

# 우수한 비주기 자기상관 특성을 갖는 새로운 다중 위상 부호열

정회원 문경하\*, 준회원 홍윤표\*\*, 준회원 최기훈\*\*, 종신회원 송홍엽\*\*

## New Polyphase Sequence with Good Nonperiodic Autocorrelation Property

Kyoung-Ha Moon\*, Yun-Pyo Hong\*\*, Ki-Hoon Choi\*\*, Hong-Yeop Song\*\* *Regular Members*

### 요약

본 논문에서는 비주기 자기상관 특성의 중요한 지표가 되는 merit factor의 관점에서 가장 우수한 비주기 자기상관 특성을 갖는 새로운 다중 위상 부호열(polyphase sequence)을 제안한다. 또한, 정수 환(integer residue ring)에서 LFSR(Linear Feedback Shift Register)을 이용한 일반적인 다중 위상 부호열 생성기를 제안하고 제안된 생성기에 기반한 다중 위상 부호열의 선형복잡도를 분석한다.

Key Words: polyphase sequence, merit factor, non-periodic autocorrelation, linear complexity.

### ABSTRACT

In this paper, we propose the new polyphase sequence with the best nonperiodic autocorrelation property in the viewpoint of the merit factors, which are important criteria for a nonperiodic autocorrelation property. We propose the general implementation of a polyphase sequence generator over an integer residue ring by using a linear feedback shift register(LFSR), in addition, we analyze the linear complexities of polyphase sequences based on the proposed implementation method.

### I. 서론

다중 위상 부호열(polyphase sequence)은 1961년 Heimiller에 의해 처음 제안되어졌으며 [1], Frank와 Chu 그리고 Golomb은 일반적인 다중 위상 부호열의 생성방법에 대해 논의하였다 [2][3][4]. 그 이후 1990년대에 Antweiler와 Bomer는 다중 위상 부호열을 실제 시스템에 적용하기 위해 비주기 자기상관 특성의 지표가 되는 merit factor를 정의하였고 Frank 부호열과 Chu 부호열의 merit factor가 부호열의 길이에 따라 선형적으로 증가함을 실험적으로 보였다 [5]. 이와 같은 연구들을 바탕으로 우수한

자기상관 특성을 갖는 다중 위상 부호열에 대한 연구가 계속적으로 행해지고 있다.

DS-CDMA(Direct Sequence Code Division Multiple Access) 또는 SSMA(Spread Spectrum Multiple Access)에서는 MAI(Multiple Access Interference)를 줄이는 것이 시스템 성능을 향상시키는 데 중요한 역할을 하게 되므로 우수한 자기상관 특성을 갖는 부호열을 사용하는 것이 필수적이다 [6]. 또한, OFDM 시스템과 CDMA 시스템에서는 다중 위상 부호열을 이용하여 crest factor를 줄이는 연구가 진행되고 있으며 레이다 시스템에서는 다중 위상 부호열을 이용하여 도플러 주파수 편

\* 현대 모비스 (moony95@mobis.co.kr), \*\* 연세대학교 대학원 전기전자공학과 (yp.hong@coding.yonsei.ac.kr)

논문번호 : 040009-0107, 접수일자 : 2004년 1월 7일

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

이효과를 얻는 연구가 진행되고 있다 [7][8].

본 논문의 구성은 다음과 같다. 2장에서는 잘 알려진 다중 위상 부호열을 생성방법에 따라 분류하고 비주기 자기상관 특성의 중요한 지표가 되는 merit factor에 대해 설명한다. 3장에서는 merit factor의 관점에서 가장 우수한 비주기 자기상관 특성을 갖는 다중 위상 부호열을 제안한다. 마지막으로 4장에서는 LFSR(Linear Feedback Shift Register)을 이용한 다중 위상 부호열 생성기를 제안하고 제안된 생성기에 기반한 다중 위상 부호열의 선형복잡도(linear complexity)를 분석한다.

## II. 다중 위상 부호열의 분류와 Merit Factor

이진 부호열(binary sequence)이 단지 두 개의 위상을 갖는 부호열을 뜻하는 반면 다중 위상 부호열은 다중 위상을 갖는 부호열을 의미한다. 다중 위상 부호열은 각각의 부호열의 길이가 제곱수인지 아닌지에 따라서 분류된다. 즉, 부호열의 길이가 제곱수일 때 생성 가능한 다중 위상 부호열은 생성방법 A로 분류되며, 부호열의 길이가 임의의 양의 정수일 때 생성 가능한 다중 위상 부호열은 생성방법 B로 분류된다. 생성방법 A 또는 생성방법 B로 분류되어지는 다중 위상 부호열은 각각의 위상표현에 따라 다음과 같이 표현될 수 있다.

생성방법 A. 부호열 길이  $N=M^2$

다중 위상 부호열  $S(s_1, s_2, \dots, s_N)$ 의 원소들은  $n$  ( $0 \leq n \leq M-1$ )과  $k$  ( $0 \leq k \leq M-1$ )에 대하여  $s_{nM+k+1} = e^{i\varphi_{n,k}}$ 으로 정의되며  $\varphi_{n,k}$ 는 각각의 부호열에 따라 다음과 같이 정의된다.

$$1) \text{ Frank 부호열 [2]: } \varphi_{n,k} = \frac{2\pi nk}{M} \quad (1)$$

2) P1 부호열 [9]:

$$\varphi_{n,k} = -\left(\frac{\pi}{M}\right)(M-2n-1)(nM+k) \quad (2)$$

3) Px 부호열 [10]:

$$\varphi_{n,k} = \begin{cases} \left(\frac{\pi}{M}\right)\left[\frac{M-1}{2} - k\right](M-2n-1), & M \text{ even} \\ \left(\frac{\pi}{M}\right)\left[\frac{M-2}{2} - k\right](M-2n-1), & M \text{ odd} \end{cases} \quad (3)$$

생성방법 B. 부호열 길이  $N$  (양의 정수)

다중 위상 부호열  $S(s_1, s_2, \dots, s_N)$ 의 원소들은  $k$

( $0 \leq k \leq N-1$ )에 대하여  $s_{k+1} = e^{i\varphi_{k+1}}$ 으로 정의되며  $\varphi_{k+1}$ 은 각각의 부호열에 따라 다음과 같이 정의된다.

1) Golomb 부호열 [3]:

$$\varphi_{k+1} = \frac{\pi(k+1)k}{N} \quad (4)$$

2) Chu 부호열 [4]:

$$\varphi_{k+1} = \begin{cases} \frac{\pi(k+2q)k}{N}, & N \text{ even} \\ \frac{\pi(k+2q+1)k}{N}, & N \text{ odd} \end{cases}, \quad (5)$$

$q$ 는 임의의 정수

$$3) \text{ P3 부호열 [11]: } \varphi_{k+1} = \frac{\pi k^2}{N} \quad (6)$$

$$4) \text{ P4 부호열 [12]: } \varphi_{k+1} = \frac{\pi(k-N)k}{N} \quad (7)$$

$S$ 가 길이  $N$ 의 복소 부호열일 때 비주기 자기상관 함수는

$$\varphi_{ss}(\tau) = \sum_{n=1}^{N-\tau} S_n \cdot S_{n+\tau}^* \quad (8)$$

으로 정의되며  $S_{n+\tau}^*$ 은  $S_{n+\tau}$ 의 공액 복소수이다. 다중 위상 부호열의 비주기 자기상관 특성의 중요한 지표인 merit factor  $F$ 와  $R$ 은 다음과 같이 정의된다.

$$F = \frac{\varphi_{ss}(0)^2}{2 \sum_{\tau=1}^{N-1} |\varphi_{ss}(\tau)|^2} \quad (9)$$

$$R = \frac{\varphi_{ss}(0)}{\max_{1 \leq \tau \leq N-1} |\varphi_{ss}(\tau)|}$$

(10)

여기서  $F$ 는 mainlobe 에너지의 전체 sidelobe 에너지에 대한 비율을 의미하고  $R$ 은 비주기 자기상관 함수의 최대값의 ( $\tau=0$ )  $\tau \neq 0$ 일 때의 최대 비주기 자기상관 함수값에 대한 비율이다. 결국 merit factor  $F$ 와  $R$ 이 클수록 우수한 비주기 자기상관 특성을 갖는다고 할 수 있다.

## III. 가장 우수한 비주기 자기상관 특성을 갖는 새로운 다중 위상 부호열

정의 1. 부호열의 길이  $N=M^2$ 인 제안된 다중 위상 부호열  $S(s_1, s_2, \dots, s_N)$ 의 원소들은  $n$

( $0 \leq n \leq M-1$ )과  $k$  ( $0 \leq k \leq M-1$ )에 대하여  $s_{nM+k+1} = e^{i\varphi_{n,k}}$ 으로 정의되며, 이 때  $\varphi_{n,k}$ 는 다음과 같다.

$$\varphi_{n,k} = \begin{cases} (-\frac{\pi}{M})[\frac{M-1}{2} - k](M-2n-1), & M \text{ even} \\ (-\frac{\pi}{M})[M-1-k](M-2n-1), & M \text{ odd} \end{cases} \quad (11)$$

제안된 부호열은 정의 1에 의해 생성방법 A로 분류된다. 부호열의 길이  $N$ 이 제곱수인 경우에 대해 지금까지 소개한 8가지 다중 위상 부호열의 merit factor  $F$ 와  $R$ 의 특성을 모의실험으로 분석한 결과를 각각 그림 1, 2가 보여주고 있다.

그림 1에서 길이  $N$ 이 짝수, 홀수에 따라 급격히 진동하면서 증가하는 곡선이 Px 부호열에 대한 결과이며, 가장 상단의 곡선이 본 논문에서 제안된 부호열에 대한 결과이다, 상단에 분포한 곡선이 Frank 부호열과 P1 부호열에 대한 동일한 결과이며, 하단에 분포한 곡선이 Golomb, P3, P4와 Chu 부호열에 대한 동일한 결과를 나타낸다.

그림 2에서 진동하며 증가하는 곡선은 Px 부호열에 대한 결과이고, 상단에 분포한 곡선이 Frank 부호열, P1 부호열과 제안된 부호열에 대한 동일한 결과이며, 하단에 분포한 곡선이 Golomb, P3, P4와 Chu 부호열에 대한 동일한 결과를 나타낸다.

따라서, 제안된 부호열이 가장 우수한 비주기 자기상관 특성을 갖는다는 것을 알 수 있다. 또한, 그림 1, 2에서 그래프의 윗부분에 분포한 곡선은 생성방법 A에 의해 생성된 다중 위상 부호열의 곡선들이고 아래부분에 분포한 곡선들은 생성방법 B에 의해 생성된 다중 위상 부호열의 곡선들이다.

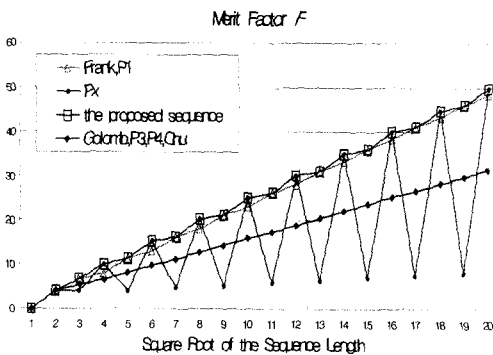


그림 1.  $\sqrt{N}$ 에 대한 Merit Factor  $F$

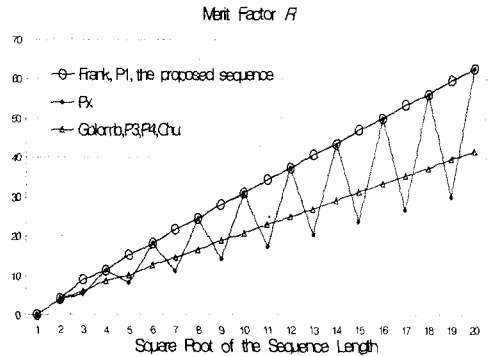


그림 2.  $\sqrt{N}$ 에 대한 Merit Factor  $R$

따라서, 생성방법 A에 의해 생성된 부호열이 생성방법 B에 의해 생성된 부호열보다 부호열의 길이  $N$ 이 제곱수인 경우에 대해 더 우수한 비주기 자기상관 특성을 나타냄을 알 수 있다. 반면에, 생성방법 B로 분류된 부호열은 임의의 길이를 갖는 다중 위상 부호열을 생성할 수 있다는 장점이 있다.

#### IV. 다중 위상 부호열의 생성기 구현 및 선형 복잡도

실제 시스템에서 부호열을 생성시키는 가장 효과적이고 일반적인 방법은 LFSR(Linear Feedback Shift Register)을 사용하는 것이며 이 때 부호열의 심볼집합은 두 가지 연산(덧셈, 곱셈)이 정의되어야 한다. 다중 위상 부호열  $S(s_1, s_2, \dots, s_N)$ 의 심볼들은  $\zeta_q$ 를 단위원의  $q$ 차 원시 근(primitive  $q$ -th root of unity)라 할 때  $\{\zeta_q^0, \zeta_q^1, \zeta_q^2, \dots, \zeta_q^{q-1}\}$ 를 심볼집합으로 갖으며, 이는 곱셈군을 이루게 된다. 그러나,  $S$ 의 심볼집합은 덧셈이 정의되지 못하므로 LFSR을 이용한 부호열의 생성이 불가능하다. 따라서, 다중 위상 부호열을 생성시키기 위해서는 새롭게 변형된 심볼집합을 정의할 필요가 있다.

일반적으로, 다중 위상 부호열의 심볼집합을 복소체(complex field)로 정의할 수 있다. 복소체의 원소들은 무한 자릿수를 가지므로 최소단수의 LFSR을 합성하는데 시스템에서 발생하는 계산상의 오차를 고려하지 않을 수 없다. 다시 말해서, 심볼집합이 체(field)를 이룰 때 LFSR의 연결다항식을 합성하는 BM(Berlecamp-Massey) 알고리즘을 이용하여 다중

위상 부호열을 생성하는 최소단수의 LFSR을 구현할 경우, 복소체에서 정의되는 곱셈에 대한 역(multiplicative inverse)을 구할 때 발생하여 순환적으로 증가되는 오차 때문에 다중 위상 부호열을 생성하는 LFSR을 합성할 수 없다.

그러므로 본 논문에서는, 다중 위상 부호열의 심볼집합을 심볼의 지수들이 이루는 정수환(integer residue ring)  $Z_q$ 로 정의한다. 이에 따라 수식 (12)와 같이 심볼집합  $Z_q$ 에서의 새로운 부호열  $T$ 를 정의한다.

$$T=(t_1, t_2, \dots, t_N), s_n = \zeta_q^{t_n} \quad (12)$$

그림 3과 같이 곱셈군을 형성하는 심볼집합  $V$ 를  $Z_q$ 로 변환시키면  $Z_q$ 는  $q$ 에 따라 체 또는 환(ring)을 형성하게 되므로 각각 BM 알고리즘과 RS(Reeds-Sloane) 알고리즘을 이용하여 변환된 심볼집합  $Z_q$ 위에서 정의된  $T$ 를 생성하는 최소단수 LFSR을 합성할 수 있다 [13][14][15].

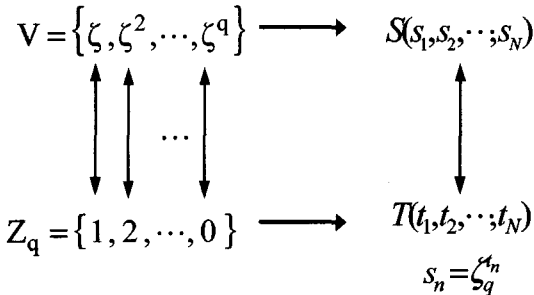


그림 7.  $V$ 와  $Z_q$  로의 심볼집합 변환

$T(t_1, t_2, \dots, t_N)$ 을 생성하는 최소단수 LFSR의 선형재관계가  $t_n = -\sum_{i=1}^L c_i \cdot t_{n-i}$ 이라 할 때  $T$ 의 최소차수의 연결 다항식  $C(x)$ 는  $C(x) = 1 + \sum_{i=1}^L c_i \cdot x^i$  된다. 이때,  $c_i$  ( $i=1, \dots, L$ )는 연결계수이고  $L$ 은  $T$ 의 형복잡도(linear complexity)이다. 이러한  $T$ 를 생성하는 최소단수 LFSR을 이용하여  $S$ 를 발생시키는 제안된 다중 위상 부호열 생성기는 그림 4와 같다. 본 논문에서는 제안된 다중 위상 부호열 생성기에 기반하여  $T$ 의 선형복잡도를  $S$ 의 선형복잡도로 간주한다. 그림 5는 각각의 다중 위상 부호열에 대해

$\sqrt{N}$ 에 대한 선형복잡도의 특성을 보여준다.

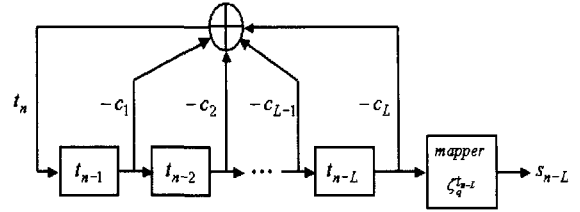


그림 3. 다중 위상 부호열 생성기

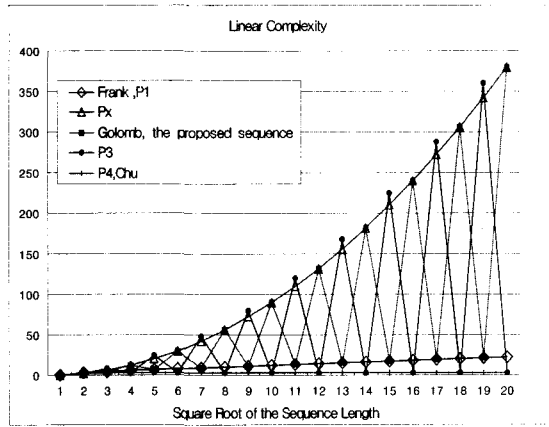


그림 4.  $\sqrt{N}$ 에 대한 선형 복잡도

$Px$  부호열의 선형복잡도는  $\sqrt{N}$ 에 대해 선형적으로 증가하였고 Frank, P1, P4, Chu 부호열의 선형복잡도는 낮게 유지되었으며 Golomb, P3 부호열과 본 논문에서 제안된 부호열은  $\sqrt{N}$ 이 홀수, 짝수나에 따라 진동하는 특성을 보였다.

### V. 결론

본 논문에서는 모의실험을 통하여 merit factor의 관점에서 가장 우수한 비주기 자기상관 특성을 갖는 다중 위상 부호열을 제안하였다. 또한, 다중 위상 부호열의 심볼집합을 변형함으로써 새로운 부호열을 정의하여 다중 위상 부호열의 생성기를 제안하였으며 제안된 생성기를 기반으로 다중 위상 부호열의 선형복잡도 역시 실험적으로 분석하였다.

실제 시스템을 구현하는데 있어서 merit factor와 선형복잡도는 중요한 고려 대상이 되므로 이 두 가지 지표에 대한 좀 더 정확한 분석이 요구된다. 따라서, 이러한 두 가지 평가 지표 관점에서 보다 우수한 다중 위상 부호열을 찾고 제안된 부호열의 merit factor와 선형 복잡도 특성에 대해 대수적으로

분석하는 연구가 필요하다.

참 고 문 헌

[1] R. C. Heimiller, "Phase Shift Pulse Codes with Good Periodic Correlation Properties," *IRE Trans. Inform. Theory*, vol. IT-7, pp. 254-257, Oct. 1961.

[2] R. L. Frank, "Polyphase Codes with Good Nonperiodic Correlation Properties," *IRE Trns. Inform. Theory*, vol. IT-9, pp. 43-45, Jan. 1963.

[3] N. Zhang and S. W. Golomb, "Polyphase Sequence with Low Autocorrelation," *IRE Trans. Inform. Theory*, vol. 39, pp. 1085-1088, May. 1993

[4] D. C. Chu, "Phase Shift Pulse Codes with Good Periodic Correlation Properties," *IRE Trans. Inform. Theory*, vol. 9, pp.43-45, July. 1972

[5] L. Bomerd and M. Antweiler, "Merit Factor of Chu and Frank Sequences," *Electronics Letters*, vol. 26, Issue. 25, Dec. 1990

[6] M. B. Pursley, "Performance Evaluation for Phase Coded Spread Spectrum Multiple Access Communication - Part I : System analysis," *IRE Trans. Com.*, vol. 25, no.8, pp.795-799, Aug. 1977

[7] Byoung-Jo Choi, Ee-Lin Kuan and Lajos Hanzo, "Crest Factor Study of MC-CDMA and OFDM," *Proc. IEEE VTC'99*, pp. 233-237, vol. 4, 1997.

[8] Y. Gen-miao and W. Shun-jun and L. Yong-jian, "Doppler Properties of Polyphase Pulse Compression Codes under Different Sidelobe Reduction Technique," *Radar, CIE Inter. Conference, Proceedings*, 2001

[9] B. L. Lewis and F. F. Kretschmer, Jr., "A New Class of Polyphase Pulse Compression Codes and Techniques," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-17, pp 364-372, May. 1981

[10] Predrag B. Rapajic and Rodney A. Kennedy "Merit Factor Based Comparison of New Polyphase Sequence," *IEEE Com. Letters*,

vol. 2, no. 10, Oct. 1998

[11] —, "Linear Frequency Modulation Derived Polyphase Pulse Compression Codes," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-18, pp 637-641, Sept. 1982

[12] —, "Doppler Property of Polyphase Coded Pulse Compression Waveforms," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-19, pp. 521-531, July. 1983.

[13] J. L. Massey, "Shift-Register Synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122-127, Jan. 1969

[14] J. A. Reed, N. J. A. Sloane, "Shift-Register Synthesis (modulo m)," *Siam J. Comp.*, vol. 14, no. 3, pp. 505-513, Aug. 1985

[15] YP Hong, YC Eun, JH Kim, and HY Song, "Linear Complexity of Sequences over Arbitrary Symbols and Constructions of Sequences over  $GF(p^k)$  whose Characteristic Polynomial is over  $GF(p)$ ," *2002 IEEE International Symposium on Information Theory*, June 30-July 5, Palais de Beaulieu, Lausanne, Switzerland.

문 경 하(Kyoung-Ha Moon)

정회원

2002년 2월 : 성균관대학교  
전자공학과 졸업 (공학사)

2004년 2월 : 연세대학교  
대학원 전기전자공학과 졸업  
(공학석사)

2004년 2월~현재 :  
현대 모비스



<관심분야> Application of PN Sequences to Spread Spectrum and Crypto Systems, Block Codes and Convolutional codes

홍 윤 표 (Yun-Pyo Hong)

준회원



2000년 2월 : 연세대학교  
전자공학과 졸업 (공학사)  
2002년 2월 : 연세대학교  
대학원 전기전자공학과 졸업  
(공학석사)  
2002년 3월~현재 : 연세대학교  
대학원 전기전자공학과  
박사과정

<관심분야> Application of PN Sequences to  
Spread Spectrum and Crypto Systems, Block  
Codes and Convolutional codes

최 기 훈 (Ki-Hoon Choi)

준회원



2000년 2월 : 연세대학교  
전자공학과 졸업 (공학사)  
2002년 2월 : 연세대학교  
대학원 전기전자공학과 졸업  
(공학석사)  
2002년 3월~현재 : 연세대학교  
대학원 전기전자공학과

박사과정

<관심분야> Application of PN Sequences to  
Spread Spectrum and Crypto Systems, Block  
Codes and Convolutional codes

송 흥 엽 (Hong-Yeop Song)

중신회원



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 : Qualcomm Inc., 선임연구원  
1995년 9월~현재 : 연세대학교 전기전자공학과  
교수

<관심분야> PN Sequences, Error Correcting  
Codes, Spread Spectrum Communication  
Systems, Steam Cipher Systems