A New Family of p-Ary Sequences of Period $(p^n - 1)/2$ With Low Correlation

Ji-Youp Kim, Sung-Tai Choi, Jong-Seon No, *Senior Member, IEEE*, and Habong Chung, *Member, IEEE*

***Abstract*—For an odd prime p congruent to 3 modulo 4 and an odd integer n, a new family of p-ary sequences of period $N = \frac{p^n-1}{2}$ with low correlation is proposed. The family is constructed by shifts and additions of two decimated m-sequences with the decimation factors 2 and $2d, d = N-p^{n-1}$. The upper bound for the maximum magnitude of nontrivial correlations of this family is derived using well known Kloosterman sums. The upper bound is shown to be $2\sqrt{N+\frac{1}{2}} = \sqrt{2p^n}$, which is twice the Welch's lower bound and approximately 1.5 times the Sidelnikov's lower bound. The size of the family is $2(p^n-1)$, which is four times the period of sequences.**

***Index Terms*—Autocorrelation, characters, cross-correlation, finite fields, Kloosterman sums, nonbinary sequences.**

I. Introduction

MANY families of pseudorandom sequences have been reported to have good correlation properties. Gold sequence family has low cross-correlation and large family size [1]. Kasami sequence family [2] [3] has lower cross-correlation than that of Gold, but it has smaller family size. Gold and Kasami sequence families are optimal with respect to the Sidelnikov's and the Welch's lower bounds, respectively. Besides these binary sequence families, there have been many researches on nonbinary sequence families. Liu and Komo [4] generalized Kasami sequence family to nonbinary case. Helleseth [5] investigated into various cross-correlations between m-sequences and its decimation. From these results, p-ary sequence families of period $p^n - 1$, maximum correlation bound $1 + 2\sqrt{p^n}$, and family size $p^n + 1$ has been constructed [6]. Based on the result of Trachenberg [7], a nonbinary sequence family with the correlation bound $1 + \sqrt{p^{n+1}}$ and family size $p^n + 1$ is obtained [6]. Kumar and Moreno [6] designed an asymptotically optimal family with the correlation upper bound $1 + \sqrt{p^n}$.

More recently, Kim *et al.* [8] constructed M-ary sequence families from Sidelnikov sequences. Han and Yang [9] proposed M-ary sequence families having the same upper bound for the maximum correlation magnitudes, but larger family size. Yu and Gong [10] refined the Weil bound to construct polyphase sequence families including some known families in [9] as special case. They also presented the array structure of M-ary Sidelnikov sequences and constructed M-ary sequence families with low correlation from column sequences of the array structure in [11]. Schmidt [12] proposed nested families of polyphase sequences which have prime period.

This paper presents a new construction of a p-ary sequence family with low correlation. For a prime p of $3 \bmod 4$ and an odd integer n, a new p-ary sequence family of period $\frac{p^n-1}{2}$ having maximum correlation magnitude $\sqrt{2p^n}$ is constructed. This maximum correlation magnitude is asymptotically twice the Welch's lower bound and 1.5 times the Sidelnikov's lower bound, but its family size is four times the period of sequences. This family can be obtained from shifts and additions of two decimated p-ary m-sequences by 2 and $2d$, $d = \frac{p^n-1}{2} - p^{n-1}$, and the size of the family is $2(p^n - 1)$. To our best knowledge, the new family is the first reported p-ary sequence family having period $\frac{p^n-1}{2}$ with low correlation.

II. Preliminaries

A. Correlation and Trace Functions

Let p be a prime and $\mathbb{F}_{p^n}$ be the finite field with p^n elements. For p-ary sequences $a(t)$ and $b(t)$ of period N, the correlation function at τ between $a(t)$ and $b(t)$ is defined as

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

where ω is a primitive p-th root of unity. Suppose that $\mathcal{S}$ is a family of p-ary sequences. Then the maximum correlation value R_{max} of $\mathcal{S}$ is defined as

$$R_{\max} = \{|R_{a,b}(\tau)||a(t), b(t) \in \mathcal{S}, \tau \neq 0 \text{ or } a(t) \neq b(t)\}.$$

Let n and m be positive integers such that $m|n$. Then the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is defined as

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

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

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

where α is a primitive element of $\mathbb{F}_{p^n}$.

Manuscript received March 18, 2010; revised October 04, 2010; accepted December 20, 2010. Date of current version May 25, 2011. This work was supported by a Grant from the National Research Foundation of Korea (NRF) funded by the Korean government (MEST) (No. 2010-0000867) and by the IT R&D program of MKE/KEIT (KI001809, Intelligent Wireless Communication Systems in 3 Dimensional Environment). This work was presented in part at the 2010 IEEE International Symposium on Information Theory, Austin, TX, June 2010.

J.-Y. Kim, S.-T. Choi, and J.-S. No are with the Department of Electrical Engineering and Computer Science, INMC, Seoul National University, Seoul 151-744, Korea (e-mail: lakroforce@ccl.snu.ac.kr; stchoi@ccl.snu.ac.kr; 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. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2133730

B. Characters

For a prime p and an integer n, a group homomorphism from $\mathbb{F}_{p^n}$ to $\mathbb{C}^\times = \mathbb{C}\backslash\{0\}$ is called an additive character of $\mathbb{F}_{p^n}$, where $\mathbb{C}$ denotes the complex field. Additive characters are usually denoted by χ. The canonical additive character χ_1 is defined as $\chi_1(x) = e^{\frac{2\pi i}{p}\mathrm{tr}_1^n(x)}$, where $i = \sqrt{-1}$. It is known that any additive character can be expressed as $\chi_a(x) = \chi_1(ax)$ for some $a \in \mathbb{F}_{p^n}$. Trivial additive character χ_0 is a character which maps every element of $\mathbb{F}_{p^n}$ into 1. The conjugate character of χ is the character such that $\bar{\chi}(x) = \overline{\chi(x)}$, where $\bar{()}$ denotes complex conjugate.

Similarly, a multiplicative character is defined as a group homomorphism from the multiplicative group $\mathbb{F}_{p^n}^\times = \mathbb{F}_{p^n}\backslash\{0\}$ to $\mathbb{C}^\times$. Multiplicative characters are usually denoted by ψ. Every multiplicative character can be given as

$$\psi_j(\alpha^k) = e^{\frac{2\pi ijk}{p^n-1}}$$

for some $0 \le j, k < p^n - 1$. Here ψ_0 is called a trivial multiplicative character. Conjugate characters of multiplicative characters are defined similarly as in the case of additive characters.

The quadratic character η, one of the multiplicative characters is defined as

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

C. Gaussian Sums and Kloosterman Sums

For a multiplicative character ψ and an additive character χ, the Gaussian sum $G(\psi, \chi)$ is defined as

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_{p^n}^\times} \psi(c)\chi(c).$$

The following lemmas for the Gaussian sum are needed for proof of the main theorem.

Lemma 1 [13]: Let ψ be a multiplicative character and χ an additive character of $\mathbb{F}_{p^n}$. Then the Gaussian sum $G(\psi, \chi)$ satisfies

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

and

$$|G(\psi,\chi)| = \sqrt{p^n} \quad \text{for } \psi \ne \psi_0 \text{ and } \chi \ne \chi_0.$$

□

Let a and b be elements of $\mathbb{F}_{p^n}$ and χ be an additive character of $\mathbb{F}_{p^n}$. Then the Kloosterman sum $K(\chi; a, b)$ is defined as

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

The following is a well-known upper bound on the Kloosterman sum.

Lemma 2 [13]: 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

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

□

The Kloosterman sum can be generalized to include a multiplicative character. 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

$$K(\psi, \chi, a, b) = \sum_{y \in \mathbb{F}_{p^n}^\times} \psi(y)\chi(ay + by^{-1}). \tag{2}$$

Many results are reported for the Gaussian and the Kloosterman sums. Here we list some of them which are used in this paper.

Lemma 3 [13]: Let ψ be a multiplicative character and χ an additive character of $\mathbb{F}_{p^n}$. The generalized Kloosterman sum defined in (2) reduces to a Gaussian sum if $ab = 0$, in the sense that

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

□

Lemma 4 [13]: Let η be the quadratic character of $\mathbb{F}_{p^n}$, p an odd prime, 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 5 [13]: Let η be the quadratic character of $\mathbb{F}_{p^n}$, p an odd prime, and $a, b \in \mathbb{F}_{p^n}$ with $ab = e^2$ for some $e \in \mathbb{F}_{p^n}^\times$. Then we have

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

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

In this paper, the following notations are used:

- p is an odd prime $(3 \bmod 4)$;
- n is an odd positive integer;
- $N = \frac{p^n-1}{2}$;
- $d = N - p^{n-1}$;
- α is a primitive element of $\mathbb{F}_{p^n}$;
- ω is a primitive p-th root of unity;
- $QR = \{a \in \mathbb{F}_{p^n}^\times | x^2 = a \text{ has a solution in } \mathbb{F}_{p^n}\}$;
- $QNR = \{a \in \mathbb{F}_{p^n}^\times | x^2 = a \text{ has no solution in } \mathbb{F}_{p^n}\}$.

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 $N = (p^n - 1)/2$. In order to construct the sequence family, the sequence $s(2t)$ and its decimated sequence $s(2dt)$ are considered. Since $\gcd(N, d) = 1$, the period of $s(2dt)$ is also N. The family S of our interest is defined as

$$S = \bigcup_{j=1}^{4} S_j$$

where

$$S_1 = \{s(2t) + s(2d(t+j)) | 0 \le j < N\}$$
$$S_2 = \{s(2t+1) + s(2d(t+j)) | 0 \le j < N\}$$
$$S_3 = \{s(2t) + s(2d(t+j)+1) | 0 \le j < N\}$$
$$S_4 = \{s(2t+1) + s(2d(t+j)+1) | 0 \le j < N\}.$$

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 $2\sqrt{N+\frac{1}{2}} = \sqrt{2p^n}$.

IV. Correlation Bound and Size of Sequence Family

The upper bound on the correlation magnitude of the sequence family $\mathcal{S}$ is derived in the main theorem. For the proof of the main theorem, Theorem 7, we need the following.

Lemma 6: For a and $b \in \mathbb{F}_{p^n}$, let $L(\chi_1; a, b)$ be defined as

$$L(\chi_1; a, b) = \sum_{y \in \mathbb{F}_{p^n}^{\times}} \eta(y) \omega^{\mathrm{tr}_1^n(ay + by^{-1})}$$

where η is the quadratic character. Then we have

$$|L(\chi_1; a, b)| \le 2\sqrt{p^n}.$$

Proof: We consider the following three cases:
i) $ab = 0$;
In this case, we can use Lemma 3. Since $|\eta(x)| \le 1$ for any $x \in \mathbb{F}_{p^n}$, we have

$$\begin{aligned} |L(\chi_1; a, b)| &= \left| \sum_{y \in \mathbb{F}_{p^n}^{\times}} \eta(y) \omega^{\mathrm{tr}_1^n(ay + by^{-1})} \right| \\ &= |K(\eta, \chi_1, a, b)| \\ &\le \begin{cases} |G(\bar{\eta}, \chi_1)| & \text{if} a = 0, b \ne 0 \\ |G(\eta, \chi_1)| & \text{if} a \ne 0, b = 0 \\ |G(\eta, \chi_0)| & \text{if} a = 0, b = 0. \end{cases} \end{aligned}$$

Since η is not trivial, Lemma 1 indicates that

$$|L(\chi_1; a, b)| \le \sqrt{p^n}.$$

ii) $ab \in QR$;
Here $ab = e^2$ for some $e \in \mathbb{F}_{p^n}^{\times}$. Then by applying Lemma 5, we have

$$\begin{aligned} |L(\chi_1; a, b)| &= |K(\eta, \chi_1, a, b)| \\ &= |\eta(b) G(\eta, \chi_1)(\chi_1(2e) + \chi_1(-2e))| \\ &\le 2|G(\eta, \chi_1)| \\ &\le 2\sqrt{p^n}. \end{aligned}$$

iii) $ab \in QNR$;
Using $\eta(ab) = -1$ and Lemma 4, we have

$$\begin{aligned} |L(\chi_1; a, b)| &= |K(\eta, \chi_1, a, b)| \\ &= 0. \end{aligned}$$

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

$$|L(\chi_1; a, b)| \le 2\sqrt{p^n}.$$

□

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

Proof: First we consider the cross-correlation of sequences in S_1. All the other cases can be similarly proved. The cross-correlation function between two sequences in S_1, $s(2t)+s(2d(t+j))$ and $s(2t) + s(2d(t+k))$, is given as

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2(t+\tau)}) + \mathrm{tr}_1^n(\alpha^{2d(t+\tau+j)}) - \mathrm{tr}_1^n(\alpha^{2t}) - \mathrm{tr}_1^n(\alpha^{2d(t+k)})} \\ &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(\alpha^{2t}(\alpha^{2\tau}-1)) + \mathrm{tr}_1^n(\alpha^{2dt}(\alpha^{2d(\tau+j)} - \alpha^{2dk}))}. \end{aligned} \quad (3)$$

Let $a = \alpha^{2\tau} - 1$ and $b' = \alpha^{2d(\tau+j)} - \alpha^{2dk}$. Then (3) can be written as

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

Since $2dt = -2p^{-1}t \pmod{p^n - 1}$, we have

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

Let $b = b'^p$. Then we have

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a\alpha^{2t} + b\alpha^{-2t})} \\ &= \sum_{t=0}^{N-1} \omega^{\mathrm{tr}_1^n(a(\alpha^t)^2 + b(\alpha^t)^{-2})} \\ &= \sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay + by^{-1})}. \end{aligned} \quad (4)$$

In order to compute $R(\tau)$ in (4), we can use the Kloosterman sum and the generalized Kloosterman sum given as

$$\begin{aligned} K(\chi_1; a, b) &= \sum_{y \in \mathbb{F}_{p^n}^{\times}} \omega^{\mathrm{tr}_1^n(ay + by^{-1})} \\ &= \sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay + by^{-1})} + \sum_{y \in QNR} \omega^{\mathrm{tr}_1^n(ay + by^{-1})} \\ L(\chi_1; a, b) &= \sum_{y \in \mathbb{F}_{p^n}^{\times}} \eta(y) \omega^{\mathrm{tr}_1^n(ay + by^{-1})} \\ &= \sum_{y \in QR} \omega^{\mathrm{tr}_1^n(ay + by^{-1})} - \sum_{y \in QNR} \omega^{\mathrm{tr}_1^n(ay + by^{-1})}. \end{aligned}$$

From Lemma 6, we have an upper bound for $L(\chi_1; a, b)$, namely $|L(\chi_1; a, b)| \le 2\sqrt{p^n}$.

TABLE I
VALUES OF a AND b FOR EACH CASE

Sequence set 1	Sequence set 2	a	b
$\mathcal{S}_1$	$\mathcal{S}_1$	$\alpha^{2\tau}-1$	$(\alpha^{2d(\tau+j)}-\alpha^{2dk})^p$
$\mathcal{S}_1$	$\mathcal{S}_2$	$\alpha^{2\tau}-\alpha$	$(\alpha^{2d(\tau+j)}-\alpha^{2dk})^p$
$\mathcal{S}_1$	$\mathcal{S}_3$	$\alpha^{2\tau}-1$	$(\alpha^{2d(\tau+j)}-\alpha^{2dk+1})^p$
$\mathcal{S}_1$	$\mathcal{S}_4$	$\alpha^{2\tau}-\alpha$	$(\alpha^{2d(\tau+j)}-\alpha^{2dk+1})^p$
$\mathcal{S}_2$	$\mathcal{S}_2$	$\alpha^{2\tau+1}-\alpha$	$(\alpha^{2d(\tau+j)}-\alpha^{2dk})^p$
$\mathcal{S}_2$	$\mathcal{S}_3$	$\alpha^{2\tau+1}-1$	$(\alpha^{2d(\tau+j)}-\alpha^{2dk+1})^p$
$\mathcal{S}_2$	$\mathcal{S}_4$	$\alpha^{2\tau+1}-\alpha$	$(\alpha^{2d(\tau+j)}-\alpha^{2dk+1})^p$
$\mathcal{S}_3$	$\mathcal{S}_3$	$\alpha^{2\tau}-1$	$(\alpha^{2d(\tau+j)+1}-\alpha^{2dk+1})^p$
$\mathcal{S}_3$	$\mathcal{S}_4$	$\alpha^{2\tau}-\alpha$	$(\alpha^{2d(\tau+j)+1}-\alpha^{2dk+1})^p$
$\mathcal{S}_4$	$\mathcal{S}_4$	$\alpha^{2\tau+1}-\alpha$	$(\alpha^{2d(\tau+j)+1}-\alpha^{2dk+1})^p$

Since p is an odd prime which is $3 \bmod 4$ and n is an odd integer, -1 is nonsquare. Therefore, as y runs through QR, $-y$ does through QNR and we have

$$\overline{\sum_{y\in QR}\omega^{\mathrm{tr}_1^n(ay+by^{-1})}}=\sum_{y\in QNR}\omega^{\mathrm{tr}_1^n(ay+by^{-1})}.$$

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

From the previous argument, we can set

$$\sum_{y\in QR}\omega^{\mathrm{tr}_1^n(ay+by^{-1})}=u+vi$$

and

$$\sum_{y\in QNR}\omega^{\mathrm{tr}_1^n(ay+by^{-1})}=u-vi$$

where u, v are real numbers.

From the definitions of the Kloosterman and the generalized Kloosterman sums, we obtain

$$K(\chi_1;a,b)=2u \tag{5}$$
$$L(\chi_1;a,b)=2vi. \tag{6}$$

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 $\tau=N=0(\mathrm{mod}N)$. Also note that

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

Therefore, we have

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

It is easy to check that $a=b=0$ corresponds to the in-phase autocorrelation. Therefore, from Lemma 2, we have $|K(\chi_1;a,b)|\leq 2\sqrt{p^n}$.

Thus, from Lemmas 2 and 6 and (5) and (6), we have

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

Finally, we obtain

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

The proof for cross-correlation bound in each of the other cases is quite similar, because the cross-correlation expression eventually becomes the Kloosterman sum over the quadratic residue as in (3) using the same technique. The only differences are values of constants a and b in (3). We summarize values of a and b for each case in Table I.

Thus, the proof is complete. □

Immediately from the proof of Theorem 7, it is manifest that all sequences in S are cyclically inequivalent. Thus we have the following theorem.

Theorem 8: The family size of S is $4N$. □

The new family is not optimal with respect to the Welch bound, which is rather insensitive to the family size. In fact, the upper bound of the correlation magnitudes of the proposed sequence family is approximately twice the Welch's lower bound, but its family size is four times the period of the sequences. On the other hand, the Sidelnikov lower bound [6] on the maximum correlation magnitude depends not only on the period but also on the family size. Here, we are going to measure how close the family is from the optimality with respect to the Sidelnikov's bound given below.

Lemma 9 [6]: Let S be a family of M p-ary sequences of period N, where p is an odd prime. Let $R_{\max}$ be the maximum magnitude of correlation values. Then

$$R_{\max}^2>\frac{k+1}{2}(2N-k)-\frac{2^kN^{2k+1}}{M(k!)^2\binom{2N}{k}}$$

for all $k\geq 0$. □

Here, let $k=1$ and $M=4N$. Then we have

$$R_{\max}^2>2N-1-\frac{2N^3}{4N2N}=2N-1-\frac{1}{4}N=\frac{7}{4}N-1.$$

TABLE II
COMPARISON OF WELL-KNOWN FAMILIES OF SEQUENCES (p IS A PRIME)

Family	Alphabet	Period N	R_{max}	Family size
Gold, odd n [1]	2	2^n-1	$1+\sqrt{2(N+1)}$	$N+2$
Gold, even n [1]	2	2^n-1	$1+2\sqrt{N+1}$	$N+2$
Kasami [2] [3]	2	2^n-1	$1+\sqrt{N+1}$	$\sqrt{N}$
Trachtenberg [7]	odd p	p^n-1	$1+\sqrt{(N+1)p}$	$N+2$
Helleseth [5]	odd p	p^n-1	$1+2\sqrt{N+1}$	$N+2$
Kumar, Moreno [6]	odd p	p^n-1	$1+\sqrt{N+1}$	$N+1$
Liu, Komo [4]	odd p	p^n-1	$1+\sqrt{N}$	$\sqrt{N}$
$\mathcal{V}^{(c_1)}$ [11]	$M>2$ even	p^n-1 (odd p)	$2\sqrt{N+1}+2$	$N+M-1$
$\mathcal{V}$ [11]	M	p^n-1 (odd p)	$3\sqrt{N+1}+1$	$(\frac{N}{2}+1)(M-1)$
$\tilde{\mathcal{U}}$ [11]	M even	p^n-1 (odd p)	$2\sqrt{N+1}+6$	$(N+1)\frac{M}{2}-1$
$\mathcal{U}$ [11]	M	p^n-1 (odd p)	$3\sqrt{N+1}+5$	$\frac{M(M-1)(N-1)}{2}+M-1$
Ω_r [12] $(0\le r\le p-2)$	p	p	$(r+1)\sqrt{N}+2$	$(N-2)N^r$
$\mathcal{L}$ $(p=2)$ [8]	M	2^n-1	$3\sqrt{N+1}+5$	$(M-1)^2(\frac{N-1}{2})+M-1$
$\mathcal{L}$ (p odd prime) [8]	M	p^n-1	$3\sqrt{N+1}+5$	$(M-1)^2(\frac{N}{2}-1)+\frac{M(M-1)}{2}$
$\mathcal{F}_{\mathbf{r}}^{(a)}$ [9]	M	p	$2\sqrt{N}+5$	$\frac{N-1}{2}+M-1$
$\mathcal{F}_{\mathbf{r}}$ [9]	M	p	$3\sqrt{N}+4$	$\frac{(M-1)^2(N-1)}{2}+M-1$
$\tilde{\mathcal{F}}_{\mathbf{s}}$ [9]	M	p^n-1	$2\sqrt{N+1}+6$	$\frac{(M-1)}{2}N+\lfloor\frac{M-1}{2}\rfloor$
$\mathcal{G}_{\mathbf{r}}^{(\delta,2)}, \delta\neq 0$ [10]	M	p	$4\sqrt{N}+7$	$(M-1)+(\frac{N-1}{2})(M-1)^2$ $+\frac{(N-1)(N-3)}{8}(M^2-3M+3)$
$\mathcal{H}_{\mathbf{r}}^{(2)}$ [10]	M	p	$5\sqrt{N}+6$	$(M-1)+(\frac{N-1}{2})(M-1)^2$ $+\frac{(N-1)(N-3)}{8}(M-1)^3$
$\mathcal{G}_{\mathbf{s}}^{(\delta,2)}, \delta\neq 0$ [10]	M	p^n-1	$4\sqrt{N+1}+8$	$(M-1)+(\frac{N-2}{2})(M-1)^2$ $+\frac{(N-2)(N-4)}{8}(M^2-3M+3)$
$\mathcal{H}_{\mathbf{s}}^{(2)}$ [10]	M	p^n-1	$5\sqrt{N+1}+7$	$(M-1)+(\frac{N-2}{2})(M-1)^2$ $+\frac{(N-2)(N-4)}{8}(M-1)^3$
New	p = 3 mod 4	$\frac{p^n-1}{2}$	$2\sqrt{N+\frac{1}{2}}$	$4N$

Thus

$$R_{\max} > \sqrt{\frac{7}{4}N-1} \approx 1.3228\sqrt{N}.$$

Therefore, we can see that the maximum magnitude of the nontrivial correlation values of the proposed family is approximately $0.7\sqrt{N}$ larger than the Sidelnikov's bound. Table II shows the parameters of some well known sequence families and the new family derived in this paper.

V. CONCLUSION

In this paper, a new family of p-ary sequences with low correlation is constructed. The family can be constructed in $\mathbb{F}_{p^n}$, with a prime p of $3 \bmod 4$ and an odd integer n. The period of sequences are $\frac{p^n-1}{2}$. Sequences in the family are obtained using shifts and additions of decimated m-sequences $s(2t)$ and $s(2dt)$ with the decimation factor $d=N-p^{n-1}$. The upper bound for the magnitude of nontrivial correlation values of the sequence family can be deduced by the Kloosterman sums, which is approximately 1.5 times the Sidelnikov's lower bound. The size of the sequence family is $2(p^n-1)$, 4 times the period of the sequences.

ACKNOWLEDGMENT

The authors thank the anonymous reviewers for their valuable comments and suggestions that improved the paper.

REFERENCES

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

[2] T. Kasami, Weight Distribution Formular for Some Class of Cyclic Codes Coordinated Science Laboratory, Univ. of Illinois, Urbana, Tech. Rep. R-285 (AD 632574), Apr. 1966.

[3] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in *Cambinatorial Mathematics and Its Applications*. Chapel Hill, NC: Univ. of North Carolina Press, 1969.

[4] 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.

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

[6] 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.

[7] H. M. Trachtenberg, "On the Cross-Correlation Functions of Maximal Recurring Sequences," Ph.D. dissertation, Univ. of Southern California, Los Angeles, 1970.

[8] Y. S. Kim, J. S. Chung, J. S. No, and H. Chung, "New families of M-ary sequences with low correlation constructed from Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768–3774, Aug. 2008.

[9] Y. K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1815–1823, Apr. 2009.
[10] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6376–6387, Dec. 2010.
[11] N. Y. Yu and G. Gong, "New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4061–4070, Aug. 2010.
[12] K.-U. Schmidt, "Sequence families with low correlation derived from multiplicative and additive characters," *IEEE Trans. Inf. Theory* [Online]. Available: www.sfu.ca/ksa39/pub/char_seq.pdf, to be published
[13] R. Lidl and H. Niederreliter, *Finite Fields, Vol. 20, Encyclopedia of Mathematics and Its Applications*. Amsterdam, The Netherlands: Addison-Wesley, 1983.

Ji-Youp Kim received the B.S. degree in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 2009, where he is currently pursuing the Ph.D. degree in electrical engineering and computer science.

His area of research interests includes pseudorandom sequences, error-correcting codes, and communications theory.

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 pursuing the Ph.D. degree in electrical engineering and computer science.

His area of research interests includes pseudo random sequences, error-correcting codes, and communications theory.

Jong-Seon No (S'80–M'88–SM'10) 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, 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 area of research interests includes 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, Korea, 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.