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

Nam Yul Yu and Guang Gong

Department of Electrical and Computer Engineering, University of Waterloo,
200 University Avenue West, Waterloo, Ontario, Canada
nyyu@engmail.uwaterloo.ca, ggong@calliope.uwaterloo.ca

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. In the second order DHT of a binary generalized Gordon-Mills-Welch (GMW) sequence, we show that there exist realizations which can be theoretically determined by the second order DHT in its subfield. Furthermore, we show that complete realizations of any binary two-level autocorrelation sequence with respect to a quadratic residue (QR) sequence by the second order DHT are theoretically determined.

1 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 [6]. 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 used for the analysis of a new two-level autocorrelation sequence. The r-th order iterative DHT can transform one class of two-level autocorrelation sequences into another inequivalent class of such sequences, a process called *realization* [6]. 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 $n \leq 17$ [6].

In this paper, the DHT based on binary generalized GMW sequences and quadratic residue sequences are investigated. The binary generalized GMW sequence has the trace representation of an orthogonal function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ which is a composition of a component orthogonal function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ and a trace function, where $\mathbb{F}_{2^m}$ is a subfield of $\mathbb{F}_{2^n}$ [7] [12]. In the DHT of the sequence, we show that there exist the realizations which can be theoretically determined by the realizations of a sequence corresponding to the component orthogonal function in the subfield. In the realizations, we note that the DHT of a binary generalized GMW sequence in the finite field is inherited from the DHT of its binary component sequence in the subfield.

In addition, using special properties of QR sequences, the realizations of any binary two-level autocorrelation sequence with respect to a QR sequence by the second order DHT are discussed. We show that the complete realizations can be theoretically determined and 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 2, we give some preliminary reviews of concepts and notations on sequences that we will use in this paper. In Section 3, the realizations of the binary generalized GMW sequences by the second order DHT are investigated. Mathematical proofs and experimental results are provided. In Section 4, the realizations of any binary two-level autocorrelation sequence based on a QR sequence are investigated. In Section 5, concluding remarks are given.

2 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.

- $\mathbb{Z}$ is the integer ring, $\mathbb{Z}_m$ the ring of integers modulo m, and $\mathbb{Z}_m^* = \{r \in \mathbb{Z}_m | r \neq 0\}$.
- $\mathbb{F}_Q = GF(Q)$ is the finite field with Q elements and $\mathbb{F}_Q^*$ the multiplicative group of $\mathbb{F}_Q$.
- For positive integers n and m, 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.,

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

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

2.1 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

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

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

2.2 Autocorrelation

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

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

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 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.*

2.3 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

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

2.4 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 [6]. If $f(x)$ is a trace representation of $\underline{\mathbf{a}}$ and autocorrelation function of $\underline{\mathbf{a}}$ defined in (1) is $C_{\underline{\mathbf{a}}}$, then

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

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

2.5 Decimation-Hadamard 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 $v \in \mathbb{Z}^*_{2^n-1}$, 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 $t \in \mathbb{Z}^*_{2^n-1}$. Then,

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

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

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

is called a *realization* of $f(x)$ with respect to $u(x)$, and (v,t) is called a *realizable pair* [6].

3 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 binary generalized GMW sequence $\underline{\mathbf{a}} = \{a_i\}$ is defined by an evaluation of $f(x)$ at α^i [4], where α is a primitive element in $\mathbb{F}_{2^n}$ and $f(x)$ is given by

$$f(x) = h(x) \circ Tr^n_m(x^k) = h\left(Tr^n_m(x^k)\right).$$

Here, $f(x)$ is an orthogonal function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In particular, if $h(x) = Tr^m_1(x^v)$ for v with $\gcd(v, 2^m-1) = 1$ and $v \neq 1$, then the evaluation of $f(x)$ is a GMW sequence [7] [12]. For more details of GMW sequences, see [10] and [5].

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 $\mathbb{F}_{2^m}$, i.e.,

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

or equivalently,

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{e(\mu^b x)+h(x^a)} = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{e(\mu x)+g(x^c)} \qquad (3)$$

for $\mu \in \mathbb{F}_{2^m}$. In this realization, (a, b) is called a *realizable pair* of $h(x)$ with respect to $e(x)$ [6]. 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*.

In Gong and Golomb's work [6], 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 $e(x) = h(x)$. In the following, we consider the result in case of $e(x) \neq h(x)$, i.e., asymmetric case.

Lemma 1. *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

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

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 the 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.e.,

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

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

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

Theorem 1. *Let n be a composite integer 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. Let $f(x)$, $u(x)$ and $c(x)$ be orthogonal functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by

$$f(x) = h(x^v) \circ Tr_m^n(x), \quad u(x) = e(x) \circ Tr_m^n(x), \quad c(x) = g(x) \circ Tr_m^n(x)$$

where v is a decimation factor in $\mathbb{Z}_{2^m-1}^*$ with $\gcd(v, 2^m - 1) = 1$. Then, 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

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

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

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

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

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

where both $*$ and $*'$ are nonzero elements in $\mathbb{F}_{2^m}$ and δ'_ϵ is defined for ϵ in $\Gamma=\{\epsilon\in\Psi|\zeta\neq0\text{ and }\mu\neq0)\}$. Furthermore, we can express δ'_ϵ as follows.

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

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

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

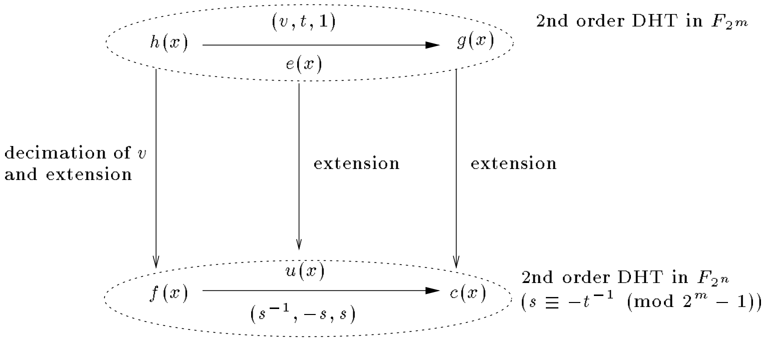
$(v,t,1)$
$h(x)$
$g(x)$
$e(x)$
2nd order DHT in F_{2^m}
decimation of v and extension
extension
extension
$u(x)$
$f(x)$
$c(x)$
$(s^{-1},-s,s)$
2nd order DHT in F_{2^n}
$(s \equiv -t^{-1} \pmod{2^m-1})$

Fig. 1. Relation of orthogonal functions in Theorem 1

If $(v,t,1)$ is a realizable triple of $h(x)$ with respect to $e(x)$ which realizes $g(x)$, then $(-vt, t^{-1}, -t^{-1})$ is also a realizable triple from Lemma 1. Thus, $(va^{-1}, -a, a)$ is a realizable triple for $a \equiv -t^{-1} \pmod{2^m-1}$ if $(v,t,1)$ is a realizable triple. From (3),

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

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

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

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

Fig. 1 describes the relation of the orthogonal functions in Theorem 1 by the second order DHT. In Fig. 1, $c(x)$, a realization of $f(x)$ in $\mathbb{F}_{2^n}$ is determined by

Table 1. Complete theoretical determination of realizations of GMW sequences for $n = 10$ ($h(x) = Tr_1^5(x)$)

v	$f(x)$	t	$g(x)$	$(s^{-1}, -s, s)$	$c(x)$
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

the extension of $g(x)$, a realization of $h(x)$ in $\mathbb{F}_{2^m}$, where $f(x) = h(x^v) \circ Tr_m^n(x)$ represents a binary generalized GMW sequence with period $2^n - 1$. Furthermore, the corresponding realizable triples $(s^{-1}, -s, s)$ are determined by the realizable triple $(v, t, 1)$ in the subfield. In the DHT of a binary generalized GMW sequence in a finite field, we see that there exist the realizations and realizable triples which are theoretically determined by the realizations and realizable triples of a binary component sequence in its subfield. In the realizations, therefore, the DHT in a finite field is inherited from the DHT in its subfield in terms of a binary generalized GMW sequence.

Tables 1 and 2 show complete lists of realizations and realizable triples determined from Theorem 1 for the binary GMW and generalized GMW sequences for $n = 10$, respectively. In each case, both $e(x)$ and $u(x)$ represent m-sequences with period 31. Note that $u(x)$ can be any function whose subfield factorization is possible. The value of s in each realizable triple is a coset leader satisfying

Table 2. Complete theoretical determination of realizations of generalized GMW sequences for $n = 10$ $(h(x) = Tr_1^5(x + x^5 + x^7))$

v	$f(x)$	t	$g(x)$	$(s^{-1}, -s, s)$	$c(x)$
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

$s \equiv -t^{-1} \pmod{2^m - 1}$ and $\gcd(s, 2^n - 1) = 1$. The numbers in each function column under the label of a function represent trace exponents of the function.

In Table 1, $h(x) = Tr_1^5(x)$. Thus, $f(x) = Tr_1^5(x^v) \circ Tr_5^{10}(x)$ represents a binary GMW sequence with period 1023 for each v with $\gcd(v, 31) = 1$ and $v \neq 1$. Table 1 shows that 10 realizable triples in each realization are determined 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 1, we note that all binary GMW sequences and one binary generalized GMW sequence can be realized by the second order DHT of the binary GMW sequences and those realizations are theoretically determined by the realizations in the subfield $\mathbb{F}_{2^5}$. In Table 2, $h(x) = Tr_1^5(x + x^5 + x^7)$. Thus, $f(x) = h(x^v) \circ Tr_5^{10}(x)$ represents a binary generalized GMW sequence with period 1023 for each v with $\gcd(v, 31) = 1$. It is shown that 10 realizable triples in each realization are determined 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 the binary GMW and generalized GMW sequences for $n = 10$, we interestingly observed that there are no other realizations than the ones from Table 1 and 2.

4 Realizations on Quadratic Residue (QR) Sequences

In this section, we study the realization of binary two-level autocorrelation sequences with respect to QR sequences by the second order DHT.

4.1 Basic properties of QR sequences

A QR sequence $\underline{\mathbf{q}} = \{q_i\}$ with period $p \equiv 3 \pmod 4$ is defined by

$$q_i = \begin{cases} 1, & \text{if } i = 0 \pmod{p} \\ 0, & \text{if } i = \text{QR} \pmod{p} \\ 1, & \text{if } i = \text{QNR} \pmod{p}. \end{cases} \tag{4}$$

where 'QR' and 'QNR' represent quadratic residue and non-residue, respectively. For more details of quadratic residues, see [9]. Similarly, we can consider another distinct class of a QR sequence $\underline{\mathbf{q}}' = \{q'_i\}$ with the same period.

$$q'_i = \begin{cases} 1, & \text{if } i = 0 \pmod{p} \\ 1, & \text{if } i = \text{QR} \pmod{p} \\ 0, & \text{if } i = \text{QNR} \pmod{p}. \end{cases} \tag{5}$$

The QR sequences with period p have two-level autocorrelation if and only if $p \equiv 3 \pmod 4$ [3]. Also, it has been known that there are only two cyclically distinct QR sequences with the same period, i.e., one is $\underline{\mathbf{q}} = \{q_i\}$ in (4) and the other is $\underline{\mathbf{q}}^{(d)} = \{q_{di}\}$ where d is QNR and $\underline{\mathbf{q}}^{(d)} = \underline{\mathbf{q}}'$ in (5).

Any QR sequence has its own trace representation [11] [1]. 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 a QR sequence is called a *quadratic residue (QR) function.*

The cross-correlation of two distinct QR sequences with period $2^n - 1$ can be derived by using a similar way in [8]. This is stated as follows.

Proposition 1. *Let $\underline{\mathbf{a}} = \{a_i\}$ and $\underline{\mathbf{b}} = \{b_i\}$ be two shift distinct QR sequences with period $2^n - 1$ 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,*

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

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

Lemma 2. *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

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

Otherwise,

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

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 $\widehat{u}_{u'}(y) = C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) + 1$, where $y = \alpha^\tau$ for $y \neq 0$, the result follows from Proposition 1. □

4.2 Realizations of binary two-level autocorrelation sequences with respect to QR sequences

Let $f(x)$ be an orthogonal function and $u(x)$ a QR function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In the second order DHT of $f(x)$ with respect to $u(x)$ defined by (2), if $\lambda = 0$,

$$\widehat{f_u}(v,t)(0) = 2^n \tag{6}$$

from [6]. For λ in $\mathbb{F}^*_{2^n}$, we have

$$\begin{aligned}
\widehat{f_u}(v,t)(\lambda) &= \sum_{x,z\in\mathbb{F}_{2^n}} (-1)^{u(z)+u(\lambda^{-t}z^t x)+f(x^v)} \quad (\lambda y = z)\\
&= \sum_{y,z\in\mathbb{F}_{2^n}} (-1)^{u(z)+u(y^t z^t)+f((\lambda y)^{vt})} \quad (\lambda^{-t}x = y^t)\\
&= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{f((\lambda y)^{vt})} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{u(z)+u(y^t z^t)}\\
&= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{f((\lambda y)^{vt})}\ \widehat{u}_g(y)
\end{aligned} \tag{7}$$

where (v,t) is a decimation pair and $g(x) = u(x^t)$. First of all, we consider the second order DHT in (7) when t is QR.

Lemma 3. *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 (7), $g(x) = u(x^t) = u(x)$ if t is QR. From Lemma 2, $\widehat{u}_g(y)$ has nonzero value 2^n only at $y = 1$, and zero at all other y's in $\mathbb{F}_{2^n}$. Therefore, the result follows from (6) and (7). □

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 firstly consider the case where $f(x)$ is not a QR function.

Lemma 4. *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 4, we need the following property of the orthogonal function $f(x)$.

Lemma 5. *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 $\{a_i\}$ be a sequence represented by $f(x)$. 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 [4], i.e., $a_{2i} = a_i$. 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 (Proof of Lemma 4). In the second order DHT given in (7), $\widehat{f_u}(v,t)(\lambda)$ should be $\pm 2^n$ for any λ in $\mathbb{F}_{2^n}^*$ if it is a valid realization [6]. To prove Lemma 4, therefore, it is sufficient to show that $\widehat{f_u}(v,t)(1)$ can be neither 2^n nor -2^n when t is QNR.

On the contrary, 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.,

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

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

$$\delta + \rho = 2^{n-1} - 1. \tag{8}$$

From Lemma 2 and Lemma 5,

$$\begin{aligned}\widehat{f_u}(v,t)(1) &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y^{vt})}\ \widehat{u}_{u'}(y)\\ &= (-1)^{f(1)}(-2^n + 4) + 4\delta - 4(2^{n-1} - 1 - \delta)\end{aligned} \tag{9}$$

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, i.e., $|\delta - \rho| = kn$ for some integer k. From (9), $\delta = 2^{n-2}$ or 0 if $\widehat{f_u}(v,t)(1) = \pm 2^n$. In case of $\delta = 0$, $\rho = 2^{n-1} - 1$ from (8). 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 4, 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 4, however, the realization of a QR function $f(x)$ may exist even though t is QNR. In this case, the realization depends on another decimation factor v.

Lemma 6. *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,*

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

for λ in $\mathbb{F}_{2^n}$.

Proof. If $f(x) = u(x)$, then (7) becomes

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

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

$$\widehat{f_u}(v,t)(\lambda) = \sum_{z \in \mathbb{F}_{2^n}^*} (-1)^{u(z)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{u(x) + u(\lambda^t z^{-t} x)} = \sum_{z \in \mathbb{F}_{2^n}^*} (-1)^{u(z)} \; \widehat{u}_u(\lambda^t z^{-t})$$

where $x = z^t y^t$. Since $u(x)$ is orthogonal, $\widehat{u}_u(\lambda^t z^{-t})$ has nonzero value 2^n only at $\lambda z^{-1} = 1$. Combined with (6), 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,

$$\begin{aligned} \widehat{f_u}(v,t)(\lambda) &= \sum_{z \in \mathbb{F}_{2^n}^*} (-1)^{u(z)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{u(x) + u(\lambda^{vt} z^{-vt} x^v)} \\ &= \sum_{z \in \mathbb{F}_{2^n}^*} (-1)^{u(z)} \; \widehat{u}_{u'}((\lambda z^{-1})^t) \end{aligned} \tag{10}$$

where $x = z^t y^t$. If $\widehat{f_u}(v,t)(\lambda)$ in (10) is evaluated at $\lambda = 1$, then

$$\begin{aligned} \widehat{f_u}(v,t)(1) =& (-1)^{u(1)} \widehat{u}_{u'}(1) + \sum_{j \in \Theta} (-1)^{u(\alpha^j)} \cdot \widehat{u}_{u'}(\alpha^{-jt}) \\ &+ \sum_{j \in \Theta^c} (-1)^{u(\alpha^j)} \cdot \widehat{u}_{u'}(\alpha^{-jt}) = 3 \cdot 2^n - 8 \end{aligned}$$

Table 3. Realizations 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

where $\Theta = \{j \in \mathbb{Z}^*_{2^n-1} | j \text{ is QR}\}$ and $\Theta^c = \{j \in \mathbb{Z}^*_{2^n-1} | j \text{ is QNR}\}$. Since $\widehat{f_u}(v,t)(1) \neq \pm 2^n$, it is enough to show that there exists no realization of $f(x) = u(x)$ when both v and t are QNR. □

Lemma 7. *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*

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

for λ in $\mathbb{F}_{2^n}$.

Proof. This result follows by applying the similar procedure of the proof of Lemma 6. □

From Lemma 3, 4, 6, and 7, we have the main theorem on the realizations of any binary two-level autocorrelation sequence with respect to a QR sequence.

Theorem 2. *Let $u(x)$ and $u'(x)$ be QR functions representing distinct QR sequences with period $2^n - 1$ and $f(x)$ be an orthogonal function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In the second order DHT of $f(x)$ with respect to $u(x)$, the realizations of $f(x)$ are completely determined by $f(x)$ and its decimation pair (v,t) as listed in Table 3.*

In Table 3, 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) and $f(x)$ is not a QR function, then (v,t) realizes $f(x^{vt})$, 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 3, we note that the complete realizations of any binary two-level autocorrelation sequence with respect to a QR sequence are theoretically determined, and a valid realization is either a self-realization or a QR sequence.

5 Conclusion

The second order DHT of special classes of binary two-level autocorrelation sequences has been investigated. Firstly, we showed that in the second order DHT of a binary generalized GMW sequence in a finite field, there exist realizations and corresponding realizable triples which can be theoretically determined by the realizations and realizable triples of its component sequence in the subfield. In the realizations, the DHT in a finite field is inherited from the DHT in its subfield in terms of a binary generalized GMW sequence. Secondly, we showed that the complete realizations of any binary two-level autocorrelation sequence with respect to a QR sequence can be theoretically determined, and a valid realization is either a self-realization or a QR sequence.

References

1. Dai, Z. D., Gong, G., Song, H. Y.: Trace representation and linear complexity of binary e-th residue sequences. Proceedings of International Workshop on Coding and Cryptography (WCC2003), Versailles, France. (2003) 121-133
2. Dillon, J. F., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields and Their Applications 10. (2004) 342-389
3. Golomb, S. W.: Shift Register Sequences. Holden-day, Oakland, CA (1967). Revised edition: Aegean Park Press, Laguna Hills, CA (1982)
4. Golomb, S. W., Gong, G.: Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar. Cambridge University Press (2005)
5. Gong, G.: q-ary cascaded GMW sequences. IEEE Transactions on Information Theory. 42(1). (1996) 263-267
6. Gong, G., Golomb, S. W.: The decimation-Hadamard transform of two-level autocorrelation sequences. IEEE Transactions on Information Theory, 48(4). (2002) 853-865
7. Gordon, B., Mills, W. H., Welch, L. R.: Some new difference sets. Canadian J. Math. 14(4). (1962) 614-625
8. Gottesman, S. R., Grieve, P. G., Golomb, S. W.: A class of pseudonoise-like pulse compression codes. IEEE Transactions on Aerospace and Electronic Systems. 28(2). (1992) 355-362
9. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number theory (2nd ed.). Springer-Verlag, New York (1991)
10. Klapper, A., Chan, A. H., Goresky, M.: Cascaded GMW sequences. IEEE Transactions on Information Theory. 39(1). (1993) 177-183
11. No, J. S., Lee, H. K., Chung, H., Song, H. Y., Yang, K.: Trace representation of Legendre sequences of mersenne prime period. IEEE Transactions on Information Theory. 42(6). (1996) 2254-2255
12. Scholtz, R. A., Welch, L. R.: GMW sequences. IEEE Transactions on Information Theory. 30(3). (1984) 548-553