Crosscorrelation of q-ary Power Residue Sequences of Period p

July 10, 2006

Young-Joon Kim, Hong-Yeop Song

School of Electrical and Electronic Engineering,

Yonsei University, Seoul, Korea.

Guang Gong

Department of Electrical and Computer Eng.,

University of Waterloo, Waterloo, Ontario, Canada.

Habong Chung

School of Electrical and Electronic Eng.,

Hongik University, Seoul, Korea.

Contents

- Introduction – Example and Definition
- Autocorrelation - review
- Crosscorrelation of two q-ary PRS
- Crosscorrelation of two decimations of two q-ary PRS
- Big Picture
- Comments

Example

- Ternary PRS (p=13, q=3, μ=2)

n	1	2	3	4	5	6	7	8	9	10	11	12
n^3	1	8	1	12	8	8	5	5	1	12	5	12

  - $C_0 = 2^0 \cdot C_0$ = {1,5,8,12}
  - $C_1 = 2^1 \cdot C_0$ = {2,10,3,11}
  - $C_2 = 2^2 \cdot C_0$ = {4,7,6,9}

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

Definition

- p : an odd prime
- q : a divisor of p-1
- μ : a primitive root mod p
- Coset Partition
  - C_0 : a set of q-th power residues mod p
  - $C_i = \mu^i \cdot C_0 \quad \text{for} \quad 0 \le i \le q-1$

◆ A q-ary PRS is defined as, for n = 0, 1, 2,…, p-1,

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

Some Properties (Known)

- Lemma 1 ('69, Sidel'nikov)
  - $\{s(n)\}$: q-ary PRS of period p
  - w : a primitive q-th root of unity
    - $s(1)=0$
    - For $u\neq 0$, $v\neq 0$ (mod p),
      $s(u)+s(v)\equiv s(uv)$
      $s(u)-s(v) \equiv s(u/v)$
    - For any $u\neq 0$ (mod p)

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

    - $\sum_{n=1}^{p-1} w^{s(n)} = 0$

- When p=13, q=3, μ=2
  - $s(1)=0$
  - $s(2)+s(4)=1+2\equiv 0=s(8)$
    $s(3)-s(7)=1-2\equiv 2=s(3/7)=s(6)$
  - Since 13≡1 (mod 6),
    $s(1)=s(12)=0$, $s(2)=s(11)=1$
    etc.
  - $\sum_{n=1}^{12} w^{s(n)} = 4(w^0 + w^1 + w^2) = 0$

Autocorrelation

- Theorem 1 ('69, Sidel'nikov)
  - $\{s(n)\}$: a q-ary PRS of period p
  - w : a complex q-th root of unity
  - Autocorrelation of a q-ary PRS $\{s(n)\}$

$$R_s(\tau) = \sum_{x=0}^{p-1} w^{s(x+\tau)-s(x)} = \begin{cases} -1 - j2\beta(\tau) & \text{if } p \equiv q+1 \pmod{2q} \\ -1 + 2\alpha(\tau) & \text{if } p \equiv 1 \pmod{2q} \end{cases}$$

where $\alpha(\tau)$ and $\beta(\tau)$ are the real and imaginary part of $w^{s(\tau)}$.

$$\Rightarrow \qquad |R_s(\tau)| \le 3$$

How many distinct q-ary PRS ?

- change the primitive root mod p
- example (p=13, q=3)
  - using $\mu = 2, 6, 7, 11 = 2^1, 2^5, 2^{11}, 2^7$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s_1(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0
$s_5(n)$	0	0	2	2	1	0	1	1	0	1	2	2	0
$s_{11}(n)$	0	0	2	2	1	0	1	1	0	1	2	2	0
$s_7(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0

  - They are not all distinct!

Answer - Characterization

- Theorem 2
  - μ : a primitive root mod p
  - $\{s_i(n)\}$ and $\{s_j(n)\}$: q-ary PRS using μ^i and μ^j, respectively

  THEN $\exists v$ (mod q) such that $s_i(n) \equiv v \cdot s_j(n)$ (mod q), $\forall n$,

  where v is a solution to $j \equiv iv$ (mod p-1).

- Theorem 3
  - Denote by U_n the multiplicative group of integers mod n
  - p = an odd prime, q = a divisor of p-1

  THEN $U_{p\text{-}1} \equiv U_q$ (mod q)

- Corollary 1
  - The number of all the distinct q-ary PRS of period p is $\Phi(q)$.

Crosscorrelation of q-ary PRS

- Crosscorrelation between two q-ary sequences $\{s_1(n)\}$ and $\{s_2(n)\}$ of period p

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

- Theorem 4

  Two distinct q-ary PRS $\{s_1(n)\}$ and $\{s_2(n)\}$ of period p have:

$$\left|C_{s_1,s_2}(\tau)\right| \le \sqrt{p} + 2$$

Now, we have a sequence set with

- $\Phi(q)$ distinct PRS's of period p
- autocorrelation ≤ 3
- crosscorrelation $\le \sqrt{p}+2$

Interesting Observation

- Corollary 2 (2-level crosscorrelation)
  - p : an odd prime
  - q : a divisor of p-1
  - When $p \equiv q+1 \pmod{2q}$ and q even, consider a q-ary PRS $\{s(n)\}$.

For two distinct PRS $\{k_1 s(n)\}$ and $\{k_2 s(n)\}$ with $k_1 + k_2 \equiv 0 \pmod{q}$,

$$\left|C_{k_1 s, k_2 s}(\tau)\right| = \begin{cases} 1, & \tau = 0 \\ \sqrt{p}, & \tau \neq 0 \end{cases}$$

How good ?

- Welch's bound('74, Welch)
  - Periodic correlation bound of a signal set **S** with M signals of length L

$$C_{\max} \geq \sqrt{\frac{L^2(M-1)}{ML-1}}$$

  - $C_{\max} = \max\{R_{\max}^{\mathbf{a}}, C_{\max}^{\mathbf{a},\mathbf{b}} \mid \mathbf{a},\mathbf{b}(\neq \mathbf{a}) \in \mathbf{S}\}$

- Comparison with Welch's bound in the PRS's set

$$\sqrt{p} + 2 = C_{\max} \geq \sqrt{\frac{p^2(\phi(q)-1)}{p\phi(q)-1}} \approx \sqrt{p} \qquad (@\ p >> 1,\ \phi(q) >> 1)$$

Decimation of q-ary PRS

- Example (p=13, q=3, μ = 2)
  - Ternary sequences obtained by d-decimation of PRS of period 13

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(dn)\|_{d\in C_0}$	0	0	1	1	2	0	2	2	0	2	1	1	0
$s(dn)\|_{d\in C_1}$	0	1	2	2	0	1	0	0	1	0	2	2	1
$s(dn)\|_{d\in C_2}$	0	2	0	0	1	2	1	1	2	1	0	0	2

  - If $d_i, d_j \in C_k$, then $s(d_i n) = s(d_j n), \quad \forall n$
  - If $d_i \in C_k,\ d_j \in C_{l(\neq k)}$, then $s(d_i n) - s(d_j n) = k - l, \quad \forall n(\neq 0)$
  - The number of all the distinct decimations of a q-ary PRS is q.

    (They are not in general PRS.)

Crosscorrelation of two different decimation groups – VERY GOOD

- Theorem 5
  - $\{s(n)\}$: a q-ary PRS of period p
  - $D(s(n))$: set of all the decimations of $\{s(n)\}$
  - $D(ks(n))$: set of all the decimations of $\{ks(n)\}$
  - Crosscorrelation of

    any $\{s_1(n)\}=\{s(d_1 n)\} \in D(s(n))$ and

    any $\{s_2(n)\}=\{ks(d_2 n)\} \in D(ks(n))$:

$$\left| C_{s_1,s_2}(\tau) \right| \leq \sqrt{p} + 2$$

Crosscorrelation inside a single decimation group – NOT GOOD

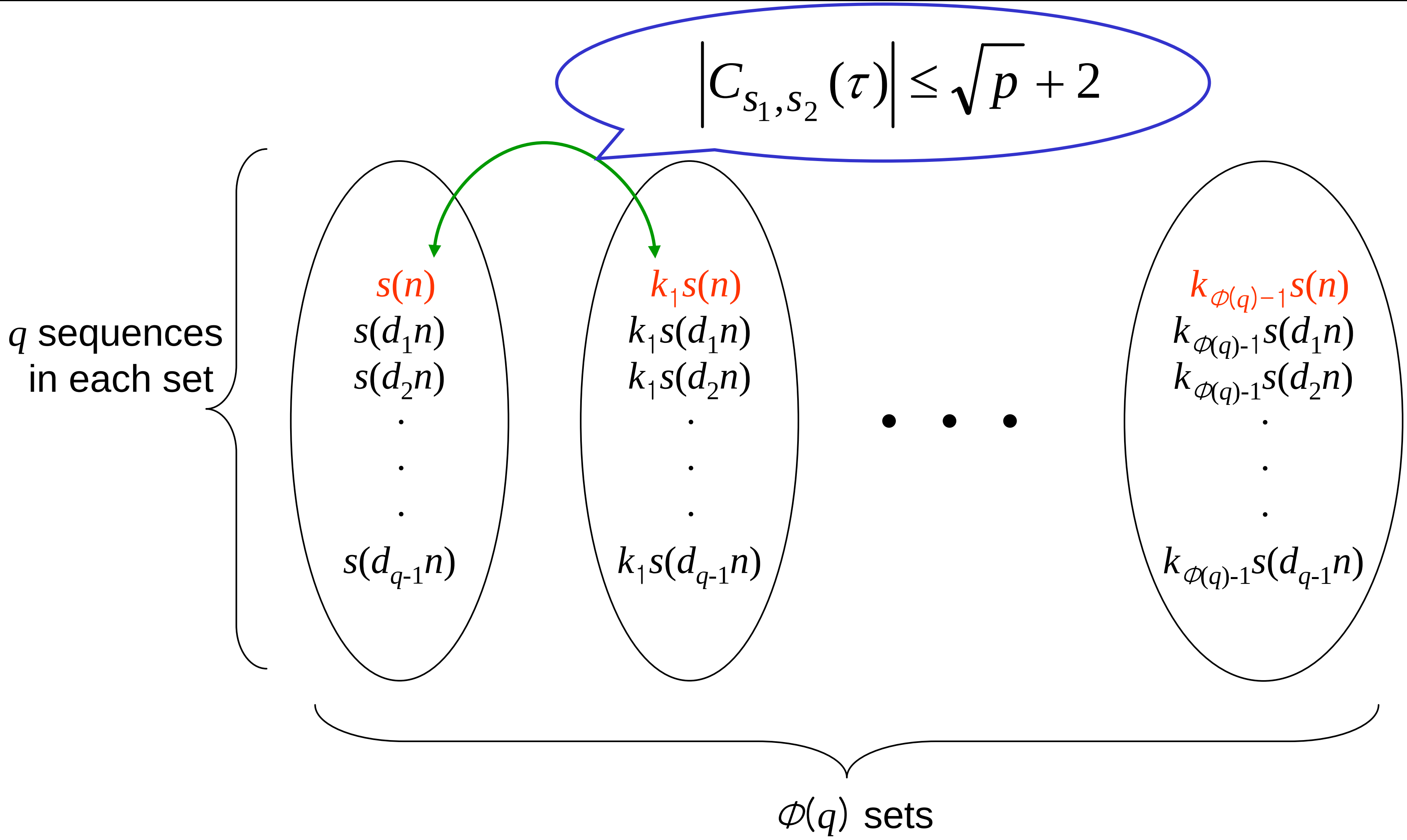
- Theorem 6
  - $\{s(n)\}$: a q-ary PRS of period p
  - $D(s(n))$: a set of all decimations of $\{s(n)\}$
  - Crosscorrelation of any two distinct q-ary sequences $\{s_1(n)\}=\{s(d_1 n)\} \in D(s(n))$ and $\{s_2(n)\}=\{s(d_2 n)\} \in D(s(n))$ of period p

$$C_{s_1,s_2}(\tau) = \begin{cases} 1+(p-1)w^{-m}, & \text{if } \tau = 0 \\ w^{s(\tau)}[1-w^{-m}]+w^{-m}R_s(\tau), & \text{if } \tau \neq 0 \end{cases}$$

where m is an integer satisfying $\frac{d_2}{d_1} \in C_{m\neq 0}$.

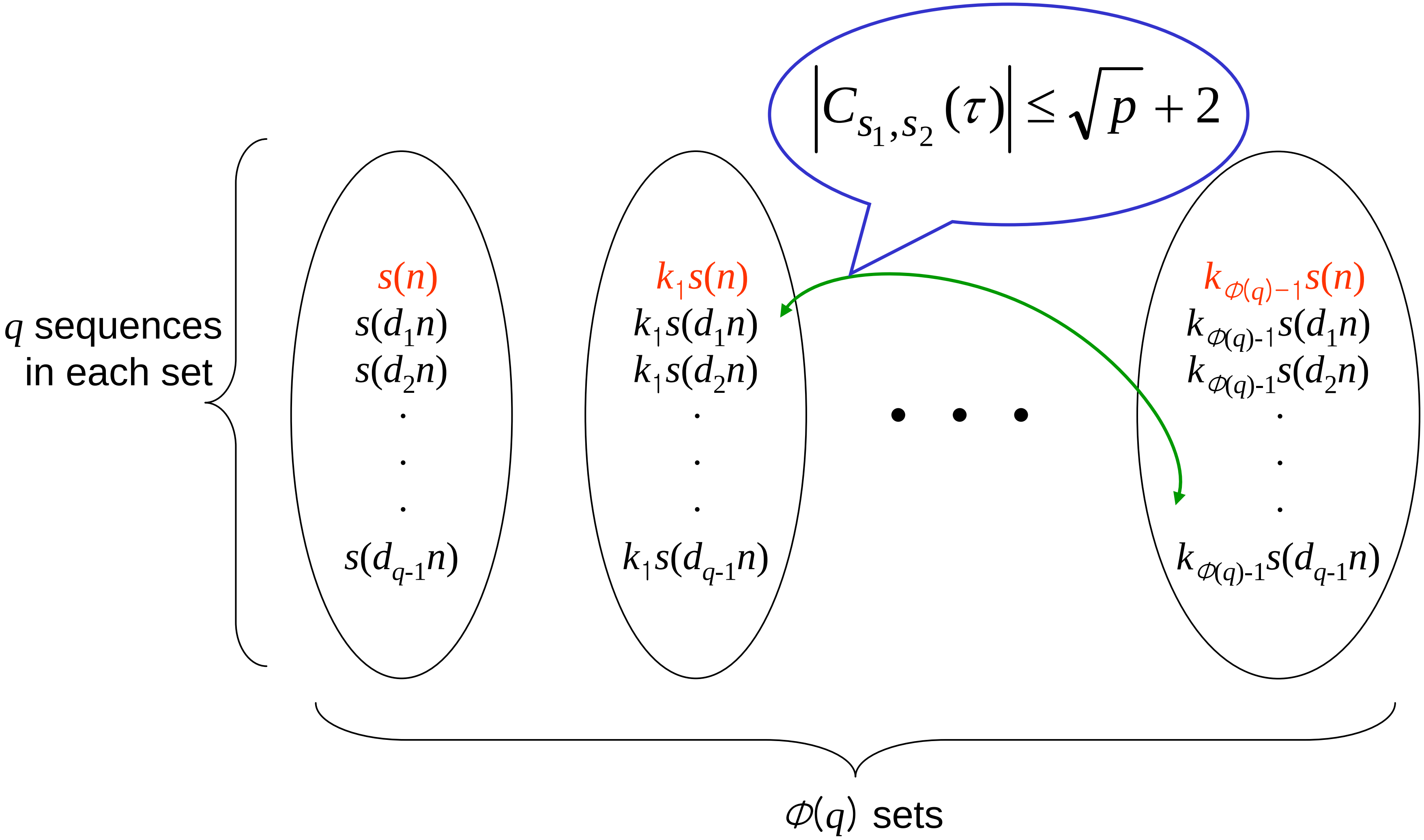
$$\Rightarrow \quad \left|C_{s_1,s_2}(\tau)\right| = \begin{cases} \approx p, & \tau = 0 \\ \leq 5, & \tau \neq 0 \end{cases}$$

Big Picture

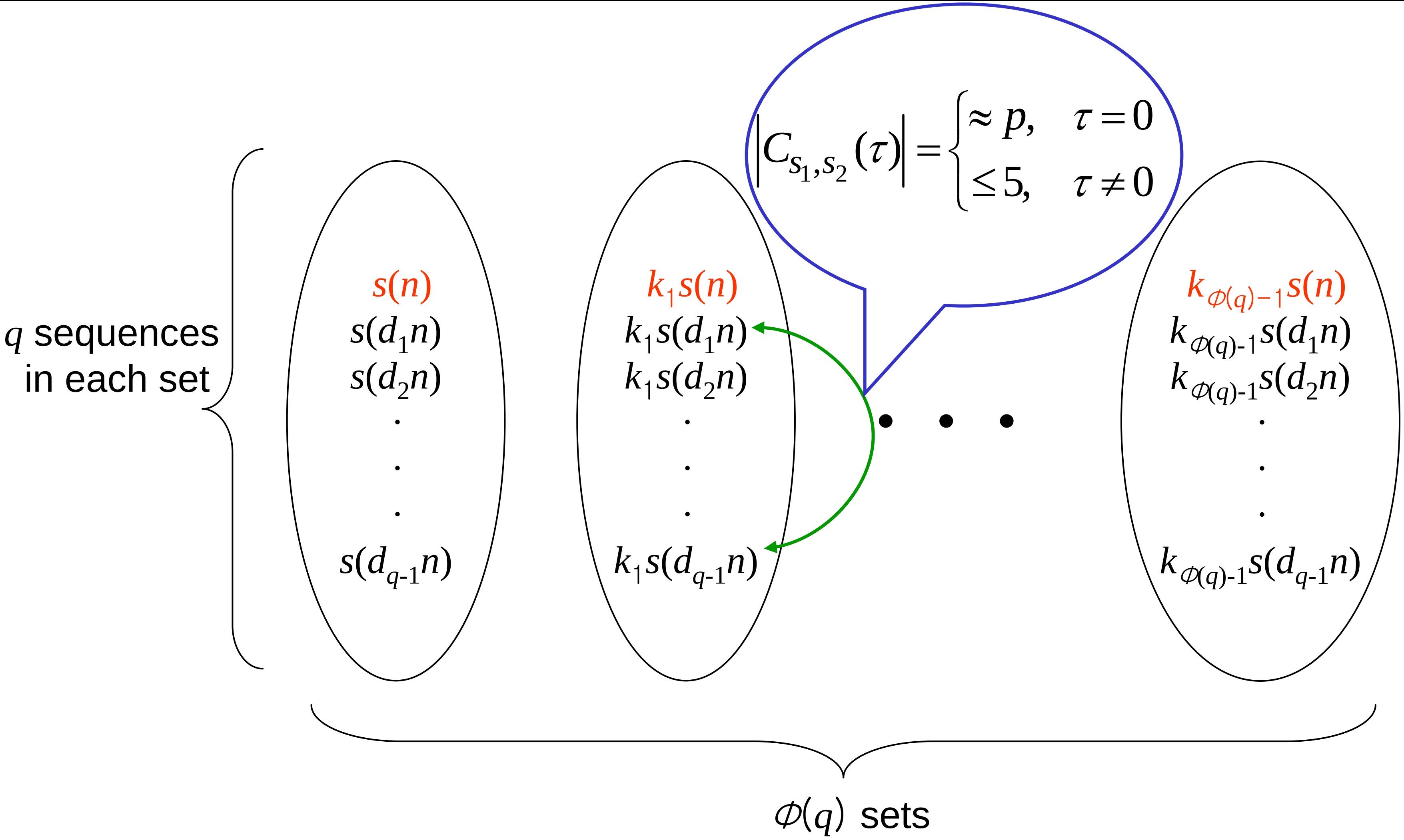


$\left|C_{s_1,s_2}(\tau)\right| \le \sqrt{p}+2$
q sequences in each set
$s(n)$
$s(d_1 n)$
$s(d_2 n)$
$s(d_{q-1} n)$
$k_1 s(n)$
$k_1 s(d_1 n)$
$k_1 s(d_2 n)$
$k_1 s(d_{q-1} n)$
$k_{\Phi(q)-1} s(n)$
$k_{\Phi(q)-1} s(d_1 n)$
$k_{\Phi(q)-1} s(d_2 n)$
$k_{\Phi(q)-1} s(d_{q-1} n)$
$\Phi(q)$ sets

Big Picture


$\left|C_{s_1,s_2}(\tau)\right| \le \sqrt{p} + 2$
q sequences in each set
$s(n)$
$s(d_1 n)$
$s(d_2 n)$
$s(d_{q-1} n)$
$k_1 s(n)$
$k_1 s(d_1 n)$
$k_1 s(d_2 n)$
$k_1 s(d_{q-1} n)$
$k_{\Phi(q)-1} s(n)$
$k_{\Phi(q)-1} s(d_1 n)$
$k_{\Phi(q)-1} s(d_2 n)$
$k_{\Phi(q)-1} s(d_{q-1} n)$
$\Phi(q)$ sets

Big Picture


$|C_{s_1,s_2}(\tau)| = \begin{cases} \approx p, & \tau = 0 \\ \leq 5, & \tau \neq 0 \end{cases}$
q sequences in each set
$s(n)$
$s(d_1 n)$
$s(d_2 n)$
$s(d_{q-1} n)$
$k_1 s(n)$
$k_1 s(d_1 n)$
$k_1 s(d_2 n)$
$k_1 s(d_{q-1} n)$
$k_{\Phi(q)-1} s(n)$
$k_{\Phi(q)-1} s(d_1 n)$
$k_{\Phi(q)-1} s(d_2 n)$
$k_{\Phi(q)-1} s(d_{q-1} n)$
$\Phi(q)$ sets

Comments

- There is another type of q-ary sequence $\{t(n)\}$ of length p^m-1, known as Sidel'nikov sequence (or Lempel-Cohn-Eastman sequence), where q is a divisor of p^m-1 and m is a positive integer.

- (IT-submitted)

  Crosscorrelation of a set which consists of q-ary Sidel'nikov sequence $\{t(n)\}$ of length p^m-1 and its constant multiple sequences

$$\left|C_{t_1,t_2}(\tau)\right| \le \sqrt{p^m} + 3$$