이상적인 자기상관특성을 갖는 주기가 2^n-1인 이진 의사불규칙 시퀀스의 분류

노 종선*°, 이 환근**, 정 하봉†, 양 경철††, 송 홍엽†

*건국대학교 전자공학과, **부일이동통신(주) 기술연구소

†홍익대학교 전자전기공학부, ††한양대학교 전자통신과, †연세대학교 전자공학과

On the Classification of Binary Pseudorandom Sequences of Period 2^n-1 with Ideal Autocorrelation

Jong-Seon No*, Hwan-Keun Lee**, Habong Chung†, Kyeongcheol Yang††, Hong-Yeop Song†

*Dept. of Electronic Engineering, Konkuk University

**Booil Mobile Telecomm. Corp., R&D Center

†School of Electronics and Electrical Engineering, Hong-Ik University

††Dept. of Electronic Communication Engineering, Hanyang University

†Dept. of Electronic Engineering, Yonsei University

요 약

본 논문에서는 이상적인 자기상관특성을 갖는 주기 2^n-1의 새로운 이진 의사불규칙 시퀀스(pseudorandom sequence)를 컴퓨터 search를 통하여 발견하였으며 이들 의사불규칙시퀀스를 trace함수를 이용하여 표현하였다. 또한 이상적인 자기상관특성을 갖는 주기 2^n-1의 이진 의사불규칙시퀀스들을 분류하고 그들의 개수를 나타냈다.

1. 서 론

이상적인 자기상관특성을 갖는 이진시퀀스는 확산스펙트럼 통신시스템, 레이다 시스템, 스트림 암호시스템, 부호분할 다원접속방식(CDMA) 등에서 그의 사용영역을 넓혀 왔다. 시퀀스 $\{b(t),\ t=0,1,\cdots,N-1\}$의 주기 자기상관함수 $R_b(\tau)$가 다음과 같은 값을 갖는다면 이상적인 자기상관특성을 갖는다고 한다.

$$R_b(\tau)=\begin{cases} N\ , & \text{for } \tau\equiv 0 \bmod N \\ -1\ , & \text{for } \tau\not\equiv 0 \bmod N \end{cases} \quad (1)$$

여기서 $R_b(\tau)$는 다음과 같이 정의할 수 있다.

$$R_b(\tau)=\sum_{t=0}^{N-1}(-1)^{b(t+\tau)+b(t)} \quad (2)$$

지금까지 알려진 연구결과에 따르면 이상적인 자기상관특성을 갖는 주기 2^n-1의 이진시퀀스는 m-시퀀스[8], GMW 시퀀스[11], 일반화된(generalized) GMW 시퀀스[12], Legendre 시퀀스[13], Hall's sextic residue 시퀀스[2],[14], 확장된(extended) 시퀀스[14], 그리고 생성방법이 알려지지 않은 기타(miscellaneous) 시퀀스[4]-[6],[14]로 분류할 수 있다. 일반적으로 이들 시퀀스들은 trace 함수를 이용하여 쉽게 설명할 수 있다. 2^n개의 원소들을

갖는 유한필드(finite field)를 F_{2^n}이라고 하자. 이때 $m|n$에 대하여 F_{2^n}에서 F_{2^m}으로의 선형매핑(linear mapping)인 trace 함수 $tr_m^n(\cdot)$는 다음과 같이 표현할 수 있다.

$$tr_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}} \tag{3}$$

본 논문에서는 이상적인 자기상관특성을 갖는 주기 2^n-1의 새로운 이진시퀀스를 발견하였고 이들을 분류하고 개수를 나타내었다. 2절에서 이상적인 자기상관특성을 갖는 주기 2^n-1의 이진시퀀스들을 분류하고 표 I에 그들의 개수를 나타냈다. 3절에서는 주기가 $2^{20}-1$인 시퀀스를 예로서 나타내었다.

2. 이상적인 자기상관특성을 갖는 이진시퀀스들의 분류

$\{a(t), t=0,1,\cdots,N-1\}$와 $\{b(t), t=0,1,\cdots,N-1\}$를 주기가 $N=2^n-1$인 이진 시퀀스라고 가정하자. 이때, 모든 t에 대해 $b(t)=a(r[t+\tau])(\text{mod } N)$을 만족하는 정수 r과 τ가 존재한다면, 이들 두 시퀀스 $\{a(t)\}$와 $\{b(t)\}$는 동치(equivalent)이다. 그렇지 않은 경우는 비동치(inequivalent)의 관계가 있다고 한다.

본 절에서는 새롭게 발견한 시퀀스들을 포함하여 비동치 이진 시퀀스의 개수를 표 I에 분류하였다. 표 I에서는 편의를 위해 다음과 같은 약어를 사용하였다.

m : m-시퀀스
L : Legendre 시퀀스
H : Hall's sextic residue 시퀀스
G : GMW 시퀀스
GG : 일반화된 GMW 시퀀스 (generalized GMW sequences)
E : 확장된 시퀀스 (extended sequences)
NS : 발견된 새로운 시퀀스
M : 기타 시퀀스

표 I에서는 511까지의 주기에 대해서 이상적인 자기상관특성을 갖는 시퀀스를 컴퓨터 모의실험으로 모두 찾았다[4]-[6]. 주기 31의 Hall's sextic residue 시퀀스는 m-시퀀스와 동일하다. GMW 시퀀스의 특수한 경우가 m-시퀀스이며 m-시퀀스는 이미 분류가 되었으므로, 비동치 GMW 시퀀스의 개수에서 m-시퀀스는 제외하였다. 같은 이유로, 비동치의 일반화된 GMW 시퀀스의 개수에서 m-시퀀스와 GMW 시퀀스의 경우에 해당되는 종류의 개수는 제외되었다. 또한 GMW 시퀀스와 일반화된 GMW 시퀀스는 짧은 주기의 m-시퀀스로부터 확장된 시퀀스로 생각할 수 있으므로, 비동치의 확장된 시퀀스의 개수에서 제외하였다[14]. 그리고 앞서 언급했듯이 $n=7,8,9$인 경우에는 아직은 생성방법이 알려지지 않은 비동치의 기타 시퀀스들이 각각 한 종류씩 존재한다[4]-[6],[14].

다음의 예에서는 trace 함수를 이용하여 이상적인 자기상관특성을 가지며 주기가 $2^{20}-1$인 각각의 이진시퀀스들을 표현하고, 비동치의 이진시퀀스들의 개수를 보였다.

3. EXAMPLE

α를 $F_{2^{20}}$의 원시원이라고 가정하고, β를 $F_{2^{10}}$의 원시원이라고 가정하자.

1) m-시퀀스 :

$$tr_1^{20}(\alpha^t) \tag{4}$$

여기서 m-시퀀스의 개수는 1개라는 것은 쉽게 알 수 있다.

2) GMW 시퀀스 :

$$tr_1^4\{[tr_4^{20}(\alpha^t)]^{\gamma_1}\}, \tag{5}$$

$$tr_1^5\{[tr_5^{20}(\alpha^t)]^{\gamma_2}\}, \tag{6}$$

$$tr_1^{10}\{[tr_{10}^{20}(\alpha^t)]^{\gamma_3}\}, \tag{7}$$

여기서 $\gcd(15,\gamma_1)=1$, $\gcd(31,\gamma_2)=1$, $\gcd(1023,\gamma_3)=1$이다. 따라서 m-시퀀스를 제외한 모든 비동치 GMW 시퀀스의 개수는 모두 $1+5+59=65$개다.

3) 일반화된 GMW 시퀀스 (generalized GMW sequences) :

$$tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha^t)]^{\gamma_2}\}]^{\gamma_1}\} \tag{8}$$

여기서 $\gcd(31,\gamma_1)=1$이며, $\gcd(1023,\gamma_2)=1$이다. 따라서 GMW 시퀀스를 제외한 모든 비동치의 일반화된 GMW 시퀀스의 개수는 모두 $5\times59=295$개이다.

4) 확장된 시퀀스(extended sequences) :

표 I. 이상적인 자기상관특성을 갖는 주기 2^n-1의 비동치 이진 시퀀스의 개수

n	m	L	H	G	GG	E	NS	M	Total
3	1	0	0	0	0	0	0	0	1
4	1	0	0	0	0	0	0	0	1
5	1	1	0	0	0	0	0	0	2
6	1	0	0	1	0	0	0	0	2
7	1	1	1	0	0	0	2	1	6
8	1	0	0	1	0	0	1	1	4
9	1	0	0	1	0	0	1	1	4
10	1	0	0	5	0	2	1	≥0	≥9
11	1	0	0	0	0	0	2	≥0	≥3
12	1	0	0	7	5	0	0	≥0	≥13
13	1	1	0	0	0	0	1	≥0	≥3
14	1	0	0	17	0	62	1	≥0	≥81
15	1	0	0	6	0	2	1	≥0	≥10
16	1	0	0	16	15	32	1	≥0	≥65
17	1	1	1	0	0	0	2	≥0	≥5
18	1	0	0	53	52	96	0	≥0	≥202
19	1	1	0	0	0	0	2	≥0	≥4
20	1	0	0	65	295	≥180	1	≥0	≥542
21	1	0	0	18	0	62	1	≥0	≥82
22	1	0	0	175	0	≥352	0	≥0	≥528
23	1	0	0	0	0	0	2	≥0	≥3
24	1	0	0	165	1736	≥ 32	0	≥0	≥1934

4-a) 확장된 Legendre 시퀀스 (extended Legendre sequences) :

$$tr_1^5\{[tr_5^{20}(\alpha^t)]^\gamma\}+tr_1^5\{[tr_5^{20}(\alpha^t)]^{5\gamma}\}+tr_1^5\{[tr_5^{20}(\alpha^t)]^{7\gamma}\} \tag{9}$$

여기서 $\gcd(31,\gamma)=1$이다. 또한 비동치의 확장된 Legendre 시퀀스의 개수는 모두 2개이다.

4-b) 주기가 1023인 확장된 Legedre 시퀀스

$$tr_1^5\{[tr_5^{10}(\beta^t)]^{\gamma_1}\}+tr_1^5\{[tr_5^{10}(\beta^t)]^{5\gamma_1}\}+tr_1^5\{[tr_5^{10}(\beta^t)]^{7\gamma_1}\} \tag{10}$$

를 확장한 시퀀스 :

$$tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha^t)]^{\gamma_2}\}]^{\gamma_1}\}+tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha^t)]^{\gamma_2}\}]^{5\gamma_1}\}+tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha^t)]^{\gamma_2}\}]^{7\gamma_1}\} \tag{11}$$

여기서 $\gcd(31,\gamma_1)=1$이며, $\gcd(1023,\gamma_2)=1$이다. 따라서 확장된 Legendre 시퀀스를 제외한 확장된 Legedre 시퀀스를 확장한 비동치 시퀀스의 개수는 모두 $2\times59=118$개이다.

4-c) 주기 1023의 새롭게 발견된 시퀀스

$$tr_1^{10}(\beta^t)+tr_1^{10}(\beta^{11t})+tr_1^{10}(\beta^{15t})+tr_1^{10}(\beta^{39t})+tr_1^{10}(\beta^{127t}) \tag{12}$$

를 확장한 시퀀스 :

$$tr_1^{10}\{[tr_{10}^{20}(\alpha^t)]^\gamma\}+tr_1^{10}\{[tr_{10}^{20}(\alpha^t)]^{11\gamma}\}+tr_1^{10}\{[tr_{10}^{20}(\alpha^t)]^{15\gamma}\}+tr_1^{10}\{[tr_{10}^{20}(\alpha^t)]^{39\gamma}\}+tr_1^{10}\{[tr_{10}^{20}(\alpha^t)]^{127\gamma}\} \tag{13}$$

여기서 $\gcd(1023,\gamma)=1$이다. 주기 1023의 새롭게 발견된 시퀀스를 확장한 비동치 시퀀스의 개수는 모두 60개이다.

5) 주기 1023의 새롭게 발견된 시퀀스 :

$$tr_1^{20}(\alpha^t)+tr_1^{20}(\alpha^{127t})+tr_1^{20}(\alpha^{3969t})+tr_1^{20}(\alpha^{12287t})+tr_1^{20}(\alpha^{16383t}) \tag{14}$$

새롭게 발견된 이상적인 자기상관특성을 갖는 시퀀스의 개수는 1개이다.

[참고문헌]

[1] R. Lidl and H. Niederreiter, Finite Fields, vol. 20 of *Encrypedia of Mathe- matics and Its Applications*, Addison- Wesley, Reading, MA, 1983.

[2] L. D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, Springer-Verlag, 1971.

[3] D. Jungnickel, "Difference sets," in *Contemporary Design Theory*, J. H. Dinitz and D. R. Stinson, Eds., John Wiley and Sons, Inc., pp. 241-324, 1992.

[4] L. D. Baumert and H. Fredricksen, "The cyclotomic numbers of order 18 with applications to difference sets," *Math. Comp.*, vol. 21, no. 98, pp. 204-219, 1967.

[5] U. Cheng, "Exhaustive Construction of (255,127,63)-Cyclic Difference Sets," *J. Combinatorial Theory*, vol. A-35, pp. 115- 125, 1983.

[6] R. Drier, "(511,255,127) cyclic difference sets," IDA talk, July 1992.

[7] S. W. Golomb, "On the classification of balanced binary sequences of period 2^n-1,"*IEEE Trans, Inform. Thoery*, vol. IT-26, pp. 730-732, Nov. 1980.

[8] S. W. Golomb, *Shift Register Sequen- ces.* Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA 1982.

[9] J. -S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans.Inform. Theory*, vol. IT-35, pp.371- 379, Mar. 1989.

[10] J. -S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertion, Univ. of Southern California, Los Angeles, CA, May 1988.

[11] R. A. Scholtz and L. R. Welch, "GMW Sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548-553, May 1984.

[12] J. -S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory*, vol. 42-35, pp. 260-262, Jan. 1996.

[13] J. -S. No, H. -K. Lee, H. Chung, H. -Y. Song, and K. Yang, "Trace represent- ation of Legendre sequences of Mersenne prime period," To appear in *IEEE Trans. Inform. Theory*, Nov. 1996.

[14] J. -S. No, K. Yang, H. Chung, and H. -Y. Song, "On the construction of binary sequences with ideal autocorrelation property," *Proceedings of 1996 IEEE Inte- rnational Symposium on Information Theory and Its Applications*(ISITA '96), pp. 837-840, Victoria, B.C., Canada, Sept. 17-20, 1996.

[15] J. -S. No, K. Yang, H. Chung, and H. -Y. Song, "A New Family of Binary Sequences with Optimal Correlation Properties," *Proceedings of 1996 IEEE International Symposium on Information Theory and Its Applications*(ISITA '96), pp.841-844, Victoria, B.C., Canada, Sept. 17-20, 1996.

본 연구는 정보통신연구관리단의 대학기초연구 지원사업의 연구비지원에 의한 결과입니다.
