Crosscorrelation of q-ary Power Residue Sequences of Period p is Upper Bounded by $\sqrt{p}+2$

Young-Joon Kim, Hong-Yeop Song
Department of Electrical and Electronics Engineering
Yonsei University, Seoul, Korea
E-mail: {yj.kim, hy.song}@coding.yonsei.ac.kr

and

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
Email: ggong@calliope.uwaterloo.ca

Abstract

Let p be an odd prime, q be a divisor of $p-1$ and μ be a primitive root mod p. A q-ary power residue sequence (PRS) $\{s(n)\}$ of period p is defined as $s(n)=k$ if $n \in C_k$ where $C_k = \{\mu^{qt+k} | t = 0, 1, 2, ..., T-1\}$ where $T=(p-1)/q$. In this paper, we prove that the maximum absolute value of the periodic crosscorrelation of two distinct q-ary PRS's of period p is upper bounded by $\sqrt{p}+2$.
Keywords: Non-binary PN Sequences, Polyphase Sequences, Correlation property.

1 Introduction

Green and Green [1] had defined q-ary sequences of period p, and proved its autocorrelation magnitude is upper bounded by 3. In this paper, we prove the crosscorrelation magnitude is upper bounded by $\sqrt{p}+2$, which was conjectured by Kim based on some extensive computation data provided in [2]. For this, we will give the definition of q-ary sequences of period p in this section, and reviewed some earlier works in Section 2. Final section is to state and prove the main result. For the discussion on possible application of these sequences, see [1] and [2].

Definition 1 ([1][2]) *Let p be an odd prime and q be a divisor of $p-1$. Let $T=(p-1)/q$ and μ be a primitive root mod p. The nonzero integers mod p can be partitioned into q cosets C_i, $0 \le i \le q-1$, where C_0 is the set of the q-th power residues mod p, and $C_i = \mu^i \cdot C_0$ for $i > 0$.*

The q-ary power residue sequence (q-ary PRS) $\{s(n)\}$ taking values on $\mathbf{Z}_q$ of period p is defined as, for $n = 0, 1, 2, ..., p-1$,

$$s(n) = \begin{cases} 0 & \text{if } n \equiv 0 \pmod{p} \\ i & \text{if } n \in C_i \text{ for } i \in Z_q \end{cases}$$

Complex equivalents (q-phase PRS):

$$a(n) = w^{s(n)} \quad \text{for} \quad n = 0, 1, 2, ..., p-1,$$

where w be a complex primitive q-th root of unity.

Example 1 *An example of ternary PRS (when p=13, q=3, μ=2) is shown below:*

i	0	1	2	3	4	5	6	7	8	9	10	11
$2^i \pmod{13}$	1	2	4	8	3	6	12	11	9	5	10	7

$C_0 = \{1, 5, 8, 12\}$
$C_1 = \mu^1 \cdot C_0 = 2 \cdot C_0 = 2 \cdot \{1, 5, 8, 12\} = \{2, 10, 3, 11\}$
$C_2 = \mu^2 \cdot C_0 = 2^2 \cdot C_0 = 4 \cdot \{1, 5, 8, 12\} = \{4, 7, 6, 9\}$

Therefore, a ternary PRS $\{s(n)\}$ and (its complex equivalent) 3-phase PRS $\{a(n)\}$ of length 13 are given as follows:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0
$a(n)$	1	1	w^1	w^1	w^2	1	w^2	w^2	1	w^2	w^1	w^1	1

where $w = \exp(j\frac{2\pi}{3})$.

2 Earlier Works - Summary

Lemma 1 ([1]) *Let $\{s(n)\}$ be a q-ary PRS of period p and $\{a(n)\}$ be the (complex) q-phase PRS with $a(n) = w^{s(n)}$, where w is a complex primitive q-th root of unity. Then,*

(i) $s(1) = 0$ *and hence* $a(1) = 1$.

(ii) *For $u \neq 0, v \neq 0$, we have*

$$a(u) \cdot a(v) = a(uv) \quad \textit{and} \quad a(u) \cdot a(v)^* = a(u/v).$$

(iii) *For any $u \in Z_p^*$, we have*

$$a(-u) = w^{s(-u)} = \begin{cases} -a(u), & \textit{if } p \equiv q+1 \pmod{2q} \\ a(u), & \textit{if } p \equiv 1 \pmod{2q} \end{cases}$$

(iv) $\sum_{n=1}^{p-1} a(n) = 0$.

Theorem 1 (Autocorrelation [1]) *Let $\{s(n)\}$ be a q-ary PRS of period p and $\{a(n)\}$ be the complex q-phase PRS with $a(n) = w^{s(n)}$, where w is a complex primitive q-th root of unity. If $a(u) = \alpha(u) + j\beta(u)$ where $\alpha(u)$ and $\beta(u)$ are the real and imaginary part of $a(u)$ respectively, then the autocorrelation of the q-phase PRS $\{a(n)\}$, for any $\tau \not\equiv 0 \pmod{p}$, is given as follows:*

$$R_a(\tau) = \sum_{x=0}^{p-1} a(x)a(x+\tau)^* = \begin{cases} -1 - j \cdot 2\beta(\tau), & \textit{if } p \equiv q+1 \textit{ mod } 2q \\ -1 + 2\alpha(\tau), & \textit{if } p \equiv 1 \textit{ mod } 2q \end{cases}$$

(Therefore, we have $|R_a(\tau)| \leq 3$.)

How are two distinct q-ary PRS of length p from two different primitive roots mod p related?

Theorem 2 ([2]) *Let μ be a primitive root mod p. Let a q-ary PRS $\{s(n)\}$ be constructed using μ^i and $\{t(n)\}$ be constructed using μ^j, where both i and j are relatively prime to $p-1$. Then, there exists a constant $v \pmod q$ such that $t(n) \equiv v^{-1} \cdot s(n) \pmod q$ for all n, where v is a solution to $j \equiv i \cdot v \pmod{p-1}$.*

Example 2 *When $p = 13$, there exist $\phi(12) = 4$ primitive roots in $\mathbf{Z}_{13}$. These are $2^1 = 2,\ 2^5 = 6,\ 2^7 = 11,\ 2^{11} = 7$. We take $q = 3$ in this example and see how ternary PRS changes according to the choice of the primitive roots.*

μ	C_0	C_1	C_2
2	$\{1,5,8,12\}$	$\{2,10,3,11\}$	$\{4,7,6,9\}$
6	$\{1,5,8,12\}$	$\{6,4,9,7\}$	$\{10,11,2,3\}$
11	$\{1,5,8,12\}$	$\{11,3,10,2\}$	$\{4,7,6,9\}$
7	$\{1,5,8,12\}$	$\{7,9,4,6\}$	$\{10,11,2,3\}$

So a ternary PRS $\{s(n)\}$ of length 13 using $\mu = 2, 6, 11, 7$ are given as follows.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(n)$ *with* $\mu = 2$	0	0	1	1	2	0	2	2	0	2	1	1	0
$s(n)$ *with* $\mu = 6$	0	0	2	2	1	0	1	1	0	1	2	2	0
$s(n)$ *with* $\mu = 11$	0	0	1	1	2	0	2	2	0	2	1	1	0
$s(n)$ *with* $\mu = 7$	0	0	2	2	1	0	1	1	0	1	2	2	0

Corollary 1 ([2]) *Let μ be a primitive root mod p. Let a q-ary PRS $\{s(n)\}$ be constructed using μ^i and $\{t(n)\}$ be constructed using μ^j, where both i and j are relatively prime to $p-1$. Then, $s(n) \equiv t(n)$ (mod q) for all n if and only if $i \equiv j$ (mod q) if and only if $v \equiv 1$ (mod q).*

Two q-ary PRS $\{s_1(n)\}$ and $\{s_2(n)\}$ of the same period p are related as a constant multiple of each other. Conversely, can all the other q-ary PRS's be constructed by multiplying an integer t satisfying $(t, q) = 1$ to any one q-ary PRS instead of changing a primitive root?

Theorem 3 ([2]) *Let p be an odd prime and q be a divisor of $p-1$. Then,*

$$U_{p-1} \equiv U_q \pmod q.$$

where U_{p-1} and U_q are the unit groups of $\mathbf{Z}_{p-1}$ and $\mathbf{Z}_q$, respectively.

Corollary 2 ([2]) *The number of all the distinct q-ary PRS of period p is $\phi(q)$.*

Remark 1 *The total of $\phi(q)$ q-ary PRS of period p can be generated either by (A) taking all possible primitive roots mod p in* Definition 1 *or by (B) multiplying all possible constants* (that are relatively prime to q) *to any one given q-ary PRS of period p. In* Example 2, *the second sequence can be obtained by multiplying* 2 (mod 3) *to all the terms of the first sequence.*

3 Crosscorrelation of q-phase PRS

The periodic crosscorrelation between two q-phase sequences $a(n)$ and $b(n)$ (of period p) is defined by

$$C_{a,b}(\tau) = \sum_{n=0}^{p-1} a(n)b(n+\tau)^* = \sum_{n=0}^{p-1} w^{s_1(n)-s_2(n+\tau)}$$

where w is a complex primitive q-th root of unity, $a(n) = w^{s_1(n)}$ and $b(n) = w^{s_2(n)}$.

Theorem 4 (Main) *Let p be an odd prime and q be a divisor of $p-1$. The crosscorrelation of two distinct q-phase PRS $\{a(n)\}$ and $\{b(n)\}$ of length p is upper-bounded by $\sqrt{p}+2$, i.e.,*

$$|C_{a,b}(\tau)| \leq \sqrt{p} + 2.$$

For the proof the main theorem, we need the following:

Lemma 2 *Let $\{s(n)\}$ be a q-ary PRS and $\{a(n)\}$ be its complex equivalent q-phase PRS. For any integer $m = 1, 2, ..., q-1$, we have*

$$\sum_{n=1}^{p-1} a(n^m) = 0.$$

Proof: To see this, simply observe that $s(n) = i$ if $n \in C_i$, and that note that $s(n^m)$ takes the value j if n^m belongs to the coset C_j. All it takes is the index of the cosets which are $0, 1, 2, ..., q-1$.

If $(m, q) = 1$, then the map $n \to n^m$ is a permutation of Z_p^*, and we are done, since $s(n^m)$ takes all the values $0, 1, ..., q-1$ exactly T times, where $Tq = p - 1$.

If $(m, q) = d > 1$, let $q/d = q_1$. Then, $s(n^m)$ takes all the values $0, d, 2d, ..., (q_1 - 1)d$ exactly dT times, and by symmetry, the sum of their complex equivalents becomes zero. ■

Proof of Main Theorem: We now calculate the crosscorrelation of $\{a(n)\}$ and $\{b(n)\}$ where

$$a(n) = w^{s(n)} \quad \text{and} \quad b(n) = w^{ks(n)} = \left(w^{s(n)}\right)^k = a(n)^k,$$

where k is any given integer from 1 to $q-1$ with $(k, q) = 1$.

Note that it becomes the autocorrelation when $k = 1$. Therefore, we will assume that $k > 1$. Note that when $n \neq 0$, we have $b(n) = a(n)^k = a(n^k)$ from Lemma 1.

We will first take care of the case where $\tau = 0$ as follows:

$$\begin{aligned} C_{a,b}(\tau = 0) &= \sum_{n=0}^{p-1} a(n)b(n)^* = \left(\sum_{n=0}^{p-1} a(n)^* b(n)\right)^* \\ &= a(0)b(0)^* + \left(\sum_{n=1}^{p-1} a(n)^* a(n^k)\right)^* \\ &= 1 + \left(\sum_{n=1}^{p-1} a(n^{k-1})\right)^* \\ &= 1, \quad \text{from Lemma 2, since} \quad 1 < k < q. \end{aligned}$$

We now assume that $\tau \neq 0$. Then

$$
\begin{aligned}
C_{a,b}(\tau) &= \sum_{0 \le n < p} a(n+\tau) b(n)^* \\
&= a(\tau) b(0)^* + a(0) b(-\tau)^* + \sum_{\substack{0 \le n < p \\ n \ne 0 \\ n \ne -\tau}} a(n+\tau) a(n^k)^* \\
&= a(\tau) + b(-\tau)^* + \sum_{\substack{1 \le n < p \\ n \ne -\tau}} a\left(\frac{n+\tau}{n^k}\right). \qquad (1)
\end{aligned}
$$

Denote the third term of (1) by $\delta(\tau)$. Since magnitude of the sum of the first two terms cannot exceed 2, it is now sufficient to show that, for any $\tau \neq 0$,

$$|\delta(\tau)|^2 \le p.$$

Observe the following:

$$
\begin{aligned}
|\delta(\tau)|^2 &= \sum_{\substack{x \in Z_p^* \\ x \ne -\tau}} a\left(\frac{x+\tau}{x^k}\right) \left(\sum_{\substack{y \in Z_p^* \\ y \ne -\tau}} a\left(\frac{y+\tau}{y^k}\right) \right)^* \\
&= \sum_{\substack{x \in Z_p^* \\ x \ne -\tau}} \sum_{\substack{y \in Z_p^* \\ y \ne -\tau}} a\left(\frac{x+\tau}{x^k}\right) a\left(\frac{y+\tau}{y^k}\right)^* \\
&= \sum_{\substack{x \in Z_p^* \\ x \ne -\tau}} \sum_{\substack{y \in Z_p^* \\ y \ne -\tau}} a\left(\left(\frac{x+\tau}{y+\tau}\right)\left(\frac{y}{x}\right)^k\right)
\end{aligned}
$$

Substitute $1/x$ instead of x. Then

$$
|\delta(\tau)|^2 = \sum_{\substack{x \in Z_p^* \\ x \ne -1/\tau}} \sum_{\substack{y \in Z_p^* \\ y \ne -\tau}} a\left(\left(\frac{1+\tau x}{yx+\tau x}\right)(yx)^k\right)
$$

How many terms are in the above double summation ? There are $(p-2)^2$ terms. These can be re-ordered according to whether $yx = 1$ or $yx \neq 1$.

$$
\begin{aligned}
|\delta(\tau)|^2 &= \sum_{\substack{yx=1 \\ x \in Z_p^* - \{-1/\tau\} \\ y \in Z_p^* - \{-\tau\}}} a(1) \quad + \sum_{\substack{yx \neq 1 \\ x \in Z_p^* - \{-1/\tau\} \\ y \in Z_p^* - \{-\tau\}}} a\left(\left(\frac{1+\tau x}{yx+\tau x}\right)(yx)^k\right) \\
&= p - 2 + \sum_{\substack{yx \neq 1 \\ x \in Z_p^* - \{-1/\tau\} \\ y \in Z_p^* - \{-\tau\}}} a\left(\left(\frac{1+\tau x}{yx+\tau x}\right)(yx)^k\right) \qquad (2)
\end{aligned}
$$

Now, all we have to show is that the last term of (2) is less than or equal to 2. We will denote the term by $\Delta(\tau)$. We now change the variables from x and y to x and $yx = z$ so that

$$
\begin{aligned}
\Delta(\tau) &= \sum_{\substack{yx \neq 1 \\ x \in Z_p^* - \{-1/\tau\} \\ y \in Z_p^* - \{-\tau\}}} a\left(\left(\frac{1+\tau x}{yx+\tau x}\right)(yx)^k\right) \\
&= \sum_{\substack{x \in Z_p^* - \{-1/\tau\} \\ z \in Z_p^* - \{1, -\tau x\}}} a\left(\left(\frac{1+\tau x}{z+\tau x}\right)z^k\right)
\end{aligned}
$$

We put further $\tau x = u$. Then, we have

$$
\begin{aligned}
\Delta(\tau) &= \sum_{\substack{u \in Z_p^* - \{-1\} \\ z \in Z_p^* - \{1, -u\}}} a\left(\left(\frac{1+u}{z+u}\right)z^k\right) \\
&= \sum_{\substack{z \in Z_p^* - \{1\} \\ u \in Z_p^* - \{-1, -z\}}} a(z^k)a\left(\frac{1+u}{z+u}\right) \\
&= \sum_{z \in Z_p^* - \{1\}} a(z^k) \sum_{u \in Z_p^* - \{-1, -z\}} a\left(\frac{1+u}{z+u}\right)
\end{aligned}
$$

The inner sum of the above can be computed to be the sum of $a(x)$ for all $x \in Z_p^*$ except for two terms which are $a(1)$ and $a(z^{-1})$ since the map

$u \to \frac{1+u}{z+u}$ is one-to-one for $u \in Z_p^* - \{-1, -z\}$. Therefore,

$$\begin{aligned}
\Delta(\tau) &= \sum_{z \in Z_p^* - \{1\}} a(z^k)(-a(1) - a(z^{-1})) \\
&= -\sum_{z \in Z_p^* - \{1\}} a(z^k) - \sum_{z \in Z_p^* - \{1\}} a(z^{k-1}) \\
&= a(1) + a(1) = 2.
\end{aligned}$$

This completes the proof of main Theorem. ■

Acknowledgement: Hong-Yeop Song wishes to acknowledge Prof. Guang Gong of University of Waterloo who invited him with great hospitality to visit University of Waterloo from January 17 to February 7, 2004.

References

[1] D. H. Green and P. R. Green, "Polyphase Related-Prime Sequences," *IEE Proceedings, Compute. Digit. Tech.* vol. 148, no. 2, pp. 53-62, March 2001.

[2] Young-Joon Kim, *On the Crosscorrelation of Polyphase Power Residue Sequences*, MS Thesis, Dept. Electrical and Electronics Engineering, Yonsei University, Feb. 2004.