{a}}$ be a binary sequence of period $t|(2^n-1)$ and let $f(x)$ be the trace representation of $\underline{\mathbf{a}}$. Let $0 < s < t$. Then a sequence $\underline{\mathbf{b}} = \{b_i\}$ whose elements are given by

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

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

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

For example,

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

where $Tr(x)$ is the trace function from $\mathbb{F}_{2^s}$ to $\mathbb{F}_2$. If $\underline{\mathbf{a}}$ is an m-sequence of period 2^n-1 and $(s, p^n-1) = 1$, then $\underline{\mathbf{a}}^{(s)}$, the s-decimation of $\underline{\mathbf{a}}$, is also an m-sequence.

C. Autocorrelation

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

$$C_{\underline{\mathbf{a}}}(\tau) = \sum_{i=0}^{t-1} (-1)^{a_{i+\tau}+a_i}, \quad 0 \le \tau \le t-1. \tag{2}$$

where τ is a phase shift of the sequence $\underline{\mathbf{a}}$ and the indices are computed modulo t, the period of $\underline{\mathbf{a}}$. If $\underline{\mathbf{a}}$ has a period $2^n - 1$ and

$$C_{\underline{\mathbf{a}}}(\tau) = \begin{cases} -1, & \text{if } \tau \not\equiv 0 \bmod 2^n-1 \\ 2^n-1, & \text{if } \tau \equiv 0 \bmod 2^n-1, \end{cases}$$

then we say that the sequence $\underline{\mathbf{a}}$ has an *(ideal) 2-level autocorrelation function.*

D. Hadamard Transform and the Inverse Transform

Let $f(x)$ be a polynomial function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. With a trace function $Tr(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, the Hadamard transform of $f(x)$ is defined by

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

The inverse formula is given by

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

E. Orthogonal Function

Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ with $f(0) = 0$. If

$$C_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(\lambda x))+f(x)} = \begin{cases} 0, & \text{if } \lambda \neq 1 \\ 2^n, & \text{if } \lambda = 1 \end{cases}$$

for $\lambda \in \mathbb{F}_{2^n}$, then we say that $f(x)$ is *orthogonal over* $\mathbb{F}$. Orthogonal function is a trace representation of a two-level autocorrelation sequence [1]. If $f(x)$ is a trace representation of $\underline{\mathbf{a}}$ and autocorrelation function of $\underline{\mathbf{a}}$ defined in (2) is $C_{\underline{\mathbf{a}}}$, then

$$C_{\underline{\mathbf{a}}}(\tau) = -1 + C_f(\lambda),$$

where $\lambda = \alpha^\tau \in \mathbb{F}_{2^n}^*$.

F. Decimation-Hadmard Transform (DHT)

Let $u(x)$ be orthogonal over $\mathbb{F}_2$ and $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For an integer $v \in \mathbb{Z}_{q-1}^*$, we define

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

Then, $\widehat{f}_u(v)(\lambda)$ is called *the first-order decimation-Hadamard transform (DHT) of* $f(x)$ *with respect to* $u(x)$, the first order DHT for short. With this notation, let $t \in \mathbb{Z}_{q-1}^*$. Then,

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

is called the *second order decimation-Hadamard transform of* $f(x)$ *(with respect to* $u(x)$*), the second order DHT* for short. In DHT, the Hadamard transform is generalized by the use of the orthogonal function $u(x)$ instead of $Tr(x)$.

If $\widehat{f}_u(v,t)(\lambda) \in \{\pm 2^n\}$ for all λ in $\mathbb{F}_{2^n}$, the function $c(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ determined by

$$(-1)^{c(\lambda)} = \frac{1}{2^n} \widehat{f}_u(v,t)(\lambda), \tag{3}$$

is called a *realization* of $f(x)$ with respect to $u(x)$, and (v,t) is called a *realizable pair* [1].

III. Realizations on Binary Generalized GMW Sequences

In this section, the decimation-Hadamard transform based on the binary generalized Gordon-Mills-Welch (GMW) sequences is investigated.

Let n be a composite integer, m a proper factor of n, and $h(x)$ an orthogonal function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For k with $gcd(k, 2^n - 1) = 1$, a generalized GMW sequence $\underline{\mathbf{a}} = \{a_i\}$ is defined by an evaluation of $f(x)$ at α^i [6], where α is a primitive elements in $\mathbb{F}_{2^n}$, and $f(x)$ is given by

$$f(x) = h(x) \circ Tr_m^n(x^k).$$

Here, $f(x)$ is an orthogonal function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In particular, if $h(x) = Tr_m^n(x^v)$ for v with $gcd(v, 2^m - 1) = 1$ and $v \neq 1$, then an evaluation of $f(x)$ is a GMW sequence [7] [8]. For more details of GMW sequences, see [9], [10], and [11]. It is noted that the generalized GMW sequence is defined by the extension of one orthogonal function $h(x)$ from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ to another orthogonal function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by the composition with a trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

For orthogonal functions $h(x), e(x)$ and $g(x)$ from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, let $g(x)$ be a realization of $h(x)$ with respect to $e(x)$ by the second order DHT in $\mathbb{F}_{2^m}$. Also, the extension of each orthogonal function can be considered by the composition with trace functions as follows.

$$\begin{aligned} f(x) &= h(x^v) \circ Tr_m^n(x) \\ u(x) &= e(x) \circ Tr_m^n(x) \\ c(x) &= g(x) \circ Tr_m^n(x), \end{aligned} \tag{4}$$

where v is a decimation factor in $\mathbb{Z}_{2^m-1}^*$ of $gcd(v, 2^m - 1) = 1$. Just as $g(x)$ is a realization of $h(x)$ with respect to $e(x)$ in the subfield $\mathbb{F}_{2^m}$, $c(x)$ can be a realization of $f(x)$ with respect to $u(x)$ in the extension field $\mathbb{F}_{2^n}$. Before proving this result, we extend the realization and its realizable pairs given by (3).

If $g(x)$ is a realization of $h(x)$ with respect to $e(x)$ by the second order DHT in $\mathbb{F}_{2^m}$, then

$$\begin{aligned} (-1)^{g(\mu^c)} &= \frac{1}{2^m} \cdot \widehat{h}_e(a,b)(\mu) \\ &= \frac{1}{2^m} \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{e(\mu y) + e(y^b x) + h(x^a)}, \end{aligned}$$

for $\mu \in \mathbb{F}_{2^m}$. In this realization, (a, b) is called a *realizable pair* of $h(x)$ with respect to $e(x)$ [1]. In this paper, we also use a triple (a, b, c) to indicate the realization including the decimation value of $g(x)$. From now on, the triple is called a *realizable triple.*

For (a, b, c) realizable triple, we consider the following Lemma.

Lemma 1: If (a, b, c) is a realizable triple of $h(x)$ with respect to $e(x)$ which realizes $g(x)$ by the second order DHT in $\mathbb{F}_{2^m}$, then

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{e(\mu^b x) + h(x^a)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{e(\mu x) + g(x^c)}.$$

Proof. From (a, b, c) realizable triple,

$$\frac{1}{2^m} \widehat{h}_e(a,b)(x) = (-1)^{g(x^c)}$$

Hadamard transform of both sides with respect to $e(x)$ is

$$\frac{1}{2^m} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{e(\mu x)} \widehat{h}_e(a,b)(x) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{e(\mu x) + g(x^c)}.$$

Since the left hand side is the inverse Hadamard transform of $\widehat{h}_e(a,b)(x)$, it becomes b-decimation of the first order DHT of $h(x)$ with respect to $e(x)$. So,

$$\begin{aligned}\widehat{h}_e(a)(\mu^b) &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{e(\mu^b x)+h(x^a)} \\ &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{e(\mu x)+g(x^c)}\end{aligned}$$

□

In Gong and Golomb's work [1], it is determined that if (v,t) is a realizable pair of $h(x)$ with respect to $e(x)$, there are at most six realizable pairs related to this pair for the case of $e(x)=h(x)$, which are given by (v,t), $(t,-(vt)^{-1})$, $(-(vt)^{-1},v)$, (t^{-1},v^{-1}), $(v^{-1},-vt)$, and $(-vt,t^{-1})$. In the following, we consider the result in case of $e(x)\neq h(x)$, i.e, asymmetric case.

Lemma 2: Let $(v,t,1)$ be a realizable triple of $h(x)$ with respect to $e(x)$ which realizes $g(x)$ by the second order DHT in $\mathbb{F}_{2^m}$, where $e(x)\neq h(x)$. Then, there exists another realizable triple $(-vt,t^{-1},-t^{-1})$ of $h(x)$ with respect to $e(x)$ which realizes $g(x)$.

Proof. If $(v,t,1)$ and (a,b,c) are realizable triples of $h(x)$, then

$$\begin{aligned}(-1)^{g(\mu)} &= \frac{1}{2^m}\sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{e(\mu y)+e(y^t x)+h(x^v)} \\ &= \frac{1}{2^m}\sum_{z,w\in\mathbb{F}_{2^m}} (-1)^{e(\mu^{c^{-1}} z)+e(z^b w)+h(w^a)}.\end{aligned}$$

Here, (a,b,c) can be a realizable triple if and only if there exists a variable change from (x,y) to (w,z) in a function $e(x)$ such that the above equality is true. In this case, only two kinds of variable changes are possible for $e(x)\neq h(x)$.

i) $x^v = w^a, \quad y^t x = \mu^{c^{-1}} z, \quad \mu y = z^b w.$

ii) $x^v = w^a, \quad y^t x = z^b w, \quad \mu y = \mu^{c^{-1}} z.$

A nontrivial realizable triple (a,b,c) can be obtained from i), and we can easily check $(a,b,c) = (-vt,t^{-1},-t^{-1})$. On the other hand, a realizable triple obtained from ii) is $(v,t,1)$. Thus, a triple $(-vt,t^{-1},-t^{-1})$ is a realizable triple corresponding to $(v,t,1)$ realizable triple. □

In the following, we will show the main theorem on the second order DHT of the binary generalized GMW sequences.

Theorem 1: Let n be a composite number and m a proper factor of n. Let (v, t, 1) be a realizable triple of $h(x)$ with respect to $e(x)$ which realizes $g(x)$ in $\mathbb{F}_{2^m}$. In other words,

$$\frac{1}{2^m}\widehat{h}_e(v,t)(\mu) = (-1)^{g(\mu)}, \quad \mu \in \mathbb{F}_{2^m},$$

where $h(x)$, $g(x)$ and $e(x)$ are orthogonal functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, respectively. For orthogonal functions $f(x), u(x)$ and $c(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined in (4), there exists a realizable triple $(s^{-1}, -s, s)$ of $f(x)$ with respect to $u(x)$ which realizes $c(x)$ by the second order DHT in $\mathbb{F}_{2^n}$, where $s \equiv -t^{-1} \pmod{2^m - 1}$. Precisely,

$$\widehat{f}_u(s^{-1})(\lambda^{-s}) = \widehat{c}_u(s)(\lambda), \quad \lambda \in \mathbb{F}_{2^n}$$

or equivalently,

$$\frac{1}{2^n}\ \widehat{f}_u(s^{-1}, -s)(\lambda) = (-1)^{c(\lambda^s)}, \quad \lambda \in \mathbb{F}_{2^n}.$$

Proof. Let's consider a decimation of the first order DHT of $f(x)$ with respect to $u(x)$ by the decimation pair (s^{-1}, $-s$). Then,

$$\begin{aligned}
\widehat{f}_u(s^{-1})(\lambda^{-s}) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{u(\lambda^{-s}x)+f(x^{s^{-1}})} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{e(Tr_m^n(\lambda^{-s}x))+h((Tr_m^n(x^{s^{-1}}))^v)} \\
&= \sum_{\theta\in\mathbb{F}_{2^n}} (-1)^{e(Tr_m^n(\theta^s))+h((Tr_m^n(\lambda\theta))^v)}
\end{aligned}$$

where $\lambda^{-s}x = \theta^s$. By decomposition of $\theta = \sigma\epsilon$ with $\sigma \in \mathbb{F}_{2^m}$, we have

$$\begin{aligned}
&\widehat{f}_u(s^{-1})(\lambda^{-s}) \\
=&\sum_{\epsilon\in\Psi}\sum_{\sigma\in\mathbb{F}_{2^m}^*} (-1)^{e(\sigma^a Tr_m^n(\epsilon^s))+h(\sigma^v(Tr_m^n(\lambda\epsilon))^v)} + 1 \\
=&\sum_{\epsilon\in\Psi}\sum_{\sigma\in\mathbb{F}_{2^m}} (-1)^{e(\sigma^a Tr_m^n(\epsilon^s))+h(\sigma^v(Tr_m^n(\lambda\epsilon))^v)} - d + 1
\end{aligned} \tag{5}$$

where $d = (2^n-1)/(2^m-1)$, $s \equiv a \pmod{2^m-1}$, and $\Psi = \{1, \alpha, \alpha^2, \cdots, \alpha^{d-1}\}$ where α is a primitive element in $\mathbb{F}_{2^n}$. Let

$$\delta_\epsilon = \sum_{\sigma\in\mathbb{F}_{2^m}} (-1)^{e(\sigma^a Tr_m^n(\epsilon^s))+h(\sigma^v(Tr_m^n(\lambda\epsilon))^v)}.$$

With $(\zeta, \mu) = (Tr_m^n(\epsilon^s), Tr_m^n(\lambda\epsilon))$ and the orthogonality of $h(x)$ and $e(x)$, we obtain

$$\delta_\epsilon = \begin{cases} 0, & \text{if } (\zeta,\mu) = (0,*) \text{ or } (*',0) \\ 2^m, & \text{if } (\zeta,\mu) = (0,0) \\ \delta'_\epsilon, & \text{otherwise} \end{cases} \tag{6}$$

where both $*$ and $*'$ are nonzero elements in $\mathbb{F}_{2^m}$ and δ'_ϵ is defined for ϵ in $\Gamma = \{\epsilon \in \Psi | \zeta \neq 0 \text{ and } \mu \neq 0)\}$. Furthermore, we can express δ'_ϵ as follows.

$$\begin{aligned} \delta'_\epsilon &= \sum_{\rho \in \mathbb{F}_{2^m}} (-1)^{e\left(\rho^a \frac{Tr_m^n(\epsilon^s)}{(Tr_m^n(\lambda\epsilon))^a}\right) + h(\rho^v)} \\ &= \sum_{w \in \mathbb{F}_{2^m}} (-1)^{e\left(w \frac{Tr_m^n(\epsilon^s)}{(Tr_m^n(\lambda\epsilon))^a}\right) + h(w^{va^{-1}})} \end{aligned}$$

where $\rho = \sigma Tr_m^n(\lambda\epsilon)$ and $w = \rho^a$. With $\eta = \frac{Tr_m^n(\lambda\epsilon)}{(Tr_m^n(\epsilon^s))^{a-1}}$, we get

$$\delta'_\epsilon = \sum_{w \in \mathbb{F}_{2^m}} (-1)^{e(\eta^{-a}w) + h(w^{va^{-1}})}. \tag{7}$$

If $(v, t, 1)$ is a realizable triple of $h(x)$ with respect to $e(x)$ which realizes $g(x)$, a triple $(-vt, t^{-1}, -t^{-1})$ is also a realizable triple from Lemma 2. That is, $(va^{-1}, -a, a)$ is a realizable triple for $a \equiv -t^{-1} \pmod{2^m - 1}$ if $(v, t, 1)$ is a realizable triple. From Lemma 1, the realizable triple $(va^{-1}, -a, a)$ realizes $g(x^a)$ by the second order DHT of $h(x)$ with respect to $e(x)$. Thus,

$$\begin{aligned} \delta'_\epsilon &= \sum_{w \in \mathbb{F}_{2^m}} (-1)^{e(\eta^{-a}w) + h(w^{va^{-1}})} \\ &= \sum_{w \in \mathbb{F}_{2^m}} (-1)^{e(\eta w) + g(w^a)} \\ &= \sum_{w \in \mathbb{F}_{2^m}} (-1)^{e\left(w \frac{Tr_m^n(\lambda\epsilon)}{(Tr_m^n(\epsilon^s))^{a-1}}\right) + g(w^a)} \\ &= \sum_{y \in \mathbb{F}_{2^m}} (-1)^{e(yTr_m^n(\lambda\epsilon)) + g(y^a Tr_m^n(\epsilon^s))}, \end{aligned}$$

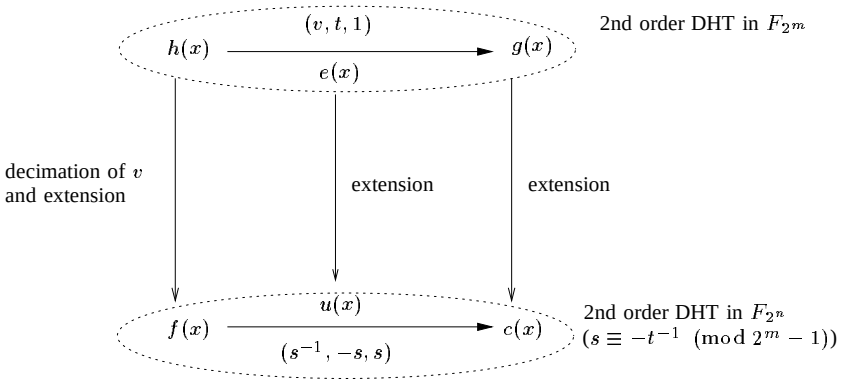

Fig. 1. Relation of orthogonal functions in Theorem 1

where $y = \frac{w}{(Tr_m^n(\epsilon^s))^{a^{-1}}}$. Finally,

$$
\begin{aligned}
&\widehat{f}_u(s^{-1})(\lambda^{-s}) \\
&= \sum_{\epsilon \in \Psi} \delta_\epsilon - d + 1 \\
&= \sum_{\epsilon \in \Gamma} \delta'_\epsilon + N \cdot 2^m - d + 1 \\
&= \sum_{\epsilon \in \Gamma} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{e(yTr_m^n(\lambda\epsilon)) + g(y^a Tr_m^n(\epsilon^s))} + N \cdot 2^m - d + 1 \\
&= \sum_{\epsilon \in \Psi} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{e(yTr_m^n(\lambda\epsilon)) + g(y^a Tr_m^n(\epsilon^s))} - d + 1 \\
&= \sum_{\epsilon \in \Psi} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{e(Tr_m^n(\lambda y\epsilon)) + g(Tr_m^n((y\epsilon)^s))} - d + 1 \\
&= \sum_{z \in \mathbb{F}_{2^n}} (-1)^{e(Tr_m^n(\lambda z)) + g(Tr_m^n(z^s))}, \quad (z = y\epsilon) \\
&= \sum_{z \in \mathbb{F}_{2^n}} (-1)^{u(\lambda z) + c(z^s)} \\
&= \widehat{c}_u(s)(\lambda)
\end{aligned}
$$

where N is the number of elements for $(\zeta, \mu) = (0, 0)$ in Ψ, and $c(x) = g(x) \circ Tr_m^n(x)$. □

Fig. 1 describes a relation of orthogonal functions in Theorem 1. A realization of $f(x)$ in $\mathbb{F}_{2^n}$ is determined by the extension of the realization of $h(x)$ in subfield $\mathbb{F}_{2^m}$, where $f(x) = h(x^v) \circ Tr_m^n(x)$ represents a binary generalized GMW sequence with a period of $2^n - 1$. In other words, the corresponding realizable triples of the binary generalized GMW sequence $f(x)$ can be predicted by the realizable triple

of $h(x)$ by the second order DHT in the subfield. This result is rather surprising because $(s^{-1}, -s, s)$ is a self realizable triple of any binary two-level autocorrelation sequence by the second order symmetric DHT obtained in [1].

For the case that $e(x)$ and $u(x)$ are trace functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, and from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, respectively, if we start from a binary GMW sequence corresponding to $f(x) = Tr_1^m(x^v) \circ Tr_m^n(x)$, then a binary GMW sequence corresponding to $c(x) = Tr_1^m(x^v) \circ Tr_m^n(x)$ can be realized in $\mathbb{F}_{2^n}$ when the second order DHT of $h(x) = Tr_1^m(x)$ produces the self realization $g(x) = Tr_1^m(x^v)$ in $\mathbb{F}_{2^m}$ for each v with $gcd(v, 2^m - 1) = 1$ and $v \neq 1$. Thus, all known binary GMW sequences are realized by the second order DHT of the sequences. In order to get all known binary generalized GMW sequences with the same $f(x)$, however, the realization $g(x)$ must have every decimation of all known binary orthogonal functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, which is not generally guaranteed because there exist at most six realizable pairs for a specific realization $g(x)$ in $\mathbb{F}_{2^m}$ [1]. The experimental results confirmed that if we start from a binary GMW sequence, then we can obtain all known binary GMW sequences and at most six decimation distinct classes of binary generalized GMW sequences with a form of $g(x^d) \circ Tr_m^n(x)$, where $g(x)$ is a realization of $h(x) = Tr_1^m(x)$ in $\mathbb{F}_{2^m}$, and d is a decimation factor of $g(x)$ in the realization [1].

Tables I and II show complete lists of realizations and realizable triples predicted from Theorem 1 for the binary GMW sequences for $n = 8$ and 10, respectively. Table III shows the list for the binary generalized GMW sequences for $n = 10$. In Table V and VI in Appendix I, the predicted realizations and selected realizable triples of binary GMW sequences for $n = 14$ are listed. For $n = 18$ and $m = 9$, the predicted ones of binary GMW sequences are available in [12]. In each case, $e(x)$ just represents an m-sequence with $m = 4, 5, 7$ and 9, respectively, and $u(x)$ represents an m-sequence with $n = 8, 10, 14$ and 18, respectively. Note that $u(x)$ can be any trace function whose subfield factorization is possible. The value of s in each realizable triple is a coset leader satisfying $s \equiv -t^{-1} \pmod{2^m - 1}$ and $gcd(s, 2^n - 1) = 1$. Numbers in each function column under the label of a function represent trace exponents of the function.

In Table I, $h(x) = Tr_1^4(x)$ and $(v, t) = (7, 1)$ is a unique realizable pair of m-sequence by the second order DHT in $\mathbb{F}_{2^4}$ except for $v = 1$ for which $f(x)$ does not represent a GMW sequence, instead, an m-sequence. In each realization, eight realizable triples satisfying $s \equiv -t^{-1} \pmod{15}$ can be obtained, which are exactly the same as the ones obtained from experiments of the second order DHT of $f(x)$ with respect to $u(x)$ which realizes $c(x)$.

In Table II, $h(x) = Tr_1^5(x)$. Thus, $f(x) = Tr_1^5(x^v) \circ Tr_5^{10}(x)$ represents a binary GMW sequence with a period of 1023 for each v with $gcd(v, 31) = 1$ and $v \neq 1$. Table II shows that ten realizable

TABLE I

COMPLETE THEORETICAL PREDICTION OF REALIZATIONS OF GMW SEQUENCES FOR $n = 8$ ($h(x) = Tr_1^4(x)$)

v	$f(x)$	t	$g(x)$	$(s^{-1}, -s, s)$	$c(x)$
7	7, 11, 13, 37	1	7	(7,91,37), (11,23,29), (13,19,59), (29,61,11), (37,31,7), (43, 53, 43), (59,47,13), (127,1,127)	7, 11, 13, 37

triples in each realization can be predicted in $\mathbb{F}_{2^{10}}$. Those exactly match the experimental results of the second order DHT of $f(x)$ with respect to $u(x)$ in $\mathbb{F}_{2^{10}}$. From Table II, it is noted that all binary GMW sequences and one binary generalized GMW sequence can be realized by the second order DHT of the binary GMW sequences.

In Table III, $h(x) = Tr_1^5(x + x^5 + x^7)$. Thus, $f(x) = h(x^v) \circ Tr_5^{10}(x)$ represents a binary generalized GMW sequence with a period of 1023 for each v with $gcd(v, 31) = 1$. It is shown that ten realizable triples in each realization can be predicted and all binary generalized GMW sequences can be realized by the second order DHT of the binary generalized GMW sequences, which matches the experimental results.

In the experiments of the second order DHT of binary GMW sequences for $n = 8, 10$, and 14, it is observed that if we compare predicted ones to the realizations from the experiments, no other realizations than the prediction ones are realized!

IV. REALIZATIONS ON QUADRATIC RESIDUE SEQUENCES

In this section, we investigate the realization of any orthogonal functions with respect to quadratic residue functions, or equivalently the realization of binary two-level autocorrelation sequences with respect to quadratic residue (QR) sequences by the second order DHT. Firstly, we recall some properties of QR sequences.

A. Quadratic residues and non-residues

Let p be an odd prime integer and i an integer. Then, i is said to be a *quadratic residue (QR)* $(\mathrm{mod}\ p)$ if there is an integer x such that $x^2 \equiv i\ (\mathrm{mod}\ p)$ for non-zero i [13]. Otherwise, i is said to be a *quadratic non-residue (QNR)* $(\mathrm{mod}\ p)$. We list several properties that we will use in this section whose proof can be found in [13], or easily derived from the number theory in [13].

Fact 1: Let a be an element in $\mathbb{Z}_p^*$. Then, a is QR (or QNR) if and only if a^{-1} is also QR (or QNR).

TABLE II

COMPLETE THEORETICAL PREDICTION OF REALIZATIONS OF GMW SEQUENCES FOR $n = 10$ $(h(x) = Tr_1^5(x))$

v	$f(x)$ $= Tr_1^5(x^v) \circ Tr_5^{10}(x)$	t	$g(x)$	$(s^{-1}, -s, s)$	$c(x)$ $= g(x) \circ Tr_5^{10}(x)$
3	3, 17	1	3	(23,221,89), (29,35,247), (61,109,151), (85,343,85), (89,125,23), (91,101,215), (151,47,61), (215,157,91), (247,95,29), (511,1,511)	3, 17
		3	1, 5, 7	(7,73,439), (19,53,175), (25,367,41), (59,13,191), (107,239,49), (149,115,103), (205,383,5), (245,119,71), (379,83,235), (479,181,173)	1, 5, 7, 9, 19, 25, 69
		5	11	(13,59,79), (53,19,251), (73,7,127), (83,379,37), (115,149,347) (119,245,43), (181,479,17), (239,107,167), (367,25,223), (383,205,179)	11, 13, 21, 73
5	5, 9	1	5	(23,221,89), (29,35,247), (61,109,151), (85,343,85), (89,125,23), (91,101,215), (151,47,61), (215,157,91), (247,95,29), (511,1,511)	5, 9
		3	7	(7,73,439), (19,53,175), (25,367,41), (59,13,191), (107,239,49), (149,115,103), (205,383,5), (245,119,71), (379,83,235), (479,181,173)	7, 19, 25, 69
7	7, 19, 25, 69	1	7	(23,221,89), (29,35,247), (61,109,151), (85,343,85), (89,125,23), (91,101,215), (151,47,61), (215,157,91), (247,95,29), (511,1,511)	7, 19, 25, 69
		11	5	(5,179,205), (41,223,25), (49,167,107), (71,43,245), (103,347,149), (173,17,479), (175,251,19), (191,79,59), (235,37,379), (439,127,7)	5, 9
11	11, 13, 21, 73	1	11	(23,221,89), (29,35,247), (61,109,151), (85,343,85), (89,125,23), (91,101,215), (151,47,61), (215,157,91), (247,95,29), (511,1,511)	11, 13, 21, 73
		7	3	(17,173,181), (37,235,83), (43,71,119), (79,191,13), (127,439,73), (167,49,239), (179,5,383), (223,41,367), (251,175,53), (347,103,115)	3, 17
		11	1, 5, 7	(5,179,205), (41,223,25), (49,167,107), (71,43,245), (103,347,149), (173,17,479), (175,251,19), (191,79,59), (235,37,379), (439,127,7)	1, 5, 7, 9, 19, 25, 69
15	15, 23, 27, 29, 77, 85, 89, 147	1	15	(23,221,89), (29,35,247), (61,109,151), (85,343,85), (89,125,23), (91,101,215), (151,47,61), (215,157,91), (247,95,29), (511,1,511)	15, 23, 27, 29, 77, 85, 89, 147

Fact 2: For each element a, b in $\mathbb{Z}_p^*$,

$$ab = \begin{cases} \text{QR}, & \text{if } (a, b) = \text{(QR, QR) or (QNR, QNR)} \\ \text{QNR}, & \text{if } (a, b) = \text{(QR, QNR) or (QNR, QR).} \end{cases}$$

Fact 3: Let a be an element in $\mathbb{Z}_p^*$ with $p \equiv 3 \pmod 4$. If a is QR (or QNR), then $-a$ is QNR (or QR).

TABLE III

COMPLETE THEORETICAL PREDICTION OF REALIZATIONS OF GENERALIZED GMW SEQUENCES FOR $n = 10$

$(h(x) = Tr_1^5(x + x^5 + x^7))$

v	$f(x)$ $= h(x^v) \circ Tr_5^{10}(x)$	t	$g(x)$	$(s^{-1}, -s, s)$	$c(x)$ $= g(x) \circ Tr_5^{10}(x)$
1, 5, 7	1, 5, 7, 9, 19, 25, 69	1	1, 5, 7	(23,221,89), (29,35,247), (61,109,151), (85,343,85), (89,125,23), (91,101,215), (151,47,61), (215,157,91), (247,95,29), (511,1,511)	1, 5, 7, 9, 19, 25, 69
		3	11	(7,73,439), (19,53,175), (25,367,41), (59,13,191), (107,239,49), (149,115,103), (205,383,5), (245,119,71), (379,83,235), (479,181,173)	11, 13, 21, 73
		11	3	(5,179,205), (41,223,25), (49,167,107), (71,43,245), (103,347,149), (173,17,479), (175,251,19), (191,79,59), (235,37,379), (439,127,7)	3, 17
3, 11, 15	3, 17, 11, 13, 21, 73, 15, 23, 27, 29, 77, 85, 89, 47	1	3, 11, 15	(23,221,89), (29,35,247), (61,109,151), (85,343,85), (89,125,23), (91,101,215), (151,47,61), (215,157,91), (247,95,29), (511,1,511)	3, 17, 11, 13, 21, 73, 15, 23, 27, 29, 77, 85, 89, 47

B. Cross-correlation of QR sequences

Using the concept of QR and QNR, a quadratic residue (QR) sequence $\underline{\mathbf{q}} = \{q_i\}$ with a period of $p \equiv 3 \pmod 4$ is defined by

$$q_i = \begin{cases} 1, & \text{if } i = 0 \pmod p \\ 0, & \text{if } i = \text{QR} \pmod p \\ 1, & \text{if } i = \text{QNR} \pmod p. \end{cases} \tag{8}$$

Similarly, we can consider another distinct class of QR sequence $\underline{\mathbf{q}}' = \{q_i'\}$ with the same period.

$$q_i' = \begin{cases} 1, & \text{if } i = 0 \pmod p \\ 1, & \text{if } i = \text{QR} \pmod p \\ 0, & \text{if } i = \text{QNR} \pmod p. \end{cases} \tag{9}$$

QR sequences with a period of p are known to have two-level autocorrelation if and only if $p \equiv 3 \pmod 4$ [14]. Also, it has been known that there are only two shift distinct QR sequences with the same period, i.e., one is $\underline{\mathbf{q}} = \{q_i\}$ and the other is $\underline{\mathbf{q}}^{(d)} = \{q_i^d\}$ where d is QNR, and $\underline{\mathbf{q}}^{(d)} = \underline{\mathbf{q}}'$, defined by (9). Furthermore, we have

$$q_i' = q_{-i}, \quad i = 0, 1, \cdots, p-1.$$

In other words, two shift distinct quadratic residue sequences are reciprocal.

Any QR sequence has its own trace representation [15] [16]. Let $p = 2^n - 1$. If the trace representation of the QR sequence $\underline{\mathbf{q}}$ is $u(x)$, then the trace representation of $\underline{\mathbf{q}}'$ is $u'(x) = u(x^d)$ for any QNR d in $\mathbb{Z}_p^*$. As

the QR sequence is a two-level autocorrelation sequence for $p \equiv 3 \pmod 4$, both trace representations $u(x)$ and $u'(x)$ are orthogonal functions, respectively. In this paper, the trace representation of QR sequence is called a *quadratic residue (QR) function*.

The cross-correlation of two distinct QR sequences with a period of $2^n - 1$ can be derived by using a similiar way in [17]. This is stated as follows.

Proposition 1: Let a_i and b_i be two shift distinct QR sequences with a period of $2^n - 1$ and their trace representations $u(x)$ and $u'(x)$ (or $u'(x)$ and $u(x)$), respectively. The cross-correlation of these two QR sequences has three values as shown below,

$$C_{a,b}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{a_i + b_{i+\tau}} = \begin{cases} -2^n + 3, & \text{if } \tau = 0 \\ 3, & \text{if } \tau = \text{QR (or QNR)} \\ -1, & \text{if } \tau = \text{QNR (or QR).} \end{cases}$$

C. Hadamard transform of QR functions

From the auto- and cross-correlation property of a QR sequence, the Hadamard transform of a QR function with respect to itself or its distinct QR function is easily derived.

Lemma 3: The Hadamard transform of $u(x)$ with respect to $g(x) = u(x^d)$ is defined by

$$\widehat{u}_g(y) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{u(x) + g(yx)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{u(x) + u(y^d x^d)}.$$

If d is QR, then

$$\widehat{u}_g(y) = \widehat{u}_u(y) = \begin{cases} 2^n, & \text{if } y = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Otherwise,

$$\widehat{u}_g(y) = \widehat{u}_{u'}(y) = \begin{cases} -2^n + 4, & \text{if } y = 1 \\ 4, & \text{if } y = \alpha^i \text{ for QR (or QNR) } i \\ 0, & \text{if } y = 0 \text{ or } \alpha^i \text{ for QNR (or QR) } i \end{cases} \tag{10}$$

where α is a primitive element in $\mathbb{F}_{2^n}$.

Proof: If d is QR, then $g(x) = u(x^d) = u(x)$. Thus, the result follows from the fact that $u(x)$ is orthogonal. If d is QNR, on the other hand, then $g(x) = u(x^d) = u'(x)$. Since $\widehat{u}_{u'}(y) = C_{a,b}(\tau) + 1$, where $y = \alpha^\tau$ for $y \neq 0$, the result follows from Proposition 1. □

From Lemma 3, the Hadamard transform $\widehat{u}_{u'}(y)$ of $u(x)$ with respect to $u'(x)$ is determined by whether each i at $y = \alpha^i$ is a quadratic residue or non-residue, which is similar to the QR sequence itself.

D. Realizations of orthogonal functions with respect to QR functions

Let $f(x)$ and $u(x)$ be orthogonal functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. If $u(x)$ is a QR function, then the second order DHT of $f(x)$ with respect to $u(x)$ is given by

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

If $\lambda = 0$,

$$\widehat{f_u}(v,t)(0) = 2^n \tag{11}$$

from [1]. For λ in $\mathbb{F}_{2^n}^*$, we have

$$\begin{aligned}
\widehat{f_u}(v,t)(\lambda) &= \sum_{x,z\in\mathbb{F}_{2^n}} (-1)^{u(z)+u(\lambda^{-t} z^t x)+f(x^v)} \quad (\lambda y = z) \\
&= \sum_{y,z\in\mathbb{F}_{2^n}} (-1)^{u(z)+u(y^t z^t)+f((\lambda y)^{vt})} \quad (\lambda^{-t} x = y^t) \\
&= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{f((\lambda y)^{vt})} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{u(z)+u(y^t z^t)} \\
&= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{f((\lambda y)^{vt})}\ \widehat{u}_g(y),
\end{aligned} \tag{12}$$

where (v,t) is a decimation pair and $g(x) = u(x^t)$. First of all, we consider the second order DHT when t is QR.

Lemma 4: Let $f(x)$ be an orthogonal function and $u(x)$ a QR function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, respectively. With a decimation pair of (v,t), if t is QR, the realization of $f(x)$ with respect to $u(x)$ by the second order DHT is a self-realization. Precisely,

$$\widehat{f_u}(v,t)(\lambda) = 2^n \cdot (-1)^{f(\lambda^{vt})}$$

for λ in $\mathbb{F}_{2^n}$.

Proof: In (12), $g(x) = u(x^t) = u(x)$ if t is QR. From Lemma 3, $\widehat{u}_g(y)$ has a non-zero value 2^n only at $y = 1$, and zero at all other y's in $\mathbb{F}_{2^n}$. Therefore, the result follows from (11) and (12). □

When t is QNR, on the other hand, $\widehat{u}_g(y)$ becomes the Hadamard transform of $u(x)$ with respect to $u'(x)$. In this case, we consider the case where $f(x)$ is not a QR function.

Lemma 5: Let $f(x)$ be an orthogonal function which is not a QR function and $u(x)$ a QR function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, respectively. If t is QNR, then the second order DHT of $f(x)$ with respect to $u(x)$ with a decimation pair (v,t) does not produce any realization for any v.

In order to prove Lemma 5, we need the following property of the orthogonal function $f(x)$.

Lemma 6: If $f(x)$ is an orthogonal function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ where 2^n-1 is prime, then $f(1)=1$.

Proof: Let

$$a_i = f(\alpha^i), \quad i = 0, 1, \cdots,$$

where α is a primitive element of $\mathbb{F}_{2^n}$. Since $f(x)$ is orthogonal, $\{a_i\}$ is balanced with 2^{n-1} 1's and $2^{n-1}-1$ 0's in one period. Furthermore, $\{a_i\}$ satisfies the coset-constant property [6], i.e.,

$$a_{2i} = a_i, \quad i = 0, 1, \cdots.$$

For a prime $p = 2^n - 1$, all nonzero cosets modulo p have the same size n, and $\{a_i\}$ is constant with 0 or 1 on a coset. This gives $\frac{p-1}{2} = 2^{n-1}-1$ 1's and $\frac{p-1}{2}$ 0's. Thus, $a_0 = f(1) = 1$ in order to obtain 2^{n-1} 1's. □

Proof of Lemma 5: In the second order DHT given in (12), $\widehat{f}_u(v,t)(\lambda)$ should be $\pm 2^n$ for any λ in $\mathbb{F}_{2^n}^*$ if it is a valid realization [1]. To prove Lemma 5, therefore, it is sufficient to prove that $\widehat{f}_u(v,t)(1)$ can be neither 2^n nor -2^n when t is QNR.

Assume $\widehat{f}_u(v,t)(1) = \pm 2^n$ when $f(x)$ is not a QR function and t is QNR. Let δ and ρ be the numbers of QR and QNR indices satisfying $f(\alpha^{ivt}) = 0$ in a period of the sequence corresponding to $f(x)$, i.e.,

$$\delta = |\{i|\ f(\alpha^{ivt}) = 0 \text{ and } i \text{ is QR in } \mathbb{Z}_{2^n-1}^*\}|,$$

$$\rho = |\{i|\ f(\alpha^{ivt}) = 0 \text{ and } i \text{ is QNR in } \mathbb{Z}_{2^n-1}^*\}|.$$

From the balance property of $f(x)$,

$$\delta + \rho = 2^{n-1} - 1. \tag{13}$$

From Lemma 3 and Lemma 6,

$$\begin{aligned} \widehat{f}_u(v,t)(1) &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y^{vt})}\ \widehat{u}_g(y) \\ &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y^{vt})}\ \widehat{u}_{u'}(y) \\ &= (-1)^{f(1)}(-2^n+4) + 4\delta - 4(2^{n-1}-1-\delta) \\ &= \pm 2^n, \end{aligned} \tag{14}$$

where we assume $\widehat{u}_{u'}(y) = 4$ at $y = \alpha^i$ for QR i. If we assume that $\widehat{u}_{u'}(y) = 4$ at $y = \alpha^i$ for QNR i, then we have ρ instead of δ in the above, which does not change the final result.

Meanwhile, $f(\alpha^{ivt})$ should be constant on each coset from the coset-constant property of its corresponding sequence. Since each coset has the same size n and corresponds to either QR or QNR, the difference between numbers of QR and QNR indices of i satisfying $f(\alpha^{ivt}) = 0$ should be divisible by n to satisfy the coset-constant property, i.e.,

$$|\delta - \rho| = kn$$

for some integer k.

From (14), $\delta = 2^{n-2}$ or 0. In case of $\delta = 0$, $\rho = 2^{n-1} - 1$ from (13). Then, $|\delta - \rho| = 2^{n-1} - 1$ is divisible by n if n is odd prime. It means that $f(\alpha^{ivt})$ is just a QR sequence and $f(x)$ is a QR function. In case of $\delta = 2^{n-2}$ and $\rho = 2^{n-2} - 1$, on the other hand, $|\delta - \rho| = 1$ cannot be divided by n. With such values of δ and ρ, $f(\alpha^{ivt})$ might have different values on the same coset, which violates the coset-constant property. Thus, the case of $\delta = 2^{n-2}$ and $\rho = 2^{n-2} - 1$ is impossible.

For a QNR t, therefore, $\widehat{f_u}(v,t)(1)$ can be $\pm 2^n$ only if $f(x)$ is a QR function, which contradicts our assumption. Hence, if $f(x)$ is not a QR function, $\widehat{f_u}(v,t)(\lambda)$ cannot have a valid realization when t is QNR. □

From Lemma 5, there exist no realizations of a non-QR function $f(x)$ with respect to a QR function $u(x)$ when a decimation factor t is QNR. In the proof of Lemma 5, however, the realization of a QR function $f(x)$ may exist even though t is QNR. In this case, the realization depends on whether another decimation factor v is QR or QNR.

Lemma 7: Let $f(x)$ and $u(x)$ be the same QR functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, i.e., $f(x) = u(x)$. If t is QNR, then the second order DHT of $f(x)$ with respect to $u(x)$ with a decimation pair (v,t) produces $u(x)$ or no realization depending on whether v is QR or QNR. In other words,

$$\widehat{f_u}(v,t)(\lambda) = \begin{cases} 2^n \cdot (-1)^{u(\lambda)}, & \text{if } v \text{ is QR} \\ \text{no realization}, & \text{if } v \text{ is QNR} \end{cases}$$

for λ in $\mathbb{F}_{2^n}$.

Proof: If $f(x) = u(x)$, then (12) becomes

$$\begin{aligned} \widehat{f_u}(v,t)(\lambda) &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{u((\lambda y)^{vt})} \sum_{z \in \mathbb{F}_{2^n}} (-1)^{u(z)+u(y^t z^t)} \\ &= \sum_{z \in \mathbb{F}_{2^n}} (-1)^{u(z)} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{u((\lambda y)^{vt})+u(z^t y^t)}. \end{aligned} \tag{15}$$

If v is QR, then $u((\lambda y)^{vt}) = u((\lambda^t y^t)^v) = u(\lambda^t y^t)$. Thus,

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

where $x = z^t y^t$. Since $u(x)$ is orthogonal, $\widehat{u}_u(\lambda^t z^{-t})$ has a non-zero value 2^n only at $\lambda z^{-1} = 1$. Combined with (11), therefore,

$$\widehat{f}_u(v,t)(\lambda) = 2^n \cdot (-1)^{u(\lambda)}.$$

If v is QNR, on the other hand, then $u(x^v)$ and $u(x)$ correspond to two distinct QR sequences. Thus,

$$\begin{aligned}\widehat{f}_u(v,t)(\lambda) &= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{u(z)} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{u((\lambda y)^{vt})+u(z^t y^t)} \\ &= \sum_{z\in\mathbb{F}^*_{2^n}} (-1)^{u(z)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{u(x)+u(\lambda^{vt} z^{-vt} x^v)} \\ &= \sum_{z\in\mathbb{F}^*_{2^n}} (-1)^{u(z)}\ \widehat{u}_{u'}((\lambda z^{-1})^t)\end{aligned} \tag{16}$$

where $x = z^t y^t$. If $\widehat{f}_u(v,t)(\lambda)$ is evaluated at $\lambda = 1$, then

$$\begin{aligned}\widehat{f}_u(v,t)(1) &= \sum_{z\in\mathbb{F}^*_{2^n}} (-1)^{u(z)} \cdot \widehat{u}_{u'}(z^{-t}) \\ &= (-1)^{u(1)}\widehat{u}_{u'}(1) \\ &\quad + \sum_{j\in\Theta} (-1)^{u(\alpha^j)} \cdot \widehat{u}_{u'}(\alpha^{-jt}) \\ &\quad + \sum_{j\in\Theta^c} (-1)^{u(\alpha^j)} \cdot \widehat{u}_{u'}(\alpha^{-jt}) \\ &= (-1)\cdot(2^n - 4) + (2^{n-1} - 1)\cdot(-1)^0 \cdot 4 \\ &\quad + (2^{n-1} - 1)\cdot(-1)^1 \cdot 0 \\ &= 3\cdot 2^n - 8.\end{aligned} \tag{17}$$

where $\Theta = \{j \in \mathbb{Z}^*_{2^n-1} | j \text{ is QR}\}$ and $\Theta^c = \{j \in \mathbb{Z}^*_{2^n-1} | j \text{ is QNR}\}$. The fact that $\widehat{f}_u(v,t)(1)$ is not $\pm 2^n$ is enough to show that there exists no realization of $f(x) = u(x)$ when both v and t are QNR. □

Basically, it is possible to compute $\widehat{f}_u(v,t)(\lambda)$ in (16) for all λ in $\mathbb{F}_{2^n}$ when both v and t are QNR. This will be shown in Appendix II.

TABLE IV

REALIZATION OF $f(x)$ WITH RESPECT TO A QR FUNCTION $u(x)$

(v,t)	(QR,QR)	(QR,QNR)	(QNR,QR)	(QNR,QNR)
$f(x) = u(x)$	$u(x)$	$u(x)$	$u'(x)$	None
$f(x) = u'(x)$	$u'(x)$	None	$u(x)$	$u(x)$
Other $f(x)$	$f(x^{vt})$	None	$f(x^{vt})$	None

Lemma 8: Let $f(x)$ and $u(x)$ be distinct QR functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, i.e., $f(x) = u'(x)$. If t is QNR, then the second order DHT of $f(x)$ with respect to $u(x)$ with a decimation pair (v,t) is given by

$$\widehat{f_u}(v,t)(\lambda) = \begin{cases} 2^n \cdot (-1)^{u(\lambda)}, & \text{if } v \text{ is QNR} \\ \text{no realization}, & \text{if } v \text{ is QR} \end{cases}$$

for λ in $\mathbb{F}_{2^n}$.

Proof: This result follows by applying the similar procedure of the proof of Lemma 7. □

From Lemma 4, 5, 7, and 8, we have the main theorem.

Theorem 2: Let both $f(x)$ and $u(x)$ be orthogonal functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, where $u(x)$ is a QR function representing a quadratic residue sequence with a period of $2^n - 1$. Let $u'(x)$ be another QR function distinct from $u(x)$. Applying the second order DHT of $f(x)$ with respect to $u(x)$, the realization of $f(x)$ is completely determined by $f(x)$ and its decimation pair (v,t) as listed in Table IV.

In Table IV, each entry under (QR, QR) or the other three columns is the realization of $f(x)$ by the corresponding pair. For example, if (v,t) = (QR, QR),

a) If $f(x) = u(x)$ or $(u'(x))$, then (v,t) realizes $u(x)$ or $(u'(x))$, respectively, which is a self-realization.

b) If $f(x)$ is not a QR function, then (v,t) realizes $f(x^{vt})$, also a self-realization.

If (v,t) = (QR, QNR) and $f(x) = u'(x)$, then the entry 'None' represents that (v,t) does not produce any realization.

From Theorem 2 and Table IV, it is noted that the realization of any binary two-level autocorrelation sequence with respect to a QR sequence is either a self-realization or a QR sequence.

V. CONCLUSION

In this paper, realizations of special classes of binary two-level autocorrelation sequences by the second order DHT have been investigated. Firstly, the realization of the binary generalized GMW sequence and

corresponding realizable triples can be predicted by the second order DHT in its subfield. Secondly, the realization of any two-level autocorrelation sequence with respect to a QR sequence can also be predicted, and a valid realization is either a self-realization or a QR sequence.

APPENDIX I

COMPLETE THEORETICAL PREDICTON OF REALIZATIONS OF BINARY GMW SEQUENCES FOR $n = 14$

TABLE V

REALIZATIONS AND SELECTED REALIZABLE TRIPLES OF GMW SEQUENCES FOR $n = 14$ ($h(x) = Tr_1^7(x)$)

v	$f(x) = Tr_1^7(x^v) \circ Tr_7^{14}(x)$	t	$g(x)$	$(s^{-1}, -s, s)$	$c(x) = g(x) \circ Tr_5^{14}(x)$
3	3, 65	1	3	(95, 1207, 1897)	3, 65
		3	1, 9, 13	(31, 7663, 529)	1, 9, 17, 13, 35, 81, 289
		7	1, 9, 15	(71, 1615, 923)	1, 9, 17, 15, 71, 99, 113, 269, 325, 353, 579
		11	3, 5, 9, 19, 29,	(29, 2807, 565)	3, 65, 5, 33, 9, 17, 19, 25, 73, 273, 29, 39, 83, 105, 293, 337, 537, 547
		21	43	(53, 1391, 937)	43, 45, 53, 85, 297, 553, 561, 593
5	5, 33	1	5	(95, 1207, 1897)	5, 33
		5	9, 11, 21	(47, 305, 3835)	9, 17, 11, 49, 69, 265, 21, 37, 41, 529
		11	1, 3, 7, 19, 29	(29, 2807, 565)	1, 3, 65, 7, 67, 97, 261, 19, 25, 73, 273, 29, 39, 83, 105, 293, 337, 537, 547
		19	27	(77, 625, 1915)	27, 51, 77, 89, 281, 305, 585, 1093
7	7, 67, 97, 261	1	7	(95, 1207, 1897)	7, 67, 97, 261
		3	19, 21, 31	(31, 7663, 529)	19, 25, 73, 273, 21, 37, 41, 529, 31, 79, 103, 115, 121, 285, 333, 357, 369, 539, 587, 611, 793, 841, 1095, 1301
		9	55	(55, 875, 2383)	55, 59, 91, 93, 109, 309, 313, 345, 563, 601, 617, 817, 1107, 1109, 1125, 2341
9	9, 17	1	9	(95, 1207, 1897)	9, 17
		7	15	(71, 1615, 923)	15, 71, 99, 113, 269, 325, 353, 579
		13	1, 7, 9, 11, 23	(23, 3517, 713)	1, 7, 67, 97, 261, 9, 17, 11, 49, 69, 265, 23, 57, 75, 101, 277, 329, 531, 785
11	11, 49, 69, 265	1	11	(95, 1207, 1897)	11, 49, 69, 265
		15	3, 7, 11, 19, 21	(7, 5851, 2341)	3, 65, 7, 67, 97, 261, 11, 49, 69, 265, 19, 25, 73, 273, 21, 37, 41, 529
		19	1, 5, 13, 21, 29	(77, 625, 1915)	1, 5, 33, 13, 35, 81, 289, 21, 37, 41, 529, 29, 39, 83, 105, 293, 337, 537, 547
		23	13	(13, 1259, 1339)	13, 35, 81, 289
13	13, 35, 81, 289	1	13	(95, 1207, 1897)	13, 35, 81, 289
		27	3, 7, 11, 19, 21	(19, 2479, 869)	3, 65, 7, 67, 97, 261, 11, 49, 69, 265, 19, 25, 73, 273, 21, 37, 41, 529
		29	11	(11, 1117, 1501)	11, 49, 69, 265
		43	1, 5, 13, 21, 29	(37, 1273, 443)	1, 5, 33, 13, 35, 81, 289, 21, 37, 41, 529, 29, 39, 83, 105, 293, 337, 537, 547
15	15, 71, 99, 113, 269, 325, 353, 579	1	15	(95, 1207, 1897)	15, 71, 99, 113, 269, 325, 353, 579
		5	1, 7, 9, 11, 23	(47, 305, 3835)	1, 7, 67, 97, 261, 9, 17, 11, 49, 69, 265, 23, 57, 75, 101, 277, 329, 531, 785
		55	9	(17, 2861, 2893)	9, 17

TABLE VI

REALIZATIONS AND SELECTED REALIZABLE TRIPLES OF GMW SEQUENCES FOR $n = 14$ ($h(x) = Tr_1^7(x)$)

v	$f(x) = Tr_1^7(x^v) \circ Tr_7^{14}(x)$	t	$g(x)$	$(s^{-1}, -s, s)$	$c(x) = g(x) \circ Tr_5^{14}(x)$
19	19, 25, 73, 273	1	19	(95, 1207, 1897)	19, 25, 73, 273
		3	1, 5, 7, 11, 31	(31, 7663, 529)	1, 5, 33, 7, 67, 97, 261, 11, 49, 69, 265, 31, 79, 103, 115, 121, 285, 333, 357, 369, 539, 587, 611, 793, 841, 1095, 1301
		5	47	(47, 305, 3835)	47, 61, 87, 107, 117, 301, 341, 361, 555, 569, 595, 625, 809, 849, 1123, 1317
21	21, 37, 41, 529	1	21	(95, 1207, 1897)	21, 37, 41, 529
		3	31	(31, 7663, 529)	31, 79, 103, 115, 121, 285, 333, 357, 369, 539, 587, 611, 793, 841, 1095, 1301
23	23, 57, 75, 101, 277, 329, 531, 785	1	23	(95, 1207, 1897)	23, 57, 75, 101, 277, 329, 531, 785
		11	29	(29, 2807, 565)	29, 39, 83, 105, 293, 337, 537, 547
27	27, 51, 77, 89, 281, 305, 585, 1093	1	27	(95, 1207, 1897)	27, 51, 77, 89, 281, 305, 585, 1093
		9	1, 3, 7, 19, 29	(55, 875, 2383)	1, 3, 65, 7, 67, 97, 261, 19, 25, 73, 273, 29, 39, 83, 105, 293, 337, 537, 547
		27	9, 11, 21	(19, 2479, 869)	9, 17, 11, 49, 69, 265, 21, 37, 41, 529
		47	5	(5, 2867, 3277)	5, 33
29	29, 39, 83, 105, 293, 337, 537, 547	1	29	(95, 1207, 1897)	29, 39, 83, 105, 293, 337, 537, 547
		13	23	(23, 3517, 713)	23, 57, 75, 101, 277, 329, 531, 785
31	31, 79, 103, 115, 121, 285, 333, 357, 369, 539, 587, 611, 793, 841, 1095, 1301	1	31	(95, 1207, 1897)	31, 79, 103, 115, 121, 285, 333, 357, 369, 539, 587, 611, 793, 841, 1095, 1301
		43	21	(37, 1273, 443)	21, 37, 41, 529
43	43, 45, 53, 85, 297, 553, 561, 593	1	43	(95, 1207, 1897)	43, 45, 53, 85, 297, 553, 561, 593
		31	3	(65, 2741, 2773)	3, 65
		43	1, 9, 15	(37, 1273, 443)	1, 9, 17, 15, 71, 99, 113, 269, 325, 353, 579
		47	3, 5, 9, 19, 29	(5, 2867, 3277)	3, 65, 5, 33, 9, 17, 19, 25, 73, 273, 29, 39, 83, 105, 293, 337, 537, 547
		55	1, 9, 13	(17, 2861, 2893)	1, 9, 17, 13, 35, 81, 289
47	47, 61, 87, 107, 117, 301, 341, 361, 555, 569, 595, 625, 809, 849, 1123, 1317	1	47	(95, 1207, 1897)	47, 61, 87, 107, 117, 301, 341, 361, 555, 569, 595, 625, 809, 849, 1123, 1317
		13	1, 5, 7, 11, 31	(23, 3517, 713)	1, 5, 33, 7, 67, 97, 261, 11, 49, 69, 265, 31, 79, 103, 115, 121, 285, 333, 357, 369, 539, 587, 611, 793, 841, 1095, 1301
		27	19	(19, 2479, 869)	19, 25, 73, 273
55	55, 59, 91, 93, 109, 309, 313, 345, 563, 601, 617, 817, 1107, 1109, 1125, 2341	1	55	(95, 1207, 1897)	55, 59, 91, 93, 109, 309, 313, 345, 563, 601, 617, 817, 1107, 1109, 1125, 2341
		15	7	(7, 5851, 2341)	7, 67, 97, 261
		43	19, 21, 31	(37, 1273, 443)	19, 25, 73, 273, 21, 37, 41, 529, 31, 79, 103, 115, 121, 285, 333, 357, 369, 539, 587, 611 793, 841, 1095, 1301
63	63, 377, 881, 627, 571, 1381, 1587, 1127, 317, 2349, 1333, 2381, 825, 2405, 1139, 633, 125, 123, 373, 119, 873, 365, 619, 111, 1141, 857,1365, 349,1619, 603, 1111, 95	1	63	(95, 1207, 1897)	63, 377, 881, 627, 571, 1381, 1587, 1127, 317, 2349, 1333, 2381, 825, 2405, 1139, 633, 125, 123, 373, 119, 873, 365, 619, 111, 1141, 857,1365, 349,1619, 603, 1111, 95

TABLE VII

DISTRIBUTION OF $k = s - j$ FOR A FIXED s = QR

	k = QR	k = QNR
j = QR	$2^{n-2} - 1$	$2^{n-2} - 1$
j = QNR	$2^{n-2} - 1$	2^{n-2}

TABLE VIII

DISTRIBUTION OF $k = s - j$ FOR A FIXED s = QNR

	k = QR	k = QNR
j = QR	2^{n-2}	$2^{n-2} - 1$
j = QNR	$2^{n-2} - 1$	$2^{n-2} - 1$

APPENDIX II
COMPUTATION OF $\widehat{f_u}(v,t)(\lambda)$

In (16), it is possible to compute $\widehat{f_u}(v,t)(\lambda)$ for all λ in $\mathbb{F}_{2^n}$ when $f(x) = u(x)$ and both v and t are QNR. Before that, we have to consider the distribution of index differences.

Proposition 2: Let s, j and k be non-zero elements in $\mathbb{Z}_p^*$, where $p = 2^n - 1$ is prime and $p \equiv 3 \pmod 4$. For a fixed value of s, the difference $k = s - j$ for each value of j has the distribution of QR and QNR shown in Tables VII and VIII.

In Tables VII and VIII, the case of $s = j$ was excluded if both s and j are QR or QNR. Proposition 2 shows that the numbers of QR k's and QNR k's are almost equal for a fixed s and varying j's.

Now, we compute $\widehat{f_u}(v,t)(\lambda)$ for $\lambda \neq 1$ in $\mathbb{F}_{2^n}^*$ when $f(x) = u(x)$ and both v and t are QNR. If $\lambda = \alpha^s$ for a nonzero $s \in \mathbb{Z}_{2^n-1}^*$, (16) is represented by

$$\widehat{f_u}(v,t)(\lambda) = \sum_{j=0}^{2^n-2} (-1)^{u(\alpha^j)} \cdot \widehat{u}_{u'}(\alpha^{kt}) \tag{18}$$

where $z = \alpha^j$ and $k = s - j$.

From Tables VII and VIII, (18) has two different values according to s for a fixed $u(x)$. At first, if s is

QR,

$$\begin{aligned}\widehat{f_u}(v,t)(\lambda) =& (-1)^{u(1)}\widehat{u}_{u'}(\alpha^{st}) \\ &+ \sum_{j\in\Theta}(-1)^{u(\alpha^j)}\cdot\widehat{u}_{u'}(\alpha^{kt}) \\ &+ (-1)^{u(\alpha^j)}\widehat{u}_{u'}(1)|_{j=QR} \\ &+ \sum_{j\in\Theta^c}(-1)^{u(\alpha^j)}\cdot\widehat{u}_{u'}(\alpha^{kt}) \\ =& -2^n.\end{aligned}$$

Otherwise, if s is QNR,

$$\begin{aligned}\widehat{f_u}(v,t)(\lambda) =& (-1)^{u(1)}\widehat{u}_{u'}(\alpha^{st}) \\ &+ \sum_{j\in\Theta}(-1)^{u(\alpha^j)}\cdot\widehat{u}_{u'}(\alpha^{kt}) \\ &+ (-1)^{u(\alpha^j)}\widehat{u}_{u'}(1)|_{j=QNR} \\ &+ \sum_{j\in\Theta^c}(-1)^{u(\alpha^j)}\cdot\widehat{u}_{u'}(\alpha^{kt}) \\ =& 2^n - 8.\end{aligned}$$

Here, we assume that $u(x)$ represents q_i in (8). If $u(x)$ is assumed to represent q_i' in (9), these values are just reversed with each other. Combined with the results in (11) and (17), therefore, $\widehat{f_u}(v,t)(\lambda)$ has following four values if both v and t are QNR.

$$\widehat{f_u}(v,t)(\lambda) = \begin{cases} 0, & \text{if } \lambda = 0 \\ 3\cdot 2^n - 8, & \text{if } \lambda = 1 \\ -2^n, & \text{if } \lambda = \alpha^i \text{ for QR (or QNR) } i \\ 2^n - 8. & \text{if } \lambda = \alpha^i \text{ for QNR (or QR) } i \end{cases}$$

REFERENCES

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

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

[3] M. Ludkovski and G. Gong, "New families of ideal two-level autocorrelation ternary sequences from second order DHT," *Proceedings of the International Workshop on Coding and Cryptography*, Paris, pp. 345-354, Jan. 2001.

[4] Guang Gong, Zongduo Dai and Solomon W. Golomb, "On existence of 2-level autocorrelation sequences realized from the decimation-Hadamard transformation," *IEEE International Symposium on Information Theory*, Lausanne, Switzerland, June 30-July 5, 2002.

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

[6] S. W. Golomb and G. Gong, *Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar.* Draft, 2004, also available in "calliope.uwaterloo.ca/∼ggong/GolombGongBook.htm".

[7] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, no. 4, pp. 614-625, 1962.

[8] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. 30, no. 3, pp. 548-553, Nov. 1984.

[9] A. Klapper, A. H. Chan, and M. Goresky, "Cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 177-183, Jan. 1993.

[10] J. S. No and P. V. Kumar, "A new family of binary pseudo-random sequences having optimal periodic correlation properties and larger linear span," *IEEE Trans. Inform. Theory*, vol. 35, no. 2, pp. 371-379, Mar. 1989.

[11] G. Gong, "q-ary cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 263-267, Jan. 1996.

[12] Personal website of the first author, "http://www.comsec.uwaterloo.ca/∼nyyu/prediction18.htm".

[13] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number theory*, Springer-Verlag, New York, 2nd ed., 1991.

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

[15] J. S. No, H. K. Lee, H. Chung, H. Y. Song, and K. Yang, "Trace representation of Legendre sequences of mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 2254-2255, Nov. 1996.

[16] Z. D. Dai, G. Gong and H. Y. Song, "Trace representation and linear complexity of binary e-th residue sequences," *Proceedings of International Workshop on Coding and Cryptography (WCC2003)*, March 24-28, 2003, Versailles, France, pp.121-133.

[17] S. R. Gottesman, P. G. Grieve, and S. W. Golomb, "A class of pseudonoise-like pulse compression codes," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 28, no. 2, pp. 355-362, Apr. 1992.