

이상적인 자기상관특성을 갖는 주기가 $2^n - 1$ 인 새로운 이진 의사불규칙 시퀀스

正會員 노 종 선*, 이 환 근**

New Binary Pseudorandom Sequences of Period $2^n - 1$ with Ideal Autocorrelation

Jong-Seon No*, Hwan-Keun Lee** *Regular Members*

※본 연구는 정보통신연구관리단의 대학기초연구지원사업의 연구비지원에 의한 결과입니다.

요 약

본 논문에서는 이상적인 자기상관특성을 갖는 주기가 $2^n - 1$ 인 세 종류의 새로운 이진 의사불규칙 시퀀스(pseudorandom sequence)를 발견하였다. 이들 시퀀스들은 컴퓨터 search에 의해 발견되었으며 conjecture들을 이용하여 이들 시퀀스를 공식으로 표현하였다. 또한 이상적인 자기상관특성을 갖는 주기 $2^n - 1$ 의 이진시퀀스들을 분류하고 그들의 개수를 나타냈다.

ABSTRACT

In this paper, we present three new classes of binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation. These sequences are newly found by an extensive computer search, and the conjectures on the construction of these sequences are formulated. We also classify the binary sequences of period $2^n - 1$ with ideal autocorrelation, and enumerate them.

I. 서 론

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

*전국대학교 전자공학과
**부일이동통신(주) 기술연구소
論文番號: 97001-0103
接受日字: 1997年 1月 3日

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

여기서 $R_b(\tau)$ 는 다음과 같이 정의할 수 있다.

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

지금까지 알려진 연구결과에 따르면 이상적인 자기상관특성을 갖는 주기 2^n-1 의 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^n 개의 원소들을 갖는 유한체(finite field)를 F_2 이라고 하자. 이때 $m|n$ 에 대하여 F_2 에서 F_{2^m} 으로의 선형매핑(linear mapping)인 trace 함수 $tr_m^*(\cdot)$ 는 다음과 같이 표현할 수 있다.

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

본 논문에서는 이상적인 자기상관특성을 갖는 주기가 2^n-1 인 세 종류의 새로운 이진시퀀스를 발견하였다. II절에서 이들 시퀀스들은 컴퓨터 search에 의해서 발견되었으며, conjecture들을 이용하여 이들 시퀀스를 공식으로 표현하였다. III절에서는 이상적인 자기상관특성을 갖는 주기 2^n-1 의 이진시퀀스들을 분류하고 표 I에 그들의 개수를 나타냈다.

II. Conjectures

이상적인 자기상관특성을 갖는 주기 2^n-1 의 이진시퀀스를 이용하여 이상적인 자기상관특성을 갖는 더 긴 주기의 확장된 이진시퀀스를 만들 수 있으며, 최적의 상관값을 갖는 주기 $2^{2m}-1$ 의 이진시퀀스군도 같은 이론을 적용할 수 있다[15]. 이러한 사실로부터 이상적인 자기상관특성을 갖는 새로운 이진시퀀스에 대한 연구를 하는 것은 매우 의미있는 일이라는 것을 알 수 있다. 현재까지 알려진 기본적인 이상적인 자기상관특성을 갖는 이진시퀀스들은 다음과 같이 분

류할 수 있다.

- i) m-시퀀스[8]
- ii) 머센소수(Mersenne prime)의 주기를 갖는 Legendre 시퀀스[13]와 $n=5, 7, 17$ 에 대한 Hall's sextic residue 시퀀스[2]와 같은 residue 시퀀스
- iii) GMW 시퀀스를 포함하여 이상적인 자기상관특성을 갖는 짧은 주기의 시퀀스들로부터 더 긴 주기로 확장된 시퀀스[14]와 일반화된 GMW 시퀀스[12]

컴퓨터 search를 통해 conjecture들을 정의하고, 이를 이용하여 다음과 같은 세 가지 종류의 이상적인 자기상관특성을 갖는 주기 2^n-1 의 새로운 이진시퀀스를 표현하였다.

Conjecture 1: k 는 양의 정수이며 $n=2k+1$ 이라고 가정하자. 이때 다음과 같이 이상적인 자기상관특성을 갖는 주기 2^n-1 의 이진시퀀스 $s(t)$ 를 정의할 수 있다.

$$s(t) = tr_1^n\{\alpha^t\} + tr_1^n\{\alpha^{(2^k+1)t}\} + tr_1^n\{\alpha^{(2^k+2^{k-1}+1)t}\} \quad (4)$$

여기서 α 는 유한체 F_2 의 원시원(primitive element)이다. □

따라서 $k=1$ 이라고 가정하면 $s(t)$ 는 주기가 7인 m-시퀀스가 되며, $k=2$ 에 대해 $s(t)$ 는 주기가 31인 Legendre 시퀀스임을 알 수 있다. 컴퓨터 모의실험을 통하여 $n \leq 23$ 에 대하여 Conjecture 1이 사실임을 확인하였다.

Conjecture 2: k 를 2보다 크거나 같은 양의 정수라 가정하고 $n=3k-1$ 이라고 하자. 이때 다음과 같이 이상적인 자기상관특성을 갖는 주기 2^n-1 의 이진시퀀스 $s(t)$ 를 정의할 수 있다.

$$s(t) = tr_1^n\{\alpha^t\} + tr_1^n\{\alpha^{(2^k-1)t}\} + tr_1^n\{\alpha^{(2^{2k-2}-2^k+1)t}\} + tr_1^n\{\alpha^{(2^{2k-2}-1)t}\} + tr_1^n\{\alpha^{(2^k-1)t}\} \quad (5)$$

여기서 α 는 유한체 F_2 의 원시원(primitive element)이

다. □
 $k=2$ 일 때 $s(t)$ 는 주기가 31인 Legendre 시퀀스가 된다. 컴퓨터 모의실험을 통하여 $n \leq 23$ 에 대하여 Conjecture 2가 사실임을 확인하였다.

Conjecture 3: k 를 $k \equiv 2 \pmod 3$ 을 만족하는 양의 정수라 가정하고 $n = 3k - 2$ 라고 하면, 다음과 같이 이상적인 자기상관특성을 갖는 주기가 $2^n - 1$ 의 이진 시퀀스 $s(t)$ 를 정의할 수 있다.

$$s(t) = \text{tr}_1^n\{\alpha^t\} + \text{tr}_1^n\{\alpha^{(2^k-2^{k-1}-1)t}\} + \text{tr}_1^n\{\alpha^{(2^k-1)t}\} \\ + \text{tr}_1^n\{\alpha^{(2^{2k-3}+2^{k-1}-1)t}\} + \text{tr}_1^n\{\alpha^{(2^{2k-1}-1)t}\} \quad (6)$$

여기서 α 는 유한체 F_{2^n} 의 원시원(primitive element)이다. □

컴퓨터 모의실험을 통하여 $n \leq 22$ 에 대하여 Conjecture 3이 사실임을 확인하였다.

III. 이상적인 자기상관특성을 갖는 이진시퀀스들의 분류

$\{a(t), t=0, 1, \dots, N-1\}$ 와 $\{b(t), t=0, 1, \dots, N-1\}$ 를 주기가 $N=2^n-1$ 인 이진 시퀀스라고 가정하자. 이때, 모든 t 에 대해 $b(t) = a(r[t + \tau] \pmod N)$ 을 만족하는 정수 r 과 τ 가 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: 세 가지의 추측이론을 통해 발견된 새로운 시퀀스
- M : 기타 시퀀스(miscellaneous sequences)

표 I에서는 511까지의 주기에 대해서 이상적인 자기상관특성을 갖는 시퀀스를 컴퓨터 모의실험으로 모두 찾았다[4]-[6]. 주기가 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 존재한다[4]-[6], [14].

표 I. 이상적인 자기상관특성을 갖는 주기가 2^n-1 의 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	2	5
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

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

예: α 를 $F_{2^{20}}$ 의 원시원이라고 가정하고, β 를 $F_{2^{10}}$ 의 원시원이라고 가정하자.

1) m-시퀀스:

$$tr_1^{20}(\alpha') \tag{7}$$

여기서 m-시퀀스의 개수는 1개라는 것은 쉽게 알 수 있다.

2) GMW 시퀀스:

$$tr_1^4\{[tr_5^{20}(\alpha')]^{\gamma_1}\}, \tag{8}$$

$$tr_1^5\{[tr_5^{20}(\alpha')]^{\gamma_2}\}, \tag{9}$$

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

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 $1+5+59=65$ 개이다.

3) 일반화된 GMW 시퀀스(generalized GMW sequences):

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

여기서 $\gcd(31, \gamma_1)=1$ 이며, $\gcd(1023, \gamma_2)=1$ 이다. 따라서 GMW 시퀀스를 제외한 모든 비동치의 일반화된 GMW 시퀀스의 개수는 모두 $5 \times 59=295$ 개이다.

4) 확장된 시퀀스(extended sequences):

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

$$tr_1^5\{[tr_5^{20}(\alpha')]^{\gamma}\} + tr_1^5\{[tr_5^{20}(\alpha')]^{5\gamma}\} + tr_1^5\{[tr_5^{20}(\alpha')]^{7\gamma}\} \tag{12}$$

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

4-b) 주기가 1023인 확장된 Legendre 시퀀스

$$tr_1^5\{[tr_5^{10}(\beta')]^{\gamma_1}\} + tr_1^5\{[tr_5^{10}(\beta')]^{5\gamma_1}\} + tr_1^5\{[tr_5^{10}(\beta')]^{7\gamma_1}\} \tag{13}$$

를 확장한 시퀀스:

$$tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha')]^{\gamma_2}\}]^{\gamma_1}\} + tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha')]^{\gamma_2}\}]^{5\gamma_1}\} + tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha')]^{\gamma_2}\}]^{7\gamma_1}\} \tag{14}$$

여기서 $\gcd(31, \gamma_1)=1$ 이며, $\gcd(1023, \gamma_2)=1$ 이다. 따라서 확장된 Legendre 시퀀스를 제외한 확장된 Legendre 시퀀스를 확장한 비동치 시퀀스의 개수는 모두 $2 \times 59=118$ 개이다.

4-c) Conjecture 3에 의해 정의된 주기 1023의 새롭게 발견된 시퀀스

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

를 확장한 시퀀스:

$$tr_1^{10}\{[tr_{10}^{20}(\alpha')]^{\gamma}\} + tr_1^{10}\{[tr_{10}^{20}(\alpha')]^{11\gamma}\} + tr_1^{10}\{[tr_{10}^{20}(\alpha')]^{15\gamma}\} + tr_1^{10}\{[tr_{10}^{20}(\alpha')]^{39\gamma}\} + tr_1^{10}\{[tr_{10}^{20}(\alpha')]^{127\gamma}\} \tag{16}$$

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

5) Conjecture 2에 의해 정의된 주기 1023의 새롭게 발견된 시퀀스:

$$tr_1^{20}(\alpha') + tr_1^{20}(\alpha^{127t}) + tr_1^{20}(\alpha^{3969t}) + tr_1^{20}(\alpha^{12287t}) + tr_1^{20}(\alpha^{16383t}) \tag{17}$$

새롭게 발견된 이상적인 자기상관특성을 갖는 시퀀스의 개수는 1개이다.

참 고 문 헌

1. R. Lidl and H. Niederreiter, Finite Fields, vol. 20 of *Encyclopedia of Mathematics 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. Theory*, vol. IT-26, pp. 730-732, Nov. 1980.
 8. S. W. Golomb, *Shift Register Sequences*. 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. dissertation, 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 representation 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 International 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.



이 환근(Hwan-Keun Lee) 정희원
 1972년 5월 14일생
 1995년 2월: 서울산업대학교 공과
 대학 전자공학과 졸업(공학사)
 1997년 2월: 건국대학교 대학원 전
 자공학과 졸업(공학석사)

1997년~현재: 부일이동통신(주) 기술연구소 재직중
 ※주관심분야: 부호이론, 이동통신 시스템, 고속 무선
 호출 시스템 등

노 종선(Jong-Seon No) 정희원
 한국통신학회 논문지 1996년 3월호 참조