On the Cross-Correlation of a p-Ary m-Sequence of Period $p^{2m}-1$ and Its Decimated Sequences by $(p^m+1)^2/2(p+1)$

Sung-Tai Choi, Taehyung Lim, Jong-Seon No, *Fellow, IEEE*, and Habong Chung, *Member, IEEE*

***Abstract*—In this paper, for an odd prime p, we investigate into the cross-correlation of a p-ary m-sequence $m(t)$ of period p^n-1 and its d-decimated sequences $m(dt+l)$, $0 \le l < \frac{p^m+1}{2}$, where $d=\frac{(p^m+1)^2}{2(p+1)}$, $n=2m$, and m is an odd integer. There are $\frac{p^m+1}{2}$ distinct decimated sequences $m(dt+l)$ since $\gcd(d,p^n-1)=\frac{(p^m+1)}{2}$. It is shown that the magnitude of the cross-correlation values is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$. We also construct the sequence family $\mathcal{F}$ from these sequences, where the family size is p^m and the correlation magnitude is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$.**

***Index Terms*—Cross-correlation, decimated sequence, m-sequence, nonbinary sequence, quadratic form, sequence family.**

I. Introduction

THERE has been much research to find a decimation value d such that the cross-correlation of a p-ary m-sequence $m(t)$ and its decimated sequence $m(dt)$ is low. The values d with $\gcd(d,p^n-1)=1$ have been studied in [1], [2], [3], and [4].

There have also been some research works dealing with a decimation factor d not relatively prime to the period p^n-1. When d is not relatively prime to the period p^n-1, the decimated sequences $m(dt+l)$ have short period, $(p^n-1)/\gcd(d,p^n-1)$. For a ternary case, in [5], the authors derived the correlation distribution for $d=(3^k+1)/2$ and $\gcd(k,n)=1$, which corresponds to the Coulter–Matthews decimation. In [6], the authors derived the correlation distribution of $m(t)$ and $m(dt)$ with $d=p^k+1$, where $n/\gcd(n,k)$ is odd and p is an odd prime. In [7], the author showed that the magnitude of correlation values is upper bounded by $2\sqrt{3^n}+1$ for $d=(3^n+1)/4+(3^n-1)/2$ for ternary m-sequences. In [8], the authors extended Muller's result to any odd prime case, i.e., for $d=(p^n+1)/(p+1)-(p^n-1)/2$, and derived the upper bound as $\frac{p+1}{2}p^{\frac{n}{2}}+1$. In [12], the authors derived the correlation distribution for $d=(p^{2k}+1)^2/4$, when p is an odd prime and $n=4k$. The known decimation values d and the upper bounds of magnitude of cross-correlation values are listed in Table I.

In this paper, for an odd prime p, the upper bound on the magnitude of cross-correlation values of a p-ary m-sequence $m(t)$ and its decimation sequences $m(dt+l)$, $0 \le l < (p^m+1)/2$, is derived for $d=(p^m+1)^2/(2(p+1))$, $n=2m$, and an odd integer m. The decimated sequences $m(dt+l)$ have the period of $2(p^m-1)$ because $\gcd(d,p^n-1)=(p^m+1)/2$. It is shown that the magnitude of cross-correlation function $C_l(\tau)$ of $m(t)$ and $m(dt+l)$ is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$. We also construct the sequence family $\mathcal{F}$ by using $m(t)$ and $m(dt+l)$, where the family size is p^m and the magnitude of correlation values is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$.

II. Preliminaries

Let p be an odd prime and F_{p^n} the finite field with p^n elements. Then, the trace function $\mathrm{tr}_k^n(\cdot)$ from F_{p^n} to F_{p^k} is defined as

$$\mathrm{tr}_k^n(x)=\sum_{i=0}^{\frac{n}{k}-1}x^{p^{ki}}$$

where $x \in F_{p^n}$ and $k|n$.

Let α be a primitive element of F_{p^n}. Then, a p-ary m-sequence $m(t)$ with the period of p^n-1 can be expressed as

$$m(t)=\mathrm{tr}_1^n(\alpha^t).$$

Since $\gcd(p^n-1,d)=(p^m+1)/2$, there are $(p^m+1)/2$ distinct decimated sequences $m(dt+l)$ of period $2(p^m-1)$, $0 \le l < (p^m+1)/2$, which are defined as

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

The cross-correlation function between two p-ary sequences $a(t)$ and $b(t)$ at shift τ is defined as

$$C(\tau)=\sum_{t=0}^{p^n-2}\omega^{a(t+\tau)-b(t)}$$

where ω is a primitive pth root of unity.

The quadratic character of F_{p^n} is defined as

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

Manuscript received April 30, 2010; revised May 25, 2011; accepted August 30, 2011. Date of current version February 29, 2012. The material in this paper was presented at the 2010 IEEE International Symposium on Information Theory. This work was supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology, Korea Government under Grant 2011-0000328 and the Korea Communications Commission (KCC), Korea, under the R&D program supervised by the Korea Communications Agency (KCA) under Grant KCA-2011-08913-04003.

S.-T. Choi, T. Lim, and J.-S. No are with the Department of Electrical Engineering and Computer Science, INMC, Seoul National University, Seoul 151-744, Korea (e-mail: stchoi@ccl.snu.ac.kr; jayelish@hotmail.com; jsno@snu.ac.kr).

H. Chung is with the School of Electronics and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@hongik.ac.kr).

Communicated by N. Yul Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2177573

TABLE I
PARAMETERS OF SOME KNOWN DECIMATION VALUES FOR THE NONBINARY CASE

Researcher	Alphabet p	$\gcd(d, p^n-1)$	d	Upper bound of $\lvert C(\tau)\rvert$
Trachtenberg [1]	odd prime	1	$\frac{p^{2k}+1}{2}$, n odd, $e=\gcd(n,k)$	$1+p^{\frac{n+e}{2}}$
Trachtenberg [1]	odd prime	1	$p^{2k}-p^k+1$, n odd, $e=\gcd(n,k)$	$1+p^{\frac{n+e}{2}}$
Dobbertin *et al.* [3]	3	1	$2p^{\frac{n-1}{2}}+1$, n odd	$1+p^{\frac{n+1}{2}}$
Muller [7]	3	2	$\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$, n odd	$1+2p^{\frac{n}{2}}$
Hu *et al.* [8]	odd prime ($3 \bmod 4$)	2	$\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$, n odd	$1+\frac{p+1}{2}p^{\frac{n}{2}}$
Seo *et al.* [12]	odd prime	$\frac{p^{\frac{n}{2}}+1}{2}$	$\left(\frac{p^{\frac{n}{2}}+1}{2}\right)^2$, $n\equiv 0 \bmod 4$	$1+2p^{\frac{n}{2}}$
Seo *et al.* [13]	odd prime	$p+1$	p^k+1, n even, $\gcd(n,k)=1$	$1+p^{\frac{n}{2}+1}$
New Decimation	odd prime	$\frac{p^{\frac{n}{2}}+1}{2}$	$\frac{(p^{\frac{n}{2}}+1)^2}{2(p+1)}$, $n\equiv 2 \bmod 4$	$1+\frac{p+1}{2}p^{\frac{n}{2}}$

The Gauss sum pertaining to the quadratic character of F_p is given as the following theorem.

Theorem 1 (Theorem 5.15 [15]): Let p be an odd prime and η the quadratic character of F_p. Then,

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

where ω is a primitive pth root of unity and $j=\sqrt{-1}$. ■

A quadratic form over F_p in n indeterminates is a homogeneous polynomial in $F_p[x_1,\ldots,x_n]$ of degree 2 and can be expressed as

$$f(x_1,x_2,\ldots,x_n)=\sum_{i,j\le n}a_{ij}x_ix_j$$

where $a_{ij}\in F_p$.

Let $(F_p)^n$ denote an n-dimensional vector space over F_p. The number of solutions $(x_1,x_2,\ldots,x_n)\in(F_p)^n$ satisfying the quadratic form $f(x_1,\ldots,x_n)=b$ for any $b\in F_p$ can be determined from the rank of the quadratic form $f(x_1,x_2,\ldots,x_n)$. The following lemma explains how to determine the rank of a quadratic form.

Lemma 2 (Lemma 6 [7]): Let $f\in F_p[x_1,x_2,\ldots,x_n]$ be a quadratic form. Define

$$Z:=\{\mathbf{z}\in(F_p)^n: f(\mathbf{x}+\mathbf{z})-f(\mathbf{x})=0 \text{ for all } \mathbf{x}\in(F_p)^n\}. \tag{2}$$

Then, Z is a subspace of $(F_p)^n$ and the rank of f is defined as $\operatorname{rank}(f)=n-\dim(Z)$. ■

A quadratic form $f(\mathbf{x})$ in $(F_p)^n$ can be regarded as a mapping $f(x)$ from F_{p^n} into F_p. Thus, we will also use the term ''quadratic form" for this mapping $f(x)$ in a finite extension field F_{p^n}. In this case, Lemma 2 in a finite-field version can be restated as follows.

Corollary 3: The rank ρ of the quadratic form $f(x)$ from F_{p^n} to F_p can be determined by finding the number of coordinates that the form is independent of, i.e., $p^{n-\rho}$ is the number of $z\in F_{p^n}$, such that $f(x+z)=f(x)$, for all $x\in F_{p^n}$. ■

A quadratic form $f\in F_p[x_1,x_2,\ldots,x_k]$ in k indeterminates over F_p is said to be nondegenerate if it has a full rank, i.e., $f(x)$ can be expressed as the canonical form $a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2$ for $a_i\neq 0$. Let $\Delta=a_1a_2\cdots a_k$ denote the determinant of the quadratic form $f(x)$. If $f(x)$ is a nondegenerate quadratic form of rank k, the number of solutions x in F_{p^k} satisfying $f(x)=b\in F_p$ is determined as in the following lemma.

Lemma 4 (Theorems 6.26 and 6.27 [15]): Let η be the quadratic character of F_p. The number of solutions $N(b)$ of $f(\mathbf{x})=b$ in $(F_p)^k$, when $f(\mathbf{x})$ is a nondegenerate quadratic form in rank k with determinant Δ and $b\in F_p$, is given as follows.:

Case 1) k even;

$$N(b)=\begin{cases}p^{k-1}-\epsilon p^{\frac{k-2}{2}}, & \text{if } b\neq 0,\\ p^{k-1}+\epsilon(p-1)p^{\frac{k-2}{2}}, & \text{if } b=0\end{cases}$$

where $\epsilon=\eta((-1)^{k/2}\Delta)$.

Case 2) k odd;

$$N(b)=\begin{cases}p^{k-1}+\epsilon\eta(b)p^{\frac{k-1}{2}}, & \text{if } b\neq 0,\\ p^{k-1}, & \text{if } b=0\end{cases}$$

where $\epsilon=\eta((-1)^{(k-1)/2}\Delta)$. ■

If a nonzero quadratic form $f\in F_p[x_1,x_2,\ldots,x_n]$ has a rank $k\le n$, it can be rewritten as an equivalent canonical form, $a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2$, where all $a_i\neq 0$[15]. Hence, for any $b\in F_p$, the number of solutions of $a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2=b$ in $(F_p)^n$ is p^{n-k} times the number of solutions of the same equation in $(F_p)^k$. For a quadratic form $f\in F_p[x_1,x_2,\ldots,x_n]$ with rank k, we can decide the number of solutions $f(x)=b$ in F_{p^n}, where $b\in F_p$, from Lemma 4 and the previous fact.

Using Theorem 1 and Lemma 4, the following corollary can be stated without proof.

Corollary 5: Let $f(x)$ be a mapping from F_{p^n} to F_p corresponding to a quadratic form $f(\mathbf{x})\in F_p[x_1,x_2,\ldots,x_n]$ of rank k with determinant Δ. Then, the exponential sum $\sum_{x\in F_{p^n}}\omega^{f(x)}$ is given as follows.

Case 1) k even;

$$\sum_{x\in F_{p^n}}\omega^{f(x)}=\epsilon p^{\frac{k}{2}}p^{n-k}$$

where $\epsilon=\eta((-1)^{k/2}\Delta)$.

Case 2) k odd;

$$\sum_{x\in F_{p^n}}\omega^{f(x)}=\begin{cases}\epsilon p^{\frac{k}{2}}p^{n-k}, & \text{if } p\equiv 1 \bmod 4,\\ j\epsilon p^{\frac{k}{2}}p^{n-k}, & \text{if } p\equiv 3 \bmod 4,\end{cases}$$

where $\epsilon=\eta((-1)^{(k-1)/2}\Delta)$. ■

Let q be a prime power. A polynomial of the form

$$L(x)=\sum_i \alpha_i x^{q^i}$$

with coefficients in an extension field F_{q^m} of F_q is called a q-polynomial or linearized polynomial over F_{q^m}. If F is an arbitrary extension field of F_{q^m}, which contains all the roots of $L(x)$, then

$$L(\beta+\gamma)=L(\beta)+L(\gamma),\ \text{for all } \beta,\gamma\in F,$$
$$L(c\beta)=cL(\beta),\ \text{for all } \beta\in F \text{ and } c\in F_q.$$

Hence, the set of solutions of $L(x)=0$ in F is considered as a vector subspace over F_q, i.e., the number of solutions is a power of q.

In the remaining part of this paper, the following notations will be used:

1) $n=2m$ and m is an odd integer;
2) $d=\frac{(p^m+1)^2}{2(p+1)}$;
3) α is a primitive element of F_{p^n};
4) ω is a pth root of unity.

III. Quadratic Expression for the Cross-Correlation Function

The cross-correlation $C_l(\tau)$ between $m(t)$ and $m(dt+l)$ is given as

$$\begin{aligned}C_l(\tau)&=\sum_{t=0}^{p^n-2}\omega^{m(t+\tau)-m(dt+l)}\\&=\sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt+l})}\\&=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(ax-bx^d)},\end{aligned}\tag{3}$$

where $a=\alpha^\tau$ and $b=\alpha^l$.

Let $C(a,b)$ be the function defined by

$$C(a,b)=\sum_{x\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ax-bx^d)}.\tag{4}$$

Then, the cross-correlation $C_l(\tau)$ can be expressed as $C_l(\tau)=C(a,b)-1$. Exactly the half of the elements in $F_{p^n}^*$ are squares and the other half are nonsquares. Using $\gcd(p^{m+1}+1,p^m-1)=\gcd(p^{m+1}+1,p^m+1)=2$ and $p^{m+1}+1\equiv 2 \bmod 4$, we have $\gcd(p^{m+1}+1,p^n-1)=2$. Thus, we can represent the squares as $x=y^{p^{m+1}+1}$ and nonsquares as $x=ry^{p^{m+1}+1}$, where $y\in F_{p^n}^*$ and r is a nonsquare in $F_{p^n}^*$. Also, note that as y runs through $F_{p^n}^*$, each $x\in F_{p^n}^*$, either a square or a nonsquare appears twice. Hence, we can express $C(a,b)$ as

$$\begin{aligned}2C(a,b)=&\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^{p^{m+1}+1}-by^{d(p^{m+1}+1)})}\\&+\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ary^{p^{m+1}+1}-br^dy^{d(p^{m+1}+1)})}.\end{aligned}\tag{5}$$

Since $\frac{p^m+1+2p+1}{(p+1)}$ is an even integer, we have

$$\begin{aligned}d(p^{m+1}+1)&=\frac{(p^m+1)^2}{2(p+1)}(p^{m+1}+1)\\&=(p^{2m}-1)\frac{(p^{m+1}+2p+1)}{2(p+1)}+p^m+1.\end{aligned}$$

Thus, we have $d(p^{m+1}+1)\equiv p^m+1 \bmod p^n-1$. Hence, (5) can be rewritten as

$$\begin{aligned}2C(a,b)=&\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^{p^m+1}+1-by^{p^m+1})}\\&+\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ary^{p^m+1}+1-br^dy^{p^m+1})}.\end{aligned}\tag{6}$$

Let

$$\begin{aligned}g(y)&=\mathrm{tr}_1^n(ay^{p^m+1}+1-by^{p^m+1})\\h(y)&=\mathrm{tr}_1^n(ary^{p^m+1}+1-br^dy^{p^m+1}).\end{aligned}\tag{7}$$

If y is expressed in terms of a basis $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of F_{p^n} over F_p as $y=\sum_{i=1}^n y_i\alpha_i$, where $y_i\in F_p$, then $g(y)$ can be easily represented as the quadratic form over F_p, $g(y)=\sum_{j=1}^n(y_iy_j)g_{ij}$, where $g_{ij}=\mathrm{tr}_1^n\Big(a(\alpha_i^{p^{m+1}}\alpha_j)-b(\alpha_i^{p^m}\alpha_j)\Big)$. Note that $h(y)$ is nothing but $g(y)$ when a and b in $g(y)$ are replaced by ar and br^d, respectively. Thus, $h(y)$ is also a quadratic form with the coefficients $h_{ij}=\mathrm{tr}_1^n\Big(ar(\alpha_i^{p^{m+1}}\alpha_j)-br^d(\alpha_i^{p^m}\alpha_j)\Big)$.

From Lemma 2, Corollary 3, and Lemma 4, in order to evaluate the exponential sum $C(a,b)$, we have to find the rank of the quadratic forms $g(y)$ and $h(y)$, i.e., the number of solutions $z\in F_{p^n}$ of the equations $g(y+z)=g(y)$ and $h(y+z)=h(y)$ satisfying for all $y\in F_{p^n}$.

Lemma 6: The number of solutions $z\in F_{p^n}$, such that $g(y+z)=g(y)$ for all $y\in F_{p^n}$, equals the number of solutions $z\in F_{p^n}$ satisfying

$$L_g(z)=a^{p^{m+1}}z^{p^2}-(b^p+b^{p^{m+1}})z^p+az=0\tag{8}$$

and the number of solutions $z\in F_{p^n}$, such that $h(y+z)=h(y)$ for all $y\in F_{p^n}$, equals the number of solutions $z\in F_{p^n}$ satisfying

$$L_h(z)=(ar)^{p^{m+1}}z^{p^2}-((br^d)^p+(br^d)^{p^{m+1}})z^p+arz=0,\tag{9}$$

where r is a nonsquare in F_{p^n}.

Proof: The equation $g(y+z)=g(y)$ can be written as

$$\mathrm{tr}_1^n\big(a(y+z)^{p^{m+1}+1}-b(y+z)^{p^m+1}\big)=\mathrm{tr}_1^n(ay^{p^{m+1}+1}-by^{p^m+1}).\tag{10}$$

Then, (10) can be rewritten as

$$\begin{aligned}\mathrm{tr}_1^n\Big(y^{p^{m+1}}\big\{a^{p^{m+1}}z^{p^2}-(b^p+b^{p^{m+1}})z^p+az\big\}\\+az^{p^{m+1}+1}-bz^{p^m+1}\Big)=0.\end{aligned}\tag{11}$$

Hence, (11) holds for all $y\in F_{p^n}$ if and only if

$$\mathrm{tr}_1^n(az^{p^{m+1}+1}-bz^{p^m+1})=0\tag{12}$$

and (8) are satisfied simultaneously.

Next, we will show that all solutions $z \in F_{p^n}$ satisfying (8) also satisfy (12). From (8), we have

$$(b^p + b^{p^{m+1}})z^p = a^{p^{m+1}} z^{p^2} + az$$

and raising to the p^{i-1} power gives

$$(b^{p^i} + b^{p^{m+i}})z^{p^i} = a^{p^{m+i}} z^{p^{i+1}} + a^{p^{i-1}} z^{p^{i-1}}. \tag{13}$$

Using (13), (12) can be rewritten as

$$\begin{aligned}
&\mathrm{tr}_1^n(az^{p^{m+1}+1} - bz^{p^m+1}) \\
&= \sum_{i=1}^{n} a^{p^i}(z^{p^{m+i+1}+p^i}) - \frac{1}{2}\sum_{i=1}^{n}(b^{p^i} + b^{p^{m+i}})(z^{p^{m+i}+p^i}) \\
&= \sum_{i=1}^{n} a^{p^i}(z^{p^{m+i+1}+p^i}) \\
&\quad - \frac{1}{2}\sum_{i=1}^{n}(a^{p^{m+i}} z^{p^{i+1}+p^{m+i}} + a^{p^{i-1}} z^{p^{i-1}+p^{m+i}}) = 0
\end{aligned}$$

where $j = m + i$ and $k = i - 1$. Hence, we only need to calculate the number of solutions for (8) to determine the number of solutions for $g(y + z) = g(y)$. The case of $h(y)$ can be proved similarly. ∎

From Lemma 6, we have to find out the number of solutions $z \in F_{p^n}$ of (8) and (9) to find the rank of $g(y)$ and $h(y)$, respectively. Since the degrees of (8) and (9) are both p^2 and they are both linearized forms, the possible number of solutions for both equations is $1, p$, or p^2. Now, we will use the following lemma to show that at least one of the two equations, $L_g(z) = 0$ and $L_h(z) = 0$, has just one solution.

Lemma 7: When a is a nonsquare in F_{p^n}, the equation $L_g(z) = 0$ has $z = 0$ as its only solution in F_{p^n}.

Proof: Since it is trivial that $z = 0$ is a solution, we have to show that

$$a^{p^{m+1}} z^{p^2-1} - (b^p + b^{p^{m+1}})z^{p-1} + a = 0 \tag{14}$$

has no solution in $F_{p^n}^*$, when a is a nonsquare in $F_{p^n}^*$.

The previous equation can be rewritten as

$$a^{p^{m+1}} z^{p^2-p} + az^{1-p} = b^p + b^{p^{m+1}}. \tag{15}$$

The right-hand side of (15) is expressed as $\mathrm{tr}_m^n(b^p)$, which is an element in F_{p^m}. Thus, in order to prove the lemma, we should show

$$\left\{ z \in F_{p^n}^* \,\middle|\, a^{p^{m+1}} z^{p^2-p} + az^{1-p} \in F_{p^m} \right\} = \phi \tag{16}$$

where a is a nonsquare in F_{p^n}.

Suppose that there exists $z \in F_{p^n}^*$, such that

$$a^{p^{m+1}} z^{p^2-p} + az^{1-p} \in F_{p^m}.$$

Then, we have

$$\left(a^{p^m+1}\right)^p \left(\frac{z^{p-1}}{a}\right)^p + \left(\frac{a}{z^{p-1}}\right) \in F_{p^m}. \tag{17}$$

Let $\xi = a^{p^m+1}$ and $\eta = \frac{z^{p-1}}{a}$. Then, (17) can be rewritten as

$$(\xi\eta)^p + \frac{1}{\eta} \in F_{p^m}.$$

Hence, we have

$$\left((\xi\eta)^p + \frac{1}{\eta}\right)^{p^m} - \left((\xi\eta)^p + \frac{1}{\eta}\right) = 0. \tag{18}$$

Since ξ is an element in F_{p^m}, (18) can be rewritten as

$$(\xi\eta)^p \left(\eta^{p^m-1} - 1\right)^p = \frac{\eta^{p^m-1} - 1}{\eta^{p^m}}. \tag{19}$$

Since η is a nonsquare in F_{p^n}, η is not in F_{p^m}. Thus, we have $\eta^{p^m-1} - 1 \neq 0$ and (19) can be rewritten as

$$(\xi\eta)^p \left(\eta^{p^m-1} - 1\right)^{p-1} = \frac{1}{\eta^{p^m}}. \tag{20}$$

From (20), we have

$$\xi^p \eta^{p^m+1} = \left(\frac{1}{\eta^{p^m} - \eta}\right)^{p-1}. \tag{21}$$

Now, we are ready to show that there are no such ξ and η satisfying the previous equation. Since $\xi^p \eta^{p^m+1} = \left(a^{p^m+1}\right)^{p-1} \left(z^{p^m+1}\right)^{p-1}$, (21) implies that

$$\left((az)^{p^m+1}(\eta^{p^m} - \eta)\right)^{p-1} = 1.$$

In other words, (21) implies that $(az)^{p^m+1}(\eta^{p^m} - \eta)$ is in F_p^*. But, this is not true since $(\eta^{p^m} - \eta)$ is not in $F_{p^m}^*$, while $(az)^{p^m+1}$ is in $F_{p^m}^*$. Hence, (18) does not hold and the proof is completed. ∎

Clearly, either a or ar is a nonsquare. Thus, at least one of the two, i.e., (8) and (9), has a single solution. Also, we can show that $L_h(z) = 0$ always has a single solution if $b = 1$.

Lemma 8: When $l = 0$, i.e., $b = 1$,

$$L_h(z) = (ar)^{p^{m+1}} z^{p^2} - (r^{dp} + r^{dp^{m+1}})z^p + arz = 0 \tag{22}$$

has $z = 0$ as its only solution in F_{p^n}, where r is a nonsquare in F_{p^n}.

Proof: Since we have

$$dp(p^m - 1) = \frac{(p^m+1)^2}{2(p+1)} p(p^m - 1) = \frac{p^n - 1}{2}\frac{p^m + 1}{p+1} p$$

and $\frac{p^m+1}{p+1}$ is an odd integer, any nonsquare r satisfies

$$r^{dp} + r^{dp^{m+1}} = r^{dp}(1 + r^{dp(p^m-1)}) = 0.$$

From $r^{dp} + r^{dp^{m+1}} = 0$, (22) can be rewritten as

$$arz\left((ar)^{p^{m+1}-1} z^{p^2-1} + 1\right) = 0.$$

Since $p^2 - 1 | p^{m+1} - 1$, $(ar)^{p^{m+1}-1} z^{p^2-1} = u^{p^2-1}$ for some $u \in F_{p^n}$. But there is no such u in F_{p^n} satisfying $u^{p^2-1} = -1$, since $p^2 - 1$ does not divide any odd multiples of $\frac{p^n-1}{2}$. ∎

The discussion on the ranks of $g(y)$ and $h(y)$ so far can be summarized as follows.

Corollary 9: The possible ranks of $g(y)$ and $h(y)$ are as follows.

Case 1. $a=\alpha^{\tau}$ is a square in $F_{p^n}^*$ or $b=\alpha^l=1$.

$$(r_g,r_h)=\begin{cases}(n,n), & \text{if } L_g(z)=0 \text{ has one solution},\\ (n-1,n), & \text{if } L_g(z)=0 \text{ has } p \text{ solutions},\\ (n-2,n), & \text{if } L_g(z)=0 \text{ has } p^2 \text{ solutions}.\end{cases}$$

Case 2. $a=\alpha^{\tau}$ is a nonsquare in $F_{p^n}^*$ and $b=\alpha^l\neq 1$.

$$(r_g,r_h)=\begin{cases}(n,n), & \text{if } L_h(z)=0 \text{ has one solution},\\ (n,n-1), & \text{if } L_h(z)=0 \text{ has } p \text{ solutions},\\ (n,n-2), & \text{if } L_h(z)=0 \text{ has } p^2 \text{ solutions},\end{cases}$$

where r_g and r_h denote the ranks of g and h, respectively, and $z\in F_{p^n}$. ■

IV. Upper Bound on Cross-Correlation Magnitudes

In this section, the upper bound on the magnitude of the cross-correlation function $C_l(\tau)$ of p-ary m-sequence $m(t)$ and its decimated sequences $m(dt+l)$ in (3) will be derived.

Theorem 10: Let $n=2m$, p be an odd prime, and $d=\frac{(p^m+1)^2}{2(p+1)}$, where m is an odd integer. Then, the magnitude of $C_l(\tau)$ in (3) is upper bounded by

$$|C_l(\tau)|\le \frac{p+1}{2}p^{\frac{n}{2}}+1.$$

Proof: Using $g(y)$ and $h(y)$ in (7), (6) can be rewritten as

$$2C(a,b)=\sum_{y\in F_{p^n}}\omega^{g(y)}+\sum_{y\in F_{p^n}}\omega^{h(y)}.$$

Recall that both $g(y)=\mathrm{tr}_1^n(ay^{p^{m+1}+1}-by^{p^m+1})$ and $h(y)=\mathrm{tr}_1^n(ary^{p^{m+1}+1}-br^dy^{p^m+1})$ are the quadratic forms and r is a nonsquare in F_{p^n}. Let ϵ_g and ϵ_h be the values defined in Lemma 4 corresponding to the quadratic forms of $g(y)$ and $h(y)$, respectively.

Due to Corollary 9, the following three cases should be considered to determine the value of $C(a,b)$.

Case 1. Rank of $g(y)=n$ and rank of $h(y)=n$.
From Corollary 5, we have

$$\begin{aligned}2C(a,b)&=\sum_{y\in F_{p^n}}\omega^{g(y)}+\sum_{y\in F_{p^n}}\omega^{h(y)}\\&=p^{\frac{n}{2}}(\epsilon_g+\epsilon_h).\end{aligned}\tag{23}$$

Thus, we obtain $|C_l(\tau)|=|-1+C(a,b)|\le p^{\frac{n}{2}}+1$.

Case 2. Rank of $g(y)=n$ and rank of $h(y)=n-1$ (or rank of $g(y)=n-1$ and rank of $h(y)=n$).
From Corollary 5, we have

$$\begin{aligned}2C(a,b)&=\sum_{y\in F_{p^n}}\omega^{g(y)}+\sum_{y\in F_{p^n}}\omega^{h(y)}\\&=\begin{cases}p^{\frac{n}{2}}\epsilon_g+p^{\frac{n}{2}}\epsilon_h\sqrt{p}, & \text{if } p\equiv 1 \bmod 4,\\ p^{\frac{n}{2}}\epsilon_g+jp^{\frac{n}{2}}\epsilon_h\sqrt{p}, & \text{if } p\equiv 3 \bmod 4.\end{cases}\end{aligned}\tag{24}$$

In this case, when $p\equiv 1 \bmod 4$, we have $|C_l(\tau)|=|-1+C(a,b)|\le\frac{1+\sqrt{p}}{2}p^{\frac{n}{2}}+1$ and when $p\equiv 3 \bmod 4$, we have $|C_l(\tau)|=|-1+C(a,b)|\le\frac{\sqrt{1+p}}{2}p^{\frac{n}{2}}+1$.

Case 3. Rank of $g(y)=n$ and rank of $h(y)=n-2$ (or rank of $g(y)=n-2$ and rank of $h(y)=n$).
From Corollary 5, we have

$$\begin{aligned}2C(a,b)&=\sum_{y\in F_{p^n}}\omega^{g(y)}+\sum_{y\in F_{p^n}}\omega^{h(y)}\\&=p^{\frac{n}{2}}\epsilon_g+p^{\frac{n}{2}+1}\epsilon_h.\end{aligned}\tag{25}$$

We also have $|C_l(\tau)|=|-1+C(a,b)|\le\frac{p+1}{2}p^{\frac{n}{2}}+1$. Hence, the magnitude of $C_l(\tau)$ is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$. ■

From Theorem 10, (23), (24), and (25), the possible values of the cross-correlation function are given as follows.

1) For $p=3$,

$$\Big\{-1,-1\pm p^{n/2},\ -1\pm\frac{1+\sqrt{p}i}{2}p^{n/2},\ -1\pm\frac{1-\sqrt{p}i}{2}p^{n/2},-1\pm\frac{1+p}{2}p^{n/2}\Big\}.$$

2) For $p\equiv 3 \bmod 4$ $(\neq 3)$,

$$\Big\{-1,-1\pm p^{n/2},-1\pm\frac{1+\sqrt{p}i}{2}p^{n/2},-1\pm\frac{1-\sqrt{p}i}{2}p^{n/2},\ -1\pm\frac{1+p}{2}p^{n/2},-1\pm\frac{1-p}{2}p^{n/2}\Big\}.$$

3) For $p\equiv 1 \bmod 4$,

$$\Big\{-1,-1\pm p^{n/2},-1\pm\frac{1+\sqrt{p}}{2}p^{n/2},-1\pm\frac{1-\sqrt{p}}{2}p^{n/2},\ -1\pm\frac{1+p}{2}p^{n/2},-1\pm\frac{1-p}{2}p^{n/2}\Big\}.$$

In each case, there are two pairs of the correlation values occurring the same number of times. Taking this fact into account, deriving the exact distribution of cross-correlation values, i.e., the number of occurrences of each correlation value requires seven independent equations for $p=3$ and nine equations otherwise, which does not seem to be an easy task. We leave this as a future work.

V. Construction of a New Family

In this section, we construct a family of p-ary sequences of period p^n-1 with low correlation using a p-ary m-sequence $m(t)$ and its $\frac{p^m+1}{2}$ distinct decimated sequences $m(dt+l)$ defined in (1). An immediate candidate for the family is a Gold-like sequence family.

Let $\mathcal{F}'$ be the sequence family defined by

$$\mathcal{F}'=\{s_\beta(t)\,|\,\beta\in F_{p^n},\ 0\le t<p^n-1\}$$

TABLE II
COMPARISON WITH GOLD-LIKE SEQUENCE FAMILIES

Family	Alphabet	Period N	Family Size	$\lvert C_{\max}\rvert$
Gold (n odd) [9]	2	2^n-1	$N+2$	$\sqrt{2(N+1)}+1$
Gold (n even) [9]	2	2^n-1	$N+2$	$2\sqrt{N+1}+1$
No *et al.*[10]	2	2^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Trachtenberg [1]	odd p	p^n-1	$N+1$	$\sqrt{p(N+1)}+1$
Kumar *et al.*[6]	odd p	p^n-1	$N+1$	$\sqrt{N+1}+1$
Helleseth [2]	odd p	p^n-1	$N+1$	$2\sqrt{N+1}+1$
Olsen *et al.*[11]	p	p^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Seo *et al.* [13]	odd p	p^n-1	$N+1$	$p\sqrt{N+1}+1$
Jang *et al.* [14]	odd p	p^n-1	$N+1$	$\sqrt{N+1}+1$
New Family	odd p	p^n-1	$\sqrt{N+1}$	$\frac{p+1}{2}\sqrt{N+1}+1$

* p is a prime number.

* p is a prime number.

where $s_\beta(t)=\mathrm{tr}_1^n(\alpha^t+\beta\alpha^{dt})$. For two sequences $s_{\beta_1}(t)$ and $s_{\beta_2}(t)$ in the family $\mathcal{F}'$, the correlation function between the two sequences is expressed as

$$\begin{aligned}C(\tau)&=\sum_{t=0}^{p^n-2}\omega^{s_{\beta_1}(t+\tau)-s_{\beta_2}(t)}\\&=\sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}+\beta_1\alpha^{d(t+\tau)})-\mathrm{tr}_1^n(\alpha^t+\beta_2\alpha^{dt})}\\&=\sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^n(\alpha^t(\alpha^\tau-1)+\alpha^{dt}(\beta_1\alpha^{d\tau}-\beta_2))}.\end{aligned}\tag{26}$$

From (26) and Theorem 10, it can be easily checked that except for $\tau=0$ and $\beta_1\neq\beta_2$, the correlation function is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$. Now, let us check the case when $\tau=0$ and $\beta_1\neq\beta_2$. For the case when $\tau=0$ and $\beta_1\neq\beta_2$, $C(\tau)$ in (26) can be rewritten as

$$C(0)=\sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^n(\alpha^{dt}(\beta_1-\beta_2))}.$$

The evaluation of $C(0)$ requires the following lemma.

Lemma 11 ([2]): Let p be an odd prime, $D|(p^n-1)$, and suppose $D|(p^r+1)$ for some integer r. Suppose that e is the least integer such that $D|(p^e+1)$.

1) For an even D, an odd $\frac{p^e+1}{D}$, and an odd $\frac{D}{2e}$,

$$\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^D)}=\begin{cases}p^n, & \text{if } a=0,\\(-1)^{\frac{n}{2e}+1}(D-1)p^{\frac{n}{2}}, & \text{if } a\in C_{\frac{D}{2}},\\(-1)^{\frac{n}{2e}}p^{\frac{n}{2}}, & \text{if } a\notin C_{\frac{D}{2}}.\end{cases}$$

2) For all other cases,

$$\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^D)}=\begin{cases}p^n, & \text{if } a=0,\\(-1)^{\frac{n}{2e}+1}(D-1)p^{\frac{n}{2}}, & \text{if } a\in C_0,\\(-1)^{\frac{n}{2e}}p^{\frac{n}{2}}, & \text{if } a\notin C_0,\end{cases}$$

where $C_j=\{\alpha^{Di+j}\in F_{p^n}^*|0\le i<\frac{p^n-1}{D},\ 0\le j<D\}$. ■

Now, let us apply Lemma 11 to our case. Since $\gcd(d,p^n-1)=\frac{(p^m+1)}{2}$, set $D=\frac{(p^m+1)}{2}$. Then, $e=m$ and $(p^e+1)/D=2$.

Define the set K as

$$K=\{\alpha^{Di}\mid 0\le i<2(p^m-1)\}.$$

Then, for two sequences $s_{\beta_1}(t)$ and $s_{\beta_2}(t)$ in the family $\mathcal{F}'$, such that $\beta_1-\beta_2\in K$, we have

$$\begin{aligned}C(0)&=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n((\beta_1-\beta_2)x^d)}=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(\alpha^{Di}x^d)}\\&=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(\alpha^{Di}x^D)}=\sum_{x\in F_{p^n}^*}\omega^{\mathrm{tr}_1^n(x^D)}=\frac{p^n-p^{\frac{n}{2}}}{2}-1\end{aligned}$$

which far exceeds $\frac{p+1}{2}p^{\frac{n}{2}}+1$.

Hence, in order to obtain the sequence family with the maximum correlation magnitude of $\frac{p+1}{2}p^{\frac{n}{2}}+1$, we have to devise a method of excluding the sequences $s_{\beta_1}(t)$ and $s_{\beta_2}(t)$ in $\mathcal{F}'$ satisfying $\beta_1-\beta_2\in K$ from F_{p^n}.

Note that K can be partitioned into $F_{p^m}^*$ and $K_2=K\backslash F_{p^m}^*$ for even i and odd i, respectively. Let $K_2\cup\{0\}=\{\zeta_0,\zeta_1,\zeta_2,\ldots,\zeta_{p^m-1}\}$ and $F_{p^m}=\{\gamma_0,\gamma_1,\gamma_2,\ldots,\gamma_{p^m-1}\}$, where $\zeta_0=\gamma_0=0$.

The set $K_2\cup\{0\}$ has an interesting property stated in the following lemmas.

Lemma 12: Let p be an odd prime. $K_2\cup\{0\}$ is closed under addition.

Proof: Let $\alpha^{D(2i_1+1)}$ and $\alpha^{D(2i_2+1)}\in K_2\cup\{0\}$ for integers i_1 and i_2. Then, we have

$$\alpha^{D(2i_1+1)}+\alpha^{D(2i_2+1)}=\alpha^D(\alpha^{D(2i_1)}+\alpha^{D(2i_2)}).$$

Since $\alpha^{D(2i_1)},\alpha^{D(2i_2)}\in F_{p^m}^*$, $\alpha^{D(2i_1)}+\alpha^{D(2i_2)}\in F_{p^m}$ and $\alpha^{D(2i_1+1)}+\alpha^{D(2i_2+1)}\in K_2\cup\{0\}$. ■

Lemma 13: Let p be an odd prime. $\{x+y\mid x\in K_2\cup\{0\}\text{ and }y\in F_{p^m}\}=F_{p^n}$.

Proof: Since $|K_2\cup\{0\}|=p^m$ and $|F_{p^m}|=p^m$, it is enough to show that all the elements $x+y, x\in K_2\cup\{0\}$ and $y\in F_{p^m}$, are distinct. Suppose that $x_1+y_1=x_2+y_2$, where $x_i\in K_2\cup\{0\}$ and $y_i\in F_{p^m}$. Then, $x_1-x_2=y_2-y_1$ and Lemma 12 implies that $x_1-x_2=y_2-y_1=0$, i.e., $x_1=x_2$ and $y_1=y_2$. ■

By finding a proper set $\mathcal{Z}=\{b_0,b_1,\ldots\}\subseteq F_{p^n}$, such that $b_i-b_j\notin K, i\neq j$, we can construct a sequence family $\mathcal{F}$ with

the maximum magnitude $\frac{p+1}{2}p^{\frac{n}{2}}+1$ of cross-correlation values as in the following theorem.

Theorem 14: Let $d=\frac{(p^m+1)^2}{2(p+1)}$ and $n=2m$, where m is an odd integer. Let $K_2\cup\{0\}=\{\zeta_0,\zeta_1,\zeta_2,\ldots,\zeta_{p^m-1}\}$ and $F_{p^m}=\{\gamma_0,\gamma_1,\gamma_2,\ldots,\gamma_{p^m-1}\}$, where $\zeta_0=\gamma_0=0$. Let $\mathcal{Z}=\{\zeta_i+\gamma_i \mid 0\le i\le p^m-1\}$. Let $\mathcal{F}$ be the sequence family defined by

$$\mathcal{F}=\{s_b(t)=\mathrm{tr}_1^n(\alpha^t+b\alpha^{dt}) \mid b\in\mathcal{Z}, 0\le t<p^n-1\}.$$

Then, the magnitude of correlation values of two sequences in $\mathcal{F}$ is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$ and its family size is $p^{\frac{n}{2}}$.

Proof: It is enough to show that for $i\neq j, \zeta_i+\gamma_i-(\zeta_j+\gamma_j)\notin K$:

$$\zeta_i+\gamma_i-(\zeta_j+\gamma_j)=(\zeta_i-\zeta_j)+(\gamma_i-\gamma_j)=\zeta+\gamma$$

where $\zeta\in K_2$ and $\gamma\in F_{p^m}^*$. Therefore, from Lemmas 12 and 13, we can easily see that $\zeta+\gamma\notin K_2$ and $\zeta+\gamma\notin F_{p^m}$, and thus, $\zeta+\gamma\notin K$. ■

Some known sequence families with low correlation are listed in Table II.

VI. Conclusion

In this paper, we have derived the upper bound on the magnitudes on cross-correlation values of a p-ary m-sequence $m(t)$ and its decimation sequences $m(dt+l)$ for $d=(p^m+1)^2/(2(p+1))$. The upper bound is equal to $\frac{p+1}{2}p^{\frac{n}{2}}+1$. We have also constructed the sequence family $\mathcal{F}$ by using the same decimation value, where the family size is p^m and the magnitude of correlation values is upper bounded by $\frac{p+1}{2}p^{\frac{n}{2}}+1$.

Acknowledgment

The authors would like to thank the associate editor and the anonymous reviewers for their valuable comments and suggestions that greatly improved the quality of this paper.

References

[1] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," Ph.D. dissertation, Univ. 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, T. Helleseth, P. V. Kumar, and H. Martinsen, "Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1473–1481, May 2001.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Z. Hu, X. Li, D. Mills, E. Muller, W. Sun, W. Williems, Y. Yang, and Z. Zhang, "On the cross-correlation of sequences with the decimation factor $d=\frac{p^n+1}{p+1}-\frac{p^n-1}{2}$," *Applicable Algebra Eng. Commun. Comput.*, vol. 12, pp. 255–263, 2001.

[9] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154–156, Jan. 1968.

[10] J.-S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 371–379, Mar. 1989.

[11] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 858–864, Nov. 1982.

[12] 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, pp. 3140–3149, Jul. 2008.

[13] E.-Y. Seo, Y.-S. Kim, J.-S. No, and D.-J. Shin, "Cross-correlation distribution of p-ary m-sequence and its $p+1$ decimated sequences with shorter period," *IEICE Trans. Fund. Electron., Commun. Comput. Sci.*, vol. E90-A, no. 11, pp. 2568–2574, Nov. 2007.

[14] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, "New family of p-ary sequences with optimal correlation property and large linear span," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1839–1844, Aug. 2004.

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

[16] S. T. Choi, T. Lim, J. S. No, and H. Chung, "On the cross-correlation of a ternary m-sequence of period $3^{4k+2}-1$ and its decimated sequences by $\frac{(3^{2k+1}+1)^2}{8}$," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010, pp. 1268–1271.

[17] Y. S. Kim, J. S. Chung, J. S. No, and D. J. Shin, "New families of p-ary sequences with good correlation and large linear complexity," *IEEE Trans. Inf. Theory.*, submitted for publication.

Sung-Tai Choi received the B.S. degree in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 2006, where he is currently working toward the Ph.D. degree in electrical engineering and computer science.

His area of research interests includes pseudorandom sequences, wireless communication, error-correcting codes, and cyptography.

Taehyung Lim received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 2004 and 2006, respectively, and is currently pursuing the Ph.D. degree in electrical and computer engineering, University of California, San Diego.

His research interests include pseudorandom sequences, error correcting codes, and communication theory.

Jong-Seon No (S'80–M'88–SM'10–F'12) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988.

He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the Department of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently a Professor. His research interests include error-correcting codes, sequences, cryptography, space-time codes, LDPC codes, and wireless communication systems.

Habong Chung (S'86–M'89) received the B.S. degree from Seoul National University, Seoul, in 1981, and the M.S. and the Ph.D. degrees from the University of Southern California, Los Angeles, in 1985 and 1988, respectively.

From 1988 to 1991, he was an Assistant Professor in the Department of Electrical and Computer Engineering, the State University of New York at Buffalo. Since 1991, he has been with the School of Electronic and Electrical Engineering, Hongik University, Seoul, where he is a Professor. His research interests include coding theory, combinatorics, and sequence design.