짧고 효과적인 주파수 도약 수열 생성

준회원 김 영 준*, 김 대 선*, 종신회원 송 홍 엽*

Short and Efficient Frequency Hopping Codes

Young-Joon Kim*, Dae-Son Kim* ***Associate Members***, Hong-Yeop Song* ***Lifelong Member***

요 약

본 논문에서는 주파수 도약 시스템에 사용될 짧은 길이의 도약 수열의 생성법 세가지를 제안한다.

우선, 기존에 알려져 있는 한개 일치수열과 다상 멱 잉여류 수열의 생성법에 대해 설명하고, 한개 일치수열의 변형으로 얻어진 생성법 하나와 다상 멱 잉여류 수열을 이용한 방법 두개를 제안한다. 다상 멱 잉여류 수열에서 '최적 지움위치'를 지운 수열이 제안된 세가지 수열들 중에서 가장 좋은 상관특성을 가지고, 그 다음은 첫번째 위치 지운 수열, 한개 일치 수열의 변형 수열 순으로 상관특성이 좋음을 확인한다. 또한 이들 세 수열이 심볼이 균형성이 우수하고 쉽게 구현될 수 있음을 설명한다.

Key Words : frequency hopping, Hamming correlation, balance, power residue, optimal deletion

ABSTRACT

In this paper we propose three methods to generate short hopping sequences for the frequency hopping system. First, we explain the one coincidence set of sequences and the polyphase power residue seqences which have been known previously, and we suggest a method by modifying the one coincidence sequence and two methods by using the power residue sequences. We verify that the optimal position deleted-power residue sequences have the best Hamming autocorrelation property and the first position deleted-power residue sequences and the modified one coincidence sequences follows with respect to Hamming autocorrelation. We also explain that these sequences have the good balance property and can be implemented with low complexity.

Ⅰ. 서 론

주파수 도약은 대역 확산 신호 전송 방식에서 사용되는 기본적인 변조 방식중의 하나이다[1, 2]. 주파수 도약은 전파의 전송 도중에 주파수변경을 되풀이하는데 이는 인가되지 않은 간섭이나 통신 방해를 최소화하기 위해서이다. 주파수 도약 시스템은 중심 주파수를 도약 수열에 따라 변경하며 이는 주파수 합성기를 통해 이루어진다.

주파수 도약 시스템은 일반적으로 도약의 경향이 쉽게 노출되는 것을 방지하기 위해 도약 주파수의 개수에 비해 훨씬 긴 길이의 주기를 갖는 도약 수열을 사용한다. 그러므로 이러한 시스템에서 주파수 영역에서 충돌은 불가피하고, 충돌의 횟수는 종종 해밍 상관값으로 측정이 된다. 길이 n인 두개의 수열 $X=\mathrm{x(j)}$와 $Y=\mathrm{y(j)}$의 해밍 상관값 H_{XY}는 다음과 같이 정의된다[1, 3].

$$H_{X,Y}(\tau)=\sum_{j=0}^{n-1}h[x(j),y(j+\tau)],\quad 0\le\tau<n$$

여기서 $h[x,y]$는 x와 y가 같으면 1, 다르면 0이고,

※ 본 연구는 한국과학재단 특정기초연구(R01-2003-000-10330-0)지원으로 수행되었음.

* 연세대학교 전기전자공학과 부호및정보이론 연구실({yj.kim, ds.kim, hy.song}@coding.yonsei.ac.kr)

논문번호 : KICS2006-01-029, 접수일자 : 2006년 1월 16일, 최종논문접수일자 : 2006년 4월 12일

$j+\tau$는 mod n으로 계산된다. 상관값이 높다는 것은 충돌의 확률이 높음을 의미하므로 낮은 해밍 상관 특성을 갖는 도약 수열을 사용하는 것이 바람직하다[1]. 우수한 해밍 상관값과 더불어 도약 심벌의 균형성(balance) 또한 도약 수열의 설계에서 중요하게 고려되는 요소이다[3]. 왜냐하면 상대적으로 높은 빈도를 갖는 심벌에 대응되는 주파수는 악의적인 공격자나 간섭자의 공격대상이 될 수 있기 때문이다. 또 하나의 고려해야 할 중요한 인자는 선형복잡도이다. 선형복잡도는 주어진 수열을 생성할 수 있는 선형 귀환 쉬프트 레지스터의 최소 단수를 말하므로 이 값이 작으면 도약 수열의 길이가 길어도 짧은 단수의 선형 귀환 레지스터로 재합성할 수 있으므로 전체 도약수열이 쉽게 노출될 위험성이 있어서 선형복잡도는 가능한 크게 되도록 설계해야 한다[3, 4]. 다시 말해, 주파수 도약 시스템에 사용될 매우 긴 길이의 도약 수열은 많은 개수의 수열, 우수한 상관 특성, 심벌개수의 균형성, 높은 선형 복잡도 등의 특성을 필요로 한다.

하지만, 주파수 도약 시스템은 종종 긴 길이의 도약 수열뿐만 아니라 짧은 길이의 도약수열도 필요로 한다. 예를 들어 동기화 혹은 주파수 참조점을 찾기 위한 목적으로 한 개 혹은 적은 개수의 파일럿 신호를 필요로 하는 경우가 있다. 이러한 경우에 수열의 길이가 짧기 때문에 선형 복잡도는 고려의 대상이 아니고 우수한 해밍 자기 상관 특성, 심벌의 균형성을 만족하는 수열을 필요로 한다.

본 논문에서는 이처럼 짧은 길이의 도약 수열을 위한 생성 방법으로 기존의 한 개 일치(one coincidence) 수열[5]과 다상 멱 잉여류 수열[6]을 설명하고 이를 변형하여 도약 수열을 생성하는 방법을 제안한다. 그리고, 이들을 최대 해밍 자기 상관, 균형성 및 구현성의 관점에서 비교한다.

Ⅱ. 주요 생성법들

이 논문 전체에서 p는 임의의 소수, q는 $p-1$의 한 약수, μ는 Z_p의 한 원시근으로 용어를 통일한다.

2.1 기존의 생성법

2.1.1 한 개 일치수열[5].

한 개 일치수열 집합 $\boldsymbol{S}=\{S^j \mid 0 \le j \le p-1\}$은 주기가 $p-1$인 수열들 S^j로 구성되어 있다. 여기서 $S^j=\{s^j(n)\}$는 다음과 같이 정의된다.

$$s^j(n)=\mu^n+j, \quad n=0,1,\cdots,p-2 \tag{1}$$

여기서 연산 μ^n+j는 mod p에서 계산된다. μ가 원시근이므로, 순환군 $<\mu>$는 곱셈군 Z_p^*의 위수가 $p-1$인 부분군이다. 따라서 S^0는 Z_p^*의 모든 원소가 한번씩 나타나는 수열이며, S^j는 S^0의 원소 각각을 j만큼 mod p 연산에서 더한 수열이다.

2.1.2 다상 멱 잉여류 수열[6]

mod p연산을 하였을 때 영이 아닌 정수들을 q개의 코셋들 $C_i(0 \le i \le q-1)$로 분할하자. 여기서 C_0는 q차 멱 잉여류(mod p)집합이고, $i>0$에 대해서 $C_i=\mu^i \cdot C_0$이다.

길이 p이고 Z_q상의 값을 원소로 갖는 q진 수열 $T=\{t(n)\}$은 다음과 같이 정의된다.

$$t(n)=\begin{cases}0, & \text{if } n \equiv 0 \bmod p \\ k, & \text{if } n \in C_k \text{ for } k \in Z_q\end{cases} \tag{2}$$

예제 1. 다음은 길이 13인 삼진 수열 $T=\{t(n)\}$ ($p=13$, $q=3$ 그리고 $\mu=2$일 때)의 생성예제이다.

n	0	1	2	3	4	5	6	7	8	9	10	11
μ^n	1	2	4	8	3	6	12	11	9	5	10	7

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

그러므로 길이 13인 삼진 수열 $T=\{t(n)\}$는 다음과 같다.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$t(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0

2.2 제안한 생성법

2.2.1 한 개 일치수열의 변형 [생성법 1]

길이 $p-1$인 수열 $A=\{a(n)\}$은 다음과 같이 정의하자.

$$a(n)=\mu^n \bmod q, \ n=0,1,\cdots,p-2. \tag{2}$$

식 (2)에서 원시근의 연속적인 멱을 mod q가 아닌 mod p연산만을 하여 얻은 수열이 한 개 일치수열이므로, 수열 $A=\{a(n)\}$는 한 개 일치수열 집

합 $\mathcal{S}$의 $S^0=\{s(n)\}$과 $a(n)\equiv s^0(n) \bmod q$의 관계로 연관되어 있다.

예제 2. $p=13$, $q=3$ 그리고 $\mu=2$일 때, 길이 12인 삼진 수열 $A=\{a(n)\}$은 다음과 같다.

n	0	1	2	3	4	5	6	7	8	9	10	11
μ^n	1	2	4	8	3	6	12	11	9	5	10	7
$a(n)$	1	2	1	2	0	0	0	2	0	2	1	1

2.2 첫 번째 위치 지운 다상 멱 잉여류 수열 [생성법 2]

엄밀히 말해, q-진 다상 멱 잉여류 수열 $T=\{t(n)\}$는 영 심벌이 다른 심벌에 비해 한 번 더 나타나므로 균형성을 만족하지 못한다. 다시 말해 영 심벌은 $(p-1)/q+1$번 그리고 나머지 심벌들은 $(p-1)/q$번 나타난다. 균형성을 맞추기 위해 0번째 위치의 심볼 영을 지움으로써 길이 $p-1$인 q진 수열 $B=\{b(n)\}$을 얻을 수 있다. 심볼 영이 다른 위치에서도 나타나지만 굳이 첫 번째 위치의 영심볼을 지우는 것은 원시근의 연속적인 멱의 mod q 연산으로부터 얻어지는 다상 멱 잉여류 수열로부터 추가적인 복잡도의 증가 없이 간단히 구현하기 위해서이다.

예제 3. 아래는 $p=13$, $q=3$ 그리고 $\mu=2$일 때 길이 12인 삼진 수열 $B=\{b(n)\}$의 예이다.

n	1	2	3	4	5	6	7	8	9	10	11	12
$b(n)$	0	1	1	2	0	2	2	0	2	1	1	0

2.3 최적 위치 지운 다상 멱 잉여류 수열 [생성법 3]

q-진 수열 $A=\{a(n)\}$가 비록 균형성을 만족하고 다상 멱 잉여류 수열로부터 쉽게 만들 수 있지만, 해밍 자기 상관값은 다상 멱 잉여류 수열 $T=\{t(n)\}$에 비해 나쁘다. 만약 서로 다른 심벌간의 개수의 차이가 2보다 크지 않다면, 0번째 위치를 지우는 것을 고집할 필요가 없다. 여기서 길이 $p-1$인 q진 수열 $C=\{c(n)\}$의 생성 방법을 찾을 수 있다. 우선 주어진 다상 멱 잉여류 수열 $T=\{t(n)\}$에서 각각의 위치를 지움으로써 얻은 수열들의 집합 U를 먼저 생성하자. 그 다음 집합 H의 원소 수열들의 최대 해밍 자기 상관값을 구하면 분명히 집합 U에는 이들 최대값들 중에서 최소값을 주는 수열이 존재한다. 이처럼 최소값을 주는 지움 위치를 앞으로 '최적 지움 위치'라 하겠다. 최적 지움 위치를 지워서 얻은 수열이 $C=\{c(n)\}$이다.

예제 4. 아래는 $p=13$, $q=3$ 그리고 $\mu=2$일 때 길이 12인 삼진 수열 $C=\{c(n)\}$의 예이다.

먼저 집합 U를 생성한 후 각 위치를 지웠을 때 최대 해밍 자기 상관값 $H_{\max}$을 구하면 다음과 같다.

지움위치	0	1	2	3	4	5	6	7	8	9	10	11	12
$H_{\max}$	4	4	4	4	5	6	6	6	6	5	4	4	4

최적 지움 위치들 : { 0, 1, 2, 3, 10, 11, 12 }
최적 지움 위치로 2를 선택하면,

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$t(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0
$c(n)$	0	0	del	1	2	0	2	2	0	2	1	1	0

$C=\{c(n)\}$=0 0 1 2 0 2 2 0 2 1 1 0 이다.

Ⅲ. 제시된 네 가지 수열들의 비교

1974년 A. Lempel과 H. Geenberger는 길이가 n이고 사용하는 심벌집합 A의 크기가 $|A|=q$인 수열 X의 최대 해밍 자기 상관값에 대한 다음과 같은 하한을 유도하였다[7].

$$H(X)\geq \frac{(n-b)(n+b-q)}{q(n-1)} \tag{3}$$

여기서 $H(X)$는 불일치 위상에서 해밍 자기상관의 최대값, 즉, $\max_{0<\tau<n} H_{XX}(\tau)$ 이고, b는 n을 mod q 연산을 하여 얻은 음이 아닌 최소의 잉여류 값이다. 제안된 세 가지 수열들과 다상 멱 잉여류 수열의 해밍 상관값을 각각 비교하고 각각의 경우에 위의 하한 식 (3)과도 비교해보겠다. 여기서 한 개 일치 수열과의 비교를 하지 않은 것은 한 개 일치수열은 $p-1$진 수열이고, 위 네 종류의 수열은 q진 수열이기 때문이다. 그림 1은 p가 401이고 q가 20일 때 Ⅱ장에서 제안된 수열들과 다상 멱 잉여류 수열의 해밍 자기 상관값이다. 각 그래프에서 가로축은 시간천이 τ를 나타내며, 세로축은 τ에서의 해밍 상관

값 $H_X(\tau)$을 나타낸다. 이 경우 최대 해밍 자기 상관값의 하한 식 (3)을 계산하면 생성법 1, 2과 3에 대해서는 길이 n이 400, 심볼 수 $q=20$이므로 19.048이고, 길이 401의 20진 다상멱 잉여류 수열 열들에서 일치하는 위치의 개수를 세는 것이므로 에 대해서는 19.05이다. 해밍 상관값은 비교하는 수 정수 값이고 위 두 경우 모두에 대해서 최대 자기 상관값의 하한은 20이다. 표 1은 100과 300사이에 있는 소수들 p에 대하여 $p-1$이 10의 배수인 경우 $q=10$으로 고정시킨 후 네가지 수열의 최대 해밍 자기상관값을 비교한 것이다. 그림 1과 표 1로부터 제안한 세가지 생성법 중에서 생성법 3이 가장 좋고, 그 다음 생성법 2, 생성법 1의 순서로 좋다. 이는 최대 해밍 상관값이 작을 수록 해밍자기 상관값이 우수하다는 관점에서 평가이다.

다음은 심벌의 균형성에 대해 비교해보자. 확실히 생성법 1과 2은 균형성을 만족한다. 다상 멱 잉여류 수열은 영이 아닌 심벌 모두가 $(p-1)/q$번씩 동일하게 나타나고, 영 심벌이 $(p-1)/q+1$번으로 한 번 더 나타나지만 주어진 길이조건 p에 대해서는 균형성 측면에서는 최적의 분포이다. 생성법 3에서는 최적 지움 위치에 따라 심벌 개수들 사이의 차이가 0(균형), 1 또는 2이다. 만약 최적 지움 위치의 심벌이 영이면 심벌 개수들 사이의 차이는 0이다. 최적 지움 위치의 심벌이 영이 아닌 경우에는 심벌 개수들 사이의 차기가 0, 1 또는 2이다. 이 경우 심벌들은 다음 세 가지 경우로 분류된다. (i) 영 심벌, (ii) 최적 지움 위치의 심벌, 그리고 (iii) 나머지 $q-2$개의 심벌이다. (i), (ii) 과 (iii)에 해당되는 심벌의 발생빈도는 각각 $\frac{p-1}{q}+1$, $\frac{p-1}{q}-1$ 그리고 $\frac{p-1}{q}$ 이므로 심벌 개수간의 차이는 0, 1 또는 2이다. 이 분포가 균형성면에서 최적은 아니지만 두 번째로 최적이므로 거의 균형성 있게 분포한다고 할 수 있다.

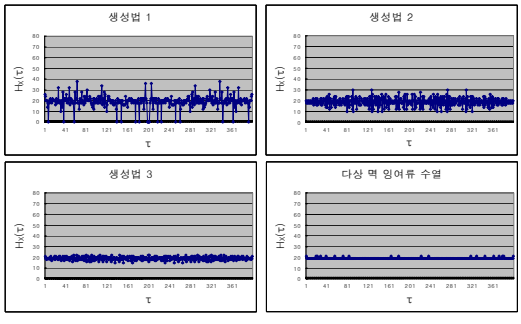

그림 1. p=401, q=20일 때 제안된 수열들과 다상 멱 잉여류 수열의 해밍 자기상관 분포

표 1. $100<p<300$사이의 $p-1$이 10의 배수인 경우 10진 수열들의 최대상관비교

p	μ	q	생성법1의 $H_{\max}$	생성법2의 $H_{\max}$	생성법3의 $H_{\max}$	다상멱잉여류수열 $H_{\max}$
101	2	10	18	16	12	11
131	2	10	22	20	15	13
151	6	10	26	22	17	15
181	2	10	32	30	21	19
191	19	10	34	24	22	19
211	2	10	38	30	23	21
241	7	10	42	32	26	25
251	6	10	44	34	28	25
271	6	10	48	36	30	27
281	3	10	50	36	31	29

Ⅳ. 구현성

제안된 네가지 수열 생성의 용이함을 보기 위해 그림 2를 보자. 그림 2는 생성법 1과 다상멱 잉여류수열의 구현을 흐름에 따라 순서도로 만든 것이다. 생성법 2과 3는 다상 멱 잉여류 수열에 기반한 것이므로 여기서는 생략하였다. 생성법 1과 다상 멱 잉여류 수열 모두 p,q와 μ만으로써 생성하기에 충분하므로 매우 간단히 구현된다. 좀더 자세히 살펴보면 생성법 1은 매 계산시 mod q연산 직전의 값을 메모리에 저장해 놓고 이 값을 mod q하여 수열 원소 값으로 내놓은 다음 메모리 저장된 값에 μ를 곱한 값으로 갱신하고 이 값을 mod q연산을 하여 다음 수열 값을 내놓는 일련의 반복 과정에 의해 쉽게 구현된다. 다상 멱 잉여류 수열은 그림 2에서 알 수 있듯이 원시근 μ의 연속적인 멱을 계산해 나가면서 각 원소가 어느 코셋에 속하는지 분류 하는 과정 '$t(k)\leftarrow n$ mod q'이 있으므로 어느 코셋에 속하는지 저장할 목적 혹은 n이 증가하는 순서로 $t(n)$을 재배치하기 위해 메모리가 더 필요하다는 차이가 있다. 물론 다상 멱 잉여류 수열과 생성법 2, 3에서 집합 C_0의 원소들에 대한 정보가 있다면 구현이 더욱 간단해짐은 자명하다. 생성법 3에서는 추가적으로 최적 지움위치에 대한 정보를 메모리나 여타 저장 장치에 저장하고 이 위치를 지우는 과정이 추가되어야 하지만, 여전히 구현은 간단하다.

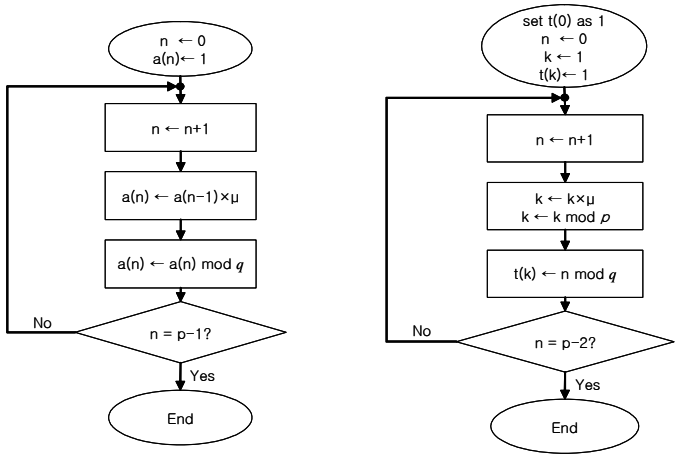

그림 2. 생성법 1과 다상멱 잉여류 수열의 생성 흐름도

Ⅴ. 결 론

본 논문에서는 주파수 도약 시스템에 사용될 수열 중에 특히 짧은 길이의 도약 수열의 세 가지 생성 방법을 제안하였다. 생성법 1은 Z_p상의 원시근 μ의 연속적인 멱을 mod q 연산을 함으로써 얻어지는 수열로 균형성을 만족한다. 생성법 2, 3은 다상 멱 잉여류 수열에 기반을 둔 수열들이다. 생성법 2은 다상 멱 잉여류 수열에서 첫 번째 위치를 지움으로써 얻어지는 수열, 생성법 3은 해밍 상관특성 관점에서 최적 지움 위치를 지워서 얻어지는 수열이다. 생성법 2 수열은 균형성을 만족하고, 생성법 3 수열은 준 최적의 균형성을 갖는다. 최대 해밍 자기 상관이 작을수록 우수하다는 관점에서 생성법 3이 가장 좋고, 그 다음으로 생성법 2 그리고 생성법 1이 좋다. 이들 생성법 들이 p, q와 μ만으로 간단히 구현될 수 있음을 확인하였다.

참 고 문 헌

[1] M. K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levitt, *Spread Spectrum Communications Handbook,* revised ed. McGraw-Hill, Inc., 1994.

[2] R. L. Peterson, R. E. Ziemer and D. E. Borth, *Introduction to Spread Spectrum Communications*, Prentice Hall, 1995.

[3] V. S. Pless and W. C. Huffman, *Handbook of Coding Theory*, North Holland, Elservier, 1998.

[4] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. Inform. Theory*, Vol. IT-15, No. 1, January 1969.

[5] A. A. Shaar and P. A. Davies, "A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems", *IEE Proceedings*, Vol. 131, Pt. F, No. 7, December 1984.

[6] V. M. Sidelnikov, "Some *k*-valued pseudo-random and nearly equidistant codes," *Probl. Pered. Inform.*, vol. 5, no. 1, pp. 16-22, 1969.

[7] A. Lempel and H. Greenberger, "Families of Sequences with Optimal Hamming Correlation Properties," *IEEE Trans. Inform. Theory*, Vol. IT-20, No. 1, January 1974.

김 영 준 (Young-Joon Kim) 준회원

2002년 2월 연세대학교 전자공학과 졸업(공학사)
2004년 2월 연세대학교 대학원 전기전자공학과 졸업(공학석사)
2004년 3월~현재 연세대학교 대학원 전기전자공학과 박사과정
<관심분야> Design of Set of PN Sequences, Application of PN Sequences to Spread Spectrum and Crypto Systems

김 대 선 (Dae-Son Kim) 준회원

2001년 2월 건국대학교 전자공학과 졸업(공학사)
2003년 2월 연세대학교 대학원 전기전자공학과 졸업(공학석사)
2006년~현재 연세대학교 대학원 전기전자공학과 박사과정
<관심분야> Error Correcting Codes, Turbo code, LDPC, MC-CDMA, Spread Spectrum Communication Systems

송 홍 엽 (Hong-Yeop Song) 종신회원

1984년 2월 연세대학교 전자공학과 졸업(공학사)
1986년 5월 USC 대학원 전자공학과 졸업(공학석사)
1991년 12월 USC 대학원 전자공학과 졸업 (공학박사)
1992년~1993년 Post Doc., USC 전자공학과
1994년~1995년 8월 Qualcomm Inc., 선임연구원
2002년 3월~2003년 2월 University of Waterloo, Canada, 방문연구교수
1995년 9월~현재 연세대학교 전기전자공학부 교수
<관심분야> PN Sequences, Error Correcting Codes, Spread Spectrum Communication Systems, Steam Cipher Systems