A New Family of p-ary Decimated Sequences with Low Correlation

Ji-Youp Kim, Sung-Tai Choi, and Jong-Seon No
Department of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea
{lakroforce, stchoi}@ccl.snu.ac.kr, jsno@snu.ac.kr

Habong Chung
Department of Electronic and Electrical Engineering
Hongik University
Seoul 121-791, Korea
habchung@hongik.ac.kr

***Abstract*—In this paper, we propose a method to construct p-ary sequence family $\mathcal{S}$ which has the period of $N = (p^n - 1)/2$ when p is an odd prime and n is an odd integer. The family has the size of $2(p^n - 1)$ and the magnitudes of correlation values between any two sequences from the family are upper bounded by $2\sqrt{N + \frac{1}{2}}$. The bound can be derived from the well-known Kloosterman sum.**

***Index Terms*—p-ary m-sequence, cross-correlation, sequence family**

I. Introduction

In the wireless communication systems employing code-division multiple-access (CDMA) scheme, a signature sequence is assigned to each user, which makes it possible to distinguish each signal from those of the other users. In design of sequences for CDMA systems, the two most important properties for the family of the sequences to have are low periodic correlation between all pairs of distinct sequences and large family size.

For the sequences of period $p^n - 1$, there have been lots of researches to construct families which have good correlation properties and large size. Kumar and Moreno [1], Liu and Komo [2] proposed p–ary sequence families with the magnitudes of correlation values less than $p^{n/2} + 1$. Also studies on the cross-correlation distribution of p-ary sequences are given in [4], [5], and [6].

In this paper, for an odd prime p and odd integer n, a new family $\mathcal{S}$ of p-ary sequence of the period of $N = (p^n - 1)/2$ is constructed. The magnitudes of correlation values of sequences from the family are upper bounded by $2\sqrt{N + \frac{1}{2}}$ and the size of the family is $2(p^n - 1)$.

II. Preliminaries

Let p be an odd prime with $p = 3 \bmod 4$ and n be an odd integer. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. The trace function $\mathrm{tr}_m^n(\cdot)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is defined as

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

where $x \in \mathbb{F}_{p^n}$ and $m|n$. Let α be a primitive element of $\mathbb{F}_{p^n}$.

Then a p-ary m-sequence $s(t)$ of period $p^n - 1$ can be expressed with the trace function as

$$s(t) = \mathrm{tr}_1^n(\alpha^t). \tag{1}$$

In this paper, the following notations are used:

- p is an odd prime ($3 \bmod 4$);
- n is an odd integer;
- $q = p^n$;
- $N = \frac{p^n-1}{2}$;
- $d = N - p^{n-1}$;
- α is a primitive element of $\mathbb{F}_{p^n}$;
- ω is a primitive p-th root of unity;
- QR is the set of nonzero squares in $\mathbb{F}_{p^n}$;
- QNR is the set of nonsquares in $\mathbb{F}_{p^n}$.

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

$$R(\tau) = \sum_{t=0}^{N-1} \omega^{a(t+\tau)-b(t)}.$$

III. Definition of Sequence Family

Let $s(t)$ be an m-sequence of period $p^n - 1$ defined in (1). Since $p^n - 1$ is even, the decimated sequence $s(2t)$ has the period $N = (p^n - 1)/2$. We consider the sequence $s(2t)$ and its decimated sequence $s(2dt)$. Note that the period of the sequence $s(2dt)$ is also N, because gcd(N, d) = 1. Then the family S of the sequences of period N is defined as

$$S = \cup_{i=1}^{4} S_i$$

where

$$\begin{aligned}
S_1 &= \{s(2t) + s(2d(t+i)) | 0 \le i < N\} \\
S_2 &= \{s(2t+1) + s(2d(t+i)) | 0 \le i < N\} \\
S_3 &= \{s(2t) + s(2d(t+i)+1) | 0 \le i < N\} \\
S_4 &= \{s(2t+1) + s(2d(t+i)+1) | 0 \le i < N\}.
\end{aligned}$$

In the following section, we will show that the magnitude of cross-correlation and nontrivial autocorrelation values of the p-ary sequences in S are upper bounded by $2\sqrt{N + \frac{1}{2}}$, which is roughly twice of the square root of the period.

IV. Cross-Correlation Bound

First we consider the cross-correlation of sequences in S_1. The cases for the others can be similarly proved. The cross-correlation function between two sequences in S_1 is defined as

$$R_{ij}(\tau) = \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)})+\mathrm{tr}_1^n(\alpha^{2d(t+\tau+i)})-\mathrm{tr}_1^n(\alpha^{2t})-\mathrm{tr}_1^n(\alpha^{2d(t+j)})}$$
$$= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2t}(\alpha^{2\tau}-1))+\mathrm{tr}_1^n(\alpha^{2dt}(\alpha^{2d(\tau+i)}-\alpha^{2dj}))}. \quad (2)$$

Let $a = \alpha^{2\tau}-1, b' = \alpha^{2d(\tau+i)}-\alpha^{2dj}$. Then (2) can be written as

$$R_{ij}(\tau) = \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a\alpha^{2t}+b'\alpha^{2dt})}.$$

Here, note that

$$\begin{aligned} 2dt &= 2(N-p^{n-1})t \\ &= 2(\frac{p^n-1}{2}-p^{n-1})t \\ &= (p^n-1-2p^{n-1})t \\ &= -2p^{n-1}t \\ &= -2p^{-1}t \pmod{p^n-1}. \end{aligned}$$

Then, we have

$$\begin{aligned} \mathrm{tr}_1^n(\alpha^{2dt}b') &= \mathrm{tr}_1^n(\alpha^{-2p^{-1}t}b') \\ &= \mathrm{tr}_1^n((\alpha^{-2p^{-1}t}b')^p) \\ &= \mathrm{tr}_1^n(\alpha^{-2t}b'^p). \end{aligned}$$

Let $b'^p = b$. Then

$$\begin{aligned} R_{ij}(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a\alpha^{2t}+b\alpha^{-2t})} \\ &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a(\alpha^t)^2+b(\alpha^t)^{-2})} \\ &= \sum_{y\in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}. \end{aligned} \quad (3)$$

The above sum is closey related to Kloosterman sum. The Kloosterman sum $K(\chi;a,b)$ is defined as

$$K(\chi;a,b) = \sum_{y\in\mathbb{F}_{p^n}^\times} \chi(ay+by^{-1})$$

where χ is an additive character of $\mathbb{F}_{p^n}$, $\mathbb{F}_{p^n}^\times = \mathbb{F}_{p^n}\backslash\{0\}$, and $a,b\in\mathbb{F}_{p^n}$. In this case, $\chi(x) = \omega^{\mathrm{tr}_1^n(x)}$. Therefore, we have the following relation.

$$\begin{aligned} K(\chi;a,b) &= \sum_{y\in\mathbb{F}_{p^n}^\times} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} \\ &= \sum_{y\in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} + \sum_{y\in QNR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}. \end{aligned}$$

We can also define $L(\chi;a,b)$ as

$$L(\chi;a,b) = \sum_{y\in QR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})} - \sum_{y\in QNR} \omega^{\mathrm{tr}_1^n(ay+by^{-1})}.$$

Let η be the quadratic character defined as

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

Then using the quadratic character η, we have

$$L(\chi;a,b) = \sum_{y\in\mathbb{F}_{p^n}^\times} \eta(y)\omega^{\mathrm{tr}_1^n(ay+by^{-1})}.$$

$L(\chi;a,b)$ is a special type of the generalized Kloosterman sum. There are many results for the generalized Kloosterman sums. They can be found in [3] as Theorem 5.11, Exercise 5.83, Exercise 5.84, and Exercise 5.85, which are summarized as follows.

Lemma 1: [3] Let ψ be a multiplicative and χ an additive character of $\mathbb{F}_{p^n}$. Then the Gaussian sum $G(\psi,\chi)$ satisfies

$$G(\psi,\chi) = \begin{cases} p^n-1 & \text{for } \psi=\psi_0, \chi=\chi_0 \\ -1 & \text{for } \psi=\psi_0, \chi\neq\chi_0 \\ 0 & \text{for } \psi\neq\psi_0, \chi=\chi_0. \end{cases}$$

If $\psi\neq\psi_0$ and $\chi\neq\chi_0$, then

$$|G(\psi,\chi)| = \sqrt{p^n}$$

where ϕ_0 and χ_0 denote the trivial multiplicative character and the trivial additive character, respectively.

Lemma 2: [3] Let ψ be a multiplicative character and χ an additive character of $\mathbb{F}_{p^n}$. For $a,b\in\mathbb{F}_{p^n}$, a generalized Kloosterman sum is defined as

$$K(\psi,\chi,a,b) = \sum_{y\in\mathbb{F}_{p^n}^\times} \psi(y)\chi(ay+by^{-1}).$$

This sum reduces to a Gaussian sum if $ab=0$, in the sense that

$$K(\psi,\chi,a,b) = \begin{cases} \psi(b)G(\bar{\psi},\chi) & \text{if } a=0, b\neq 0 \\ \bar{\psi}(a)G(\psi,\chi) & \text{if } a\neq 0, b=0 \\ G(\psi,\chi_0) & \text{if } a=b=0. \end{cases}$$

Lemma 3: [3] Let η be the quadratic character of $\mathbb{F}_{p^n}$, p odd, and $a,b\in\mathbb{F}_{p^n}$ with $\eta(ab)=-1$. Then $K(\eta,\chi;a,b)=0$ for any additive character χ of $\mathbb{F}_{p^n}$.

Lemma 4: [3] Let η be the quadratic character of $\mathbb{F}_{p^n}$, p odd, and $a,b\in\mathbb{F}_{p^n}$ with $ab=d^2$ for some $d\in\mathbb{F}_{p^n}^\times$. Then we have

$$K(\eta,\chi;a,b) = \eta(b)G(\eta,\chi)(\chi(2d)+\chi(-2d))$$

for any additive character χ of $\mathbb{F}_{p^n}$.

Combining these results, we can obtain an upper bound for $L(\chi;a,b)$ as in the following lemma.

Lemma 5: The absolute value of the generalized Kloosterman sum $L(\chi; a, b)$ is bounded by $2\sqrt{p^n}$.

Proof: We consider the following 3 cases.

i) $a = 0$ or $b = 0$:

In this case, we can use Lemma 2. Since $|\eta(x)| \leq 1$ for any $x \in \mathbb{F}_{p^n}$, we have

$$\begin{aligned} |L(\chi; a, b)| &= |\sum_{y \in \mathbb{F}_{p^n}^\times} \eta(y)\omega^{tr_1^n(ay+by^{-1})}| \\ &= |K(\eta, \chi, a, b)| \\ &\leq \begin{cases} |G(\bar{\eta}, \chi)| & \text{if } a = 0, b \neq 0 \\ |G(\eta, \chi)| & \text{if } a \neq 0, b = 0 \\ |G(\eta, \chi_0)| & \text{if } a = 0, b = 0. \end{cases} \end{aligned}$$

Since η is not trivial, Lemma 1 indicates that

$$|L(\chi; a, b)| \leq \sqrt{p^n}.$$

ii) $a, b \in QR$ or $a, b \in QNR$:

Here $ab = d^2$ for some $d \in \mathbb{F}_{p^n}^\times$. Then Lemma 4 implies

$$\begin{aligned} |L(\chi; a, b)| &= |K(\eta, \chi, a, b)| \\ &= |\eta(b)G(\eta, \chi)(\chi(2d) + \chi(-2d))| \\ &\leq 2|G(\eta, \chi)| \\ &\leq 2\sqrt{p^n}. \end{aligned}$$

iii) $a \in QR, b \in QNR$ or $a \in QNR, b \in QR$:

We have $\eta(ab) = -1$. Then Lemma 3 implies

$$\begin{aligned} |L(\chi; a, b)| &= |K(\eta, \chi, a, b)| \\ &= 0 \\ &\leq \sqrt{p^n}. \end{aligned}$$

Therefore, for any $a, b \in \mathbb{F}_{p^n}$, we have

$$|L(\chi; a, b)| \leq 2\sqrt{p^n}.$$

□

Here note that since p is a $3 \bmod 4$ prime and n is an odd integer, -1 is a nonsquare. Therefore the partial sum of the Kloosterman sum over QR and QNR are complex conjugates of each other. That is,

$$\sum_{y \in QR} \omega^{-tr_1^n(ay+by^{-1})} = \sum_{y \in QNR} \omega^{tr_1^n(ay+by^{-1})}.$$

Now we are ready to show that the absolute value of cross-correlation $R_{ij}(\tau)$ is upper bounded by $2\sqrt{N + \frac{1}{2}} = 2\sqrt{\frac{p^n}{2}}$. By discussion above, we can say that

$$\sum_{y \in QR} \omega^{tr_1^n(ay+by^{-1})} = u + vi.$$

and

$$\sum_{y \in QNR} \omega^{tr_1^n(ay+by^{-1})} = u - vi.$$

By definition of the Kloosterman sum and $L(\chi; a, b)$, we obtain

$$K(\chi; a, b) = 2u \tag{4}$$

$$L(\chi; a, b) = 2vi. \tag{5}$$

A well-known upper bound for the Kloosterman sum can be found in [3], which is presented below.

Lemma 6: [3] If χ is a nontrivial additive character of $\mathbb{F}_{p^n}$ and $a, b \in \mathbb{F}_{p^n}$ are not both 0, then the Kloosterman sum $K(\chi; a, b)$ satisfies

$$|K(\chi; a, b)| \leq 2\sqrt{p^n}.$$

For cross-correlation and nontrivial autocorrelation, it can be easily shown that $a \neq 0$ or $b \neq 0$. If $a = 0$, then by definition of a, $\alpha^{2\tau} = 1$, which implies $\tau = N = 0 \pmod N$. Also note that

$$\begin{aligned} 2dp &= p(p^n - 1) - 2p^n \\ &= -2 \pmod{p^n - 1}. \end{aligned}$$

Therefore we have

$$\begin{aligned} b &= \alpha^{2d(\tau+i)p} - \alpha^{2djp} \\ &= \alpha^{-2(\tau+i)} - \alpha^{-2j} \\ &= \frac{\alpha^{-2i}}{a+1} - \alpha^{-2j}. \end{aligned}$$

Thus if $a = 0$, then $\tau = 0$ and $i = j$. This is the case when the correlation is an in-phase autocorrelation.

Therefore by Lemmas 5 and 6, we have

$$\begin{aligned} |u| &\leq \sqrt{p^n} \\ |v| &\leq \sqrt{p^n} \end{aligned}$$

from (4) and (5). Finally we obtain

$$\begin{aligned} |R_{ij}(\tau)| &= |\sum_{y \in QR} \omega^{tr(ay+by^{-1})}| \\ &= |u + vi| \\ &\leq \sqrt{2p^n} \\ &= 2\sqrt{N + \frac{1}{2}}. \end{aligned}$$

The proof for cross-correlations for all other cases is quite similar, since the cross-correlation expression eventually becomes the Kloosterman sum over the quadratic residue like (3). Thus we have the following theorem.

Theorem 7: The magnitudes of cross-correlations and nontrivial autocorrelations of sequences in S are upper bounded by $2\sqrt{N + \frac{1}{2}}$.

V. Size of Sequence Family

The family size of S is $2(p^n - 1)$, which is 4 times larger than the period. In the following theorem, we can show that any two sequences in S are cyclically inequivalent.

Theorem 8: The family size of S is $2(p^n - 1)$. More precisely, there are no cyclically equivalent sequences in S.

Proof: Suppose that there are two sequences $v(t)$ and $w(t)$ in S which are cyclically equivalent each other. Let $R(\tau)$ be a cross-correlation between $v(t)$ and $w(t)$. Then there exists τ_0 such that $0 \le \tau_0 < N$ and $R(\tau_0) = N$. Recall that any cross-correlation values of sequences in S can be written as a Kloosterman sum over the quadratic residues. Let

$$R(\tau_0) = \sum_{y \in QR} \omega^{tr_1^n(ay+by^{-1})} = u + vi$$
$$\sum_{y \in QNR} \omega^{tr_1^n(ay+by^{-1})} = u - vi.$$

Since $R(\tau_0) = N$, we have $v = 0$. Therefore $u = N$. Thus

$$K(\chi; a, b) = 2u = 2N \Longrightarrow K(\chi; a, b) = p^n - 1.$$

It is known that if $K(\chi; a, b) = p^n - 1$, then $a, b = 0$. Therefore it suffices to show that $a, b = 0$ implies $v(t) = w(t)$. It is already discussed that $a, b = 0$ implies $v(t) = w(t)$ when $v(t), w(t) \in S_1$. The proofs for the case of S_2, S_3, S_4 are similar. It is also easily verified that if $v(t) \in S_k$ and $w(t) \in S_l$ for $k \neq l$, then $a \neq 0$ or $b \neq 0$. For example, let $l = 1$, $k = 2$. Then

$$\begin{aligned}
&R_{ij}(\tau_0) \\
&= \sum_{t=0}^{N-1} \omega^{tr_1^n(\alpha^{2(t+\tau_0)}) + tr_1^n(\alpha^{2d(t+\tau_0+i)}) - tr_1^n(\alpha^{2t+1}) - tr_1^n(\alpha^{2d(t+j)})} \\
&= \sum_{t=0}^{N-1} \omega^{tr_1^n(\alpha^{2t}(\alpha^{2\tau_0}-\alpha)) + tr_1^n(\alpha^{2dt}(\alpha^{2d\tau_0+2di} - \alpha^{2dj}))} \\
&= \sum_{t=0}^{N-1} \omega^{tr_1^n(\alpha^{2t}(\alpha^{2\tau_0}-\alpha)) + tr_1^n(\alpha^{2dpt}(\alpha^{2dp\tau_0+2dpi} - \alpha^{2dpj}))} \\
&= \sum_{t=0}^{N-1} \omega^{tr_1^n(\alpha^{2t}(\alpha^{2\tau_0}-\alpha)) + tr_1^n(\alpha^{-2t}(\alpha^{-2\tau_0-2i} - \alpha^{-2j}))} \\
&= \sum_{y \in QR} \omega^{tr_1^n(ay+by^{-1})}
\end{aligned}$$

where $a = \alpha^{2\tau_0} - \alpha$ and $b = \alpha^{-2\tau_0-2i} - \alpha^{-2j}$. Since $\alpha^{2\tau_0} \in QR$ and $\alpha \in QNR$, we can conclude that $a \neq 0$. The proofs for the other cases are similar. □

VI. An Example

For $p = 3$, $n = 3$, we have $N = 13$ and $d = 4$. Let α be a primitive element of $\mathbb{F}_3$ with a minimal polynomial x^3+2x+1. Then the sequence family is given as:

$S_1 = \{(0020022220020), (1201121211021), (0012111121002), (1122010221111), (2221001222202), (0211211200110), (0110011012221), (2101012100001), (2011020011100), (1111102122120), (2112220202022), (2120101001010), (2202212021220)\}$

$S_2 = \{(0110220002100), (1021022020101), (0102012200112), (1212211000221), (2011202001012), (0001112012220), (0200212121001), (2221210212111), (2101221120210), (1201000201200), (2202121011102), (2210002110120), (2022110100000)\}$

$S_3 = \{(0200000101122), (0001200022011), (1010202201201), (1100221020102), (2000112212112), (1002021102210), (1021110000222), (1212002010012), (0121222111212), (2210120120211), (0102100210200), (2022201110121), (1220210112000)\}$

$S_4 = \{(0020201210202), (0121101101121), (1100100010011), (1220122102212), (2120010021222), (1122222211020), (1111011112002), (1002200122122), (0211120220022), (2000021202021), (0222001022010), (2112102222201), (1010111221110)\}$

In general, the number of correlation values or the correlation distribution is irregular. For instance, the cross-correlation distribution between $a(t) = (1201121211021)$ and $b(t) = (0102012200112)$ is given as:

$$R_{ab}(\tau) = \begin{cases}
-3.5 + 2.59808i & \text{once} \\
1 & 3 \text{ times} \\
4 & 2 \text{ times} \\
-3.5 - 2.59808i & \text{once} \\
-5 & \text{once} \\
4 + 5.19615i & \text{once} \\
-2 + 5.19615i & \text{once} \\
-2 - 5.19615i & \text{once} \\
-2 & \text{once} \\
-0.5 - 2.59808i & \text{once}
\end{cases}$$

But for $c(t) = (0001200022011)$ and $d(t) = (1100100010011)$, the cross-correlation is

$$R_{cd}(\tau) = \begin{cases}
-0.5 + -2.59808i & 2\text{times} \\
4 + 5.19615i & 2\text{times} \\
-0.5 + 2.59808i & 3\text{times} \\
2.5 + -2.59808i & 2\text{times} \\
-2 & 2\text{times} \\
1 & 2\text{times}.
\end{cases}$$

Note that the number of cross-correlation values and the correlation distribution are different.

Acknowledgement

This work was supported by the IT R&D program of MKE/KEIT[KI001809, Intelligent Wireless Communication Systems in 3 Dimensional Environment] and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0000867).

References

[1] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inf. Theory*, vol. 37, pp. 603-616, May 1991.

[2] S.C. Liu and J.F. Komo, "Nonbinary Kasami sequences over $GF(p)$," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1409-1412, Jul. 1992.
[3] R.Lidl and H.Niederreliter, *Finite Fields*. Amsterdam, The Netherlands: Addison-Wesley, 1983, vol.20, Encyclopedia of Mathematics and its Applications.
[4] E. N. Muller, "On the crosscorrelation of sequences over $GF(p)$ with short periods," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 289-295, Jan. 1999.
[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] 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.