# 서로 다른 3개의 m-시퀀스의 합으로 표현된 4레벨 자기상관 특성과 균형 특성을 갖는 시퀀스들의 전수조사 결과 분석

김강산, 송민규, 송홍엽

연세대학교

제27회 통신정보 합동학술대회

## ▪ 연구 개요 및 목적

- 서로 다른 2개의 m-시퀀스의 합으로 표현된 시퀀스의 특성: 골드(Gold) 시퀀스, 카자미(Kasami) 시퀀스 등에서 많은 연구가 진행됨
- 본 논문은 $2^7 - 1$ 길이까지의 4레벨 자기상관 특성과 균형특성을 갖는 시퀀스의 전수조사를 통해 서로 다른 3개의 m-시퀀스의 합으로 표현된 시퀀스의 특성을 파악하려 함

## ▪ 사전 지식

- m-시퀀스는 트레이스 함수(Trace Function)로 표현됨
- 길이 $2^n - 1$의 서로 다른 3개의 m-시퀀스 합은 데시메이션(Decimation)과 시프트(Shift)관점에서 일반성을 잃지 않고 다음과 같이 표현할 수 있음

$$S(t) = Tr(\alpha^t) + Tr(\alpha^{at+i}) + Tr(\alpha^{bt+j})$$

(a,b,i,j는 $0 \sim 2^n - 1$ 의 정수 )

## ▪ 명명법

- (a, b)조합: 주어진 $a, b$에 대해 $Tr(\alpha^t) + Tr(\alpha^{at+i}) + Tr(\alpha^{bt+j})$로 나타낼 수 있는 4레벨 자기상관 특성과 균형특성을 갖는 시퀀스들의 집합

## ▪ (a,-1)조합에 따른 |(a,-1)조합| 의 조사

| n=5 | | n=6 | | n=7 | |
|---|---|---|---|---|---|
| (a,-1)조합 개수 | \|(a,-1)조합\| | (a,-1)조합 개수 | \|(a,-1)조합\| | (a,-1)조합 개수 | \|(a,-1)조합\| |
| 2 | 각, 5 | 4 | 각, 0 | 8 | 각, 0 |

- n=5, 6, 7에 대해 각각 모든 |(a,-1)조합|은 동일함
- (a,-1)조합의 시퀀스들은 $Tr(\alpha^t) + Tr(\alpha^{at+i}) + Tr(\alpha^{-t+j})$ 으로 표현됨

## ▪ 분석

- n=5, 6, 7에 대해 |(a,-1)조합| 은 각각 모두 동일하고 모든|(a,b)조합|에 대해 최솟값이 나옴
- 특히 n=6,7인 경우 이 값이 0이 됨
- 이는 특정 n 이상에서 |(a,-1)조합|=0이라는 가설을 세울 수 있음

- **|(a,b)조합|에 따른 (a,b)조합의 개수**

| n=5 | | n=6 | | n=7 | |
|---|---|---|---|---|---|
| **\|(a,b)조합\|** | (a,b) 조합 개수 | \|(a,b)조합\| | (a,b) 조합 개수 | \|(a,b)조합\| | (a,b)조합 개수 |
| **5** | 2 | 0 | 7 | 0 | 35 |
| 426 ≤ | 2 | 78≤ | 5 | 1 | 5 |
| | | | | 2927≤ | 6 |

  - n=5, 6, 7에서 데시메이션과 시프트 관점에서 중복되지 않도록 하는 (a,b) 조합의 개수는 각각 4개, 12개, 46개임

- **분석**
  - |(a,b)조합|의 차이가 많이 나는 부분이 생김(5→426), (0 →78) 등등
  - n=6. n=7의 경우 원소의 개수가 0이 되는 (a,b)조합이 있음
  - 이는 자기상관 특성이 (a,b)조합과 관련이 있음을 의미
  - 특정 (a,b)조합에 대해 4레벨 자기상관특성과 균형특성을 갖는 시퀀스의 존재성 및 무존재성을 생각할 수 있음

- **결론**
  - 앞의 전수조사 결과를 바탕으로 트레이스의 데시메이션 조합에 따라 자기상관특성이 바뀜을 추측할 수 있음.
  - 특정 (a,b)조합에 대해 시퀀스의 무존재성을 생각해 볼 수 있음
  - 전수조사 이외의 엄밀한 분석을 통한 추가연구가 필요함

- **향후 연구 계획**
  - n이상에서 |(a,b)조합|=0이 됨을 증명
- **참고문헌**


*[1]* Golomb, Solomon W., and Guang Gong. *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005

[2] Song, Hong-Yeop. "Feedback shift register sequences." *Encyclopedia of Telecommunications* 2003.

[3] Cinteza, M., I. Marghescu, and T. Radulescu. "Design of PN Sequence Families with Bounded Correlation Properties, Using Genetic Algorithms." *Computer as a Tool, 2005. EUROCON 2005. The International Conference on*. Vol. 2. IEEE, 2005.