

완전한 자기상관을 가지는 페르마-뮈트 수열

CSDI
박기현, 송홍엽
연세대학교, 통신 신호 설계 연구실

2015 / 06 / 25
2015 한국통신학회 하계종합학술발표회



페르마 몫 수열



▶ 페르마 몫 (Fermat-quotient)

$$Q(t) \triangleq \frac{t^{p-1} - 1}{p}$$

- ▶ $t \not\equiv 0 \pmod{p}$ 에서 항상 정수 (페르마의 소정리)
- ▶ p 는 홀수 소수

▶ 페르마 몫 수열 $\mathbf{q} = (q(0), q(1), \dots)$

$$q(t) \triangleq \begin{cases} Q(t) \bmod p & \text{if } t \not\equiv 0 \pmod{p} \\ 0 & \text{otherwise} \end{cases}$$

- ▶ p 진 수열, 주기 p^2





페르마 몫 수열의 예



- ▶ $p = 5, \mathbf{q} = (0, 0, 3, 1, 1, 0, 4, 0, 4, 2, 0, 3, 2, 2, 3, 0, 2, 4, 0, 4, 0, 1, 1, 3, 0)$

$$\mathbf{q} = \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$$

$p \times p$
Array form

- ▶ $p = 7, \mathbf{q} = (0, 0, 2, 6, 4, 6, 1, 0, 6, 5, 1, 2, 3, 2, 0, 5, 1, 3, 0, 0, 3, 0, 4, 4, 5, 5, 4, 4, 0, 3, 0, 0, 3, 1, 5, 0, 2, 3, 2, 1, 5, 6, 0, 1, 6, 4, 6, 2, 0)$

$$\mathbf{q} = \begin{bmatrix} 0 & 0 & 2 & 6 & 4 & 6 & 1 \\ 0 & 6 & 5 & 1 & 2 & 3 & 2 \\ 0 & 5 & 1 & 3 & 0 & 0 & 3 \\ 0 & 4 & 4 & 5 & 5 & 4 & 4 \\ 0 & 3 & 0 & 0 & 3 & 1 & 5 \\ 0 & 2 & 3 & 2 & 1 & 5 & 6 \\ 0 & 1 & 6 & 4 & 6 & 2 & 0 \end{bmatrix}$$





Main Contribution



- ▶ 페르마 몫 수열이 완전한 자기상관특성을 가짐을 확인
 - ▶ $\tau = 0$ 이 아닌 모든 τ 에서 자기상관값이 0
- ▶ 페르마 몫 수열을 포함하는 새로운 최적의 시퀀스 집합을 제안
 - ▶ p -ary, 주기 p^2 인 수열 $p - 1$ 개로 이루어진 집합
 - ▶ 집합내 모든 수열이 완전한 자기상관특성을 가짐
 - ▶ 집합내 수열간 상호상관특성이 이론적 최적값을 가짐



수열의 복소 상관값

- ▶ p -ary, 주기 N , 두 개의 정수로 표현된 다중위상수열 (polyphase sequence)

$\mathbf{u} = (u(0), u(1), \dots)$ and $\mathbf{v} = (v(0), v(1), \dots)$

상관값:

$$C(\mathbf{u}, \mathbf{v}, \tau) \triangleq \sum_{t=0}^{N-1} \omega^{u(t+\tau) - v(t)}$$

$$\omega = e^{j\frac{2\pi}{p}}$$

(복소 p 제곱근)

- ▶ $\mathbf{u} = \mathbf{v}$ 일 때, $C(\mathbf{u}, \mathbf{u}, \tau) = C(\mathbf{u}, \tau)$ 로 정의하며 이를 수열 $\mathbf{u}$ 의 자기상관값이라고 함

- ▶ 수열 s 가 모든 $\tau \neq 0 \bmod N$ 에서

$$C(s, \tau) = 0$$

을 만족할 때, 수열 s 를 완전수열 (perfect sequence)이라고 정의

정리 1-1:

페르마 몫 수열 q 는 완전수열



Sarwate Bound



- ▶ 각 수열의 길이가 N 인 사이즈 K 의 수열집합이 주어지면
- ▶ C_A : 자기상관값의 최대값
- ▶ C_C : 상호상관값의 최대값
- ▶ Bound (Sarwate, 1979):

$$\frac{C_C^2}{N} + \frac{N-1}{N(K-1)} \frac{C_A^2}{N} \geq 1$$

- ▶ 완전수열의 집합일 경우 $C_A = 0$ 이므로:

$$C_C \geq \sqrt{N}$$



- ▶ 수열쌍 $\mathbf{u}, \mathbf{v}$ 가 다음 조건을 만족시, 최적수열쌍(optimum pair)으로 정의
 - ▶ $\mathbf{u}, \mathbf{v}$ 는 완전수열
 - ▶ 상호상관값이 Sarwate bound 값에 도달, 즉:

$$\max_{0 \leq \tau < N} |C(\mathbf{u}, \mathbf{v}, \tau)| = \sqrt{N}$$

최적수열집합

- ▶ $\mathbf{F} = \{\mathbf{s}_1, \mathbf{s}_2, \mathbf{s}_3, \dots, \mathbf{s}_M\}$ 안의 모든 수열쌍이 최적수열쌍일 경우, $\mathcal{F}$ 를 최적수열집합(optimum family)으로 정의

정리 1-2:

q 가 페르마 몫 수열일 때

$F = \{q, 2q, \dots, (p-1)q\}$ 는 **최적수열집합**

▶ $s = mq$ 는 아래와 같이 정의

$$s(i) \equiv mq(i) \pmod{p}$$

▶ 예제: $p = 5$, $\mathcal{F}(q) = \{q, 2q, 3q, 4q\}$

▶ 최적수열집합, 크기 4, p 진, 주기 p^2

▶ 집합내 수열의 상호상관값: $5(\sqrt{p^2})$

$$q = (0, 0, 3, 1, 1, 0, 4, 0, 4, 2, 0, 3, 2, 2, 3, 0, 2, 4, 0, 4, 0, 1, 1, 3, 0)$$

$$2q = (0, 0, 1, 2, 2, 0, 3, 0, 3, 4, 0, 1, 4, 4, 1, 0, 4, 3, 0, 3, 0, 2, 2, 1, 0)$$

$$3q = (0, 0, 4, 3, 3, 0, 2, 0, 2, 1, 0, 4, 1, 1, 4, 0, 1, 2, 0, 2, 0, 3, 3, 4, 0)$$

$$4q = (0, 0, 2, 4, 4, 0, 1, 0, 1, 3, 0, 2, 3, 3, 2, 0, 3, 1, 0, 1, 0, 4, 4, 2, 0)$$

모두
완전수열



정리 2:

q 가 페르마 몫 수열이고

$a_1, a_2, a_3, \dots, a_{p-1}$ 이 각각 임의의 주기 p 인 p 진 수열일 때

$$F_A = \{q + a_1, 2q + a_2, \dots, (p-1)q + a_{p-1}\}$$

은 최적수열집합

▶ $s = q + a$ 는 아래와 같이 정의

$$s(i) \equiv q(i) + a(i) \pmod{p}$$

▶ 예제: $a = (0,0,1,3,3)$ 인 경우

$$q = (0,0,3,1,1,0,4,0,4,2,0,3,2,2,3,0,2,4,0,4,0,1,1,3,0)$$

$$q + a = (0,0,4,4,4,0,4,1,2,0,0,3,3,0,1,0,2,0,3,2,0,1,2,1,3)$$

	$m = 1$ $a = (0,0,0,0,0)$	$m = 2$ $a = (0,0,1,0,0)$	$m = 3$ $a = (2,0,0,3,0)$	$m = 4$ $a = (0,1,2,3,4)$
mq	$\begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 & 2 & 2 \\ 0 & 3 & 0 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \\ 0 & 4 & 3 & 0 & 3 \\ 0 & 2 & 2 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 4 & 3 & 3 \\ 0 & 2 & 0 & 2 & 1 \\ 0 & 4 & 1 & 1 & 4 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 3 & 3 & 4 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 2 & 4 & 4 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 2 & 3 & 3 & 2 \\ 0 & 3 & 1 & 0 & 1 \\ 0 & 4 & 4 & 2 & 0 \end{bmatrix}$
$q + a$	$\begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 4 & 1 & 1 \\ 0 & 4 & 1 & 4 & 2 \\ 0 & 3 & 3 & 2 & 3 \\ 0 & 2 & 0 & 0 & 4 \\ 0 & 1 & 2 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 & 3 & 4 & 1 \\ 2 & 4 & 0 & 2 & 2 \\ 2 & 3 & 2 & 0 & 3 \\ 2 & 2 & 4 & 3 & 4 \\ 2 & 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 2 & 2 & 1 \\ 0 & 4 & 4 & 0 & 2 \\ 0 & 3 & 1 & 3 & 3 \\ 0 & 2 & 3 & 1 & 4 \end{bmatrix}$
$mq + a$	$\begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 2 & 2 & 2 \\ 0 & 3 & 1 & 3 & 4 \\ 0 & 1 & 0 & 4 & 1 \\ 0 & 4 & 4 & 0 & 3 \\ 0 & 2 & 3 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 & 4 & 1 & 3 \\ 2 & 2 & 0 & 0 & 1 \\ 2 & 4 & 1 & 4 & 4 \\ 2 & 1 & 2 & 3 & 2 \\ 2 & 3 & 3 & 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 4 & 2 & 3 \\ 0 & 2 & 2 & 4 & 2 \\ 0 & 3 & 0 & 1 & 1 \\ 0 & 4 & 3 & 3 & 0 \\ 0 & 0 & 1 & 0 & 4 \end{bmatrix}$



: 최적수열집합