East Asian Mathematical Journal
Vol. 29 (2013), No. 5, pp. 529–536
http://dx.doi.org/10.7858/eamj.2013.037

NEW FAMILY OF BINARY SEQUENCES WITH FOUR-VALUED CROSS-CORRELATION

Han-Doo Kim, Sung-Jin Cho*, Min-Jeong Kwon, and Un-Sook Choi

Abstract. In this paper, we find the values and the number of occurrences of each value of the cross-correlation function $C_d(\tau)$ when $d = \frac{2^{k-1}}{2^s-1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1)$, where $n = 2k, s$ is an integer such that $2s$ divides k, and i is odd.

1. Introduction

The design of binary sequences with good correlation properties are important for many research areas in communication systems. Finding the cross-correlation between two maximal length sequences of the same period has been a meaningful research problem. For the theory of finite fields, maximal length sequences and sequences in general, we refer to [5]. The finite field with q elements will be denoted by $GF(q)$. It is well known that $q = 2^k$ for some integer $k \geq 1$. The multiplicative group of $GF(q)$ will be denoted by $GF(q)^*$. The group $GF(q)^*$ is cyclic and a primitive element of $GF(q)^*$ is a generator of $GF(q)^*$. An irreducible polynomial $f(x) \in GF(2)[x]$ of degree n is primitive over $GF(2)$ if it is the minimum polynomial of some primitive element of $GF(2^n)$. Recall that the trace function Tr_k^n from the field $GF(2^n)$ onto the subfield $GF(2^k)$ is defined by $Tr_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{(t-1)k}}$ where $t = n/k$. For the properties of the trace function, see [7]. Consider two binary m-sequences $u(t)$ and $v(t)$, $(t = 0, 1, \cdots,)$ of period $2^n - 1$. Let α be a primitive element of the finite field $GF(2^n)$. We may assume that $u(t) = Tr_1^n(\alpha^t)$ and $v(t) = u(dt)(1 \leq d \leq 2^n - 2)$ where $Tr_1^n(x) : GF(2^n) \to GF(2)$ is the well-known trace function and d is a decimation, that is, an integer satisfying $gcd(d, 2^n - 1) = 1$. The cross-correlation function $C_d(\tau)$ between the binary sequences $u(t)$ and $v(t) = u(dt)(t = 0, 1, \cdots, 2^n - 2)$ is defined for $\tau = 0, 1, \cdots, 2^n - 2$ and given by

Received December 14, 2012; Revised October 16, 2013; Accepted November 20, 2013.
2000 *Mathematics Subject Classification.* 97N70, 11G25, 94A55, 68Q87.
Key words and phrases. Cross-correlation, maximal length sequence, finite field, decimation, Niho's theorem.
This work was supported by the 2009 Inje University research grant.
*Corresponding author.

$$
\begin{aligned}
C_d(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{u(t+\tau)+v(t)} \\
&= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(\alpha^{t+\tau}+\alpha^{dt})}.
\end{aligned}
$$

One of important problems in the theory of sequences is to determine the values and the number of occurrences of each value taken on by the cross-correlation $C_d(\tau)$. Several decimations leading to three and four-valued correlation function are known.

If d is not a power of two, then the cross-correlation function takes on at least three values [11].

The well known four-valued cases are:

(4a) $d = 2^{n/2+1} - 1$, with $n \equiv 0 \pmod 4$,

(4b) $d = (2^{n/2} + 1)(2^{n/4} - 1) + 2$, with $n \equiv 0 \pmod 4$,

(4c) $d = \sum_{i=0}^{n/2} 2^{im}$, with $n \equiv 0 \pmod 4$, $0 < m < n$, $gcd(m, n) = 1$,

(4d) $d = \frac{2^k-1}{2^s-1}(2^{2k} + 2^{s+1} - 2^{k+1} - 1)$, $n = 2k$, $2s|k$,

(4e) $d = (\frac{p^{2k}+1}{2})^2$, with $n = 4k$ and p an odd prime.

(4a) and (4b) were proved by Niho [8], (4c) was proved by Dobbertin [1] and (4d) was proved by Helleseth and Rosendahl [3], and Rosendahl [9]. (4e) was proved by Seo et al. [10] and Luo [6]. In 2007, Helleseth et al. [2] proposed a d which has at most four-valued cross-correlation functions.

In this paper, we provide a family of decimations which lead to a four-valued cross-correlation. The decimations d are as follows: $d = \frac{2^k-1}{2^s-1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1)$ where $n = 2k$ and s is an integer such that $2s$ divides k, and i is odd. When $i = 1$ this is equal to $(4d)$.

2. Preliminaries

In this section we introduce some basic results and methods in order to completely determine the cross-correlations of the proposed four-valued sequence family. Let $n = 2k$, where k is an even integer and $q = 2^k$. For $x \in GF(q^2)$ we define $\overline{x} = x^q$. Then

(a) $\overline{x+y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{x}\ \overline{y}$ for all $x, y \in GF(q^2)$ and

(b) $x + \overline{x} \in GF(q)$ and $x\overline{x} \in GF(q)$ for all $x \in GF(q^2)$.

Define the unit circle of $GF(q^2)$ by $S = \{x \in GF(q^2) : x\overline{x} = 1\}$. Then S is the group of $(q+1)$-th roots of unity in $GF(q^2)$ and is a subgroup of $GF(q^2)^*$.

The following theorem is useful in finding the complete distribution of the values of $C_d(\tau)$.

Theorem 2.1 [8, 11] For some integer $d(1 \le d \le 2^n - 2)$, we have
(a) $C_d(\tau)$ is a real number,
(b) $\sum_{\tau=0}^{2^n-2}(C_d(\tau)+1) = 2^n$,
(c) $\sum_{\tau=0}^{2^n-2}(C_d(\tau)+1)^2 = 2^{2n}$,
(d) $\sum_{\tau=0}^{2^n-2}(C_d(\tau)+1)^3 = 2^{2n}b$,
where b is the number of $x \in GF(q^2)$ such that

$$(x+1)^d = x^d + 1.$$

Niho [8] and Rosendahl [9] proved the following two theorems respectively.

Theorem 2.2 Let $n = 2k$ and $y \in GF(2^n)^*$. The equation

$$x^{2^s+1} + yx^{2^s} + \overline{y}x + 1 = 0$$

has either $0, 1, 2$ or $2^{gcd(s,k)} + 1$ solutions x in S.

Theorem 2.3 Let $n = 2k$ and assume that $d \equiv 1(mod\ 2^k - 1)$. And let $C_d(\tau) + 1 = \Delta_d(\tau)$. Then $\Delta_d(\tau) = 2^k(N(y) - 1)$ where $N(y)$ is the number of $x \in \{x \in GF(2^n) : x^{2^k+1} = 1\}$ such that

$$x^d + yx + \overline{y}x^{-1} + x^{-d} = 0$$

and $y \in GF(2^n)^*$.

Lemma 2.4 Let k be even. And let s be an integer such that $2s$ divides k. Then $gcd(2^k + 1, 2^s - 1) = 1$.
Proof. Since $s/gcd(k, s) = 1$ is odd, $gcd(2^k + 1, 2^s - 1) = 1$.

Lemma 2.5 Let k be even. And let s be an integer such that $2s$ divides k. Then $gcd(2^k + 1, 2^s + 1) = 1$.
Proof. Since $2s|k$, let $k = 2as$ for some integer a. From $2^k + 1 = 2^{k-s}(2^s + 1) - 2^{k-s} + 1, gcd(2^k + 1, 2^s + 1) = gcd(2^{k-s} - 1, 2^s + 1)$. Since $\frac{k-s}{gcd(k-s,s)} = \frac{k-s}{gcd(k,s)} = \frac{k-s}{s} = \frac{2as-s}{s} = 2a - 1$ is odd, $gcd(2^{k-s} - 1, 2^s + 1) = 1$. Hence $gcd(2^k + 1, 2^s + 1) = 1$.

3. Results for four-valued cross-correlation functions

In this section, we show a family of four-valued cross-correlation functions.

Lemma 3.1 Let $n = 2k$ and s be an integer such that $2s$ divides k. And let $d = \frac{2^k-1}{2^s-1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1)$, where i is odd. Then
(a) $d \equiv 1\ (mod\ 2^k - 1)$,
(b) $d \equiv \frac{2^{ki}-2^s}{2^s-1}\ (mod\ 2^k + 1)$,
(c) $gcd(d, 2^n - 1) = 1$.
Proof. (a) Clearly $d \equiv 1\ (mod\ 2^k - 1)$.

(b) $d = 2^{k-1}\{\frac{2^k-2^s}{2^s-1}(2^k-1)+2^k+1\} \equiv \frac{2^k-2^s}{2^s-1}(mod\ 2^k+1)$.

(c) By (a) and (b), we have $gcd(d, 2^n-1) = gcd(d, 2^k+1) = gcd(\frac{2^{ki}-2^s}{2^s-1}, 2^k+1)$. Since $gcd(2^s-1, 2^k+1) = 1$ by Lemma 2.4, $gcd(\frac{2^{ki}-2^s}{2^s-1}, 2^k+1) = gcd(2^{ki}-2^s, 2^k+1)$. Since $2^{ki}-2^s \equiv -1-2^s(mod\ 2^k+1)$, by Lemma 2.5 $gcd(2^{ki}-2^s, 2^k+1) = gcd(2^k+1, 2^s+1) = 1$. Hence $gcd(d, 2^n-1) = 1$.

Lemma 3.2 Let $q = 2^k$ and $d \equiv 1(mod\ q-1)$. Then $x \in GF(q^2) \setminus \{0,1\}$ is a solution to

$$(x+1)^d = x^d + 1 \tag{1}$$

if and only if $x^{d-1} = (x+1)^{d-1} = 1$ or $x^{d-q} = (x+1)^{d-q} = 1$.

Proof. Assume that $x \in GF(q^2) \setminus \{0,1\}$ is a solution to Eq.(1). Since $(x+1)^d = x^d+1$, $(\overline{x}+1)^d = (x^q+1)^d = (x+1)^{qd} = \{(x+1)^d\}^q = (x^d+1)^q = \overline{x}^d+1$. Thus $(x\overline{x}+x+\overline{x}+1)^d = (x\overline{x})^d + x^d + \overline{x}^d + 1$. Since $x\overline{x} \in GF(q)$ and $x+\overline{x} \in GF(q)$, $x\overline{x}+x+\overline{x}+1 \in GF(q)$ and thus $(x\overline{x}+x+\overline{x}+1)^d = x\overline{x}+x+\overline{x}+1$. Therefore we have $x\overline{x}+x+\overline{x}+1 = x\overline{x}+x^d+\overline{x}^d+1$ i.e.,

$$x+\overline{x} = x^d+\overline{x}^d. \tag{2}$$

Multiplying x^{d-q-1} to both sides of Eq.(2), we obtain $x^{d-q}+x^{d-1} = x^{2d-q-1}+x^{qd+d-q-1}$. Since $d \equiv 1(mod\ q-1)$, there exists a positive integer s such that $d-1 = (q-1)s$. Since $x^{qd+d-q-1} = x^{(q+1)(d-1)} = x^{(q+1)(q-1)s} = 1$, we have $x^{2d-q-1} - x^{d-q} - x^{d-1} + 1 = (x^{d-1}-1)(x^{d-q}-1) = 0$. Thus we have $x^d = x$ or $x^d = x^q$.

(i) $x^d = x$: Since $(x+1)^d = x^d+1 = x+1$ and $x \in GF(q^2) \setminus \{0,1\}$, $(x+1)^{d-1} = 1$.

(ii) $x^d = x^q$: Since $(x+1)^d = \overline{x}+1 = (x+1)^q$ and $x \in GF(q^2) \setminus \{0,1\}$, $(x+1)^{d-q} = 1$.

Conversely, let $x^{d-1} = (x+1)^{d-1} = 1$. Then $(x+1)^d = x+1$ and $x^d = x$, and thus $(x+1)^d = x+1 = x^d+1$. Therefore x is a solution to Eq.(1). And let $x^{d-q} = (x+1)^{d-q} = 1$. Then $(x+1)^d = (x+1)^q = x^q+1 = x^d+1$. Therefore x is a solution to Eq.(1).

Lemma 3.3 Let $q = 2^k$ and $d \equiv 1(mod\ q-1)$. And let $x \in GF(q^2)^*$ be a solution to $(x+1)^d = x^d+1$. Then $(\frac{x+1}{\overline{x}+1})^{d-1} = 1$ or $(\frac{x+1}{\overline{x}+1})^{d+1} = 1$.

Proof. Since every element of $GF(q)$ is a solution to $(x+1)^d = x^d+1$, we may assume that $x \neq 1$. By Lemma 3.2, $x^d = x$ or $x^d = \overline{x}$. Since $(x+1)^d = x^d+1$, $(\overline{x}+1)^d = \overline{x}^d+1$. From $(x+1)^d(\overline{x}+1)^d = (x^d+1)(\overline{x}^d+1)$, we obtain $(x\overline{x}+x+\overline{x}+1)^d = (x\overline{x})^d + x^d + \overline{x}^d + 1$. Since $x\overline{x} \in GF(q)$ and $x+\overline{x} \in GF(q), x\overline{x}+x+\overline{x}+1 \in GF(q)$ and thus $(x\overline{x}+x+\overline{x}+1)^d = x\overline{x}+x+\overline{x}+1$. Therefore we have

$$x+\overline{x} = x^d+\overline{x}^d. \tag{3}$$

(i) $x^d = x$: Since $\overline{x}^d = \overline{x}$, we have $(\frac{x+1}{\overline{x}+1})^d = \frac{x^d+1}{\overline{x}^d+1} = \frac{x+1}{\overline{x}+1}$ and thus $(\frac{x+1}{\overline{x}+1})^{d-1} = 1$.

(ii) $x^d = \overline{x}$: Since $\overline{x}^d = x$, we have $(\frac{x+1}{\overline{x}+1})^d = \frac{x^d+1}{\overline{x}^d+1} = \frac{\overline{x}+1}{x+1}$ and thus $(\frac{x+1}{\overline{x}+1})^{d+1} = 1$.

Theorem 3.4 Assume that $d \equiv 1(mod\ 2^k - 1)$. If $gcd(d-1, 2^k+1) = gcd(d+1, 2^k+1) = 1$, then the equation

$$(x+1)^d = x^d + 1 \tag{4}$$

has exactly 2^k solutions in $GF(2^n)$.

Proof. Since $d \equiv 1\ (mod\ 2^k - 1)$, every $x \in GF(2^k)$ is a solution to Eq.(4). So we may assume that $x(\neq 0, 1)$ is a solution to Eq.(4). Since x is a solution to Eq.(4), $x^d = x$ or $x^d = \overline{x}$ by Lemma 3.2. Let $x^d = x$. By Lemma 3.3, $(\frac{x+1}{\overline{x}+1})^{d-1} = 1$. And let $x^d = \overline{x}$. By Lemma 3.3 $(\frac{x+1}{\overline{x}+1})^{d+1} = 1$. Since $gcd(d-1, 2^k+1) = gcd(d+1, 2^k+1) = 1$, $\frac{x+1}{\overline{x}+1} = 1$. Thus $\overline{x} = x$. Hence $x \in GF(2^k)$.

Lemma 3.5 Let $n = 2k$ and s be an integer such that $2s$ divides k. And let

$$d = \frac{2^{k-1}}{2^s - 1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1),$$

where i is odd. Then
(a) $gcd(d+1, 2^k+1) = 1$.
(b) $gcd(d-1, 2^k+1) = 1$.

Proof. (a) Since $gcd(2^s-1, 2^k+1) = 1$ by Lemma 2.4, $gcd(d+1, 2^k+1) = gcd((2^s-1)(d+1), 2^k+1)$. From $(2^s-1)(d+1) \equiv 2^{k-1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1) + (2^s-1) \equiv -2(mod\ 2^k+1)$, $gcd((2^s-1)(d+1), 2^k+1) = gcd(2, 2^k+1) = 1$. Hence $gcd(d+1, 2^k+1) = 1$.
(b) Since $gcd(2^s-1, 2^k+1) = 1$ by Lemma 2.4, $gcd(d-1, 2^k+1) = gcd((2^s-1)(d-1), 2^k+1)$. From $(2^s-1)(d-1) \equiv 2^{k-1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1) + (2^s-1) \equiv -2^{s+1}(mod\ 2^k+1)$, $gcd((2^s-1)(d-1), 2^k+1) = gcd(2^{s+1}, 2^k+1) = 1$, Hence $gcd(d-1, 2^k+1) = 1$.

By Lemma 3.1, $d \equiv 1(mod\ 2^k - 1)$. With Theorem 3.4 and Lemma 3.5, we obtain the following theorem.

Theorem 3.6 Let $n = 2k$ and s be an integer such that $2s$ divides k. Also let $d = \frac{2^{k-1}}{2^s-1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1)$, where i is odd. Then the cross-correlation function $C_d(\tau)$ between two m-sequences takes on the following four values:

$-1-2^k$	*occurs*	$\frac{2^{2k+s-1}-2^{k+s-1}}{2^s+1}$	*times*,
-1	*occurs*	$\frac{2^{2k}-2^k-2^s}{2^s}$	*times*,
$-1+2^k$	*occurs*	$\frac{2^{2k+s-1}-2^{2k}-2^{k+s-1}}{2^s-1}$	*times*,
$-1+2^{k+s}$	*occurs*	$\frac{2^{2k}-2^k}{2^{3s}-2^s}$	*times*.

Proof. By Lemma 3.1 $d \equiv 1(mod\ 2^k-1), d \equiv \frac{2^{ki}-2^s}{2^s-1}(mod\ 2^k+1)$ and $gcd(d, 2^n-1) = 1$. By Theorem 2.3, we obtain the following equation:

$$x^{\frac{2^{ki}-2^s}{2^s-1}} + yx + \overline{y}x^{-1} + x^{-\frac{2^{ki}-2^s}{2^s-1}} = 0 \tag{5}$$

$$x^{2^k+1} = 1.$$

Since $gcd(2^s-1, 2^k+1) = 1$ by Lemma 2.4, the number of solutions to Eq.(5) is the same as the number of solutions to the following equation replacing x by x^{2^s-1} in Eq.(5). Then we get the following:

$$yx^{2^s-1} + x^{2^{ki}-2^s} + \overline{y}x^{1-2^s} + x^{-2^{ki}+2^s} = 0. \tag{6}$$

Multiplying $x^{2^{ki}-2^s}$ to both sides, we obtain the equivalent equation:

$$yx^{2^s-1} + x^{2(2^{ki}-2^s)} + \overline{y}x^{2^{ki}-2^{s+1}+1} + 1 = 0. \tag{7}$$

Since $2^k \equiv -1(mod\ 2^k+1)$, Eq.(7) is equivalent to the following:

$$x^{2(-1-2^s)} + yx^{-2} + \overline{y}x^{-2^{s+1}} + 1 = 0. \tag{8}$$

Thus the number of solutions to Eq.(8) is the same as the number of solutions to Eq.(9):

$$x^{-1-2^s} + yx^{-1} + y^{2^k}x^{-2^s} + 1 = 0, \tag{9}$$

Therefore the number of solutions to Eq.(9) is the same as the number of solutions to the following Eq.(10):

$$x^{2^s+1} + yx^{2^s} + y^{2^k}x + 1 = 0. \tag{10}$$

Thus by Theorem 2.2 $C_d(\tau)$ is four-valued. By Theorem 2.1 and Theorem 3.4,

$$\sum_{\tau=0}^{2^n-2} (\Delta_d(\tau))^3 = 2^{2n}2^k.$$

As usual, denote by N_j the number of times Eq.(10) has exactly j solutions in S. Then we have the following:

$$\begin{aligned} N_0 + N_1 + N_2 + N_{2^s+1} &= 2^n - 1. \\ -2^k N_0 + 0 \cdot N_1 + 2^k N_2 + 2^{k+s} N_{2^s+1} &= 2^n. \\ 2^n N_0 + 0 \cdot N_1 + 2^n N_2 + 2^{n+2s} N_{2^s+1} &= 2^{2n}. \\ -2^{n+k} N_0 + 0 \cdot N_1 + 2^{n+k} N_2 + 2^{n+k+3s} N_{2^s+1} &= 2^{2n+k}. \end{aligned}$$

Solving this system, we obtain the following: $N_0 = \frac{2^{2k+s-1}-2^{k+s-1}}{2^s+1}$, $N_1 = \frac{2^{2k}-2^k-2^s}{2^s}$, $N_2 = \frac{2^{2k+s-1}-2^{2k}+2^{k+s-1}}{2^s-1}$, $N_{2^s+1} = \frac{2^{2k}-2^k}{2^{3s}-2^s}$.

By Theorem 2.3 $C_d(\tau) \in \{-1-2^k, -1, -1+2^k, -1+2^{k+s}\}$. This completes the proof.

4. Conclusion

In this paper we proposed four-valued cross-correlation functions between two maximal linear recursive sequences and found the values and the number of occurrences of each value of $C_d(\tau)$ when $d = \frac{2^{k-1}}{2^s-1}(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1)$, where $n = 2k$ and s is an integer such that $2s$ divides k, and i is odd.

References

[1] H. Dobbertin, One-to-one highly nonlinear power functions on $GF(2^n)$, AAECC Applicable Algebra in Engineering, Communication and Computing, Vol. 9, 1998, pp. 139-152.

[2] T. Helleseth, J. Lahtonen and P. Rosendahl, On Niho type cross-correlation functions of m-sequences, Finite Fields and Their Applications, Vol. 13, No. 2, 2007, pp. 305-317.

[3] T. Helleseth and P. Rosendahl, New pairs of m-sequences with 4-level cross-correlation, Finite Fields and Their Applications, Vol. 11, 2005, pp. 647-683.

[4] H.D. Kim and S.J. Cho, A new proof about the decimations with Niho type five-valued cross-correlation functions, J. Appl. Math. and Informatics, Vol. 30, No. 5-6, 2012, pp. 903-911.

[5] R. Lidl and H. Niederreiter, Finite fields, Cambridge University Press, 1997.

[6] J. Luo, Cross correlation of nonbinary Niho-type sequences, ISIT 2010, Austin, Texas, U.S.A., June 13-18, 2010, pp. 1297-1299.

[7] R. McEliece, Finite fields for computer scientists and engineers, Kluwer Academic Publishers, Boston, 1987.

[8] Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D. thesis, University of Southern California, 1972.

[9] P. Rosendahl, Niho type cross-correlation functions and related equations, Ph.D. thesis, Turku center for computer science, 2004.

[10] E.Y. Seo, Y.S. Kim, J.S. No and D.J. Shin, Cross-correlation distribution of p-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $(\frac{p^{2k}+1}{2})^2$, IEEE Trans. Inf. Theory, Vol. 54, No. 7, 2008, pp. 3140-3149.

[11] H.M. Trachtenberg, On the cross-correlation functions of maximal linear sequences, Ph.D. thesis, University of Southern California, 1970.

Han-Doo Kim
Institute of Basic Science and Department of Applied Mathematics,
Inje University, GimHae 621-749, Korea
E-mail address: mathkhd@inje.ac.kr

Sung-Jin Cho
Department of Applied Mathematics, Pukyong National University,
Busan 608-737, Korea
E-mail address: sjcho@pknu.ac.kr

Min-Jeong Kwon
Department of Applied Mathematics, Pukyong National University,
Busan 608-737, Korea

Un-Sook Choi
School of Free Major, Tongmyoung University,
Busan 608-711, Korea