Cross-Correlation Distribution of p-ary m-Sequence and Its $p+1$ Subsequences

Eun-Young Seo
School of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea.
gourb@ccl.snu.ac.kr

Young-Sik Kim
Embedded Software Center
System LSI Division
Samsung Electronics Co.
Yongin 446-711, Korea
kingsi@ccl.snu.ac.kr

Jong-seon No
School of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea.
jsno@snu.ac.kr

Dong-Joon Shin
Division of Electronics and Computer Engineering
Hanyang University
Seoul 133-791, Korea.
djshin@hanyang.ac.kr

***Abstract*— For an odd prime p, an even integer n, and $d = p^k + 1$ with $\gcd(n,k) = 1$, there are $p+1$ distinct decimated sequences $s(dt+l)$, $0 \le l < p+1$, for a p-ary m-sequence $s(t)$ of period $p^n - 1$ since $\gcd(d, p^n - 1) = p + 1$. In this paper, the cross-correlation distribution between a p-ary m-sequence $s(t)$ and its $p+1$ distinct decimated sequences $s(dt+l)$ is derived. The maximum magnitude of their cross-correlation values is $1+p\sqrt{p^n}$ if $l \equiv 0 \bmod p+1$ for $n \equiv 0 \bmod 4$ or $l \equiv (p+1)/2 \bmod p+1$ for $n \equiv 2 \bmod 4$ and otherwise, $1+\sqrt{p^n}$. Also by using $s(t)$ and $s(dt+l)$, a new family of p-ary sequences of period $p^n - 1$ is constructed, whose family size is p^n and $C_{\max}$ is $1 + p\sqrt{p^n}$.**

I. Introduction

To construct a family of p-ary sequences of period $p^n - 1$ with good correlation property, the cross-correlation distribution between a p-ary m-sequence $s(t)$ of period $p^n - 1$ and its decimated sequence $s(dt)$ with $\gcd(d, p^n - 1) = 1$ has been studied for many years [1]–[3].

There are some research results dealing with a decimation factor d which is not relatively prime to the period $p^n - 1$ [4]–[6]. Kumar and Moreno [5] derived the cross-correlation values of $s(t)$ and $s(dt)$ with $d = p^k+1$, where $n/\gcd(n,k) =$ odd. In this case, $\gcd(d, p^n - 1)$ is 2 and the maximum magnitude $C_{\max}$ of the cross-correlation values of the sequence family is $1+\sqrt{p^n}$, which is optimal with respect to the Welch bound [7]. Furthermore, in Theorem 4 of [6], Müller found the upper bound on the cross-correlation values of the sequences $s(t)$ and only one decimated sequence $s(dt)$ when n is even, $n/\gcd(n,k)$ is not divisible by 4, and d is $p^k + 1$.

For an odd prime p, an even integer n, and $d = p^k+1$ with $\gcd(n,k) = 1$, there are $p+1$ distinct decimated sequences $s(dt+l)$, $0 \le l < p+1$, of a p-ary m-sequence $s(t)$ of period $p^n - 1$ since $\gcd(d, p^n - 1) = p + 1$. In this paper, the cross-correlation distribution between a p-ary m-sequence $s(t)$ and its decimated sequences $s(dt+l)$, $0 \le l < p+1$, is derived. It is also shown that $C_{\max}$ is $1+p\sqrt{p^n}$ when $l \equiv 0 \mod p+1$ for $n \equiv 0 \mod 4$ or when $l \equiv (p+1)/2 \mod p+1$ for $n \equiv 2 \mod 4$, and for the remaining cases, $C_{\max}$ is $1+\sqrt{p^n}$. By using $s(t)$ and $s(dt+l)$, a new family of p-ary sequences of period $p^n - 1$ is constructed, whose family size is p^n and $C_{\max}$ is $1 + p\sqrt{p^n}$.

II. Preliminaries

Let p be an odd prime, F_{p^n} the finite field with p^n elements, and $F_{p^n}^* = F_{p^n} \backslash \{0\}$. Then the trace function from F_{p^n} to F_{p^m} is defined as $\mathrm{tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{p^{mi}}$, where $x \in F_{p^n}$ and $m|n$. Let α be a primitive element of F_{p^n}. Then a p-ary m-sequence $s(t)$ of period $p^n - 1$ can be written in terms of the trace function as $s(t) = \mathrm{tr}_1^n(\alpha^t)$.

Let n be an even integer and $d = p^k+1$ with $\gcd(n,k) = 1$. Since $\gcd(p^n - 1, d) = p+1$, we have $p+1$ distinct decimated sequences $s_l(dt)$ of period $(p^n - 1)/(p+1)$ using shift value l, $0 \le l < p+1$, which are defined as

$$s_l(dt) = \mathrm{tr}_1^n(\alpha^{dt+l}). \tag{1}$$

Then the cross-correlation function of m-sequence $s(t)$ and its decimated sequence $s_l(dt)$ at shift τ is defined as

$$C_l(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_l(dt)-s(t+\tau)} = \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax^d - bx)} \tag{2}$$

where ω is a primitive complex p-th root of unity, $a = \alpha^l$, and $b = \alpha^\tau$. From now on, we will use the notations $C_l(\tau)$ and $C_l(b)$, interchangeably.

Let ψ denote the canonical additive character of the additive group F_{p^n}, which is defined as $\psi(c) = e^{j2\pi \mathrm{tr}_1^n(c)/p}$, for all $c \in F_{p^n}$. All additive characters of F_{p^n} can be expressed in terms of ψ. A character χ of the multiplicative group $F_{p^n}^*$ is called a multiplicative character of F_{p^n}. Note that the quadratic character η of F_{p^n} is one of multiplicative characters defined by

$$\eta(x) = \begin{cases} 1, & \text{if } x \text{ is nonzero square in } F_{p^n} \\ -1, & \text{if } x \text{ is nonzero nonsquare in } F_{p^n} \\ 0, & \text{if } x = 0. \end{cases}$$

The Gauss sum $G(\chi, \psi)$ using these two characters becomes

$$G(\chi, \psi) = \sum_{c \in F_{p^n}^*} \chi(c)\psi(c).$$

Then for the quadratic character η, the associated Gauss sum can be explicitly evaluated as in the following theorem.

Theorem 1: [9, Theorem 5.15] Let p be an odd prime and η and ψ denote the quadratic character and canonical additive character of F_{p^n}, respectively. Then the Gauss sum is given as

$$G(\eta,\psi)=\begin{cases}(-1)^{n-1}p^{\frac{n}{2}}, & \text{if } p\equiv 1 \bmod 4\\ (-1)^{n-1}i^n p^{\frac{n}{2}}, & \text{if } p\equiv 3 \bmod 4\end{cases}$$

where $i=\sqrt{-1}$. □

III. Distribution of Cross-Correlation Values

In this section, we derive the cross-correlation distribution of a p-ary m-sequence $s(t)$ and its decimated sequences $s_l(dt)$ defined in (1) in the following theorem.

Let n be an even integer, α a primitive element of F_{p^n}, and $d=p^k+1$ with $\gcd(n,k)=1$. Define

$$Q_l(x)=\mathrm{tr}_1^n(\alpha^l x^d), \quad 0\le l<p+1. \tag{3}$$

Note that $Q_l(x)$ is a quadratic form. First, we determine the rank of the quadratic form $Q_l(x)$ defined in (3) in the following lemma.

Lemma 2: The rank of a quadratic form $Q_l(x)$ in (3) is given as

$$\begin{aligned}&Rank\ of\ Q_l(x)\\ &=\begin{cases}n-2, & \text{if } l\equiv 0 \bmod p+1 \text{ for } n\equiv 0 \bmod 4 \text{ or}\\ & \quad l\equiv \frac{p+1}{2} \bmod p+1 \text{ for } n\equiv 2 \bmod 4\\ n, & \text{otherwise.}\end{cases}\end{aligned}$$

Proof: The rank ρ of a quadratic form can be determined by finding the number of coordinates of which the quadratic form is independent, i.e., $p^{n-\rho}$ is the number of $z\in F_{p^n}$ such that $Q_l(x+z)=Q_l(x)$ for all $x\in F_{p^n}$. Then we have

$$\begin{aligned}Q_l(x+z)-Q_l(x)&=\mathrm{tr}_1^n(\alpha^l x z^{p^k}+\alpha^l x^{p^k}z+\alpha^l z^{p^k+1})\\ &=\mathrm{tr}_1^n((\alpha^{lp^k}z^{p^{2k}}+\alpha^l z)x^{p^k})+\mathrm{tr}_1^n(\alpha^l z^{p^k+1}).\end{aligned}$$

In order to satisfy $Q_l(x+z)-Q_l(x)=0$ for all $x\in F_{p^n}$, we must have

$$\alpha^{lp^k}z^{p^{2k}}+\alpha^l z=0 \tag{4}$$

$$\mathrm{tr}_1^n(\alpha^l z^{p^k+1})=0. \tag{5}$$

If $\alpha^{lp^k}z^{p^{2k}}+\alpha^l z=0$, then (5) is always satisfied because

$$\mathrm{tr}_1^n(\alpha^l z^{p^k+1})=\mathrm{tr}_1^n(\alpha^{lp^k}z^{p^{2k}}z^{p^k})=\mathrm{tr}_1^n(-\alpha^l z^{p^k+1}).$$

Now, we only have to count the number of solutions z satisfying (4), which can be rewritten as

$$\alpha^{(p^k-1)l}\alpha^{(p^{2k}-1)s}=-1=\alpha^{\frac{p^n-1}{2}m}$$

where $z=\alpha^s$ and m is some odd integer. Then we have to count the number of integers s, $0\le s<p^n-1$, satisfying the following congruence

$$(p^{2k}-1)s+(p^k-1)l\equiv\frac{(p^n-1)}{2}m \bmod p^n-1. \tag{6}$$

We will use the well-known fact that $xs\equiv y \bmod r$ has a solution s if and only if $\gcd(r,x)|y$ and in this case there are $\gcd(r,x)$ solutions. Also, we have $\gcd(p^n-1,p^{2k}-1)=p^{\gcd(n,2k)}-1=p^2-1$.

Case 1) $n\equiv 0 \bmod 4$:

It is clear that (p^2-1) devides $(p^n-1)m/2$ because $(p^n-1)/(p^2-1)$ is even. Therefore, to have solutions for (6), the following value

$$\frac{(p^k-1)l}{p^2-1}=\frac{(p^{k-1}+p^{k-2}+\cdots+p+1)l}{p+1}$$

should be an integer. From $\gcd(p^k-1,p^2-1)=p-1$, we have $\gcd(p^{k-1}+p^{k-2}+\cdots+p+1,p+1)=1$, and the above value is an integer if and only if $l\equiv 0 \bmod p+1$. Therefore, when $l\equiv 0 \bmod p+1$, we have p^2-1 solutions s of (6) as

$$s=\frac{m(p^n-1)}{2(p^{2k}-1)}-\frac{l}{p^k+1}+\big(\frac{p^n-1}{p^2-1}\big)u \tag{7}$$

where $u=0,1,2,\cdots,p^2-2$. This means that there are p^2-1 nonzero solutions z satisfying (4). Since $z=0$ also satisfies (4), the rank of the quadratic form $Q_l(x)$ is given as

$$\begin{cases}n-2, & \text{for } l\equiv 0 \bmod p+1\\ n, & \text{otherwise.}\end{cases}$$

Case 2) $n\equiv 2 \bmod 4$:

Similarly to Case 1), to have solutions for (6), p^2-1 should divide $(p^n-1)m/2-(p^k-1)l$. Since $\gcd(p^2-1,p^k-1)=p-1$, the following value

$$\frac{m(1+p^2+\cdots+p^{n-2})-\frac{2}{p+1}l(1+p+\cdots+p^{k-1})}{2}$$

should be an integer. Thus, there are p^2-1 solutions s of (6) given in (7) if and only if $l\equiv\frac{p+1}{2} \bmod p+1$. This also means that there are p^2-1 nonzero solutions z satisfying (4). Since $z=0$ also satisfies (4), the rank of the quadratic form $Q_l(x)$ is given as

$$\begin{cases}n-2, & \text{for } l\equiv\frac{p+1}{2} \bmod p+1\\ n, & \text{otherwise.}\end{cases}$$

□

Now, we derive the cross-correlation distribution of a p-ary m-sequence $s(t)$ and its decimated sequences $s_l(dt)$ defined in (1) in the following theorems.

Theorem 3: [9, Theorem 6.26] Let f be a nondegenerate quadratic form in an even number n of indeterminates over F_q, q odd. Then for $b\in F_q$, the number of solutions of the equation $f(x_1,\cdots,x_n)=b$ in F_q^n is

$$q^{n-1}+v(b)q^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}\Delta)$$

where η is the quadratic character of F_q and $\Delta=\det(f)$ and $v(b)=-1$ if $b\neq 0$ and $v(b)=q-1$ if $b=0$. □

By a nonsingular linear transformation in coordinates, the quadratic form $Q_l(x)$ with rank k can be represented as [8]

$$Q_l(x) = \sum_{i=1}^{k} a_i x_i^2 \tag{8}$$

where $a_i \in F_p^*$.

By using Theorem 4, we can obtain the following cross-correlation distribution of $s(t)$ and $p+1$ distinct decimated sequences $s_l(dt)$, where $0 \le l < p+1$.

Theorem 4: Let p be an odd prime, n an even number, and $d = p^k + 1$ with $\gcd(n,k) = 1$. Let $\Delta = a_1 \cdots a_n$ and $\Delta' = a_1 \cdots a_{n-2}$. Let η and ψ denote the quadratic character and canonical additive character of F_p, respectively. Then, the cross-correlation distribution of a p-ary m-sequence $s(t)$ and its decimated sequences $s_l(dt)$ becomes:

Case 1) $l \not\equiv 0 \bmod p+1$ for $n \equiv 0 \bmod 4$ or $l \not\equiv (p+1)/2 \bmod p+1$ for $n \equiv 2 \bmod 4$:

If $n \equiv 2 \bmod 4$ and $p \equiv 3 \bmod 4$, $0 \le \tau < p^n - 1$, the distribution of cross-correlation values is given as

$$C_l(\tau) = \begin{cases} -1 - p^{\frac{n}{2}}\eta(\Delta), & \\ \qquad p^{n-1} - (p-1)p^{\frac{n-2}{2}}\eta(\Delta) - 1 \text{ times} \\ -1 - p^{\frac{n}{2}}\eta(\Delta)\psi(u), & \\ \quad p^{n-1} + p^{\frac{n-2}{2}}\eta(\Delta) \text{ times for each } u \in F_p^* \end{cases} \tag{9}$$

and otherwise,

$$C_l(\tau) = \begin{cases} -1 + p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}\Delta), & \\ \qquad p^{n-1} + (p-1)p^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}\Delta) - 1 \text{ times} \\ -1 + p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}\Delta)\psi(u), & \\ \quad p^{n-1} - p^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}\Delta) \text{ times for each } u \in F_p^*. \end{cases} \tag{10}$$

Case 2) $l \equiv 0 \bmod p+1$ for $n \equiv 0 \bmod 4$ or $l \equiv (p+1)/2 \bmod p+1$ for $n \equiv 2 \bmod 4$:

If $n \equiv 0 \bmod 4$ and $p \equiv 3 \bmod 4$, the distribution of cross-correlation values is given as

$$C_l(\tau) = \begin{cases} -1, & p^n - p^{n-2} \text{ times} \\ -1 - p^{\frac{n}{2}+1}\eta(\Delta'), & \\ \qquad p^{n-3} + (p-1)p^{\frac{(n-4)}{2}}\eta(\Delta') - 1 \text{ times} \\ -1 - p^{\frac{n}{2}+1}\eta(\Delta')\psi(u), & \\ \quad p^{n-3} - p^{\frac{(n-4)}{2}}\eta(\Delta') \text{ times for each } u \in F_p^* \end{cases} \tag{11}$$

and otherwise,

$$C_l(\tau) = \begin{cases} -1, & p^n - p^{n-2} \text{ times} \\ -1 + p^{\frac{n}{2}+1}\eta((-1)^{\frac{n-2}{2}}\Delta'), & \\ \qquad p^{n-3} + (p-1)p^{\frac{n-4}{2}}\eta((-1)^{\frac{n-2}{2}}\Delta') - 1 \text{ times} \\ -1 + p^{\frac{n}{2}+1}\eta((-1)^{\frac{n-2}{2}}\Delta')\psi(u), & \\ \quad p^{n-3} - p^{\frac{n-4}{2}}\eta((-1)^{\frac{n-2}{2}}\Delta') \text{ times for each } u \in F_p^*. \end{cases} \tag{12}$$

Proof: From (2), we have

$$C_l(b) + 1 = \sum_{x \in F_{p^n}} \omega^{Q_l(x) - \mathrm{tr}_1^n(bx)}$$

where $b = \alpha^\tau$. It is easy to check that a nonsingular linear transformation of variables can only permute the correlation values and therefore does not affect the distribution of correlation values.

Note that $\psi(\cdot)$ is the canonical additive character of F_p, i.e., $\psi(u) = w^u$, where $u \in F_p$. From Lemma 2, the quadratic form $Q_l(x)$ has the rank n or $n-2$.

Case 1) $Q_l(x)$ has the full rank n:

For nonzero a_i's and $\mathrm{tr}_1^n(bx) = \sum_{i=1}^n b_i x_i$ where $b_i \in F_p$, the cross-correlation function can be rewritten as

$$\begin{aligned} C_l(b) + 1 &= \sum_{(x_1,\cdots,x_n) \in F_p^n} \omega^{\sum_{i=1}^n a_i x_i^2 - \sum_{i=1}^n b_i x_i} \\ &= \sum_{(x_1,\cdots,x_n) \in F_p^n} \psi\Big(\sum_{i=1}^n a_i (x_i - \frac{b_i}{2a_i})^2\Big)\psi\Big(-\sum_{i=1}^n \frac{b_i^2}{4a_i}\Big). \end{aligned}$$

Let $y_i = x_i - b_i/2a_i$ and $a_i y_i^2 = c_i$. If a_i is square (or nonsquare), then c_i will give each square (or nonsquare) of F_p twice when y_i runs through F_p. Using this fact, the value of $\sum_{y_i \in F_p} \psi(a_i y_i^2)$ can be represented as

$$\begin{aligned} \sum_{y_i \in F_p} \psi(a_i y_i^2) &= \sum_{c_i \in F_p} \psi(c_i)(1 + \eta(c_i a_i^{-1})) \\ &= \eta(a_i^{-1}) G(\eta, \psi) \end{aligned}$$

and thus

$$C_l(b) + 1 = \eta(a_1^{-1} \cdots a_n^{-1}) G^n(\eta, \psi) \psi\Big(-\sum_{i=1}^n \frac{b_i^2}{4a_i}\Big).$$

From Theorem 1, for even n, the Gauss sum is given as

$$G^n(\eta, \psi) = \begin{cases} -p^{\frac{n}{2}}, & \text{if } n \equiv 2 \bmod 4 \text{ and } p \equiv 3 \bmod 4 \\ p^{\frac{n}{2}}, & \text{otherwise} \end{cases}$$

and

$$C_l(b) + 1 = \begin{cases} -p^{\frac{n}{2}}\eta(\Delta)\psi\Big(-\sum_{i=1}^n \frac{b_i^2}{4a_i}\Big), & \\ \qquad \text{if } n \equiv 2 \bmod 4 \text{ and } p \equiv 3 \bmod 4 \\ p^{\frac{n}{2}}\eta(\Delta)\psi\Big(-\sum_{i=1}^n \frac{b_i^2}{4a_i}\Big), \qquad \text{otherwise.} \end{cases}$$

Note that $-\sum_{i=1}^n b_i^2/(4a_i)$ is another canonical quadratic form with coefficients $-1/(4a_i)$, $1 \le i \le n$. Using Theorem 3, we can obtain the number of occurrences of $C_l(b)$ for $u \in F_p^*$ and $b \in F_{p^n}^*$ as follows.

If $n \equiv 2 \bmod 4$ and $p \equiv 3 \bmod 4$, -1 is a nonsquare and the cross-correlation function is derived as (9) and otherwise, we have (10).

Case 2) $Q_l(x)$ has the rank $n-2$:

Using the fact that $a_{n-1} = a_n = 0$, the cross-correlation function can be rewritten as

$$C_l(b)+1 = \sum_{(x_1,\cdots,x_{n-2})\in F_p^{n-2}} \psi\Big(\sum_{i=1}^{n-2} a_i(x_i - \frac{b_i}{2a_i})^2\Big) \times \psi\Big(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\Big) \sum_{(x_{n-1},x_n)\in F_p^2} \psi(-b_{n-1}x_{n-1} - b_n x_n).$$

Note that the innermost summation is p^2 if $b_{n-1} = b_n = 0$ or 0, otherwise. If $b_{n-1} \neq 0$ or $b_n \neq 0$, $C_l(b)+1 = 0$ occurs $p^n - p^{n-2}$ times. If $b_{n-1} = b_n = 0$, we have

$$C_l(b)+1 = p^2\psi\Big(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\Big)\sum_{x_1\in F_p}\psi\Big(a_1\big(x_1-\frac{b_1}{2a_1}\big)^2\Big) \cdots \sum_{x_{n-2}\in F_p}\psi\Big(a_{n-2}\big(x_{n-2}-\frac{b_{n-2}}{2a_{n-2}}\big)^2\Big).$$

Let $y_i = x_i - b_i/2a_i$ and $a_i y_i^2 = c_i$. Then, similarly to Case 1), we have

$$C_l(b)+1 = \eta(a_1^{-1}\cdots a_{n-2}^{-1})G^{n-2}(\eta,\psi)\psi\Big(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\Big).$$

From Theorem 1, we have

$$C_l(b)+1 = \begin{cases} -p^{\frac{n}{2}+1}\eta(\Delta')\psi\Big(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\Big), \\ \qquad\qquad \text{if } n\equiv 0 \bmod 4 \text{ and } p\equiv 3 \bmod 4 \\ p^{\frac{n}{2}+1}\eta(\Delta')\psi\Big(-\sum_{i=1}^{n-2}\frac{b_i^2}{4a_i}\Big), \qquad \text{otherwise.}\end{cases}$$

Using Theorem 3, we can obtain the number of occurrences of $C_l(b)$ for $u \in F_p^*$ and $b \in F_{p^n}^*$ as follows.

If $n \equiv 0 \bmod 4$ and $p \equiv 3 \bmod 4$, the cross-correlation distribution is derived as in (11) and otherwise, (12) since if $n \equiv 0 \bmod 4$, -1 is a quadratic residue. □

Thus, using a p-ary m-sequence $s(t)$ and its $p+1$ decimated sequences $s_l(dt)$ in (1), we can construct a family $\mathcal{S}$ of p-ary sequences of period p^n-1 with family size p^n that has the same value of $C_{\max}$ with Gold sequence family as

$$\mathcal{S} = \{s_\beta(t) \mid \beta \in F_{p^n},\ 0 \le t \le p^n-2\}$$

$$s_\beta(t) = \mathrm{tr}_1^n(\alpha^t + \beta\alpha^{dt}),\ 0 \le t \le p^n-2,\ \beta \in F_{p^n}$$

where p is an odd prime, n is an even integer, and $d = p^k+1$ with $\gcd(n,k) = 1$. Note that when we calculate the cross-correlation values for p-ary sequences in $\mathcal{S}$, we may have the cross-correlation value $W = \sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax^d)}$, which corresponds to $C_l(b)$ with $b = 0$ in (2). From Theorem 3, we can obtain

$$W = \begin{cases} -1 - p^{\frac{n}{2}}\eta((-1)^{\frac{n}{2}}(\Delta)), \\ \qquad\qquad \text{if } Q_l(x) \text{ has full rank} \\ -1 - p^{\frac{n}{2}+1}\eta((-1)^{\frac{n-2}{2}}(\Delta')), \quad \text{otherwise.}\end{cases}$$

Thus, $C_{\max}$ for $\mathcal{S}$ becomes

$$|C_{\max}| \le p\sqrt{p^n} + 1.$$

ACKNOWLEDGMENT

This research was supported by the MIC, Korea, under the ITRC support program and by the MOE, the MOCIE, and the MOLAB, Korea, through the fostering project of the Laboratory of Excellency.

REFERENCES

[1] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences,"*Ph.D. dissertation*, Univ. of Southern California, Los Angeles, CA, 1970.

[2] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences,"*Discrete Math.*, vol. 16, pp. 209–232, 1976.

[3] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 613–627, Feb. 2006.

[4] G. J. Ness, T. Helleseth, and A. Kholosha, "On the correlation distribution of the Coulter-Matthews decimation," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2241–2247, May 2006.

[5] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 603–616, May 1991.

[6] E. N. Müller, "On the cross-correlation of sequences over $GF(p)$ with short periods," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 289–295, Jan. 1999.

[7] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.

[8] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*. New York: Dover, 1958.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983.