On the Crosscorrelation of Polyphase Power Residue Sequences

Young-Joon Kim

yj.kim @coding.yonsei.ac.kr

November, 22, 2003

Coding & Information Theory Lab.

Department of Electrical and Electronic Engineering, Yonsei Univ.

Contents

I. Introduction

II. Theory of Polyphase Power Residue Sequences

1. Binary Legendre Sequences
2. Polyphase Power Residue Sequences

III. Crosscorrelation of PPRS

IV. Concluding Remark

I. Introduction

- Motivation

✓ Sequences used in the spread spectrum communication
- need a good auto & cross-correlation

✓ Kasami and Gold generated bianry sequence families with good crosscorrelation using m-sequences.

✓ Polyphase Power Residue Sequences(shortly PPRS) have good autocorrelation

✓ Legendre sequences(special cases of PPRS with q=2)
- generation, existence condition, linear complexity(LC), trace representation have been determined and most of them are solved, but as of PPRS only autocorrelation and LC have been determined.

1. Binary Legendre Sequences of length *p*

Let p be an odd prime.

$$\{a_n\} = \begin{cases} 1 \quad , & if\ n \equiv 0 \bmod p \\ 0 \quad , & if\ n \text{ is a quadratic residue mod } p \\ 1 \quad , & otherwise \end{cases}$$

✓ Example 2.1

$p=11$, QR={1, 3, 4, 5, 9}, QNR={2, 6, 7, 8, 10}

$$a_n = \{a_0 a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10}\}$$
$$= \{1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\}$$

τ	0	1	2	3	4	5	6	7	8	9	10
$C(\tau)$	11	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

✓ Example 2.2

p=13, QR={1, 3, 4, 9, 10, 12}, QNR={2, 5, 6, 7, 8, 11}

$$a_n = \{a_0 a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12}\}$$
$$= \{1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\}$$

τ	0	1	2	3	4	5	6	7	8	9	10	11	12
$C(\tau)$	13	1	-3	1	1	-3	-3	-3	-3	1	1	-3	1

2. Polyphase Power Residue Sequences

- Preparation(1) – partitioning of nonzero integer mod p

p : odd prime

q : any divisor of p-1

T : $\dfrac{p-1}{q}$

Hence $p\text{-}1 = q \cdot T$

(If T is even, then $p \equiv 1 \pmod{2q}$

If T is odd, then $p \equiv q+1 \pmod{2q}$)

μ : primitive element in mod p

- Preparation(2) – partitioning of nonzero integer mod p

$$C_0 = \{\text{set of } q\text{-th power residues}\}$$
$$= \{\mu^0, \mu^q, \mu^{2q}, \ldots, \mu^{(T-1)q}\}$$
$$C_1 = \mu^1 \cdot C_0$$
$$= \{\mu^1, \mu^{q+1}, \mu^{2q+1}, \ldots, \mu^{(T-1)q+1}\}$$
$$\vdots$$
$$C_{q-1} = \mu^{q-1} \cdot C_0$$
$$= \{\mu^{q-1}, \mu^{2q-1}, \mu^{3q-1}, \ldots, \mu^{Tq-1}\}$$

- Constuction of q-phase Power Residue Sequences of length p

$$\{a_n\} = \begin{cases} 1, & \text{if } n \equiv 0 (\text{mod } p) \\ e^{j\frac{2\pi \cdot 0}{q}}, & \text{if } n \in C_0 \\ e^{j\frac{2\pi \cdot 1}{q}}, & \text{if } n \in C_1 \\ \vdots, & \vdots \\ e^{j\frac{2\pi \cdot (q-1)}{q}}, & \text{if } n \in C_{q-1} \end{cases}$$

Where $n = 0,1,\ldots, p\text{-}1$

✓ Example 2.3 $p = 13$, $q = 3$, $\mu = 2$

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

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

$$C_0 = \{1, 5, 8, 12\}$$

$$C_1 = \mu^1 \cdot C_0 = 2 \cdot C_0 = 2 \cdot \{1, 5, 8, 12\} = \{2, 10, 3, 11\}$$

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

Hence, 3-phase PRS of length 13 is as follows.

$$\{a_{13}\} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12})$$

$$= (1, 1, e^{j\frac{2\pi \cdot 1}{3}}, e^{j\frac{2\pi \cdot 1}{3}}, e^{j\frac{2\pi \cdot 2}{3}}, 1, e^{j\frac{2\pi \cdot 2}{3}}, e^{j\frac{2\pi \cdot 2}{3}}, 1, e^{j\frac{2\pi \cdot 2}{3}}, e^{j\frac{2\pi \cdot 1}{3}}, e^{j\frac{2\pi \cdot 1}{3}}, 1)$$

✓ Properties of q-phase PRS

1. $a_u \cdot a_v = a_{u \cdot v}$, $a_u \cdot a_v^* = a_{u/v}$ $(u \neq 0, v \neq 0)$

2. $a_1 = 1$ and

$$a_{-1} = \begin{cases} -1 , & p \equiv q+1 \ (2q) \\ 1 , & p \equiv 1 \quad (2q) \end{cases} \qquad a_{-u} = \begin{cases} -a_u , & p \equiv q+1 \ (2q) \\ a_u , & p \equiv 1 \quad (2q) \end{cases}$$

3. $\sum_{x=1}^{p-1} a_x = 0$

4. If $a_u = \alpha_u + j \cdot \beta_u$ $(\alpha_u, \beta_u \in R)$

$$R_a(\tau) = \sum_{x=0}^{p-1} a_x a_{x+\tau}^* = \begin{cases} -1 - j \cdot 2\beta_\tau , & p \equiv q+1 \mod 2q \\ -1 + 2 \cdot \alpha_\tau , & p \equiv 1 \mod 2q \end{cases} \Rightarrow |R_a(\tau)| \leq 3$$

III. Crosscorrelation of PPRS (1)

- ✓ In fact, there are $\Phi(p\text{-}1)$ primtive elements in mod p.
- ✓ Example 3.1

When $p = 13$, $\Phi(12)=4$ primitive elements (mod 13) (ex. $\mu = 2,6,11,7$)

$p = 13$, $q = 3$, $\mu=6$

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

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

$$C_0 = \{1, 5, 8, 12\}$$

$$C_1 = \mu^1 \cdot C_0 = 6 \cdot C_0 = 6 \cdot \{1, 5, 8, 12\} = \{6, 4, 9, 7\}$$

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

$$\{a_{13}\} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12})$$

$$= (1, 1, e^{j\frac{2\pi\cdot 2}{3}}, e^{j\frac{2\pi\cdot 2}{3}}, e^{j\frac{2\pi\cdot 1}{3}}, 1, e^{j\frac{2\pi\cdot 1}{3}}, e^{j\frac{2\pi\cdot 1}{3}}, 1, e^{j\frac{2\pi\cdot 1}{3}}, e^{j\frac{2\pi\cdot 2}{3}}, e^{j\frac{2\pi\cdot 2}{3}}, 1)$$

III. Crosscorrelation of PPRS (2)

✓ Table1. set of primtives which result in same PPRS, set of PPRS for given p and q

p	μ	q	Primitive set	W_{pq}
11	2	5	1 3 7 9	0 0 1 3 2 4 4 2 3 1 0 0 0 2 1 4 3 3 4 1 2 0 0 0 3 4 1 2 2 1 4 3 0 0 0 4 2 3 1 1 3 2 4 0
13	2	3	(1, 7) (5, 11)	0 0 1 1 2 0 2 2 0 2 1 1 0 0 0 2 2 1 0 1 1 0 1 2 2 0
		4	(1, 5) (7, 11)	0 0 1 0 2 1 1 3 3 0 2 3 2 0 0 3 0 2 3 3 1 1 0 2 1 2
		6	(1, 7) (5, 11)	0 0 1 4 2 3 5 5 3 2 4 1 0 0 0 5 2 4 3 1 1 3 4 2 5 0

⇒ We represents PPRS W_{pq} for super index of exponential instead of complex q-*th* roots of unity.

III. Crosscorrelation of PPRS (3)

- Crosscorrelation function between distinct two PPRS is as follows.

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

$$= \sum_{n=0}^{p-1} \omega^{s_1(n)-s_2(n+\tau)} \qquad (*)$$

- Where ω is a complex primitive q-th root of unity,

$$a_n = \omega^{s_1(n)}, \qquad b_n = \omega^{s_2(n)}$$

- Sequences $s_1(n)$ and $s_2(n)$ takes on values in Z_q

Table 2. Maximum crosscorrelation between distinct two PRS, number of larger than $p/3$ and $\sqrt{p}$

p	μ	q	(i,j)	Max	Larger	$p/3$	Larger	$\sqrt{p}$
11	2	5	(1,3)	5.213	4	3.667	4	3.317
			(1,7)	4.765	4		6	
			(1,9)	5.213	6		6	
			(3,7)	5.314	6		6	
			(3,9)	4.765	4		6	
			(7,9)	5.213	4		4	
13	2	3	(1,5)	5.568	4	4.333	4	3.606
		4	(1,7)	3.606	0		0	
		6	(1,5)	5.568	6		6	
17	3	4	(1,3)	6.083	4	5.667	8	4.123
		8	(1,3)	6.083	2		4	
			(1,5)	5.745	2		6	
			(1,7)	6.123	6		10	
			(3,5)	6.123	6		10	
			(3,7)	5.745	2		6	
			(5,7)	6.083	2		4	
19	2	3	(1,5)	6.083	0	6.333	12	4.359
		6	(1,5)	4.359	0		0	
		9	(1,5)	5.752	0		12	
			(1,7)	5.392	0		12	
			(1,11)	6.34	2		8	
			(1,13)	6.282	0		6	
			⋮	⋮	⋮		⋮	

Table 3. Number of distinct PPRS, Maximum of maximum crosscorrelation Max***Cw***, number of larger than $\sqrt{p}+2$

p	μ	q	distinct	MaxC_W	Larger	$\sqrt{p}+2$
11	2	5	4	5.314	0	5.317
13	2	3	2	5.568	0	5.606
		4	2	3.606	0	
		6	2	5.568	0	
17	3	4	2	6.083	0	6.123
		8	4	6.123	0	
19	2	3	2	6.083	0	6.359
		6	2	4.359	0	
		9	6	6.34	0	
23	5	11	10	6.796	0	6.796
29	2	4	2	5.385	0	7.385
		7	6	7.364	0	
		14	6	7.38	0	
31	3	3	2	7	0	7.568
		5	4	7.562	0	
		6	2	5.568	0	
		10	4	7.434	0	
		15	8	7.568	0	
37	2	3	2	7.81	0	8.083

$\phi(q)$

IV. Concluding Remark

- ✓ Generation of PPRS by changing primitive elements
  For fixed p and q, there exist $\phi(q)$ distinct PPRS

- ✓ Investigate the crosscorrelation of distinct PPRS having phase q for $11 \leq p \leq 521$.

- ✓ Conjecture

  Independent of p and q, maximum crosscorrelation of PPRS made by changing primtive element is upper bounded to $\sqrt{p}+2$

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