J. Appl. Math. & Informatics Vol. **31***(2013), No. 5 - 6, pp. 869 - 876*
http://dx.doi.org/10.14317/jami.2013.869

ANALYSIS OF THE SEQUENCES WITH OPTIMAL CROSS-CORRELATION PROPERTY[†]

MIN-JEONG KWON AND SUNG-JIN CHO[*]

Abstract. The design of large family size with the optimal cross-correlation property is important in spread spectrum and code division multiple access communication systems. In this paper we present the sequences with the decimation $d = 2 \cdot 2^m - 1$, calculate the cross-correlation spectrum for $0 \leq t \leq 2^n - 2$ and count the number of the value $2^m - 1$ occurring for $0 \leq \tau \leq 2^n - 2$. The sequences have the optimal cross-correlation property. The work on this paper can make it easier to count the number of the whole value occurring for $0 \leq \tau \leq 2^n - 2$.

AMS Mathematics Subject Classification : 97N70, 11G25, 94A55, 68Q87.
Key words and phrases : Finite field, decimation, cross-correlation functions, number of the occurrence.

1. Introduction

Since the 1950s linear recurring sequences in finite fields have become crucial to switching circuits and coding theory. Selmer briefed on the history of the subject concentrating on the development after 1918 [14]. Correlation functions of the sequences are important in electrical engineering. Especially if the two sequences are identical, we speak of the auto-correlation function. For maximal period sequences in $GF(2)$, the auto-correlation function was already calculated by Golomb [1] and an extension to arbitrary $GF(q)$ was given by Zierler [17]. The cross-correlation function for two maximal period sequences in $GF(2)$ was considered in Golomb [1]. The further work on correlation functions was done by many researchers [2, 3, 5, 6, 10]. In recent years, it is the primary concern to design of large family size with the good cross-correlation properties and the further work for the distribution of each value of the cross-correlation function is

Received January 31, 2013. Revised March 21, 2013. Accepted March 25, 2013. [*]Corresponding author. [†]This work was supported by the Pukyong National University Research Fund in 2012(PK-2012-41).

proceeded [4]. The sequences with good correlation properties have many applications in signal processing(spread spectrum and code division multiple access communication systems) [12, 15]. The GMW sequences and Kasami sequences are asymptotically optimal with respect to the Welch bounds [8, 13, 16]. In this paper we present the sequences with the decimation $d = 2 \cdot 2^m - 1$, calculate the cross-correlation spectrum for $0 \leq t \leq 2^n - 2$ and count the number of the value $2^m - 1$ occurring for $0 \leq \tau \leq 2^n - 2$. The sequences have the optimal cross-correlation property.

2. Preliminaries

In this section some definitions, facts and results are presented. Trace function can be computed in any field, finite or not. But in finite fields, they are more helpful tools to construct and analyze the pseudo random sequences and the results are more useful.

Definition 2.1. Assume that m divides n, then $GF(2^m)$ is a subfield of $GF(2^n)$. The trace function $Tr_m^n : GF(2^n) \to GF(2^m)$ is defined by

$$Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{m \cdot i}} = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{m(\frac{n}{m}-1)}}.$$

The basic properties of the trace function are:
(i) Tr_m^n is linear over $GF(2^m)$,
(ii) Tr_m^n is balanced, that is, every element in $GF(2^n)$ occurs exactly 2^{n-m} times,
(iii) $Tr_m^n(x^{2^m}) = Tr_m^n(x)$, and
(iv) Tr_m^n is transitive, that is, $Tr_m^n(x) = Tr_m^k\{Tr_k^n(x)\}$, whenever m divides k and k divides n.

Definition 2.2. The cross-correlation function $C(\tau)$ between the sequences $u(t)$ and $v(t)$ is defined for $\tau = 0, 1, 2, \cdots$ by

$$C(\tau) = \sum_t (-1)^{u(t+\tau)+v(t)} \tag{1}$$

In the sum (1), a cyclic shift by τ of $u(t)$ and $v(t)$ are compared bit by bit, and then the value of the cross-correlation function is the sum of the agreements and disagreements between the sequences. That is, $C(\tau)$ is the measure of the similarity between the sequences. The explanation about the importance of this measure is in detail in [9].

Definition 2.3. Decimation is an operation on sequences and it works as following : if $u(t)$ is the sequence of elements $s_0, s_1, s_2, \cdots$ of the sequence family, then the decimated sequence $u(dt)$ has the terms $s_0, s_d, s_{2d}, \cdots$. Thus $u(dt)$ is obtained by taking every dth term of $u(t)$, starting from s_0.

Since any maximal period sequences in $GF(2)$ can be obtained from a single sequence of this type by a suitable decimation, the decimation of maximal period sequences is important [1]. So the cross-correlation spectrum depends only on decimation and the choice of the maximal sequence is irrelevant [12].

Lemma 2.4 ([11]). *For m, n such that $n = 2m$, every primitive element α of $GF(2^n)$ can be presented as*

$$\alpha = \delta\gamma,$$

where δ, γ satisfy $\delta^{2^m-1} = 1, \gamma^{2^m+1} = 1$, respectively.

Proof. Since $gcd(2^m + 1, 2^m - 1) = 1$, there are integers s and k with $s(2^m - 1) + k(2^m + 1) = 1$. Then we can present the primitive element α of $GF(2^n)$ as $\alpha = \alpha^1 = \alpha^{k(2^m+1)+s(2^m-1)} = \alpha^{k(2^m+1)}\alpha^{s(2^m-1)}$. If we denote the $\alpha^{k(2^m+1)}$, $\alpha^{s(2^m-1)}$ by δ, γ respectively, then $\delta^{2^m-1} = 1, \gamma^{2^m+1} = 1$. □

From now on, let $\overline{x}$ denote x^{2^m} for each $x \in GF(2^n)^*$ for the convenience of the notation. With this notation, we can proceed our work considerably.

Lemma 2.5. *Let $S = \{x \mid x\overline{x} = 1, x \in GF(2^n)\}$. Then*

$$S \cap GF(2^m) = \{1\}$$

Proof. Since every element of S is the $(2^m + 1)$-th root of unity in $GF(2^n)$ and $gcd(2^m + 1, 2^m - 1) = 1$, $S \cap GF(2^m) = \{1\}$. □

Lemma 2.6 ([7]). *Let $w \in S \setminus \{1\}$ be fixed. Then*

$$S \setminus \{w\} = \{\frac{uw + 1}{u + w} \mid u \in GF(2^m)\}.$$

3. The spectrum and the number of the occurrences of the cross-correlation function

For even number m, $n = 2m$, r with $gcd(r, 2^m - 1) = 1$ and $d = 2 \cdot 2^m - 1$, let

$$S_r = \{s_a^r(t) \mid a \in GF(2^m), 0 \le t \le 2^n - 2\}$$

be the sequence family, where

$$s_a^r(t) = Tr_1^m([Tr_m^n(a \cdot \alpha^t + \alpha^{dt})]^r).$$

The sequence family S_r has the optimal cross-correlation property.

Lemma 3.1. *For even number m, $n = 2m$ and $d = 2 \cdot 2^m - 1$, then*
(i) $d \equiv 1(mod\ 2^m - 1)$

(ii) $d \equiv -3(mod\ 2^m + 1)$.

Lemma 3.2. *For* $0 \leq t \leq 2^m$ *and* r *with* $gcd(r, 2^m - 1) = 1$, *if we let* $N(t, \tau, r) =| \{t \mid H(t, \tau, r) = 0, 0 \leq t \leq 2^m\} \mid$ *where* $H(t, \tau, r) = [Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau))})]^r + [Tr_m^n(b\alpha^t + \alpha^{dt})]^r$, *then*

$$N(t, \tau, r) = N(t, \tau, 1).$$

Proof. To obtain the value $N(t, \tau, r)$, it is sufficient to calculate the number of t satisfying $H(t, \tau, r) = 0$. $H(t, \tau, r) = 0$ means that $[Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r = [Tr_m^n(b\alpha^t + \alpha^{dt})]^r$. Since $gcd(r, 2^m - 1) = 1$, whenever t satisfies the equation $[Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r = [Tr_m^n(b\alpha^t + \alpha^{dt})]^r$, the t also satisfies the equation $Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)}) = Tr_m^n(b\alpha^t + \alpha^{dt})$, i.e. the t satisfies the equation $H(t, \tau, 1) = 0$. So $\{t \mid H(t, \tau, r) = 0, 0 \leq t \leq 2^m\} = \{t \mid H(t, \tau, 1) = 0, 0 \leq t \leq 2^m\}$ and thus $N(t, \tau, r) = N(t, \tau, 1)$. □

Theorem 3.3. *For the sequence family* S_r, *the cross-correlation function* $C_{a,b}(\tau)$*of the sequences* s_a^r, s_b^r *is four-valued.*

Proof. The cross-correlation function of the sequences s_a^r, s_b^r in the sequence family S_r is $C_{a,b}(\tau) = \sum_{t=0}^{2^n-2}(-1)^{s_a^r(t+\tau)+s_b^r(t)}$. To obtain the value of the cross-correlation function, $s_a^r(t + \tau) + s_b^r(t)$ is needed.

$$\begin{aligned} s_a^r(t+\tau) + s_b^r(t) &= Tr_1^m([Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r) \\ &\qquad\qquad +Tr_1^m([Tr_m^n(b\alpha^t + \alpha^{dt})]^r) \\ &= Tr_1^m([Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b\alpha^t + \alpha^{dt})]^r) \end{aligned}$$

For convenience, let $Q = 2^m+1$. Then we can represent the time t with Q such as $t = Qt_1 + t_2$. Let $\alpha^Q = \beta$. Then $\beta \in GF(2^m)$. Since $d \equiv 1(mod\ 2^m - 1), \beta^d = \beta$. So

$$\begin{aligned} a\alpha^{t+\tau} + \alpha^{d(t+\tau)} &= a\alpha^{Qt_1+t_2+\tau} + \alpha^{d(Qt_1+t_2+\tau)} \\ &= a\beta^{t_1}\alpha^{t_2+\tau} + \beta^{dt_1}\alpha^{d(t_2+\tau)} \\ &= \beta^{t_1}(a\alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)}) \end{aligned}$$

and

$$\begin{aligned} b\alpha^t + \alpha^{dt} &= b\alpha^{Qt_1+t_2} + \alpha^{d(Qt_1+t_2)} \\ &= \beta^{t_1}(b\alpha^{t_2} + \alpha^{dt_2}). \end{aligned}$$

Then

$$\begin{aligned} & Tr_1^m([Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)})]^r + [Tr_m^n(b\alpha^t + \alpha^{dt})]^r) \\ = \;& Tr_1^m(\beta^{t_1r}\{[Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)})]^r + [Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})]^r\}) \\ = \;& Tr_1^m\{\beta^{t_1r}H(t_2, \tau, r)\} \end{aligned}$$

and

$$H(t_2, \tau, r) = [Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{d(t_2+\tau)})]^r + [Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})]^r.$$

From $gcd(r, 2^m - 1) = 1$ and $\beta \in GF(2^m)^*$, $\{\beta^{t_1r} \mid 0 \leq t_1 \leq 2^m - 2\} = GF(2^m)^*$. Thus

$$\begin{aligned} C_{a,b}(\tau) = & \textstyle\sum_{t=0}^{2^n-2}(-1)^{s_a^r(t+\tau)+s_b^r(t)} \\ = & \textstyle\sum_{t_1=0}^{2^m-2}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m\{\beta^{t_1 r}H(t_2,\tau,r)\}} \\ = & \textstyle\sum_{\eta\in GF(2^m)^*}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m\{\eta H(t_2,\tau,r)\}} \\ = & \textstyle\sum_{\eta\in GF(2^m)}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m\{\eta H(t_2,\tau,r)\}} - (2^m+1). \end{aligned}$$

Let $N(t_2,\tau,r) =\mid \{t_2 \mid H(t_2,\tau,r)=0, 0\le t_2\le 2^m\}\mid$. Then using the fact

$$\sum_{\eta\in GF(2^m)}(-1)^{Tr_1^m\{\eta H(t_2,\tau,r)\}} = \begin{cases} 0 & , H(t_2,\tau,r)\neq 0 \\ 2^m & , H(t_2,\tau,r)=0 \end{cases}$$

we obtain

$$\begin{aligned} C_{a,b}(\tau) = & \textstyle\sum_{\eta\in GF(2^m)}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m\{\eta H(t_2,\tau,r)\}} - (2^m+1) \\ = & N(t_2,\tau,r)2^m - (2^m+1) \\ = & \{N(t_2,\tau,r)-1\}2^m - 1. \end{aligned}$$

By Lemma 3.2, $N(t_2,\tau,r) = N(t_2,\tau,1)$. So the number of the t_2 satisfying the equation $H(t_2,\tau,1)=0$ instead of $H(t_2,\tau,r)=0$ is required. Then

$$\begin{aligned} & Tr_m^n(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}+b\alpha^{t_2}+\alpha^{dt_2}) \\ = & Tr_m^n\{(\alpha^{d\tau}+1)\alpha^{dt_2}+(a\alpha^\tau+b)\alpha^{t_2}\} \\ = & Tr_m^n\{A(\tau)\alpha^{dt_2}+B(\tau)\alpha^{t_2}\} \\ = & A(\tau)\alpha^{dt_2}+B(\tau)\alpha^{t_2}+\overline{A(\tau)}\alpha^{2^m dt_2}+\overline{B(\tau)}\alpha^{2^m t_2} \\ = & 0 \end{aligned}$$

where $A(\tau)=\alpha^\tau+1$ and $B(\tau)=a\alpha^\tau+b$. By Lemma 2.4, the primitive element α of $GF(2^n)$ can be expressed as $\delta\gamma$ satisfying $\delta^{2^m}=\delta, \gamma^{2^m}=\gamma^{-1}$ respectively. And it is obvious that $\delta^d=\delta, \gamma^d=\gamma^{-3}$ from Lemma 3.1. Moreover δ is the element of $GF(2^m)$ and γ is in S. If we replace α with $\delta\gamma$, then

$$\begin{aligned} & A(\tau)\alpha^{dt_2}+B(\tau)\alpha^{t_2}+\overline{A(\tau)}\alpha^{2^m dt_2}+\overline{B(\tau)}\alpha^{2^m t_2} \\ = & A(\tau)\delta^{dt_2}\gamma^{dt_2}+B(\tau)\delta^{t_2}\gamma^{t_2}+\overline{A(\tau)}\delta^{2^m dt_2}\gamma^{2^m dt_2}+\overline{B(\tau)}\delta^{2^m t_2}\gamma^{2^m t_2} \\ = & A(\tau)\delta^{t_2}\gamma^{-3t_2}+B(\tau)\delta^{t_2}\gamma^{t_2}+\overline{A(\tau)}\delta^{t_2}\gamma^{3t_2}+\overline{B(\tau)}\delta^{t_2}\gamma^{-t_2} \\ = & 0. \end{aligned}$$

Since $\delta^{t_2}\neq 0$,

$$\overline{A(\tau)}\gamma^{6t_2}+B(\tau)\gamma^{4t_2}+\overline{B(\tau)}\gamma^{2t_2}+A(\tau)=0. \tag{2}$$

If we substitute x with γ^{2t_2}, then $\{\gamma^{2t_2}\mid 0\le t_2\le 2^m\}=\{x\mid x\in S\}$. So the equation (2) is equivalent to

$$\overline{A(\tau)}x^3+B(\tau)x^2+\overline{B(\tau)}x+A(\tau)=0. \tag{3}$$

Since the degree of the equation (3) is three, the number of the solutions to the equation (3) is possible from 0 to 3. That is $0\le N(t_2,\tau,r)\le 3$, and $C_{a,b}(\tau)\in\{-2^m-1,-1,2^m-1,2\cdot 2^m-1\}$. Therefore the cross-correlation function $C_{a,b}(\tau)$ is four-valued. □

Now we concentrate on the cross-correlation function of $s_0^r(t) = Tr_1^m([Tr_m^n(\alpha^{dt}$ $)]^r)$ and $s_b^r(t) = Tr_1^m([Tr_m^n(b\alpha^t + \alpha^{dt})]^r)$ with $b \neq 0$ in S_r for the special case. Then the cross-correlation function is $C_{0,b}(\tau) = \{N(t_2, \tau, r) - 1\}2^m - 1$, where $N(t_2, \tau, r) =| \{t_2 \mid H(t_2, \tau, r) = 0, 0 \leq t_2 \leq 2^m\} |$. For obtaining $N(t_2, \tau, r)$, it is sufficient to solve the equation

$$\begin{cases} \overline{A(\tau)}x^3 + bx^2 + bx + A(\tau) = 0, \\ x \in S \end{cases} \tag{4}$$

where $A(\tau) = \alpha^{d\tau}+1$. Then the problem for the spectrum of the cross-correlation function is changed into the problem for the number of the solutions to the equation (4). From Lemma 2.5, $S \cap GF(2^m) = \{1\}$.

First, assume that $x = 1$ is the solution to the equation (4), i.e. $\overline{A(\tau)} = A(\tau)$.

(a) If $A(\tau) = 0$, then $x = 1$ is the only solution to the equation (4) in S and thus $C_{0,b}(0) = -2^m - 1$.

(b) If $A(\tau) \neq 0$, then we can simplify the equation (4) to the monic polynomial $x^3 + \beta^{k_1}x + \beta^{k_1}x + 1 = 0$ for some $0 \leq k_1 \leq 2^m - 2$. Then

$$x^3+\beta^{k_1}x^2+\beta^{k_1}x+1 = (x+1)(x^2+(\beta^{k_1}+1)x+1) = 0 \tag{5}$$

(i) If $k_1 = 0$ then the equation (5) has $x = 1$ as the only solution with multiplicity 3.

(ii) If $k_1 \neq 0$ then the number of the solutions to the equation $x^2 + (\beta^{k_1} + 1)x + 1 = 0$ determines that of the equation (5). If $Tr_1^4(\frac{1}{\beta^{2k_1}+1}) = 0$, then the equation (5) has $x = 1$ as the only solution in S. And if $Tr_1^4(\frac{1}{\beta^{2k_1}+1}) = 1$, then $Tr_1^8(\frac{1}{\beta^{2k_1}+1}) = 0$ by the transitivity of the trace function. So the equation (5) is factorized over $GF(2^n)$ and it has two more roots in S apart from 1. Thus there are three roots of the equation (5) and thus $C_{0,b}(\tau) \in \{-1, 2 \cdot 2^m - 1\}$.

Second, we will investigate the case $\overline{A(\tau)} \neq A(\tau)$.

(a) If any element of S does not satisfy the equation (5), then there is no solution and thus $C_{0,b}(\tau) = -2^m - 1$.

(b) If there is an element of S satisfying the equation (5), say w, then $\overline{A(\tau)}w^3 + bw^2 + bw + A(\tau) = 0$. If there is another solution to the equation (5), it is the element of $S \setminus \{w\} = \{\frac{uw+1}{u+w} \mid u \in GF(2^m)\}$ by Lemma 2.6. If we substitute $\frac{uw+1}{u+w}$ for x in (5), then

$$\begin{aligned}(\overline{A(\tau)}w^3 + bw^2 + bw + A(\tau))u^3 + (\overline{A(\tau)}w + bw^3 + b + A(\tau)w)u^2 \\ (\overline{A(\tau)}w^2+bw^3+b+A(\tau)w^2)u = \overline{A(\tau)}+bw+bw^2+A(\tau)w^3\end{aligned} \tag{6}$$

Since w is the solution to the equation (5), the coefficient of u^3 in the equation (6) is vanished. Then the degree of the equation (6) is down to 2 as follows

$$\begin{aligned}(\overline{A(\tau)}w + bw^3 + b + A(\tau)w)u^2 + (\overline{A(\tau)}w^2 + bw^3 + b + A(\tau)w^2)u \\ = \overline{A(\tau)} + bw + bw^2 + A(\tau)w^3\end{aligned} \tag{7}$$

So there is 0, 1 or 2 solutions to the equation (7) apart from w and moreover $C_{0,b}(\tau) \in \{-1, 2^m - 1, 2 \cdot 2^m - 1\}$. Thus $C_{0,b}(\tau)$ is four-valued.

Theorem 3.4. *The number of the value $C_{0,b}(\tau) = 2^m - 1$ occurring for $0 \leq \tau \leq 2^n - 2$ is 2^m.*

Proof. $C_{0,b}(\tau) = 2^m - 1$ occurs when the equation (4) has two different roots. From the result of the equation (7), it is obvious that one of them is the root with multiplicity 2. By forming the derivative it can be seen when the equation has repeated roots. Whenever $A(\tau) = 0$ there is no repeated roots, $A(\tau)$ should not be 0. By differentiating the equation (4), we obtain $x^2 = \frac{b}{\overline{A(\tau)}}$. Substitute x^2 in the equation (4), then

$$A(\tau)\overline{A(\tau)} = b^2. \tag{8}$$

Since $A(\tau) \in GF(2^n)^*$ and $b \in GF(2^m)^*$, we can replace $A(\tau), b$ with α^{k_2} $(0 < k_2 \leq 2^n - 2)$, α^{Qk_3} $(0 < k_3 \leq 2^m - 2)$, respectively. Then (8) is

$$\begin{gathered} \alpha^{Qk_2} = \alpha^{2Qk_3}, \\ Qk_2 \equiv 2Qk_3 (mod\ 2^n - 1), \\ k_2 \equiv 2k_3 (mod\ 2^m - 1). \end{gathered}$$

That is $k_2 = (2^m - 1) \cdot l + 2k_3$ with $0 \leq l \leq 2^m$. So there are $2^m + 1$ repeated roots of the equation (4).

But when $\overline{A(\tau)} = b$, there is only one solution $x = 1$ with multiplicity 3 to the equation (4). Therefore $l = k_3$ is excluded from $0 \leq l \leq 2^m$ and thus there are 2^m repeated roots with multiplicity 2. □

Example 3.5. Let $n = 8, m = 4$ and $r = 7$. Then the value of the cross-correlation function $C_{0,\beta^2}(\tau)$ between the sequences $s_0^7 = Tr_1^4([Tr_4^8(\alpha^{31t})]^7)$ and $s_{\beta^2}^7 = Tr_1^4([Tr_4^8(\beta^2\alpha^t + \alpha^{31t})]^7)$ in the sequence family $S_7 = \{s_a^7 \mid a \in GF(2^4), 0 \leq t \leq 2^n - 2\}$ is an element of $\{-17, -1, 15, 31\}$ and the value **15** occurs 16 times when τ is $22, 24, 60, 77, 86, 97, 101, 129, 143, 171, 175, 186, 195, 212, 248, 250$.

4. Conclusion

We calculated the spectrum of the cross-correlation functions $C_{0,b}(\tau)$ for $0 \leq t \leq 2^n - 2$ and counted the number of the occurrences of $C_{0,b}(\tau) = 2^m - 1$ for $0 \leq \tau \leq 2^n - 2$ between two maximal linear sequences. The sequence with four-valued cross-correlation is optimal by Welch bounds and the further work on the number of the value occurring for $0 \leq \tau \leq 2^n - 2$ is needed.

References

1. S.W. Golomb, *Shift register sequences*, Holden Day, 1967.
2. R. Gold, *Optimal binary sequences for spread spectrum multiplexing*, IEEE Transactions on Information Theory, **13** (1967), 619-621.
3. R. Gold, *Maximal recursive sequences with 3-valued recursive cross-correlation functions*, IEEE Transactions on Information Theory, **14** (1968), 154-156.
4. H.D. Kim, S.J. Cho, *A New Proof about the decimation with Niho type fice-valued cross-correlation functions*, J. Appl. Math. and Inform. **30** (2012), 903-911.
5. T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Mathematics, **16** (1976), 209-232.
6. T. Helleseth, *A note on the cross-correlation function between two binary maximal length linear sequences*, Discrete Mathematics, **23** (1978), 301-307.
7. T. Helleseth, J. Lahtonen, and P. Rosendahl,*On certain equations over finite fields and cross-correlations of m-sequences*, Coding, Cryptography and Combinatorics, Progress in Computer Science and Applied Logic, **23** (1984), 169-176.
8. T. Kasami, *Weight distribution of Bose-Chaudhuri-Hocquenghem codes*, Combinatorial Mathematics and Its Applications, Chapel Hill, N.C., University of North Carolina Press, 1969.
9. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, 1997.
10. R.J. McEliece, *Correlation properties of sets of sequences derived from irreducible cyclic codes*, Information and Control, **45** (1980), 18-25.
11. Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D thesis, University of Southern California, 1972.
12. D.V. Sarwate, M.B. Purseley, *Crosscorrelation properties of pseudorandom and related sequences*, Proceedings of the IEEE, **68** (1980), 593-619.
13. R.A. Scholtz and L.R. Welch, *GMW sequences*, IEEE Transactions on Information Theory, **30** (1984), 548-553.
14. E.S. Selmer, *Linear Recurrence Relations over Finite Fields*, University of Bergen, 1966.
15. M. Simon, J. Omura, R. Scholtz, B. Levitt, *Spread Spectrum Communications*, Computer Science Press, 1985.
16. L.R. Welch, *Lower bounds on the maximum cross-correlation of signals*, IEEE Transactions on Information Theory, **20** (1974), 397-399.
17. N. Zierler, *Linear recurring sequences*, Journal of the Society for Industrial and Applied Mathematics, **7** (1976), 31-48.

Min-Jeong Kwon received M.Pe. at Pusan National University. She is currently a doctor's course at Pukyong National University since 2007. Her research interests include finite field theory, discrete mathematics and cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 608-737, Korea.
e-mail: mjblack02@hanmail.net

Sung-Jin Cho received M.Sc. and Ph.D. at Korea University. He is currently a professor at Pukyong University since 1988. His research interests include finite field theory, discrete mathematics and cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 608-737, Korea.
e-mail: sjcho@pknu.ac.kr