최적의 자기상관 특성을 갖는 주기 p^m-1인 이진 시퀀스의 생성

정회원 노 종 선*, 정 하 봉**, 송 홍 엽***, 양 경 철****, 이 정 도*****

New Binary Sequences of Period p^m-1 with Optimal Autocorrelation

Jong-Seon No*, Habong Chung**, Hong-Yeop Song***, Kyeongcheol Yang****, Jung-Do Lee***** *Regular Members*

요 약

다항식 $(z+1)^d+az^d+b$를 이용하여 소수 p에 대해서 주기 $N=p^m-1$을 갖는 이진 시퀀스 $\{s(t)\}$의 새로운 생성방법을 제시하고, 파라메터 p,m,d,a,b의 몇몇 경우에 대해서 논한다. 이와 같은 방법으로 생성된 시퀀스들이 균형이거나 거의 균형이라는 것을 보이고, 세 가지 레벨의 최적의 자기상관값을 갖는다는 것을 증명한다. 또한, 시퀀스들이 갖는 자기상관값의 분포를 유도한다. 생성된 시퀀스들은 constant-on-the-coset 성질을 만족하고, 하나 이상의 characteristic phase가 존재한다는 것을 보인다. 생성된 시퀀스들의 여러가지 흥미로운 성질들을 제시하였고, 컴퓨터 search 결과를 제시하였다.

ABSTRACT

In this paper, we present a construction for binary sequences $\{s(t)\}$ of period $N=p^m-1$ for an odd prime p based on the polynomial $(z+1)^d+az^d+b$, and discuss them in some cases of parameters p,m,d,a and b. We show that new sequences from our construction are balanced or almost balanced, and have optimal three-level autocorrelation. We also derive the distribution of autocorrelation values they take on. The sequences satisfy constant-on-the-coset property, and we will show that there are more than one characteristic phases with constant-on-the-coset property. Some other interesting properties of these sequences will be presented. Results of an extensive computer search are summarized.

I. 서 론

이진 의사불규칙 시퀀스는 발생이 쉽고 불규칙적인 성질 때문에 공학과 과학의 여러 분야에서 사용되어 지고 있다. 잘 알려진 응용분야로는 CDMA 이동통신을 비롯한 스트림 암호화 시스템 등이 있다. 최근에 주기가 2^m-1인 이상적인 자기상관특성과 균형특성을 갖는 이진 시퀀스를 생성하는데 많은 발전이 있었다. 그것은 유한체상에서 특별한 다항식을 이용하여 시퀀스를 생성하는 것이다. 편의상 F_{p^m}을 p^m개의 원소를 갖는 유한체라 하고, $F_{p^m}^*=F_{p^m}\setminus\{0\}$이라 하자. $p=2$에 대해서 노종선, 정하봉, 윤민선은 다항식 $(z+1)^d+z^d$를 이용하여 F_{2^m}에서 주기 2^m-1의 이진시퀀스의 생성에 관하

* 서울대학교 전기공학부 ** 홍익대학교 전기전자공학부 *** 연세대학교 전기및컴퓨터 공학과
**** 포항공과대학교 전자전기공학과 ***** 현대전자 통신시스템 연구소
논문번호 : - , 접수일자 : 년 월 일

여 연구하였다.[9] 그들은 다항식 $(z+1)^d+z^d$를 이용하여 생성된 이진 시퀀스가 $m=3k\pm1$, $d=2^{2k}-2^k+1$에 대해서 균형(balanced)이고, 이상적인 자기상관특성을 갖는 시퀀스이며, m-시퀀스와는 다른 시퀀스라는 것을 conjecture로 정립하였다. 또한, 그들은 m-시퀀스가 이러한 생성방법으로 표현될 수 있다는 것을 증명하였다. Dillon은 앞서 정립한 conjecture가 모든 홀수 n에 대해서 사실임을 증명하였다.[2] Dobbertin은 Kasami power function x^d($d=2^{2k}-2^k+1$, $k<m$, $(k,m)=1$)를 연구하였고, [9]에서 제시한 다항식 $(z+1)^d+z^d$을 약간 변형하여 다항식 $(z+1)^d+z^d+1$을 이용하여 F_{2^m}에서 이진시퀀스를 발생하였다.[3] 그는 F_{2^m}에서 다항식 $(z+1)^d+z^d+1$을 이용하여 생성된 시퀀스가 trace 함수를 이용하여 표현할 수 있다는 것을 보였고, 생성된 이진시퀀스의 선형스팬(linear span)을 유도하였다. 마지막으로 그는 생성된 시퀀스가 균형이고, 이상적인 자기상관특성을 갖는다는 일반적인 conjecture를 제시하였다. 그의 conjecture는 [10]에서 제시된 몇몇 conjecture를 포함하는 것이다. [3]과 [9]에서 소개된 다항식들은 임의의 소수 p와 정수 m에 대해서 최적의 자기상관특성을 갖는 이진 시퀀스의 생성으로 일반화 될 수 있다. p^m개의 원소를 갖는 유한체를 F라 하고, F의 원소 a, b와 정수 d에 대해서 다음과 같은 F^*의 부분집합을 생각해 보자.

$$I(a,b) \triangleq \{x \mid x=(z+1)^d+az^d+b, z\in F\}\setminus\{0\} \quad (1)$$

집합 $I(a,b)$를 이용하여 생성된 시퀀스 $\{s(t)\}$는 다음과 같이 정의된다.

$$s(t) = \begin{cases} 1, & \text{if } \alpha^t \in I(a,b) \\ 0, & otherwise \end{cases} \quad (2)$$

여기서 α는 F의 원시원(primitive element)이다. $\{s(t)\}$의 주기는 p^m-1이고, a, b, d를 적절히 선택하면 시퀀스 $\{s(t)\}$는 (거의)균형이고, 최적의 자기상관특성과 constant-on-the-coset 성질을 만족한다. $p>2$에 대해서, Lempel, Cohn, Eastman은 최적의 자기상관특성을 갖는 주기 p^m-1의 이진 균형시퀀스에 대해서 연구하였다.[5] 그들은 F^*의 부분집합 $S=\{\alpha^{2i+1}-1\}$에 대해서 연구하였고, S에 의해서 생성된 시퀀스가 균형이고, 최적의 자기상관특성과 constant-on-the-coset 특성을 갖는다는 것을 보였다. 그들은 이진 시퀀스를 생성하기 위해서 다항식 $z(1-z)$를 사용하는 방법에 대해서 언급하였고, 이진 m-시퀀스가 이 방법으로 생성될 수 있다는 것을 보였다.

본 논문에서는 다항식 $(z+1)^d+az^d+b$를 이용하여 주기 $N=p^m-1$의 이진 시퀀스 $\{s(t)\}$를 생성하는 방법을 제시하고 p, m, d, a, b의 몇몇 경우에 대해서 논할 것이다. 이러한 생성방법으로 생성된 시퀀스가 균형이거나 거의 균형이고, 최적의 자기상관특성을 갖는다는 것을 보일 것이다. 또한 시퀀스들이 갖는 자기상관값의 분포(distribution)를 유도할 것이다. 생성된 시퀀스는 constant-on-the-coset 성질을 만족하고, 일반적으로 constant-on-the-coset 성질과 함께 하나 이상의 characteristic phase가 존재한다는 것을 보일 것이다. 이러한 시퀀스의 여러가지 흥미로운 성질들이 제시될 것이며, 컴퓨터 search 결과를 제시하였다.

Ⅱ. 등가관계와 랜덤성질

$\{s_1(t)\}$와 $\{s_2(t)\}$를 주기 N의 이진시퀀스라 하자. 모든 t에 대해서 $s_1(t)=s_2(t+\tau)$를 만족하는 τ가 존재한다면 $\{s_1(t)\}$는 $\{s_2(t)\}$의 cyclic shift라 하고, $\gcd(r,N)=1$을 만족하고 $s_1(t)=s_2(rt)$를 만족하는 r이 존재한다면 $\{s_1(t)\}$는 $\{s_2(t)\}$의 r-데시메이션(decimation)이라 한다. 또한 $s_1(t)=s_2(t)+1 \pmod 2$를 만족한다면 $\{s_1(t)\}$는 $\{s_2(t)\}$의 반전(complement)라 한다. $\{s_1(t)\}$가 $\{s_2(t)\}$의 cyclic shift, 데시메이션, 반전이거나 그것들의 조합이라면 두 시퀀스 $\{s_1(t)\}$와 $\{s_2(t)\}$는 서로 등가의 시퀀스라고 말한다. 주기 N의 이진 시퀀스 $\{s(t)\}$에 대해서, 한 주기 안에서 1의 개수와 0의 개수의 차를 D라 하자. 주기 N이 짝수일 때 D가 0이고, 주기 N이 홀수 일 때 D가 1이면 그 시퀀스는 균형이라고 말한다. 여기서 만약 D가 2라면 이것을 "거의 균형"이라고 정의하자. 등가의 두 시퀀스에 대해 D의 절대값은 동일하다.

$\{s(t)\}$의 주기적인 자기상관함수 $\theta(\tau)$는 다음과 같이 정의된다.

$$\theta(\tau) \triangleq \sum_{t=0}^{N-1}(-1)^{s(t)+s(t+\tau)} \quad (3)$$

$\theta(\tau)\equiv N \pmod 4$과와 $\sum_{\tau=0}^{N-1}\theta(\tau)=D^2$이라는 것은

잘 알려진 사실이다. 또한 다음 수식도 잘 알려진 사실이다.

$$\theta(\tau)=N-4\{|I|-|I\cap(I+\tau)|\} \tag{4}$$

여기서 $I=\{t|s(t)=1, 0\le t\le N-1\}$이고, $I+\tau=\{t+\tau(\bmod N)|t\in I\}$이다.

두 개의 등가의 시퀀스는 동일한 자기상관값들의 집합과 자기상관값의 분포를 갖는다. 자기상관특성의 관점에서 주기 N인 이진시퀀스가 최적이라는 것은 $\tau\ne 0(\bmod N)$일 때 자기상관값 $\theta(\tau)$의 최대값이 가능한 작아야 한다는 것을 의미한다. 그래서 주기 $N=0(\bmod 4)$일 때 가장 최적인 것으로 생각되는 것은 $\tau\ne 0(\bmod N)$일 때 $\theta(\tau)=0$인 circulant Hadamard 메트릭스이다. 이것은 $N>4$인 균형시퀀스에서는 아직 알려진 것이 없으므로 이러한 경우에 $\theta(\tau)=0$ 또는 -4가 최적의 자기상관값으로 생각할 수 있을 것이다. 또한 주기 $N=2(\bmod 4)$인 경우에는 가장 최적인 것은 $|\theta(\tau)|=2$이고, 앞으로 최적으로 언급될 것이다.

임의의 정수 $t(\bmod N=p^m-1)$에 대해서 t를 포함하는 cyclotomic coset은 $\{t, tp, tp^2, tp^3, \dots\}$으로 정의된다. 주기 N인 이진 시퀀스 $\{s(t)\}$가 동일한 cyclotomic coset에 속하는 모든 t_1, t_2에 대해, 어떤 τ에 대해, $s(t_1+\tau)=s(t_2+\tau)$를 만족한다면 constant-on-the-coset 성질을 갖는다고 한다. 이러한 constant-on-the-coset 성질을 만족하는 시퀀스 $\{s(t)\}$의 cyclic shift를 이 시퀀스의 characteristic phase라고 부른다. Constant-on-the-coset 성질은 앞에서 살펴본 등가관계에 의해서는 보존된다.

Ⅲ. 다항식 $(z+1)^d+az^d+b$를 이용한 이진 시퀀스의 생성

p^m개의 원소를 갖는 유한체를 F라 하고, $F^*=F\setminus\{0\}$라 하자. 유한체 F에 속하는 a, b와 양의 정수 d에 대해서 $f(z)$를 다음과 같이 정의하자

$$f(z)=(z+1)^d+az^d+b \tag{5}$$

F^*에서 index set $I(a,b)$를 다음과 같이 정의하자.

$$I(a,b)\triangleq\{x|x=f(z), z\in F\}\setminus\{0\} \tag{6}$$

본 논문에서 논의될 이진시퀀스는 $I(a,b)$에 대해서 다음과 같이 정의되는 시퀀스이다.

$$s_{a,b}(t)\triangleq\begin{cases}1, & \text{if } \alpha^t\in I(a,b)\\ 0, & otherwise\end{cases} \tag{7}$$

여기서 α는 F의 원시원이다.

앞으로는 $p>2$인 경우에 대해서만 논할 것이다.

$d=2$일 때, $f(z)=(z+1)^2+az^2+b=(a+1)z^2+2z+b+1$가 된다. 만약 $a+1=0$ 이면 $I(a,b)=F^*$가 된다. 만약 $a+1\ne 0$이면 다음과 같이 쓸 수 있다.

$$f(z)=(a+1)\left[\left(z+\frac{1}{a+1}\right)^2\right]-\frac{1}{a+1}+(b+1) \tag{8}$$

따라서 시퀀스$\{s_{a,b}(t)\}$는 다항식 $z^2-c(c\in F)$를 이용한 시퀀스의 cyclic shift 이다.

정리 1 : $p\ge 3$ 이고 $d=2, a, b\in F$ 에 대해서 $a+1\ne 0$이라 하자. 그러면 $\{s_{a,b}(t)\}$는 다항식 z^2-c를 이용한 시퀀스의 cyclic shift이다. 여기서 c는 F의 원소이고, b에 따라 결정된다.

이러한 가정을 이용하여 다음과 같이 정의할 수 있을 것이다.

$$I_c\triangleq\{x|x=z^2-c, z\in F\}\setminus\{0\} \tag{9}$$

I_c에 의해서 생성된 시퀀스를 $\{s_c(t)\}$라 하고, 자기상관함수를 $\theta(\tau)$라 하자. $\{s_{a,b}(t)\}$가 $\{s_c(t)\}$의 cyclic shift가 되는 경우는 두 가지 이상이 존재한다.

정리 2 : $p\ge 5, d=3, a=-1$이라 하자. 양의 정수 m과 F의 원소 b에 대해서 $\{s_{a,b}(t)\}$는 $\{s_c(t)\}$의 cyclic shift이다. 여기서 c는 F의 원소이고, b에 따라 결정된다.

증명 : $a+1=0$, $d=3$ 이므로 $f(z)=(z+1)^3-z^3+b=3z^2+3z+b+1$이다. 따라서, 완전제곱식으로 고치면, 그 결과는 쉽게 유도된다. □

정리 3 : $p=3, d=4, a=1$이고 $N=3^m-1\equiv 2(\bmod 4)$를 만족하는 홀수를 m이라 하자. F의 원소 b에 대해서 $\{s_{a,b}(t)\}$는 $\{s_c(t)\}$의 cyclic shift이다. 여기서 c는 F의 원소이고 b에 의존한다.

증명 : $f(z)=(z+1)^4+z^4+b=2(z-1)^4+b-1=2((z-1)^2)^2+b-1$이다. m은 $N=3^m-1\equiv 2(\bmod 4)$를 만족하는 홀수이므로 $(z-1)^2$은 다시 F의 원시원의 짝수승의 값을 취한다. □

만약 $c=0$이라면 다항식 z^2을 이용한 시퀀스는 010101.....이 되고, 자기상관값은 결코 $N \geq 4$인 경우에 최적일 수 없다. 이제 한 시퀀스가 이것과 등가인 시퀀스로 변환될 때 index set이 어떻게 바뀌는지 다음 보조정리에서 증명 없이 기술하였다.

보조정리 4 : α를 p^m개의 원소를 갖는 유한체 F의 원시원이라 하고, $\{s(t)\}$와 $\{s'(t)\}$를 각각 F^*에서 index set I와 I'를 이용하여 생성된 주기 $N=p^m-1$의 시퀀스라 하자. 그러면 (i) 상수 τ에 대해서 $I' = \alpha^{\tau} I$ 이면 $s'(t) = s(t-\tau)$이다. 여기서 $\alpha I \triangleq \{ax \mid x \in I\}$이다. (ii) $I' = I^e$ 이면 $s'(t) = s(rt)$이고 $\gcd(r, N) = 1$, $er \equiv 1 (\bmod N)$, $I^e \triangleq \{x^e \mid x \in I\}$이다. (iii) $I' \cup I = F^*, I' \cap I = \phi$ 이면 $s'(t) = s(t) + 1 \ (\bmod 2)$이다. 즉 F^*는 I'와 I로 분할된다는 것을 의미한다.

Ⅳ. 생성된 시퀀스의 랜덤특성

본 절에서는 $\{s_c(t)\}$가 c가 어떤 수의 제곱일 때 거의 균형이고, c가 어떤 수의 제곱이 아닐 때 균형이라는 것을 보일 것이고, 다른 흥미있는 시퀀스의 성질을 증명할 것이다. 유한체 F에서 cyclotomic coset $C_i (i=0$, 또는 $1)$를 다음과 같이 정의하자.

$$C_i = \{\alpha^{2s+i} \mid s=0,1,\ldots,N/2-1\} \qquad (10)$$

고정된 i와 j에 대해서 cyclotomic number (i,j)는 다음 방정식의 해의 개수이다.

$$1 + z_i = z_j \qquad (11)$$

여기서 $z_i \in C_i, z_j \in C_j$ 이다. Cyclotomic number의 이론으로부터 다음 보조정리에서 처럼 (i,j)를 쉽게 결정할 수 있다.[15]

보조정리 5 : (***보조정리 6***, [15]) Cyclotomic number는 다음과 같이 주어진다.

(a) $N \equiv 0 \ (\bmod 4)$이면, $(0,0) = (p^m-5)/4$;
$(0,1) = (1,0) = (1,1) = (p^m-1)/4$

(b) $N \equiv 2 \ (\bmod 4)$이면,
$(0,0) = (1,0) = (1,1) = (p^m-3)/4; (0,1) = (p^m+1)/4$

$\{s_c(t)\}$가 균형특성과 최적의 자기상관특성을 갖는다는 것을 보이기 전에 I_c에서 $z=0$일 때를 제외한 다음을 고려해 보자.

$$I_c^* \triangleq \{x \mid x = z^2 - c,\ z \in F^*\} \setminus \{0\} \qquad (12)$$

$\{s_c^*(t)\}$를 I_c^*를 이용하여 생성된 시퀀스라 하고, $\theta_c^*(\tau)$를 자기상관함수라 하자. 만약 $c \neq 0$이라면 $I_c^* = I_c \setminus \{-c\}$이 되고 $|I_c^*| = |I_c| - 1$이 된다.

정리 6 : $\{s_c(t)\}$와 $\{s_c^*(t)\}$를 각각 I_c와 I_c^*를 이용하여 생성된 주기 $N=p^m-1$인 시퀀스라 하고, α를 F의 원시원이라 할 때 $\{s_\alpha^*(t)\}$와 $\{s_1(t)\}$는 균형시퀀스이다. 또한 $\{s_\alpha(t)\}$와 $\{s_1^*(t)\}$는 거의 균형인 시퀀스이다. 더욱이

(i) $s_\alpha^*(t) = s_1(t-1) + 1$이고,

(ii) $s_\alpha(t) = s_1^*(t-1) + 1$이고,

(iii) $s_\alpha(N/2+1) = s_1(N/2) = 1$이고, $t \neq N/2$인 경우를 제외하고 $s_1(t) = s_\alpha(t+1) + 1$이다.

(iv) $s_\alpha^*(N/2) = s_1^*(N/2-1) = 1$이고, $t \neq N/2-1$인 경우를 제외하고 $s_1^*(t) = s_\alpha^*(t+1) + 1$이다. 이와 같은 관계는 다음 그림으로 설명될 수 있다.

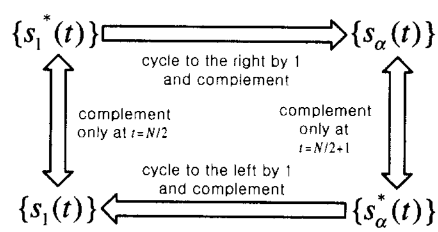


그림 1. $\{s_1^*(t)\}, \{s_1(t)\}, \{s_\alpha^*(t)\}, \{s_\alpha(t)\}$사이의 관계

증명 : 시퀀스의 균형특성과 거의 균형인 특성은 다음으로부터 유도된다.

$I_1^* = (C_0 - 1) \setminus \{0\}$ for $N/2-1$

$I_1 = \{-1\} \cup (C_0 - 1) \setminus \{0\}$ for $N/2$

$I_\alpha^* = C_0 - \alpha$ for $N/2+1$

$I_\alpha = \{-\alpha\} \cup (C_0 - \alpha)$ for $N/2+1$

여기서 $C_0 - c \triangleq \{x - c \mid x \in C_0\}$이다.

(i)는 보조정리 4에 의해서 $\alpha I_1 \cup I_\alpha^* = \phi$, $\alpha I - 1 \cap I_\alpha^* = F^*$라는 것으로 설명되고, (ii)는 $\alpha I_1 \cup I_\alpha = F^*$이고, $\alpha I_1 \cap I_\alpha = \{-\alpha\}$, $\alpha^{N/2+1} = -\alpha$이기 때문에 $I_\alpha \cap \alpha I_1^* = \phi$ $|I_\alpha| = |I_1^*| + 2 = N/2+1$이라는 사실로부터 설명된다. (iii)과 (iv)는 쉽게 유도할 수 있다. □

c가 어떤 수의 제곱이 아니라면, 보조정리 4에

의해서 $\{s_c(t)\}$는 $\{s_a(t)\}$의 cyclic shift이고, $\{s_c^*(t)\}$는 $\{s_a^*(t)\}$의 cyclic shift이다. c가 어떤 수의 제곱이라면, $\{s_c(t)\}$는 $\{s_1(t)\}$의 cyclic shift이고, $\{s_c^*(t)\}$는 $\{s_1^*(t)\}$의 cyclic shift이다. 그래서 정리 6에 의해서 $\{s_c(t)\}$가 최적의 자기상관특성을 갖는지 알아보는 것은 $\{s_1^*(t)\}$와 $\{s_a^*(t)\}$를 고려하는 것으로 충분하다.

보조정리 7 : $1-\alpha^\tau \in C_i$, $\alpha^\tau \in C_j$를 만족하는 $\tau(\not\equiv 0 \bmod 4)$에 대해서 다음의 관계식을 얻는다.

$$|I_a^* \cap \alpha^\tau I_a^*| = (i+j+1, i+1) \tag{13}$$

증명 : $x \in I_a^* \cap \alpha^\tau I_a^*$인 x에 대해서, $x = y - \alpha$, $y \in C_0$라 쓸 수 있고, $x = \alpha^\tau(z-\alpha)$, $z \in C_0$라 쓸 수 있다. 그래서 다음과 같은 식을 얻는다.

$$1+\frac{\alpha^\tau z}{\alpha(1-\alpha^\tau)} = \frac{y}{\alpha(1-\alpha^\tau)} \tag{14}$$

다음의 관계로부터 보조정리 7을 증명할 수 있다.

$$\frac{\alpha^\tau z}{\alpha(1-\alpha^\tau)} \in C_{i+j+1}, \quad \frac{y}{\alpha(1-\alpha^\tau)} \in C_{i+1} \tag{15}$$

$1-\alpha^\tau \in C_i$, $\alpha^\tau \in C_j$ □

정리 8 : 주기 N인 시퀀스 $s_a^*(t)$와 $s_1(t)$는 균형이고 최적의 자기상관특성을 갖는다. 특히 $\tau \not\equiv 0 (\bmod 4)$에 대해서 다음과 같이 된다.

$$\theta_a^*(\tau) = \begin{cases} -4\varepsilon, & \text{if } N \equiv 0 \ (\bmod 4) \\ 2-4\varepsilon, & \text{if } N \equiv 2 \ (\bmod 4) \end{cases}, \quad \varepsilon \in \{0,1\} \tag{16}$$

증명 : 식(4)와 정리 6, 보조정리 5, 보조정리 7로부터 증명된다. □

Lempel, Cohn, Eastman은 집합 $S = \{\alpha^{2i+1}-1 \mid i = 0, 1, \ldots N/2-1\}$을 이용하여 생성된 시퀀스 $s(t)$를 고려하였다.[5] $c = \alpha^{p^m-2}$이고 c가 어떤 수의 제곱이 아닐 때, $S = \alpha(C_0 - \alpha^{p^m-2})$이고 $s(t) = s_c^*(t-1)$이다. 그래서 cyclotomic number를 이용한 접근은 [5]에서의 시퀀스의 생성에 대한 또 다른 간단한 증명이 된다.

보조정리 9 : $1-\alpha^\tau \in C_i$, $\alpha^\tau \in C_j$를 만족하는 $\tau \not\equiv 0$ $(\bmod 4)$에 대해서 다음식을 만족한다.

$$|I_1^* \cap \alpha^\tau I_1^*| = (i+j, i) - 1 \tag{17}$$

증명 : $x \in I_1^* \cap \alpha^\tau I_1^*$인 x에 대해서 $x = y-1$, $y \in C_0 \backslash \{1\}$이고, $x = \alpha^\tau(z-1)$, $z \in C_0 \backslash \{1\}$라고 쓸 수 있다. 그래서 다음과 같은 관계를 얻는다.

$$1+\frac{\alpha^\tau}{1-\alpha^\tau} = \frac{y}{1-\alpha^\tau} \tag{18}$$

여기서 해는 $(y, z) = (1, 1)$이 될 수 없으므로 다음과 같은 관계로부터 증명된다.

$$\frac{\alpha^\tau z}{1-\alpha^\tau} \in C_{i+j}, \quad \frac{y}{1-\alpha^\tau} \in C_i \tag{19}$$

for $1-\alpha^\tau \in C_i$, $\alpha^\tau \in C_j$ □

정리 10 : 주기 N인 시퀀스 $\{s_1^*(t)\}$와 $\{s_a(t)\}$는 거의 균형이고 최적의 자기상관특성을 갖는다. 특히 $\tau \not\equiv 0$ $(\bmod 4)$에 대해서 다음과 같다.

$$\theta_1^*(\tau) = \begin{cases} -4\varepsilon, & \text{if } N \equiv 0 (\bmod 4) \\ 2-4\varepsilon, & \text{if } N \equiv 2 (\bmod 4) \end{cases}, \varepsilon \in \{0,1\} \tag{20}$$

증명 : (4)와 정리 6, 보조정리 5, 보조정리 9로부터 유도될 수 있다. □

정리 11 : 표 1에 나타난 u와 v에 대해서 $\{s_c(t)\}$는 다음과 같은 분포를 갖는다.

$$\theta_c(\tau) = \begin{cases} 0\ (+2, \textit{resp.}) & \text{for } u \text{ values of } \tau \\ -4\ (-2, \textit{resp.}) & \text{for } v \text{ values of } \tau \end{cases} \tag{21}$$

여기서 $N \equiv 0$ (mod 4) ($N \equiv 2$ (mod 4), *resp.*)

증명 : 다음 연립방정식을 푸는 것으로 쉽게 증명할 수 있다. $N \equiv 0 (\bmod 4)$일 때 $s_c(t)$는 균형이다. 따라서,

$$\begin{aligned} N+0u+(-4)v &= 0 \\ u+v+1 &= N, \end{aligned} \tag{22}$$

$u = (3N-4)/4$, $v = N/4$이다. 다른 경우도 비슷하게 증명될 수 있다. □

표 1. $\{s_c(t)\}$의 자기상관값 분포

	균형(D=0)	거의 균형(D=2)
$N \equiv 0 (\bmod 4)$	$u = (3N-4)/4$ $v = N/4$	$u = 3N/4$ $v = (N-4)/4$
$N \equiv 2 (\bmod 4)$	$u = (3N-2)/4$ $v = (N-2)/4$	$u = (3N-6)/4$ $v = (N+2)/4$

정리 12 : 시퀀스 $\{s_1(t)\}$와 $\{s_a(t+1)\}$는 characteristic phase가 된다. 더욱이 시퀀스 $\{s_1(t)\}$

와 $\{s_a(t+1)\}$의 $\Delta(=(p^m-1)/(p-1))$의 정수배로 cyclic shift된 시퀀스도 characteristic phase가 된다.

증명 : 주기 $N=p^m-1$과 $\Delta p \equiv \Delta \pmod N$이라는 것을 주목하자. 정수 k에 대해서, $s_1(t-k\Delta)=1$ $\Leftrightarrow$ $\alpha^{t-k\Delta}=z^2-1 \in I_1$ some z $\Leftrightarrow$ $\alpha^{tp-k\Delta p}=\alpha^{tp-k\Delta}$ $=z^{2p}-1 \in I_1$. 시퀀스 $\{s_a(t+1)\}$에 대해서, $s_a(t-k\Delta+1)=1$ $\Leftrightarrow$ $\alpha^{t-k\Delta+1}=z^2-a \in I_a$ some z

$\Leftrightarrow$ $\alpha^{tp-k\Delta p+p}=z^{2p}-a^p$

$\Leftrightarrow$ $\alpha^{tp-k\Delta+1}=\alpha^{-(p-1)}(z^{2p}-a^p) \in I_a$이 된다. □

V. 컴퓨터 Search 결과

다항식 $(z+1)^d+az^d+b$를 이용하여 생성된 최적의 자기상관특성을 갖는 균형이거나 거의 균형인 시퀀스에 대해서 컴퓨터 search한 결과를 보였다. $p \le 19$의 경우에 대해서 컴퓨터 search가 가능한 m값에 대해서 d는 2 에서 $N-1$까지, F의 모든 원소 a, b에 대해서 search 하였다.

$(z+1)^{dp}+a^pz^{dp}+b^p=(z^p+1)^d+a'(z^p)^d+b'$ 이고 $z \mapsto z^p$는 유한체 F에서의 permutation이기 때문에 d는 coset leader에 대해서만 고려하였다. 가장 놀라운 사실은 주기 p^m-1에 대해서 $D=0$, 또는 $D=2$인 이진시퀀스가 기본적으로 하나는 존재한다는 것이다. 이것은 다음과 같은 의문을 갖게 한다. 각각의 주기 $N=p^m-1$과 D ($D=0$, 또는$D=2$)에 대해서 다항식 $(z+1)^d+az^d+b$를 이용하여 생성된 최적의 자기상관특성을 가지며, II장에서의 등가관계에 비추어 유일하게 하나의 시퀀스가 존재하는가에 대한 의문을 갖게 한다. 컴퓨터 search의 결과를 아래의 표로 정리하였다. 아래의 표에는 균형이거나 거의 균형인 최적의 자기상관특성을 갖는 시퀀스가 존재하는 경우의 d를 표시하였다.

VI. 결 론

기존의 다항식을 이용한 시퀀스 생성방법을 보다 일반화하여 다항식 $(z+1)^d+az^d+b$ 에 의해 발생된 주기 p^m-1인 최적의 자기상관특성을 갖는 이진시퀀스에 대하여 생성방법과 발생된 시퀀스의 여러가지 성질을 발견하였고, 최적의 자기상관특성을 갖는 시퀀스가 발생되는 d, a, b 값을 컴퓨터 search를 통하여 정리하였다. 아직까지 3000이상의 긴 주기에서는 컴퓨터 search 시간이 오래 걸리는 관계로 시퀀스를 발생시키지 못하였으나 계속된 search를 한다면 새로운 시퀀스를 찾을 수도 있을 것이다.

표 2. 최적의 자기상관특성을 갖는 시퀀스가 존재하는 경우의 d 값 ($3 \le p \le 19$, $m \ge 2$)

$3 \le p \le 19$ and $m \ge 2$			
p	m	$N=p^m-1$	d
3	2	8	2,4,5
	3	26	2,4,14,17
	4	80	2,14,41,53
	5	242	2,4,10,14,122,161
	6	728	2,10,122,365,485
	7	2186	2,4,10,14,28,122,1094,1457
5	2	24	2,3,7,13,19
	3	124	2,3,6,43,63,99
	4	624	2,3,63,313,499
	5	3124	2,3,6,26,63,843,1043,1563,2499
7	2	48	2,3,25,41
	3	342	2,3,8,172,293
	4	2400	2,3,1201,2507
11	2	120	2,3,61,109
	3	1330	2,3,12,447,666,1209
13	2	168	2,3,85,155
17	2	288	2,3,145,271
19	2	360	2,3,181,341

참 고 문 헌

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

[2] J. F. Dillon, "Multiplicative Difference Sets via Additive Characters,"preprint, 1998

[3] Hans Dobbertin,"Kasami Power functions, permuta- tion polynomials and cyclic difference sets,"in Proceeding of *Difference Sets, Sequences and their Correlation Properties*, NATO Advanced Study Institute Workshop, held in Bad Windshiem, Germany, August 3-14, 1998.

[4] S. W. Golomb, *Shift-Register Sequences*, Holden- Day, San Francisco, CA, 1967; Aegean Park Press, laguna Hills, CA 1982.

[5] A. Lempel, M. Cohn, and W.L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. 23, No. 1, pp. 38-42, Jan. 1977.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, vol.

20 of *Encyclopedia of Mathematics and Its Applications*, Addison-Wesley, Reading, MA, 1983

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977

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

[9] J.-S. No, H. Chung, and M.-S. Yun, "Binary Pseudorandom Sequences of Period 2^m-1 with Ideal Autocorrelation Generated by the Polynomial $z^d+(z+1)^d$," *IEEE Trans. Inform. Theory*, vol. 44, No. 3, pp. 1278-1282, May 1999.

[10] J.-S. No, S. W. Golomb, Guang Gong, H.-K. Lee, and Peter Gaal, "Binary pseudorandom sequences of period 2^n-1 with ideal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 44, No. 2, pp. 814-817, Mar. 1998.

[11] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, No. 6, pp, 2254-2255, Nov. 1996.

[12] J.-S. No, H.-Y. Song, H. Chung, and K. Yang, "Extension of Binary Sequences with Ideal Autocorrelation Property," preprint, 1999

[13] D. V. Sarwate and M. B. Pursley "Cross-correlation Properties of Pseudorandom and Related Sequences," *Proceedings of IEEE*, vol. IT-68, pp. 593-619, May 1980.

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

[15] T. Storer, *Cyclotomy and Difference Sets*, Lecture Notes in Advanced Mathematics, Markham Publishing Company, Chicago, 1967.

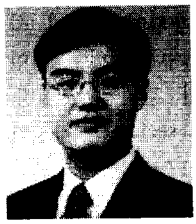
노 종 선(Jong-Seon No) 종신회원
한국통신논문지 제25권 4A호 참조

정 하 봉(Habong Chung) 정회원
한국통신논문지 제23권 5호 참조

송 홍 엽(Hong-Yeop Song) 종신회원
한국통신논문지 제25권 3A호 참조

양 경 철(Kyeongcheol Yang) 종신회원
한국통신논문지 제24권 6A호 참조

이 정 도(Jung-Do Lee) 정회원



1998년 : 건국대학교 전자공학과 (학사)
2000년 : 건국대학교 대학원 전자정보통신공학과 (석사)
2000년~현재 : 현대전자 통신시스템 연구소