큰 집합과 알파벳 개수를 가지는 단일 일치 수열군의 설계

김서영, 박서은, 이아영, 박시연, 정진호*
울산대학교

*jinho@ulsan.ac.kr

Design of One-Coincidence Sequence Sets with Large Family and Alphabet Sizes

Seoyoung Kim, Seo-Eun Park, Ayoung Lee, Si-Yeon Pak, Jin-Ho Chung*
University of Ulsan

요 약

본 논문에서는 큰 알파벳 개수를 가지는 단일 일치 수열군에 대해서 확장된 개수의 수열을 가지는 새로운 설계 방법을 제시한다. 길이에 비해서 큰 알파벳 개수를 가지는 단일 일치 수열군에 대한 연구 결과는 그 동안 많지 않았고, 알파벳 개수와 길이에 비해서 수열의 개수가 많지 않았다. 본 논문에서는 특정 길이에 대해서 확장된 집합 크기를 가지는 단일 일치 수열군의 설계 방법을 제시한다.

Ⅰ. 서 론

주파수 도약 다중 접속(Frequency-Hopping Multiple Access, FHMA) 시스템은 효율적인 주파수 도약 확산 스펙트럼(Frequency-Hopping Spread Spectrum, FHS) 설계를 통해 다양한 현대 통신 응용에서 핵심적인 역할을 한다. 예를 들어, 블루투스(Bluetooth) 통신에서는 인접 기기가 동일한 주파수 대역을 사용할 때 발생하는 간섭을 줄이기 위해 FHS 가 사용된다. 군사 통신 및 보안 전송에서도 FHS 는 도청과 전파 방해(jamming)를 방지하여 전송되는 정보의 기밀성(confidentiality)과 무결성(integrity)을 보장한다. 또한, 레이더(Radar) 시스템에서는 주파수 도약을 활용하여 탐지 및 대응 조치를 회피함으로써 복잡한 환경에서 신호의 신뢰성을 높인다. 이처럼 FHS 는 다양한 분야에서 견고한 통신 솔루션을 제공하며, FHMA 시스템 개발의 핵심 요소로 자리잡고 있다 [1-3].

이러한 FHS 시스템의 성능은 낮은 상호 상관(cross-correlation) 특성을 가진 FHS 집합의 설계에 크게 의존한다. 다중 사용자의 신호 간 간섭을 최소화하기 위한 요구를 충족시키기 위해 다양한 설계 방법들이 제시되었다. 이러한 구성 방법들은 Peng-Fan 경계(와 같은 이론적 경계값을 만족하며, 최적의 FHS 집합을 생성하는 것을 목표로 한다. 기존 연구들에서는 주로 주파수 집합의 크기보다 수열의 길이가 같거나 큰 경우가 많이 다루어져 왔다 [3-5]. 하지만 주파수 도약 시스템의 실제 운용 상황과 파라미터에 따라 주파수 집합의 크기가 수열의 길이에 비해 큰 경우에 대한 설계 역시 필요하다. 이는 더 넓은 주파수 자원을 활용하여 시스템의 유연성을 확보하고 충돌 확률을 더욱 감소시킬 수 있는 새로운 설계 패러다임의 필요성을 시사한다.

본 연구에서는 특정 길이에 대해서 기존 결과들에 비해서 확장된 수열 개수를 가지는 단일 일치 수열군의 설계 방법을 제시한다. 기존 설계 방법에 비해서 소수 배만큼 많은 수열군이면서 상관값은 동일하게 1 을 유지하는 단일 일치 수열군을 생성한다.

Ⅱ. 본론

두 개의 주파수 도약 수열 X 와 Y 의 해밍 상관 값은 다음 수식으로 정의된다:

$$H_{X,Y}(\tau) = \sum_{t=0}^{N-1} h[X(t), X(t+\tau \bmod N)]$$

단일 일치 수열군은 집합에 속한 모든 수열군이 자기 상관 값은 0, 서로 다른 수열끼리의 최대 상호 상관 값은 1 이하를 만족하는 수열군이다.

단일 일치 수열군의 설계는 주로 주파수의 개수와 수열의 길이가 비슷한 경우에 대해서 많이 이루어져왔으나, 몇몇 논문에서는 알파벳이 더 큰 경우에도 연구 결과가 발표되어 왔다 [6-8].

하지만 이러한 경우에 수열의 개수가 크지 않다는 단점이 있었다. [8]에서는 길이가 5 이면서 수열군의 개수가 20 인 단일 일치 수열군이 제시되었다. 해당 수열군은 Peng-Fan 경계에 대해서는 최적이지만, 수열군의 크기에 있어서는 알파벳 크기의 장점을 모두 살리지 못했다. 다음과 같이 길이가 5 인 100 개의 단일 일치 수열군을 생성할 수 있다.

0,5,10,15,20	1,6,11,16,21	2,7,12,17,22	3,8,13,18,23	4,9,14,19,24
0,6,12,18,24	1,7,13,19,20	2,8,14,15,21	3,9,10,16,22	4,5,11,17,23
0,7,14,16,23	1,8,10,17,24	2,9,11,18,20	3,5,12,19,21	4,6,13,15,22
0,8,11,19,22	1,9,12,15,23	2,5,13,16,24	3,6,14,17,20	4,7,10,18,21
0,9,13,17,21	1,5,14,18,22	2,6,10,19,23	3,7,11,15,24	4,8,12,16,20
0,10,20,5,15	1,11,21,6,16	2,12,22,7,17	3,13,23,8,18	4,14,24,9,19
0,12,24,6,18	1,13,20,7,19	2,14,21,8,15	3,10,22,9,16	4,11,23,5,17
0,14,23,7,16	1,10,24,8,17	2,11,20,9,18	3,12,21,5,19	4,13,22,6,15
0,11,22,8,19	1,12,23,9,15	2,13,24,5,16	3,14,20,6,17	4,10,21,7,18
0,13,21,9,17	1,14,22,5,18	2,10,23,6,19	3,11,24,7,15	4,12,20,8,16
0,15,5,20,10	1,16,6,21,11	2,17,7,22,12	3,18,8,23,13	4,19,9,24,14
0,18,6,24,12	1,19,7,20,13	2,15,8,21,14	3,16,9,22,10	4,17,5,23,11
0,16,7,23,14	1,17,8,24,10	2,18,9,20,11	3,19,5,21,12	4,15,6,22,13
0,19,8,22,11	1,15,9,23,12	2,16,5,24,13	3,17,6,20,14	4,18,7,21,10
0,17,9,21,13	1,18,5,22,14	2,19,6,23,10	3,15,7,24,11	4,16,8,20,12
0,20,15,10,5	1,21,16,11,6	2,22,17,12,7	3,23,18,13,8	4,24,19,14,9
0,24,18,12,6	1,20,19,13,7	2,21,15,14,8	3,22,16,10,9	4,23,17,11,5
0,23,16,14,7	1,24,17,10,8	2,20,18,11,9	3,21,19,12,5	4,22,15,13,6
0,22,19,11,8	1,23,15,12,9	2,24,16,13,5	3,20,17,14,6	4,21,18,10,7
0,21,17,13,9	1,22,18,14,5	2,23,19,10,6	3,24,15,11,7	4,20,16,12,8

각 수열들끼리의 상호상관값이 최대 1 이 됨을 확인할 수 있고, 하나의 수열 안에서 반복되는 주파수가 없기 때문에 자기 상관값도 0 임을 알 수 있다.

Ⅲ. 결론

본 연구에서는 기존에 설계된 단일 일치 수열군에 비해서 더 큰 사이즈를 가지는 단일 일치 수열군을 길이 5 에 대해서 제시하였다. 설계된 수열은 기존 수열군에 비해 5 배의 수열 개수를 가진다. 이를 일반적인 길이로 확장하고, 더 큰 수열군의 크기로 확장하는 것이 다음 연구 주제가 될 것이다.

ACKNOWLEDGMENT

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT). (No. RS-2023-00279714), and in part by the "Regional Innovation System & Education (RISE)" through the Ulsan RISE Center, funded by the Ministry of Education (MOE) and the Ulsan Metropolitan City, Republic of Korea.(2025-RISE-07-001).

참 고 문 헌

[1] Sarwate, D. V. Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications. In Reed-Solomon Codes and Their Applications; Wicker, S. B., Bharagava, V. K., Eds.; IEEE Press: Piscataway, NJ, USA, 1994.

[2] Simon, M. K.; Omura J. K.; Scholtz, R. A.; Levitt, B. K. Spread Spectrum Communications Handbook.; McGraw-Hill: New York, USA, 2002.

[3] Fan, P.; Darnell M. Sequence Design for Communications Applications; Research Studies Press, John Wiley & Sons: London, UK, 1996.

[4] Chung, J.-H.; Han, Y. K.; Yang, K. New classes of optimal frequency-hopping sequences by interleaving techniques. IEEE Trans. Inf. Theory 2009, 55, pp. 5783-5791.

[5] Chung, J.-H.; Yang, K. A new class of balanced near-perfect nonlinear mappings and its application to sequence design. IEEE Trans. Inf. Theory 2013, 59, pp. 1090- 1097.

[6] Cao, Z.; Ge, G.; Miao, Y. Combinatorial characterizations of one-coincidence frequency-hopping sequences. Des. Codes Crypt. 2006, 41, 177- 184.

[7] Lee, T. H.; Jung, H. H.; Chung, J.-H. A new one-coincidence frequency-hopping sequence set of length p^2-p. In Proceedings of 2018 IEEE Information Theory Workshop, Guangzhou, China, 25-29, Nov. 2018.

[8] Chung, J.-H.; Ahn, D.; Kim, D. New Constructions of One-Coincidence Sequence Sets over Integer Rings. Mathematics 2024, 12, 3316.