

Crosscorrelation Properties of Binary Sequences with Ideal Two-level Autocorrelation ^{*}

Nam Yul Yu and Guang Gong

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

Abstract. For odd n , binary sequences of period $2^n - 1$ with ideal two-level autocorrelation are investigated with respect to 3- or 5-valued cross-correlation property between them. At most 5-valued crosscorrelation of m -sequences is first discussed, which is linked to crosscorrelation of some other binary two-level autocorrelation sequences. Then, several theorems and conjectures are established for describing 3- or 5-valued crosscorrelation of a pair of binary two-level autocorrelation sequences.

1 Introduction

In code-division multiple access (CDMA) communication systems, a binary two-level autocorrelation sequence is needed to acquire accurate timing information of received signals by means of its impulse-like autocorrelation property. In cryptography, the sequence is also required for avoiding correlation attack that exploits pseudorandom sequences having weak autocorrelation property. In last few years, several new binary two-level autocorrelation sequences have been discovered; Kasami power function (KPF) sequences [3], Welch-Gong (WG) sequences [15], and Maschietti's hyperoval sequences [12]. Together with traditionally known m -sequences, Gordon-Mills-Welch (GMW) sequences [8], quadratic residue (QR) sequences, and Hall's sextic residue sequences, these are all known binary two-level autocorrelation sequences of period $2^n - 1$.

For theory and practice of sequences, it would be interesting to study cross-correlation of a pair of binary two-level autocorrelation sequences of period $2^n - 1$. For odd n , the crosscorrelation has been investigated for following pairs of binary sequences.

- An m -sequence and its decimations [6] [11] [13] [9] (Gold, Kasami, Welch, Niho, and some conjectured exponents)
- An m -sequence and a GMW sequence with the same primitive polynomial [5], and a pair of GMW sequences [1] (The crosscorrelations are reduced to crosscorrelations of m -sequences)
- An m -sequence and a decimated KPF sequence with one particular exponent [3]

^{*} This work was supported by NSERC Grant RGPIN 227700-00.

- An m -sequence and a WG sequence without decimation [7]
- An m -sequence and a hyperoval sequence without decimation [4]
- A pair of KPF sequences without decimations [10]

If maximum crosscorrelation of a pair of binary sequences of period $2^n - 1$ is much larger than its optimum value achieving the Welch [17] or the Sidelnikov bound [16], then the pair is not so attractive for communication and cryptographic applications. For odd n , therefore, 3-valued crosscorrelation, i.e., $\{0, \pm 2^{\frac{n+1}{2}}\}$, has been intensively studied by many researchers. In this work, we are also interested in 5-valued crosscorrelation, i.e., $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$, which might be suboptimal for some applications.

In this paper, we study the 3- or 5-valued crosscorrelation of a pair of binary two-level autocorrelation sequences of period $2^n - 1$ for odd n , excluding GMW, QR, and Hall's sextic residue sequences. In Section 3, at most 5-valued crosscorrelation of m -sequences is discussed, which is linked to crosscorrelation of some other sequences. In Section 4, the 3- or 5-valued crosscorrelation of following pairs is investigated.

- A 5-term KPF sequence and a decimated WG sequence with one new exponent
- An m -sequence and a decimated WG sequence with one new exponent
- An m -sequence and a decimated hyperoval sequence with several new exponents
- An m -sequence and a decimated 3-term KPF sequence with one new exponent

With the new results as well as already known ones, relations of binary two-level autocorrelation sequences are summarized with respect to 3- or 5-valued crosscorrelation. From our experiments for $n = 13, 15, 17$, and 19 , we observed that all 3- or 5-valued crosscorrelations of a pair of binary two-level autocorrelation sequences are completely described by the already known and new results listed above unless both are m -sequences.

2 Preliminaries

In this section, we give preliminary definitions and concepts related to binary two-level autocorrelation sequences. Following notations will be used throughout this paper.

- $\mathbb{F}_q = GF(q)$ is a finite field with q elements and \mathbb{F}_q^* is a multiplicative group of \mathbb{F}_q .
- Let n, m be positive integers with $m|n$. A 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 a context is clear.

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

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

$$f(x) = \sum_{i=1}^r \text{Tr}_1^{n_i}(A_i x^{t_i}), \quad A_i \in \mathbb{F}_{2^{n_i}}$$

where t_i is a coset leader of a cyclotomic coset modulo $2^{n_i} - 1$, and $n_i | n$ is a size of the cyclotomic coset containing t_i . For any sequence $\underline{a} = \{a_i\} \in \mathcal{S}$, there exists $f(x) \in \mathcal{F}$ such that $a_i = f(\alpha^i)$, $i = 0, 1, \dots$, where α is a primitive element of \mathbb{F}_{2^n} . Then, $f(x)$ is called a *trace representation* of \underline{a} . In particular, \underline{a} is an *m-sequence* if $f(x)$ consists of a single trace term. Also, $f(x)$ is called an *orthogonal function* if \underline{a} is a binary two-level autocorrelation sequence. In this paper, we will always use its trace representation to represent any binary two-level autocorrelation sequence.

2.2 Decimation of Periodic Sequences

Let \underline{a} be a binary sequence of period $2^n - 1$ and $f(x)$ be a trace representation of \underline{a} . Let $0 < s < 2^n - 1$. Then, a sequence $\underline{b} = \{b_i\}$ is said to be an *s-decimation* of \underline{a} , denoted by $\underline{a}^{(s)}$, if elements of \underline{b} are given by $b_i = a_{si}$, $i = 0, 1, \dots$, where the multiplication is computed modulo $2^n - 1$. A trace representation of $\underline{a}^{(s)}$ is $f(x^s)$, denoted by $f^{(s)}$.

2.3 Crosscorrelation

Crosscorrelation of binary sequences \underline{a} and \underline{b} of period $2^n - 1$ is defined by

$$C_{\underline{a}, \underline{b}}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{a_{i+\tau} + b_i} = -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(\lambda x) + g(x)} = -1 + C_{f,g}(\lambda)$$

where $\lambda = \alpha^\tau$ with $0 \leq \tau \leq 2^n - 2$, τ is a phase shift of the sequence \underline{a} , α is a primitive element of \mathbb{F}_{2^n} , and $f(x)$ and $g(x)$ are trace representations of \underline{a} and \underline{b} , respectively. Throughout this paper, we always use $C_{f,g}(\lambda)$ to represent the crosscorrelation of \underline{a} and \underline{b} with their trace representations $f(x)$ and $g(x)$.

If $C_{f,g}(\lambda)$ belongs to $\{0, \pm 2^{\frac{n+1}{2}}\}$, then it is called *3-valued*. If it belongs to $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$, on the other hand, it is called *5-valued*. (In fact, a term ‘3- or 5-valued’ means the number of kinds of values that $C_{f,g}(\lambda)$ takes, no matter what its actual values are. In this paper, however, we restrict the term ‘3- or 5-valued’ by the above definition.) If $f(x) = \text{Tr}(x)$, then $C_{f,g}(\lambda)$ is the *Hadamard transform* of $g(x)$. In particular, $C_{f,g}(\lambda)$ is denoted by $H_d(\lambda)$ if $f(x) = \text{Tr}(x)$ and $g(x) = \text{Tr}(x^d)$, where the distribution of $H_d(\lambda)$ is determined by d .

2.4 Parseval's Equation

Let $f(x)$, $g(x)$, and $h(x)$ be functions from \mathbb{F}_{2^n} to \mathbb{F}_2 , respectively, and $h(x)$ be orthogonal. Then,

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{g(x)+f(x)} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_{2^n}} \widehat{g}_h(x) \widehat{f}_h(x) \quad (1)$$

where $\widehat{f}_h(x) = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{h(xy)+f(y)}$.

2.5 Recently Constructed Binary Two-level Autocorrelation Sequences

In this subsection, we briefly introduce three classes of binary two-level autocorrelation sequences of period $2^n - 1$ which have been constructed recently.

Kasami Power Function (KPF) Sequences: Let k be an integer of $1 \leq k < \lfloor \frac{n}{2} \rfloor$ with $\gcd(k, n) = 1$. For $d = 2^{2k} - 2^k + 1$, consider a set

$$B_k = \{(x+1)^d + x^d + 1 \mid x \in \mathbb{F}_{2^n}\}.$$

Then, its characteristic sequence given by

$$a_i = \begin{cases} 0, & \text{if } \alpha^i \in B_k \\ 1, & \text{if } \alpha^i \notin B_k \end{cases}$$

has an ideal two-level autocorrelation, where the sequence is called the *Kasami power function (KPF) sequence* [3]. According to k with $\gcd(k, n) = 1$, there exist $\frac{\phi(n)}{2}$ inequivalent KPF sequences of period $2^n - 1$, where $\phi(\cdot)$ is the Euler-totient function. If $k = 1$, in particular, the KPF sequence is identical to an m -sequence. Let $b_k(x)$ be a trace representation of the KPF sequence. For odd n , the KPF sequence has a Hadamard equivalence given by

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x) + b_k(x^{2^k+1})} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda^{\frac{2^k+1}{3}} x) + \text{Tr}(x^3)} = H_3(\lambda^{\frac{2^k+1}{3}}) \quad (2)$$

which is 3-valued [3].

Welch-Gong (WG) Sequences: For $n = 3k \pm 1$ and $d = 2^{2k} - 2^k + 1$, consider a map $\delta_k(x) = (x+1)^d + x^d$ and a set

$$W_k = \begin{cases} \delta_k(x), & \text{if } n \text{ is even} \\ \mathbb{F}_{2^n} \setminus \delta_k(x), & \text{if } n \text{ is odd.} \end{cases}$$

Then, its characteristic sequence given by

$$a_i = \begin{cases} 0, & \text{if } \alpha^i \in W_k \\ 1, & \text{if } \alpha^i \notin W_k \end{cases}$$

has an ideal two-level autocorrelation [14]. This sequence is identical to the *Welch-Gong sequence*, which is obtained from the Welch-Gong transformation of the 5-term sequences [15]. Let $w_k(x)$ be a trace representation of the WG sequence. For odd n , the WG sequence has a Hadamard equivalence [7] given by

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + w_k(x)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda^{d^{-1}} x) + Tr(x^{2^k+1})} = H_{2^k+1}(\lambda^{d^{-1}}) \quad (3)$$

which is also 3-valued.

Hyperoval Sequences: For odd n , consider a set

$$M_k = \{x + x^k | x \in \mathbb{F}_{2^n}\}$$

where k is given as follows [12].

- i) Singer type: $k = 2$, Segre type: $k = 6$.
- ii) Glynn type I: $k = 2^\sigma + 2^\tau$ where $\sigma = \frac{n+1}{2}$ and $4\tau \equiv 1 \pmod{n}$.
- iii) Glynn type II: $k = 3 \cdot 2^\sigma + 4$ with $\sigma = \frac{n+1}{2}$.

Then, a characteristic sequence of M_k given by

$$a_i = \begin{cases} 0, & \text{if } \alpha^i \in M_k \\ 1, & \text{if } \alpha^i \notin M_k \end{cases}$$

has an ideal two-level autocorrelation, where the sequence is called the *hyperoval sequence*. In this paper, we are only interested in the Glynn type I and II hyperoval sequences because the Singer and Segre type hyperoval sequences are identical to m -sequences and the KPF sequences for $k = 2$, respectively [3].

Let $h_k(x)$ be a trace representation of the hyperoval sequence. For odd n , Dillon derived a Hadamard equivalence of the hyperoval sequence [4], i.e.,

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + h_k(x)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda^{\frac{k-1}{k}} x) + Tr(x^k)} = H_k(\lambda^{\frac{k-1}{k}}). \quad (4)$$

If k is the Glynn type I exponent in ii), then (4) is 3-valued because k is quadratic. If k is the Glynn type II exponent in iii), on the other hand, then (4) is conjectured to be at most 5-valued because $k = 3 \cdot 2^{\frac{n+1}{2}} + 4 \equiv 2^{\frac{n-1}{2}} + 2^{\frac{n-3}{2}} + 1 \pmod{2^n - 1}$ is equivalently an inverse of the exponent of Conjecture 4-6 (1) in [13] where $H_{k-1}(\lambda)$ is conjectured to be at most 5-valued. We will restate this in Conjecture 2 of this paper.

3 Some Observations of Crosscorrelation of Binary m -sequences

In this section, we recall at most 5-valued crosscorrelation of a binary m -sequence and its d -decimation, i.e., $H_d(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + Tr(x^d)}$. In terms of 3-valued $H_d(\lambda)$, many exponents d are known, i.e., Gold [6], Kasami [11], Welch, Niho [13] exponents, and their respective inverses. In terms of 5-valued $H_d(\lambda)$, on the other hand, we need to clarify known results.

Proposition 1. Let n be odd, t be a positive integer of $1 \leq t \leq \frac{n-1}{2}$, and $e = \gcd(n, t)$ with $n/e \geq 4$. Let $d(k, l) = (1 + 2^k)/(1 + 2^l)$ with positive integers k and l ($k \neq l$). Then, $H_{d(k, l)}(\lambda)$ belongs to $\{0, \pm 2^{(n+e)/2}, \pm 2^{(n+3e)/2}\}$ if a pair (k, l) is one of following three cases

$$(a) (k, l) = (5t, t), \quad (b) (k, l) = (5t, 3t), \quad (c) (k, l) = (2t, t)$$

where the multiplication is computed modulo n . If $e = 1$, in particular, $H_{d(k, l)}(\lambda)$ is at most 5-valued, i.e., $\{0, \pm 2^{(n+1)/2}, \pm 2^{(n+3)/2}\}$.

Proposition 1-(a) has been proven by Niho (Lemma 4-1 in [13]). Although he had never stated Proposition 1-(b) and (c) in [13], we believe those have been implicitly known to many coding and sequence experts. In literatures, however, we could not find an explicit proof for (b) and (c) which is not trivial. So, we present it in this section because the result is linked to crosscorrelation of some other binary two-level autocorrelation sequences in Section 4. In order to prove Proposition 1, we need to use the Kasami's Theorem on weight distribution of subcodes of the second order Reed-Muller codes, which was partly used by Niho to prove Proposition 1-(a). In the following, we consider the odd case of his original theorem in [11].

Fact 1 (Kasami [11]) For odd n , let t and u be positive integers with $1 \leq t \leq \frac{n-1}{2}$ and $1 \leq u \leq \lfloor \frac{n}{2e} \rfloor + 1$ where $e = \gcd(n, t)$. Let $A_t(u)$ be a binary cyclic code of length $2^n - 1$ whose generator polynomial is given by $g_a(x) = \prod_{i=0}^{u-1} m_{1+2^{ti}}(x)$ where $m_i(x)$ is a minimal polynomial of α^i and α is a primitive element of \mathbb{F}_{2^n} . Similarly, let $F_t(u)$ be a binary cyclic code of length $2^n - 1$ whose generator polynomial is given by $g_f(x) = \prod_{i=0}^{u-1} m_{1+2^{t(i+1)}}(x)$. Dual codes of $A_t(u)$ and $F_t(u)$ are denoted by $A_t(u)^\perp$ and $F_t(u)^\perp$, respectively. Then, $A_t(u)^\perp$ and $F_t(u)^\perp$ have the same weight distribution as those of $A_e(u)^\perp$ whose distinct weights are given by

$$\{0, 2^{n-1}, 2^{n-1} \pm 2^{(n-e)/2+ie-1}\} \text{ for } 1 \leq i \leq u-1.$$

Using Fact 1, we can prove Proposition 1.

Proof of Proposition 1. In (a) and (b), $H_{d(k, l)}(\lambda)$ is represented by

$$H_{d(k, l)}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x + x^{\frac{1+2^k}{1+2^l}})} = \begin{cases} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x^{1+2^t} + x^{1+2^{5t}})} & \text{for (a)} \\ \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x^{1+2^{3t}} + x^{1+2^{5t}})} & \text{for (b)}. \end{cases}$$

Then, we can consider codes \mathcal{R}_5 and $\mathcal{R}_{5/3}$ given by

$$\begin{aligned} \mathcal{R}_5 &= \{\text{Tr}(\alpha x^{1+2^t} + \beta x^{1+2^{5t}}) | \alpha, \beta \in \mathbb{F}_{2^n}\}, \\ \mathcal{R}_{5/3} &= \{\text{Tr}(\gamma x^{1+2^{3t}} + \delta x^{1+2^{5t}}) | \gamma, \delta \in \mathbb{F}_{2^n}\} \end{aligned}$$

which are subcodes of a dual of $F_t(u)$ for $u = 3$ where $F_t(u)$ has zeros $1 + 2^{t(2i+1)}$, $i = 0, 1, 2$. For any t of $1 \leq t \leq \frac{n-1}{2}$, therefore, weight distributions of

Table 1. (k, l) pairs and $d(k, l)$'s for 5-valued crosscorrelation of $Tr(x)$ and $Tr(x^{d(k, l)})$

n	(k, l)	$d(k, l)$	n	(k, l)	$d(k, l)$	n	(k, l)	$d(k, l)$	n	(k, l)	$d(k, l)$
9	$(2, 1)^{*,o}$	43	13	$(4, 2)^{+,o}$	1645	15	$(7, 4)^o$	2895	17	$(4, 3)^*$	14571
9	$(4, 1)^{*,o}$	11	13	$(5, 3)^{+,o}$	1367	15	$(6, 5)^+$	1119	17	$(5, 3)^+$	21847
9	$(4, 2)^{*,o}$	109	13	$(6, 3)^{+,o}$	939	15	$(7, 5)^*$	3229	17	$(6, 3)^o$	14679
11	$(2, 1)^{*,+,o}$	171	13	$(5, 4)^{+,o}$	1461	17	$(2, 1)^o$	10923	17	$(7, 3)^o$	15019
11	$(5, 1)^{*,+,o}$	11	13	$(6, 4)^*$	497	17	$(4, 1)^+$	2731	17	$(6, 4)^*$	11567
11	$(4, 2)^{*,+,o}$	423	15	$(2, 1)^o$	2731	17	$(5, 1)^*$	11	17	$(8, 4)^o$	7831
11	$(4, 3)^{*,+,o}$	235	15	$(5, 1)^*$	11	17	$(7, 1)^*$	43	17	$(6, 5)^o$	12909
11	$(5, 3)^{*,+,o}$	343	15	$(7, 1)^o$	43	17	$(8, 1)^o$	171	17	$(7, 5)^o$	13917
13	$(2, 1)^{+,o}$	683	15	$(4, 2)^o$	6567	17	$(3, 2)^*$	3277	17	$(8, 5)^*$	4003
13	$(5, 1)^*$	11	15	$(5, 2)^*$	205	17	$(4, 2)^o$	26221	17	$(7, 6)^+$	10587
13	$(6, 1)^{+,o}$	43	15	$(5, 3)^+$	5463	17	$(7, 2)^*$	205	17	$(8, 6)^*$	2143
13	$(3, 2)^*$	205	15	$(5, 4)^*$	1943	17	$(8, 2)^+$	26317			

\mathcal{R}_5 and $\mathcal{R}_{5/3}$ are immediate from Fact 1, and consequently $H_{d(k, l)}(\lambda)$ belongs to $\{0, \pm 2^{\frac{n+e}{2}}, \pm 2^{\frac{n+3e}{2}}\}$ for both (a) and (b).

In (c), on the other hand, $A_t(3)$ generated by $g_a(x)$ has zeros $\{2, 1+2^t, 1+2^{2t}\}$, so a code \mathcal{R}_2 given by

$$\mathcal{R}_2 = \{Tr(\zeta x^{1+2^t} + \eta x^{1+2^{2t}}) | \zeta, \eta \in \mathbb{F}_{2^n}\}$$

is also a subcode of a dual of $A_t(3)$. From Fact 1, therefore, it is clear that $H_{d(k, l)}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x^{1+2^t} + x^{1+2^{2t}})}$ belongs to $\{0, \pm 2^{\frac{n+e}{2}}, \pm 2^{\frac{n+3e}{2}}\}$. \square

Lemma 1. For odd n , let k and l be positive integers of $1 \leq k, l \leq \frac{n-1}{2}$ ($k \neq l$), and $d(k, l) = \frac{1+2^k}{1+2^l}$. Then, $H_{d(n-k, l)}(\lambda)$, $H_{d(k, n-l)}(\lambda)$, and $H_{d(n-k, n-l)}(\lambda)$ have the same correlation spectrum as $H_{d(k, l)}(\lambda)$. Furthermore, $H_{d(l, k)}(\lambda)$ also belongs to the same correlation spectrum as $H_{d(k, l)}(\lambda)$.

Proof. Note that $H_{d \cdot 2^j}(\lambda) = H_d(\lambda)$ for any integer j [9]. Since $2^{n-k} \cdot (1+2^k) = 2^{n-k} + 2^n \equiv 2^{n-k} + 1 \pmod{2^n - 1}$, we see that $1+2^k$ and $1+2^{n-k}$ belong to the same cyclotomic coset. Hence, $d(k, l)$ belongs to the same cyclotomic coset as $d(n-k, l)$. Therefore, $H_{d(k, l)}(\lambda)$ and $H_{d(n-k, l)}(\lambda)$ have the same correlation distribution. By the similar way, cases of $H_{d(k, n-l)}(\lambda)$ and $H_{d(n-k, n-l)}(\lambda)$ are simply proved. From $d(l, k) = d(k, l)^{-1}$, furthermore, it is immediate that $H_{d(k, l)}(\lambda)$ and $H_{d(l, k)}(\lambda)$ belong to the same correlation spectrum. \square

Table 1 shows (k, l) pairs and $d(k, l) = \frac{1+2^k}{1+2^l}$ corresponding to 5-valued $H_{d(k, l)}(\lambda)$ in computer experiments. We only list pairs of $1 \leq l < k \leq \frac{n-1}{2}$ which are enough to cover the other possible pairs from Lemma 1. Each pair of ‘*’ is due to (a), ‘+’ due to (b), and ‘o’ due to (c) in Proposition 1, respectively. For odd $n = 9 - 17$, Proposition 1 is verified from the experiments.

4 Crosscorrelation of a Pair of Binary Two-level Autocorrelation Sequences

4.1 A Pair of KPF Sequences

In [10], Hertel investigated crosscorrelation of two distinct KPF sequences for odd n . (She called the sequences as Dillon-Dobbertin (DD) sequences after their discoverers' name.)

Fact 2 (Hertel [10]) *For odd n , let k and l be distinct positive integers with $\gcd(n, k) = \gcd(n, l) = 1$. Let $b_k(x)$ and $b_l(x)$ be trace representations of two distinct KPF sequences, respectively. Then,*

$$C_{b_k, b_l}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b_k(\lambda x) + b_l(x)} = H_{d(k, l)}(\lambda^{\frac{1}{1+2^k}}), \quad \lambda \in \mathbb{F}_{2^n}$$

where $d(k, l) = \frac{1+2^k}{1+2^l}$. If $(k, l) = (3t, t)$, in particular, $C_{b_k, b_l}(\lambda)$ is 3-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}\}$.

Corollary 1. *With the notation of Proposition 1 and Fact 2, if a pair (k, l) is one of the pairs in Proposition 1, then $C_{b_k, b_l}(\lambda)$ is at most 5-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$.*

Proof. Corollary 1 is immediate from combining Proposition 1 and Fact 2. \square

From Corollary 1, it is obvious that crosscorrelation of $b_k(x)$ and $b_l(x)$ with a (k, l) pair in Table 1 is 5-valued.

4.2 5-term KPF Sequences and Welch-Gong (WG) Sequences

The WG sequences are obtained from the Welch-Gong transformation of KPF sequences for $k = \frac{n+1}{3}$, where the KPF sequences always have five trace terms [3] [15]. By the Parseval's equation exploited in [10], we derive a theorem on crosscorrelation of the 5-term KPF and the WG sequences.

Theorem 1. *Let n be odd and $n = 3k+1$. Let $b_k(x)$ and $w_k(x)$ be trace representations of the KPF sequences and the WG sequences, respectively. For $s = \frac{1}{2^k+1}$, crosscorrelation of the two sequences given by*

$$C_{b_k, w_k^{(s)}}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b_k(\lambda x) + w_k(x^s)} = H_{\frac{2^k+1}{3}}(\lambda)$$

is 3-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}\}$.

Proof. Applying the Parseval's equation in (1),

$$\begin{aligned}
C_{b_k, w_k^{(s)}}(\lambda) &= \frac{1}{2^n} \sum_{x \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{b_k(\lambda y) + Tr(xy^{\frac{1}{2^k+1}})} \sum_{z \in \mathbb{F}_{2^n}} (-1)^{w_k(z^s) + Tr(xz^{\frac{1}{2^k+1}})} \\
&= \frac{1}{2^{2n}} \sum_{x, z \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{b_k(y) + Tr(x\lambda^{-\frac{1}{2^k+1}} y^{\frac{1}{2^k+1}})} \\
&\quad \cdot \sum_{u \in \mathbb{F}_{2^n}} (-1)^{w_k(u^s) + Tr(zu^s)} \sum_{v \in \mathbb{F}_{2^n}} (-1)^{Tr(xv^{\frac{1}{2^k+1}}) + Tr(zv^s)}.
\end{aligned} \tag{5}$$

If $s = \frac{1}{2^k+1}$, then we have

$$\sum_{v \in \mathbb{F}_{2^n}} (-1)^{Tr(xv^{\frac{1}{2^k+1}}) + Tr(zv^s)} = \sum_{v \in \mathbb{F}_{2^n}} (-1)^{Tr((x+z)v^{\frac{1}{2^k+1}})} = \begin{cases} 2^n, & \text{if } x = z \\ 0, & \text{if } x \neq z. \end{cases}$$

If the Hadamard equivalences (2) and (3) are applied to (5), then we have

$$\begin{aligned}
C_{b_k, w_k^{(s)}}(\lambda) &= \frac{1}{2^n} \sum_{x \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda^{-\frac{1}{3}} x^{\frac{2^k+1}{3}} y) + Tr(y^3)} \sum_{u \in \mathbb{F}_{2^n}} (-1)^{Tr(x^b u) + Tr(u^a)} \\
&= \frac{1}{2^n} \sum_{y \in \mathbb{F}_{2^n}} \sum_{u \in \mathbb{F}_{2^n}} (-1)^{Tr(y^3) + Tr(u^a)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda^{-\frac{1}{3}} x^{\frac{2^k+1}{3}} y) + Tr(xu^b)}
\end{aligned}$$

where $a = 2^k + 1$ and $b = (2^{2k} - 2^k + 1)^{-1}$. From $3k = n \pm 1$, it is clear that $b^{-1} \cdot \frac{2^k+1}{3} = \frac{2^{3k}+1}{3} \equiv 1 \pmod{2^n - 1}$. Thus, we have $b \equiv \frac{2^k+1}{3} \pmod{2^n - 1}$. Consequently,

$$\begin{aligned}
C_{b_k, w_k^{(s)}}(\lambda) &= \frac{1}{2^n} \sum_{y \in \mathbb{F}_{2^n}} \sum_{u \in \mathbb{F}_{2^n}} (-1)^{Tr(y^3) + Tr(u^a)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr((\lambda^{-\frac{1}{3}} y + u)x^{\frac{2^k+1}{3}})} \\
&= \sum_{u \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda u^3 + u^a)} = \sum_{u \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda u) + Tr(u^{\frac{2^k+1}{3}})} = H_{\frac{2^k+1}{3}}(\lambda)
\end{aligned} \tag{6}$$

where $y = \lambda^{\frac{1}{3}} u$. In (6), $\frac{2^k+1}{3} \equiv b = (2^{2k} - 2^k + 1)^{-1}$. Since it is an inverse of the Kasami exponent with $\gcd(n, k) = 1$, we see that $H_{\frac{2^k+1}{3}}(\lambda)$ is 3-valued and so is $C_{b_k, w_k^{(s)}}(\lambda)$. \square

4.3 m -sequences and Welch-Gong (WG) Sequences

In an effort to search for new two-level autocorrelation sequences, Gong and Golomb proposed the *decimation-Hadamard transform (DHT)* in [7]. With respect to orthogonal functions $f(x)$ and $h(x)$, they defined a *realizable pair* (v, t)

of $g(x)$ in the DHT by generalizing the Hadamard equivalence developed in [3], i.e.,

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{h(\lambda^t x) + f(x^v)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{h(\lambda x) + g(x)}. \quad (7)$$

They also showed that there exist at most 6 realizable pairs for the realization. Among them, we will use the fact that if (v, t) is a realizable pair of $g(x)$, then $(t, -(vt)^{-1})$ is also a realizable pair of $g(x^{(vt)^{-1}})$ [7] from which we have

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{h(\lambda^{-(vt)^{-1}} x) + f(x^t)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{h(\lambda x) + g(x^{(vt)^{-1}})}. \quad (8)$$

Using this, we establish a theorem on crosscorrelation of m -sequences and WG sequences.

Theorem 2. *Let n be odd and $n = 3k \pm 1$, and $d = 2^{2k} - 2^k + 1$. Let $w_k(x)$ be a trace representation of the WG sequences. For $s = \frac{d}{2^k + 1}$, crosscorrelation of m -sequences and the WG sequences given by*

$$C_{Tr, w_k^{(s)}}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + w_k(x^s)} = H_{d-1}(\lambda^{-s})$$

is 3-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}\}$.

Proof. From the Hadamard equivalence of (3), we have a realizable pair $(v, t) = (2^k + 1, d^{-1})$ in (7) where $f(x) = h(x) = Tr(x)$ and $g(x) = w_k(x)$. From (8), therefore, we have

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda^{-\frac{d}{2^k+1}} x) + Tr(x^{d^{-1}})} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + w_k(x^{\frac{d}{2^k+1}})}.$$

Thus, $C_{Tr, w_k^{(s)}}(\lambda) = H_{d-1}(\lambda^{-s})$ for $s = \frac{d}{2^k+1}$. Since d is the Kasami exponent with $\gcd(n, k) = 1$, $H_{d-1}(\lambda^{-s})$ is 3-valued and so is $C_{Tr, w_k^{(s)}}(\lambda)$. \square

4.4 m -sequences and Hyperoval Sequences

Applying (8) to hyperoval sequences with the Hadamard equivalence of (4), we can derive another Hadamard equivalence, i.e.,

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + h_k(x^{\frac{1}{k-1}})} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda^{-\frac{1}{k-1}} x) + Tr(x^{\frac{k-1}{k}})} = H_{\frac{k-1}{k}}(\lambda^{-\frac{1}{k-1}}). \quad (9)$$

From (9), we consider a theorem for the Glynn type II hyperoval sequences.

Theorem 3. *Let n be odd and $k = 3 \cdot 2^\sigma + 4$ where $\sigma = \frac{n+1}{2}$. Let $h_k(x)$ be a trace representation of the Glynn type II hyperoval sequences. For $s = \frac{1}{k-1}$,*

crosscorrelation of m -sequences and the Glynn type II hyperoval sequences given by

$$C_{Tr, h_k^{(s)}}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + h_k(x^s)} = H_{\frac{k-1}{k}}(\lambda^{-s}) \quad (10)$$

is at most 5-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$.

Proof. From (9), $C_{Tr, h_k^{(s)}}(\lambda)$ is determined by a decimation factor $\frac{k-1}{k}$ of a trace function. Note that the cyclotomic coset that $\frac{k-1}{k}$ belongs to does not change by multiplying its numerator and denominator by $2^{\frac{n-1}{2}}$ and $2^{\frac{n-3}{2}}$, respectively. Then,

$$\begin{aligned} \frac{k-1}{k} &\equiv \frac{2^{\frac{n-1}{2}}}{2^{\frac{n-3}{2}}} \cdot \frac{(k-1)}{k} = \frac{2^{\frac{n-1}{2}}}{2^{\frac{n-3}{2}}} \cdot \frac{3 \cdot (1 + 2^{\frac{n+1}{2}})}{(2^{\frac{n+3}{2}} + 2^{\frac{n+1}{2}} + 4)} \equiv \frac{3 \cdot (1 + 2^{\frac{n-1}{2}})}{(1 + 2^{\frac{n-1}{2}})^2} \\ &= \frac{1+2}{1+2^{\frac{n-1}{2}}} \pmod{2^n-1}. \end{aligned}$$

Hence, $\frac{k-1}{k} \equiv \frac{1+2^\mu}{1+2^\nu} = d(\mu, \nu)$ in Proposition 1 where $\mu = 1$ and $\nu = \frac{n-1}{2}$. Since $2\nu = n - \mu$, we have $(n - \mu, \nu) = (2t, t)$ with $t = \frac{n-1}{2}$, a pair of Proposition 1-(c). From $e = \gcd(n, t) = \gcd(n, \frac{n-1}{2}) = 1$, we see that $H_{d(n-\mu, \nu)}(\lambda)$ is at most 5-valued and so is $H_{d(\mu, \nu)}(\lambda)$ from Lemma 1. \square

In terms of the Glynn type I hyperoval sequences, on the other hand, $k = 2^\sigma + 2^\tau$ where $\sigma = \frac{n+1}{2}$ and $\tau = \frac{n+1}{4}$ or $\tau = \frac{3n+1}{4}$ such that $4\tau \equiv 1 \pmod{n}$. Using the similar approach to the proof of Theorem 3, we can establish the following equivalence of $\frac{k-1}{k}$.

$$\frac{k-1}{k} \equiv \begin{cases} 2^{\frac{n-1}{2}} - 2^{\frac{n+1}{4}} + 1, & \text{if } \tau = \frac{n+1}{4} \\ 2^{\frac{n+1}{2}} - 2^{\frac{n+3}{4}} + 1, & \text{if } \tau = \frac{3n+1}{4}. \end{cases} \quad (11)$$

In (11), we see that $\frac{k-1}{k}$ is equivalent to the decimation factor r in Conjecture 4-6 (3) and (4) of [13], where $H_r(\lambda)$ is conjectured to be at most 5-valued. Together with our experimental results, we establish the following conjecture.

Conjecture 1. Let n be odd and $k = 2^\sigma + 2^\tau$ where $\sigma = \frac{n+1}{2}$ and $4\tau \equiv 1 \pmod{n}$. Let $h_k(x)$ be a trace representation of the Glynn type I hyperoval sequences. For $s = \frac{1}{k-1}$, crosscorrelation of m -sequences and the Glynn type I hyperoval sequences given by $C_{Tr, h_k^{(s)}}(\lambda)$ in (10) is at most 5-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$.

With respect to crosscorrelation of m -sequences and the Glynn type II hyperoval sequences, we also observed another exponent corresponding to at most 5-valued crosscorrelation. Together with (4) which is conjectured to be at most 5-valued for the Glynn type II hyperoval sequences, we establish Conjecture 2.

Conjecture 2. For odd n , let $h_k(x)$ be a trace representation of the Glynn type II hyperoval sequences. For $s = 1$ or $\frac{1}{3}$, crosscorrelation of m -sequences and the Glynn type II hyperoval sequences given by $C_{Tr, h_k^{(s)}}(\lambda)$ is at most 5-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$.

Conjectures 1 and 2 have been verified for odd $n = 9 - 19$ through computer experiments.

4.5 m -sequences and 3-term KPF Sequences

In [3], the 3-term KPF sequences are represented by

$$b_k(x) = \text{Tr}(x + x^{2^k+1} + x^{2^k-1}), \quad k = \frac{n+1}{2}$$

where n is odd. On the other hand, T_3 sequences, or 3-term sequences with ideal two-level autocorrelation which had been conjectured in [15] are represented by

$$T_3(x) = \text{Tr}(x + x^r + x^{r^2}), \quad r = 2^{\frac{n-1}{2}} + 1.$$

With the equivalence under modulo $2^n - 1$, we see that the T_3 sequences are decimation of the 3-term KPF sequences, i.e., $T_3(x) = b_k(x^{2^k+1})$ where $k = \frac{n+1}{2}$. Using this relation, we establish the following theorem.

Theorem 4. *Let n be odd and $k = \frac{n+1}{2}$. Let $b_k(x)$ be a trace representation of the 3-term KPF sequences. For $s = 2^k - 1$, crosscorrelation of m -sequences and the 3-term KPF sequences given by*

$$C_{T_r, b_k^{(s)}}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x) + b_k(x^s)}$$

is at most 5-valued, i.e., $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$.

Proof. In [2], Chang *et al.* showed that a binary cyclic code represented by

$$\mathcal{T} = \{\text{Tr}(ax + bx^r + cx^{r^2}) | a, b, c \in \mathbb{F}_{2^n}, r = 2^{\frac{n-1}{2}} + 1\}$$

is a dual of a triple error correcting cyclic code and has five nonzero distinct weights. Then, crosscorrelation of m -sequences and the T_3 sequences given by $C_{T_r, T_3}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x) + T_3(x)}$ is at most 5-valued - in fact, 3-valued - because the exponent in the summation is a codeword of \mathcal{T} . In the following, we can consider another at most 5-valued crosscorrelation $C_{T_r(r^2), T_3}(\lambda)$ where the exponent is also a codeword of \mathcal{T} . Note that $2^{\frac{n+1}{2}} \cdot r = 2^n + 2^{\frac{n+1}{2}} \equiv 1 + 2^k \pmod{2^n - 1}$, and thus $r \equiv 2^k + 1$. Therefore, $T_3(x) = b_k(x^r)$ where $k = \frac{n+1}{2}$. Then,

$$\begin{aligned} C_{T_r(r^2), T_3}(\lambda) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda^{r^2} x^{r^2}) + T_3(x)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda^{r^2} x) + T_3(x^{r^{-2}})} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda^{r^2} x) + b_k(x^{r^{-1}})} = C_{T_r, b_k^{(s)}}(\lambda^{r^2}) \end{aligned}$$

where $s = r^{-1} = (2^k + 1)^{-1} \equiv 2^k - 1 \pmod{2^n - 1}$. Hence, $C_{T_r, b_k^{(s)}}(\lambda)$ is at most 5-valued. \square

5 Conclusion and Discussion

In this paper, we have studied 3- or 5-valued crosscorrelation of a pair of binary two-level autocorrelation sequences given by

$$C_{f,g^{(s)}}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(\lambda x) + g(x^s)}$$

where n is odd, and $f(x)$ and $g(x)$ are trace representations of the pair, excluding GMW, QR, and Hall's sextic residue sequences.

If $f(x) = g(x) = Tr(x)$, all known exponents s 's of 3- or 5-valued $C_{f,g^{(s)}}(\lambda)$ are (a) Gold, Kasami, Welch, Niho exponents, and their respective inverses; (b) the exponents of Proposition 1; (c) the other exponents conjectured by Niho [13] and their inverses. Otherwise, all known exponents s 's of 3- or 5-valued $C_{f,g^{(s)}}(\lambda)$ for the corresponding $f(x)$ and $g(x)$ are (a) $s = 2^k + 1$ from (2), or $s = 1$ from (3) and (4); (b) s 's from Fact 2 and Theorems 1 - 4; (c) s 's from Conjectures 1 and 2. With the classification, we can summarize relations of binary two-level autocorrelation sequences with respect to 3- or 5-valued crosscorrelation by Fig. 1, where a solid line is for exactly 3-valued crosscorrelation and a dotted line for at most 5-valued crosscorrelation. (For small n , it may be 3-valued in some cases.) In Fig. 1, the crosscorrelations corresponding to the exponents s with '*' are proved or conjectured in this paper.

From the observation of our experiments for $n = 13, 15, 17$, and 19, it is interesting that the exponents and relations in Fig. 1 completely describe all 3- or 5-valued crosscorrelations of binary two-level autocorrelation sequences unless both are m -sequences.

Acknowledgment

The authors would like to thank Professor Tor Helleseth for helpful comments on Proposition 1.

References

1. Antweiler, M.: Cross-correlation of p -ary GMW sequences. IEEE Trans. Inform. Theory, Vol. 40 (1994) 1253-1261
2. Chang, A., Gaal, P., Golomb, S. W., Gong, G., Helleseth, T., Kumar, P. V.: On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code. IEEE Trans. Inform. Theory, Vol. 46-2 (2000) 680-687
3. Dillon, J. F., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields and Their Applications 10 (2004) 342-389
4. Dillon, J. F.: Multiplicative difference sets via additive characters. Designs, Codes and Cryptography, Vol. 17 (1999) 225-235
5. Games, R. A.: Crosscorrelation of m -sequences and GMW-sequences with the same primitive polynomial. Discrete Applied Mathematics, Vol. 12 (1985) 139-146

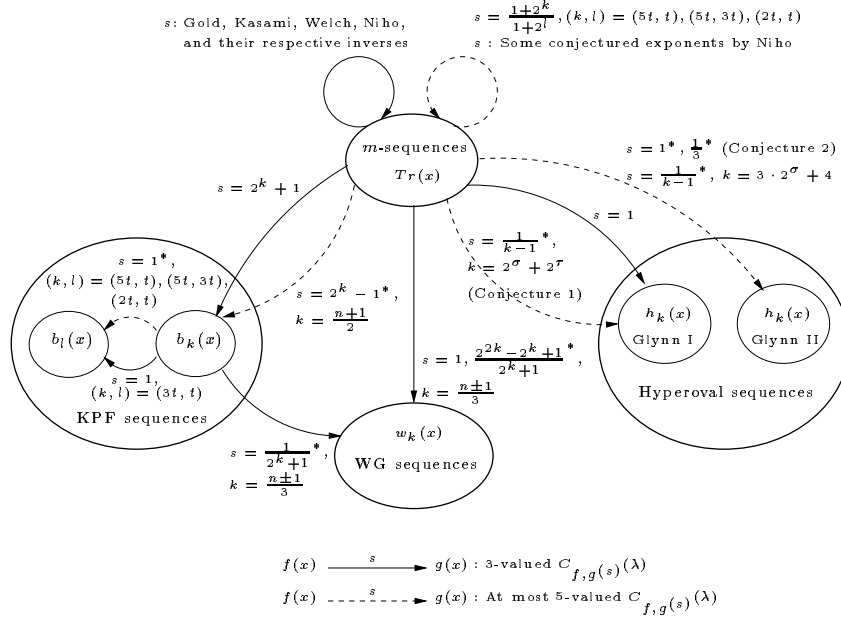


Fig. 1. Relations of binary two-level autocorrelation sequences with respect to 3- or 5-valued crosscorrelation ($\gcd(n, t) = 1$, $\sigma = \frac{n+1}{2}$, and $4\tau \equiv 1 \pmod{n}$). The crosscorrelations corresponding to the exponents s with '*' are proved or conjectured in this paper.

6. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Inform. Theory, Vol. 14 (1968) 154-156
7. Gong, G., Golomb, S. W.: The decimation-Hadamard transform of two-level autocorrelation sequences. IEEE Trans. Inform. Theory, Vol. 48-4 (2002) 853-865
8. Gordon, B., Mills, W. H., Welch, L. R.: Some new difference sets. Canadian Journal of Mathematics, Vol. 14-4 (1962) 614-625
9. Helleseeth, T., Kumar, P. V.: Sequences with Low Correlation. A chapter in Handbook of Coding Theory. Edited by Pless, V. and Huffman, C. Elsevier Science Publishers (1998)
10. Hertel, D.: Cross-correlation properties of perfect binary sequences. Lecture Notes in Computer Science, Vol. 3486. Edited by Helleseeth, T. et al. Springer-Verlag (2005) 208-219
11. Kasami, T.: Weight enumerators for several classes of subcodes of the 2nd-order Reed-Muller codes. Information and Control, Vol. 18 (1971) 369-394
12. Maschietti, A.: Difference sets and hyperovals. Designs, Codes and Cryptography, Vol. 14 (1998) 89-98
13. Niho, Y.: Multi-valued cross-correlation functions between two maximal linear recursive sequences. Ph.D. Dissertation. University of Southern California (1972)
14. No, J. S., Chung, H. C., Yun, M. S.: Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z + 1)^d$. IEEE Trans. Inform. Theory, Vol. 44-3 (1998) 1278-1282

15. No, J. S., Golomb, S. W., Gong, G., Lee, H. K., Gaal, P.: Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation. IEEE Trans. Inform. Theory, Vol.44-2 (1998) 814-817
16. Sidelnikov, V. M.: On mutual correlation of sequences. Soviet Math. Dokl, Vol. 12 (1971) 197-201
17. Welch, L. R.: Lower bounds on the maximum cross correlation of signals. IEEE Trans. Inform. Theory, Vol. IT-20 (1974) 397-399