p진 통합시퀀스 : 이상적인 자기상관특성을 갖는 p진 d-동차시퀀스

정회원 노 종 선*

p-ary Unified Sequences : p-ary Extended d-Form Sequences with Ideal Autocorrelation Property

Jong-Seon No* *Regular Member*

요 약

본 논문에서는 소수 *p*에 대해 이상적인 자기상관특성을 갖는 *p*진 *d*-동차시퀀스를 발생시키기 위한 생성방법을 제안하고 Helleseth와 Kumar, Martinsen이 찾아낸 3진 *d*-동차시퀀스를 이용한 이상적인 자기상관특성을 갖는 3진 *d*-동차시퀀스를 소개하였다. *p*진 확장시퀀스(기하시퀀스의 특별한 경우)의 발생 방법과 *p*진 *d*-동차시퀀스의 발생 방법을 조합하면 이진과 *p*진 확장시퀀스, *d*-동차시퀀스 모두를 포함하는 매우 일반적인 형태의 이상적인 자기상관특성을 갖는 *p*진 통합(확장 *d*-동차)시퀀스의 발생 방법을 제안하였다. 또한, Helleseth와 Kumar, Martinsen이 발견한 이상적인 자기상관특성을 갖는 3진 시퀀스로부터, 이상적인 자기상관특성을 갖는 3진 통합시퀀스를 생성하였다.

ABSTRACT

In this paper, for a prime number *p*, a construction method to generate *p*-ary *d*-form sequences with ideal autocorrelation property is proposed and using the ternary sequences with ideal autocorrelation found by Helleseth, Kumar and Martinsen, ternary *d*-form sequences with ideal autocorrelation property are introduced. By combining the methods for generating the *p*-ary extended sequences (a special case of geometric sequences) and the *p*-ary *d*-form sequences, a construction method of *p*-ary unified (extended *d*-form) sequences which also have ideal autocorrelation property is proposed, which is very general class of *p*-ary sequences including the binary and nonbinary extended sequences and d-form seuqences. From the ternary sequences with ideal autocorrelation by Helleseth, Kumar and Martinsen, ternary unified sequences with ideal autocorrelation property are also generated.

Ⅰ. 서 론

이상적인 자기상관특성을 갖는 의사 불규칙 시퀀스는 이동통신시스템의 다중접속방식의 표준으로 이용되는 코드분할 다중접속(CDMA) 방식과 같은 확산대역 통신시스템에서 많이 응용되고 있다. CDMA 시스템을 위한 신호의 설계는 그 응용에 있어 흥미로운 연구 주제로 각광받고 있다. CDMA 시스템에 사용되는 신호의 설계에 있어서 가장 중요한 연구분야의 하나가 좋은 자기상관특성을 갖는 의사 불규칙 시퀀스이다[1][2]. 현재까지의 대부분의 연구가 이상적인 자기상관특성을 갖는 이진 시퀀스에 대한 연구이거나, 최적의 상호상관특성을 갖는 이진 시퀀스군에 대한 연구였다. Chan과 Games는 기하시퀀스[4]를 소개하였고 Chan과 Golesky, Klapper에 의해 기하시퀀스에 관한 많은 연구들이 수행되었다[5]. 또한 No와 Yang, Chung, Song에 의해 확장시퀀스라 불리는 이상적인 자기상관특성을

* 서울대학교 전기·컴퓨터공학부(jsno@snu.ac.kr)
논문번호 : 010253-0917, 접수일자 : 2001년 9월 17일
※ 본 연구는 BK21과 ITRC 지원 및 관리로 수행되었습니다.

갖는 시퀀스에 관한 연구가 수행되었다[12]. 기하시퀀스는 q진 m-시퀀스에 비선형 feedforward 함수를 적용함으로써 의사 불규칙 시퀀스를 발생시키는 방법을 제공하였다. 또한 기하시퀀스는 m-시퀀스와 GMW 시퀀스[14], 직렬(일반화된) GMW 시퀀스, 확장시퀀스를 포함하는 매우 큰 시퀀스군이다. Klapper는 동차함수(차수가 d인 경우 d-동차)를 이용하여 d-동차시퀀스라 불리는 시퀀스를 만드는 또 다른 방법을 제시하였다. $d=2$인 d-동차시퀀스는 특별한 경우로 No-시퀀스에 포함된다[10][11]. 또한 그는 좋은 상관특성을 갖는 시퀀스군인 trace-norm (TN) 시퀀스를 찾아내기도 했다. TN 시퀀스는 $d=2$인 d-동차시퀀스와 몇몇 일반화된 No-시퀀스로 여겨진다. 그런데 Klapper가 시퀀스를 발생시키는 새로운 방법으로 d-동차시퀀스를 소개하였지만, 그의 논문 대다수는 좋은 상호상관특성을 갖는 시퀀스군에 관한 것들이었다. 또한 현재까지는 자명한 경우인 GMW 시퀀스와 직렬(일반화된) GMW 시퀀스를 제외한 이상적인 자기상관특성을 갖는 이진 또는 p진 d-동차시퀀스는 아직까지 발표되지 않았다. 또한 이상적인 자기상관특성을 갖는 d-동차시퀀스를 만드는데 이용할 수 있는 d-동차함수를 찾는 일 역시 쉬운 일이 아니다.

최근, Z_4시퀀스와 p진 시퀀스 같은 좋은 상관 특성을 갖는 비이진 시퀀스가 많이 발견되었고 몇몇 연구 결과들이 발표되었다. Helleseth와 Kumar, Martinsen은 p진 m-시퀀스와 직렬(일반화된) p진 GMW 시퀀스를 제외하고는 최초로 이상적인 자기상관특성을 갖는 비이진 시퀀스인 3진 시퀀스를 발견하였다.

본 논문에서는 이상적인 자기상관특성을 갖는 p진 d-동차시퀀스를 발생시키는 방법을 제안하고 Helleseth와 Kumar, Martinsen이 찾아낸 이상적인 자기상관특성을 갖는 3진 시퀀스를 이용하여 이진과 비이진의 경우에서 유일하게 이상적인 자기상관특성을 갖는 d-동차시퀀스인 3진 d-동차시퀀스를 발생시키는 방법을 소개하겠다. p진 확장시퀀스(몇몇 기하시퀀스의 특별한 경우)의 생성 방법과 p진 d-동차시퀀스의 발생 방법을 조합함으로써, 통합시퀀스(unified sequence)라 불리는 p진 d-동차시퀀스의 생성방법이 제안된다. 통합시퀀스는 d-동차시퀀스와 확장시퀀스를 포함하는 매우 일반화된 시퀀스의 분류이다. 마지막으로 3진 통합시퀀스는 Helleseth와 Kumar, Martinsen이 찾아낸 이상적인 자기상관특성을 갖는 3진 시퀀스로부터 만들어진다.

Ⅱ. 사전지식

$s(t)$가 다음과 같은 주기가 $N=p^n-1$인 F_p상의 시퀀스라고 하자.

$$s(t)\in F_p,\ t=0,\ 1,\ 2,\ \cdots,N-1$$

단, 위 식에서 p는 소수이며, F_p는 p개의 원소를 갖는 유한체이다. p진 시퀀스 $s(t)$가 시퀀스에서 '0'의 개수가 F_p상의 0이 아닌 각각의 원소의 개수보다 1번 적게 나올 경우 균형(balance)이라 한다. 또한, 시퀀스 $s(t)$에서 0이 아닌 τ, $1\le\tau\le N$에 대해 시퀀스의 차인 $s(t)-s(t+\tau)$ mod p가 균형일 경우 이 시퀀스는 차균형(difference-balance)을 이룬다고 한다. 단, 이 경우 $t+\tau$는 mod N 연산을 한다. 이제 ω가 1의 p차 원시원이라 하자. 그러면 시퀀스 $s(t)$의 주기적 자기상관 함수는 다음과 같이 정의된다.

$$R(\tau)=\sum_{t=0}^{N-1}\omega^{s(t)-s(t+\tau)}$$

이 때, 시퀀스 $s(t)$의 주기적 자기상관 함수 $R(\tau)$값이 다음과 같이 주어지면, $s(t)$는 이상적인 자기상관특성을 갖는다고 한다.

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

p진 시퀀스인 $s(t)$가 다음을 만족하면 $s(t)$를 특성시퀀스 또는 특성위상시퀀스이라 한다.

$$s(t)-s(pt),\ \text{for all } t$$

또한, 0이 아닌 위상 변화에 대해 시퀀스가 차균형이라면, 그 시퀀스는 F_p상에서 이상적인 자기상관특성을 갖는다는 것은 쉽게 보일 수 있다.

이제 q가 소수의 멱승이고 F_q가 q개의 원소를 갖는 유한체라 하자. 또한, 몇몇 정수 e와 m에 대해 $n=em>1$이라 하자. 그러면 [3]에서 정의된 trace 함수 $tr_m^n(\cdot)$은 F_{p^n}에서 그 하위체인 F_{p^m}으로의 사상이 되고 다음과 같이 정의된다.

$$tr_m^n(x)=\sum_{i=0}^{e-1}x^{p^{mi}},$$

단, 위 식에서 x는 유한체 F_{p^n}의 원소이다.

Trace함수를 이용하면, 주기가 $N=p^n-1$인 p진 m-시퀀스 $m(t)$는 다음과 같이 쉽게 표현 될 수 있다.

$$m(t) = tr_1^n(\alpha^t) \quad (1)$$

단, p는 소수이고 α는 유한체 F_{p^n}의 원시원이다.

또한 (1)에서 정의한 m-시퀀스가 균형성과 차균형성을 갖는다는 것은 쉽게 증명될 수 있다. 더 나아가서 m-시퀀스는 다음과 같은 다중 특성위상 특성을 갖는다 :

정리 1 : $T = \frac{p^n - 1}{p-1}$이라 하자. 이 때, $m(t)$가 (1)에서 정의된 m-시퀀스라 하면, 이 시퀀스는 모든 $t, 0 \le t \le N-1$과 $i, 0 \le i \le p-2$에 대해 다음과 같이 $p-1$개의 서로 다른 특성위상을 갖는다.

$$m(t-iT) = m(p(t-iT)),$$

증명 : 시퀀스 $m(t-iT)$는 다음과 같이 나타낼 수 있다.

$$m(t-iT) = tr_1^n(\alpha^{-iT} \cdot \alpha^t)$$

단, α^T는 $F_p = \{0, 1, 2, 3, \cdots, p-1\}$의 원시원이다. 따라서 위의 등식은 다음과 같이 다시 쓸 수 있다.

$$m(t-iT) = \alpha^{-iT} \cdot tr_1^n(\alpha^t)$$

위 식에서 α^{-iT}는 F_p상의 0이 아닌 원소이다. 따라서 $m(t)$가 특성위상을 가짐에 따라 $\alpha^{iT} \cdot tr_1^n(\alpha^t)$ 역시 $i, 0 \le i \le p-2$에 대해 특성 위상을 가지게 된다. □

Klapper는 $d-$동차시퀀스를 만드는데 사용되는 $d-$동차 함수 $H(x)$에 대해 소개하였다. 그의 논문에서 F_{p^n}에서 F_{p^m}상의 $d-$동차 함수는 모든 $x \in F_{p^n}$과 $y \in F_{p^m}$에 대해 다음을 만족하는 차수가 d인 동차 함수를 의미한다.

$$H(yx) = y^d H(x) \quad (2)$$

$d-$동차 함수 $H(x)$를 이용하여, 그는 다음과 같은 $d-$동차시퀀스를 생성하였다.

정의 2 [Klapper [6]] : m, n이 $m|n$인 정수이고, p는 소수, α는 F_{p^n}의 원시원, $T = (p^n-1)/(p^m-1)$에 대해 $\beta = \alpha^T$이라 하자. 이 때, $1 \le r \le p^m - 2$인 p^m -1과 서로 소인 정수 r에 대해 주기가 $p^n - 1$인 $d-$동차시퀀스는 다음과 같이 정의된다.

$$c_d(t) = tr_1^m([H(\alpha^t)]^r) \quad (3)$$

단, 위 식에서 $x \in F_{p^n}$, $y \in F_{p^m}$이다. □

기하시퀀스의 특별한 경우로 No와 Yang, Chung, Song[12]은 이상적인 자기상관 특성을 갖는 이진 시퀀스가 주어졌을 때 보다 긴 주기를 갖고 이상적인 자기상관특성을 갖는 이진 시퀀스의 생성 방법인 확장시퀀스라 불리는 이상적인 자기상관특성을 갖는 시퀀스를 발견하였다. 이제 다음의 정리에서 이진에서 p진으로 확장함으로써 이진 확장시퀀스의 생성법을 p진 확장 시퀀스의 생성법으로 쉽게 변환할 수 있다.

정리 3 : m, n이 $m|n$인 양수이고, p는 소수, α는 F_{p^n}의 원시원, $T = (p^n-1)/(p^m-1)$에 대해 $\beta = \alpha^T$이라 하자. 이제, 주어진 집합 I에 대해 주기가 $M = p^m - 1$인 다음과 같이 주어진 시퀀스 $b(t_1)$가 이상적인 자기상관특성을 갖는다고 가정하자.

$$b(t_1) = \sum_{a \in I} tr_1^m(\beta^{at_1})$$

그러면 $1 \le r \le M-1$이고 M과 서로소인 정수 r에 대해 다음과 같이 정의된 주기가 $N = p^n - 1$인 p진 확장 시퀀스는 이상적인 자기상관특성을 가진다.

$$c(t) = \sum_{a \in I} tr_1^m\{[tr_m^n(\alpha^t)]^{ar}\} \quad □$$

위 정리에 대한 증명은 이진 확장 시퀀스의 증명[12]과 거의 같고 따라서 본 논문에서는 증명을 생략한다. 다음 장에 나오는 $d-$동차 함수로부터 $d-$동차시퀀스를 생성하는 것은 이상적인 자기상관특성을 갖는 시퀀스를 만드는 새로운 방법이다.

Ⅲ. p진 $d-$동차시퀀스

$d-$동차시퀀스를 생성시키기 위해서는, 우선 그에 따른 $d-$동차 함수를 찾아야 한다. 그러나 GMW 시퀀스와 직렬 GMW 시퀀스와 같은 자명한 경우를 제외하고는 이상적인 자기상관특성을 갖는 $d-$동차 함수를 만드는데 이용되는 $d-$동차 함수를 찾는 것은 쉽지 않은 일이다. 따라서 이제까지 대부분의 $d-$동차시퀀스에 대한 연구는 TN 시퀀스[6]와 같이 좋은 상호상관특성을 갖는 $d-$동차시퀀

스군에 대해서 이루어져 왔다. 그런데 TN 시퀀스가 이상적인 자기상관특성을 갖는 $d-$동차시퀀스를 포함하는 $d-$동차시퀀스군이기는 하지만 그것은 직렬 GMW 시퀀스이다. 최근 Klapper는 $d-$동차시퀀스군을 이루는 시퀀스들의 자기상관 값을 포함한 $d-$동차 함수를 이용하여 만든 $d-$동차시퀀스군의 상호 상관 값을 유도하였다. (3)에서처럼 주기가 p^n-1인 이상적인 자기상관특성을 갖는 $d-$동차시퀀스를 생성시키기 위해서는 먼저 (2)를 만족시키는 $d-$동차 함수를 찾아야만 한다. 이는 Klapper에 의해 이미 발표되었고[6] 본 논문에서는 이를 다음과 같이 약간 변형하여 사용한다.

정리 4 : m, n이 $m|n$인 양수이고, p는 소수, $M=p^m-1$, α는 F_{p^n}의 원시원, $T=(p^n-1)/(p^m-1)$에 대해 $\beta=\alpha^T$이라 하자. 이제 M과 서로 소인 $1\le d\le M-1$인 d에 대해 $H(\alpha^t)$가 $d-$동차 함수라 하면, M과 서로 소이고 $1\le r\le M-1$인 정수 r에 대해 주기가 p^n-1인 $d-$동차시퀀스가 다음과 같이 주어진다 하자.

$$c_d(t)=tr_1^m([H(\alpha^t)]^r) \tag{4}$$

이 때, 위 시퀀스가 이상적 자기상관특성을 갖는다는 것과 0이 아닌 위상변화 τ에 대해 다음 집합의 크기가 $\dfrac{p^{n-m}-1}{p^m-1}$이라는 것은 동치이다.

$$\{t|H(\alpha^t)=H(\alpha^{t+\tau}),\ 0\le t\le T-1\}$$

증명 : 우선 t_1과 t_2가 다음과 같이 T를 기저로 하는 t의 전개에 쓰이는 단위라 하자.

$$t=t_1\cdot T+t_2,\ 0\le t_1\le M-1,\ 0\le t_2\le T-1$$

그러면 p진 d동차시퀀스 $c_d(t)$의 차는 다음과 같이 2차원적인 표현으로 다시 쓸 수 있다.

$$\begin{aligned}c_d(t)= &\ c_d(t+\tau)\\ =&\ tr_1^m\{[H(\alpha^t)]^r\}-tr_1^m\{[H(\alpha^{t+\tau})]^r\}\\ =&\ tr_1^m\{\beta^{drt_1}\{[H(\alpha^{t_2})]^r-[H(\alpha^{t_2+\tau})]^r\}\}\end{aligned}$$

단, 위 식에서 dr은 M과 서로 소이고 하위시퀀스는 $H(\alpha^{t_2})=H(\alpha^{t_2+\tau})$인 경우 모두 0인 시퀀스가 되고, $H(\alpha^{t_2})\ne H(\alpha^{t_2+\tau})$인 경우 균형성을 갖는 p진 m-시퀀스 $tr_1^m(\beta^{drt_1})$의 순환 이동이 된다. 따라서 m-시퀀스의 균형성으로부터 다음이 성립함을 알 수 있다.

$$\sum_{t=0}^{M-1}\omega^{tr_1^m(\beta^t)}=-1$$

단, 위 식에서 ω는 1의 p차 원시원이다. 또한, 임의의 0이 아닌 τ에 대해 t_2가 0에서 $T-1$까지 변함에 따라 $H(t_2)=H(t_2+\tau)$는 $A=\dfrac{p^{n-m}-1}{p^m-1}$번 발생하게 된다. 그러므로 임의의 0이 아닌 τ에 대해 시퀀스 $c_d(t)$의 자기상관 값은 다음과 같이 구할 수 있다.

$$R(\tau)=\sum_{t=0}^{N-1}\omega^{c_d(t)-c_d(t+\tau)}=-1$$

따라서 $c_d(t)$는 모든 0이 아닌 τ에 대해 이상적인 자기상관특성을 갖는다. □

이상적인 자기상관특성을 갖는 p진 $d-$동차시퀀스를 만들기 위해서는 정리 4에서 유도된 성질을 만족하는 $d-$동차 함수 $H(\alpha^t)$를 먼저 찾아야만 한다. 따라서 다음 정리에서는 $d-$동차시퀀스를 생성하는데 사용될 수 있는 $d-$동차 함수에 대해 제안한다.

정리 5 : m, n이 $m|n$인 양수이고, p는 소수, α는 F_{p^n}의 원시원이라 하자. 또한 주어진 집합 I의 모든 원소 s가 p^m-1과 서로 소인 주어진 d에 대해 $s\equiv d \bmod (p^m-1)$을 만족시킨다 하자. 그러면 다음과 같이 주어진 F_{p^n}에서 F_{p^m}으로의 함수는 F_{p^n}에서 F_{p^m}상의 $d-$동차 함수이다.

$$H(\alpha^t)=\sum_{s\in I}tr_m^n(\alpha^{st}) \tag{5}$$

증명 : 우선 β가 F_{p^m}의 원소라 하자. 그러면 다음이 성립한다.

$$\begin{aligned}H(\beta\alpha^t)\ &=\sum_{s\in I}tr_m^n((\beta\alpha^t)^s)\\ &=\beta^d\cdot H(\alpha^t)\end{aligned}$$

단, 위 식에서 $s\equiv d \bmod (p^m-1)$이므로 주어진 집합 I의 모든 s에 대해 $\beta^s=\beta^d$가 성립한다. □

정리 4와 5를 이용하면, 다음의 정리에 나오는 것과 같은 이상적인 자기상관특성을 갖는 p진 $d-$동차시퀀스를 생성할 수 있다.

정리 6 : m, n이 $m|n$인 양수이고, p는 소수, $M=p^m-1$, α는 F_{p^n}의 원시원,

$T=(p^n-1)/(p^m-1)$에 대해 $\beta=\alpha^T$이라 하자. 또한, M과 서로 소인 d에 대해 주어진 집합 I의 모든 원소 s가 $s\equiv d \bmod M$을 만족한다 하자. 이 때, 다음과 같이 주어지는 주기가 $N=p^n-1$인 p진 시퀀스가 이상적인 자기상관특성을 갖는다고 가정하자.

$$c(t)=\sum_{s\in I} tr_1^n(\alpha^{st}) \qquad (6)$$

그러면 $1\le r\le M-1$이고 M과 서로 소인 주어진 정수 r에 대해 다음과 같이 주어진 주기가 N인 p진 $d-$동차시퀀스 $c_d(t)$는 이상적인 자기상관특성을 갖는다.

$$c_d(t)=tr_1^m\{[\sum_{s\in I} tr_m^n(\alpha^{st})]^r\} \qquad (7)$$

증명 : 우선 t_1과 t_2가 다음과 같이 T를 기저로 하는 t의 전개에 쓰이는 단위라 하자.

$$t=t_1\cdot T+t_2,\ 0\le t_1\le M-1,\ 0\le t_2\le T-1$$

그러면, (6)의 p진 시퀀스는 다음과 같이 t_1, t_2에 대해 나타낼 수 있다.

$$\begin{aligned} c(t) &= \sum_{s\in I} tr_1^m\{tr_m^n(\alpha^{st_1T+st_2})\} \\ &= tr_1^m\{\beta^{dt_1}\cdot \sum_{s\in I} tr_m^n(\alpha^{st_2})\} \end{aligned}$$

단, 위 식에서 $s\equiv d \bmod (p^m-1)$이므로 주어진 집합 I의 모든 s에 대해 $\beta^s=\beta^d$가 성립한다. 이제 $g(t_2)$가 다음과 같이 정의된 함수라 하자.

$$\beta^{d\cdot g(t_2)}=\sum_{s\in I} tr_m^n(\alpha^{st_2}) \qquad (8)$$

그러면 시퀀스 $c(t)$는 다음과 같이 쓸 수 있다.

$$c(t)=tr_1^m\{\beta^{d(t_1+g(t_2))}\}$$

단, 위 식에서 $c(t)$의 하위시퀀스는 $0\le t_2\le T-1$의 임의의 고정된 t_2에 대해 $g(t_2)=-\infty$인 경우는 주기가 M인 0시퀀스이고, 다른 경우는 주기가 M인 p진 decimated 시퀀스 $tr_1^m(\beta^{t_1})$의 위상 변화가 된다. 우선 $c(t)$가 이상적인 자기상관특성을 가졌다고 가정하자. 이 때, $c(t)$의 시퀀스의 차는 다음과 같이 나타난다.

$$\begin{aligned} c(t)-c(t+\tau) &= tr_1^m\{\beta^{d(t_1+g(t_2))}\}-tr_1^m\{\beta^{d(t_1+g(t_2+\tau))}\} \\ &= tr_1^m\{\beta^{d(t_1+g(t_2))}-\beta^{d(t_1+g(t_2+\tau))}\} \end{aligned}$$

그러면 시퀀스 $c(t)$의 자기상관 함수 $R(\tau)$는 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned} R(\tau) &= \sum_{t_2=0}^{T-1}\sum_{t_1=0}^{M-1}\omega^{c(t_1T+t_2)-c(t_1T+t_2+\tau)} \\ &= \sum_{t_2=0}^{T-1}\sum_{t_1=0}^{M-1}\omega^{tr_1^m\{\beta^{d(t_1+g(t_2))}-\beta^{d(t_1+g(t_2+\tau))}\}} \end{aligned}$$

이제 $R_{sub}(\tau,t_2)$가 다음과 같이 정의된 임의의 고정된 $0\le t_2\le T-1$인 t_2에 대해 모두 0이 아닌 하위시퀀스의 자기상관 함수라 하자.

$$R_{sub}(\tau,t_2)=\sum_{t_1=0}^{M-1}\omega^{tr_1^m\{\beta^{d(t_1+g(t_2))}-\beta^{d(t_1+g(t_2+\tau))}\}}$$

하위시퀀스 역시 p진 m-시퀀스이므로 하위시퀀스의 자기상관 함수 값은 다음과 같은 값을 취한다.

$$R_{sub}(\tau,t_2)=\begin{cases} p^m-1, & \text{if } g(t_2)=g(t_2+\tau) \\ -1, & \text{if } g(t_2)\ne g(t_2+\tau) \end{cases}$$

따라서 시퀀스 $c(t)$의 자기상관함수는 $0\le t_2\le T-1$인 t_2상에서 다음과 같은 $R_{sub}(\tau,t_2)$의 합으로 나타낼 수 있다.

$$R(\tau)=\sum_{t_2=0}^{T-1}R_{sub}(\tau,t_2)$$

이제, 임의의 0이 아닌 τ에 대해 $0\le t_2\le T-1$로 t_2가 변함에 따라 $g(t_2)=g(t_2+\tau)$가 A번 발생하고 $g(t_2)\ne g(t_2+\tau)$가 $T-A$번 발생한다고 가정하자. 이 때, 시퀀스 $c(t)$와 그 하위시퀀스가 모두 이상적인 자기상관특성을 가진다는 가정을 이용하면, 임의의 0이 아닌 τ에 대해 다음의 등식이 성립함을 알 수 있다.

$$\begin{aligned} R(\tau) &= A\cdot(p^m-1)+(T-A)\cdot(-1) \\ &= (-1) \end{aligned}$$

위의 관계로부터 A는 $\frac{p^{n-m}-1}{p^m-1}$로 계산되고, 따라서 t_2가 0에서 $T-1$까지 변하는 동안 임의의 0이 아닌 τ에 대해 $g(t_2)=g(t_2+\tau)$가 $\frac{p^{n-m}-1}{p^m-1}$번 발생하게 된다. 이제, $d-$동차시퀀스 $c_d(t)$가 이상적인 자기상관특성을 갖는다는 것을 증명하겠다. 우선 그 전에 $d-$동차시퀀스 $c_d(t)$의 차를 다음과 같이 2차원적으로 나타낼 수 있다.

$$\begin{aligned} c_d(t)-c_d(t+\tau) &= tr_1^m\{\beta^{drt_1}\cdot[\sum_{s\in I} tr_m^n(\alpha^{st_2})]^r\} \\ &\quad - tr_1^m\{\beta^{drt_1}\cdot[\sum_{s\in I} tr_m^n(\alpha^{s(t_2+\tau)})]^r\} \end{aligned}$$

위 식에 함수 $g(t_2)$를 사용하면 $d-$동차시퀀스 $c_d(t)$의 차는 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned} c_d(t) - c_d(t+\tau) &= tr_1^m\{\alpha^{Tdrt_1}[\beta^{d\cdot g(t_2)}]^r\} \\ &\quad - tr_1^m\{\alpha^{Tdrt_1}[\beta^{d\cdot g(t_2+\tau)}]^r\} \\ &= tr_1^m\{\beta^{dr(t_1+g(t_2))}\} \\ &\quad - tr_1^m\{\beta^{dr(t_1+g(t_2+\tau))}\} \end{aligned}$$

단, 위 식에서 dr은 M과 서로 소이고 $\gcd(dr, p^m-1)=1$이므로, 하위시퀀스는 0시퀀스이거나 위상이 변화된 p진 m-시퀀스 $tr_1^m(\beta^{drt_1})$이다. 이제까지의 결과로부터, t_2가 0에서 $T-1$까지 변함에 따라 임의의 0이 아닌 τ에 대해 $g(t_2)=g(t_2+\tau)$는 $A=\dfrac{p^{n-m}-1}{p^m-1}$번 발생한다는 것을 알 수 있다. 또한, 시퀀스 $c(t)$의 자기상관 값을 구하는 것과 유사한 방식으로 임의의 0이 아닌 τ에 대해 시퀀스 $c_d(t)$의 자기상관 값을 다음과 같이 계산 할 수 있다.

$$\begin{aligned} R_d(\tau) &= A\cdot(p^m-1)+(T-A)\cdot(-1) \\ &= -1 \end{aligned}$$

위 식에 의해 시퀀스 $c_d(t)$가 이상적인 자기상관특성을 가짐을 알 수 있다. □

Helleseth와 Kumar, Martinsen은 다음의 정리와 같은 p진 m-시퀀스와 p진 직렬 GMW 시퀀스를 제외하고는 최초의 이상적인 자기상관특성을 갖는 비이진 시퀀스인 새로운 3진 시퀀스를 찾아내었다.

정리 7 [Helleseth, Kumar, Martinsen[9]]: $s=3^{2m}-3^m+1$이고 $n=3m$, α는 $F_{3^{3m}}$의 원시원이라 하자. 이 때, 다음과 같이 주어지는 주기가 $3^{3m}-1$인 3진 시퀀스는 이상적인 자기상관특성을 갖는다.

$$c(t) = tr_1^n(\alpha^t)+tr_1^n(\alpha^{st}) \tag{9}$$

□

이제, e, k는 정수이고 $m=e\cdot k$라 하자. 이 때 (9)의 시퀀스의 계수들의 집합 I는 다음과 같이 $I=\{1,\ 3^{2ek}-3^{ek}+1\}$로 주어진다.

단, 위 식에서 $3^{2ek}-3^{ek}+1\equiv 1 \bmod 3^k-1$이다. 따라서 주어진 집합 I의 모든 원소는 1 mod 3^k-1이 성립하고 시퀀스는 이상적인 자기상관특성을 갖는다. 또한 (9)에서 주어진 시퀀스는 정리 6에서 가정한 시퀀스(6)의 계수들의 집합인 I의 조건을 만족한다. 그러므로 별도의 증명 없이 이상적인 자기상관특성을 갖는 3진 $d-$동차시퀀스가 다음과 같이 주어질 수 있다.

정리 8 : $s=3^{2ek}-3^{ek}+1$이고, 양수 e, k에 대해 $n=3ek$, α는 $F_{3^{3ek}}$의 원시원이라 하자. 또, r은 3^k-1과 서로 소인 $1\le r\le 3^k-2$인 정수라 하자. 이때 다음과 같이 주어지는 3진 $d-$동차시퀀스는 이상적인 자기상관특성을 갖는다.

$$c_d(t) = tr_1^k\{[tr_k^{3ek}(\alpha^t)+tr_k^{3ek}(\alpha^{st})]^r\} \qquad □$$

이제까지는 정리 9에서 정의된 이상적인 자기상관특성을 갖는 3진 $d-$동차시퀀스가 이진과 비이진 시퀀스를 통틀어 이상적인 자기상관특성을 갖는 유일한 $d-$동차시퀀스였다. 또한 이진의 경우 정리 4에서 유도된 특성을 만족하는 $d-$동차 함수가 아직 발표되지 않았다. 따라서 GMW 시퀀스와 직렬 GMW 시퀀스를 제외하고는 이상적인 자기상관특성을 갖는 이진 $d-$동차시퀀스는 없다.

Ⅳ. p진 통합시퀀스

이번 장에서는 다음 정리에서와 같이 $d-$동차시퀀스의 생성 방법과 확장시퀀스의 생성 방법을 조합한 통합시퀀스(확장 $d-$동차시퀀스)라 불리는 새로운 시퀀스의 생성방법을 제안한다.

정리 9 : m, n이 $m|n$인 양의 정수이고 p는 소수, α는 F_{p^n}의 원시원, $T=\dfrac{p^n-1}{p^m-1}$에 대해 $\beta=\alpha^T$이라 하자. 이때, 계수들의 집합 I에 대해 다음과 같이 주어진 주기가 $M=p^m-1$인 시퀀스 $b_u(t_1)$가 이상적인 자기상관특성을 가졌다고 가정하자.

$$b_u(t_1) = \sum_{a\in I} tr_1^m(\beta^{at_1}) \tag{10}$$

이제, 어떤 계수들의 집합인 J에 대해 J의 모든 원소 s가 M과 서로 소인 d에 대해 $s\equiv d \bmod p^m-1$를 만족한다 하자. 또한, 다음과 같이 주어진 주기가 $N=p^n-1$인 p진 시퀀스 $c(t)$가 이상적인 자기상관특성을 가졌다고 가정하자.

$$c(t)=\sum_{s\in J} tr_1^n(\alpha^{st})$$

이 때, M과 서로 소인 $1\le r\le M-1$인 정수 r에 대해 주기가 $N=p^n-1$인 통합시퀀스 $c_u(t)$는 다음과 같이 정의되고 이 시퀀스는 이상적인 자기상관특성을 갖는다.

$$c_u(t)=\sum_{a\in I} tr_1^m\{[\sum_{s\in J} tr_m^n(\alpha^{st})]^{ar}\} \quad (11)$$

증명 : 정리 6의 증명과 유사하게, t_1과 t_2가 다음과 같이 T를 기저로 하는 t의 전개에 쓰이는 단위라 하자.

$$t=t_1\cdot T+t_2,\ 0\le t_1\le M-1,\ 0\le t_2\le T-1$$

이 때, (11)의 p진 통합시퀀스 $c_u(t)$는 다음과 같이 2차원적으로 전개 할 수 있다.

$$\begin{aligned} c_u(t)&=\sum_{a\in I} tr_1^m\{\alpha^{asrTt_1}[\sum_{s\in J} tr_m^n(\alpha^{st_2})]^{ar}\}\\ &=\sum_{a\in I} tr_1^m\{\beta^{adrt_1}[\beta^{d\cdot g(t_2)}]^{ar}\}\\ &=\sum_{a\in I} tr_1^m\{\beta^{adr(t_1+g(t_2))}\}\end{aligned}$$

단, 위 식에서 $g(t_2)$는 (8)에서 정의된 함수이다. 또한 $\gcd(dr,M)=1$이므로 $c_u(t)$의 하위시퀀스는 $0\le t_2\le T-1$에서 고정된 임의의 t_2에 대해 $g(t_2)=-\infty$인 경우 주기가 M인 0시퀀스가 되고, 그 이외의 경우는 다음과 같이 주어진 주기가 $M=p^m-1$인 (10)의 p진 시퀀스를 dr로 decimated시킨 시퀀스의 위상 변화가 된다.

$$b_u(drt_1)=\sum_{a\in I} tr_1^m(\beta^{adrt_1})$$

이제 하위시퀀스 $b_u(drt_1)$역시 이상적인 자기상관특성을 가졌다고 가정하자. 이 때, 다음과 같이 정의된 하위시퀀스 $b_u(drt_1)$의 자기상관함수 $R_{u,sub}(\tau,t_2)$의 값은 p^m-1이거나 -1이 된다.

$$\begin{aligned} &R_{u,sub}(\tau,t_2)\\ &\quad=\sum_{t_1=0}^{M-1}\omega^{b_u(dr(t_1+g(t_2)))-b_u(dr(t_1+g(t_2+\tau)))}\end{aligned}$$

즉, 다음이 성립한다.

$$R_{u,sub}(\tau,t_2)=\begin{cases} p^m-1, & \text{if } g(t_2)=g(t_2+\tau)\\ -1, & \text{if } g(t_2)\ne g(t_2+\tau)\end{cases}$$

따라서 통합시퀀스 $c_u(t)$의 차는 다음과 같이 나타낼 수 있다.

$$\begin{aligned} &c_u(t)-c_u(t+\tau)\\ &=\sum_{a\in I} tr_1^m\{\beta^{adrt_1}[\beta^{d\cdot g(t_2)}]^{ar}\}\\ &\quad-\sum_{a\in I} tr_1^m\{\beta^{adrt_1}[\beta^{d\cdot g(t_2+\tau)}]^{ar}\}\\ &=\sum_{a\in I} tr_1^m\{\beta^{adr(t_1+g(t_2))}\}-\sum_{a\in I} tr_1^m\{\beta^{adr(t_1+g(t_2+\tau))}\}\end{aligned}$$

그러므로 통합시퀀스 $c_u(t)$의 자기상관 값은 다음과 같이 주어진다.

$$\begin{aligned} R(\tau)&=\sum_{t_2=0}^{T-1}\sum_{t_1=0}^{M-1}\omega^{b_u(dr(t_1+g(t_2)))-b_u(dr(t_1+g(t_2+\tau)))}\\ &=\sum_{t_2=0}^{T-1} R_{u,sub}(\tau,t_2)\end{aligned}$$

정리 6에서 시퀀스의 자기상관 값과 유사하게 임의의 0이 아닌 τ에 대해 통합시퀀스 $c_u(t)$의 자기상관 값은 $0\le t_2\le T-1$인 t_2상에서 이상적인 자기상관특성을 갖는 하위시퀀스의 자기상관함수의 합의 형태로 나타난다. 정리 6의 증명에서 임의의 0이 아닌 τ에 대해 t_2가 0에서 $T-1$까지 변할 때, $g(t_2)=g(t_2+\tau)$가 $A=\frac{p^{n-m}-1}{p^m-1}$번 발생한다는 것은 이미 증명하였다. 따라서 임의의 0이 아닌 τ에 대해 통합시퀀스 $c_u(t)$의 자기상관 값은 -1로 계산된다. 그러므로 통합시퀀스 $c_u(t)$는 이상적인 자기상관특성을 갖는다. □

통합시퀀스는 $d-$동차시퀀스와 확장시퀀스를 포함하는 매우 일반적인 시퀀스의 분류이다. 즉, $J=\{1\}$일 경우 (11)에서 정의된 통합시퀀스는 다음과 같은 이상적인 자기상관특성을 갖는 통합시퀀스가 된다.

$$c_u(t)=\sum_{a\in I} tr_1^m\{[tr_m^n(\alpha^t)]^{ar}\} \quad (12)$$

정리 9에서 $m=3k$이고 양의 정수 e와 k에 대해 $n=9ek$라 하자. 이 때, 정리 9와 Helleseth와 Kumar, Martinsen이 찾아낸 이상적인 자기상관특성을 갖는 3진 시퀀스를 이용하면 별도의 증명 없이 $m=3k$, $n=9ek$에 대해 통합시퀀스를 만들 수 있다.

정리 10 : e, k는 양수이고, $m=3k$, $n=9ek$, α는 $F_{3^{9ek}}$의 원시원 $T=\frac{3^{9ek}-1}{3^{3k}-1}$에 대해 $\beta=\alpha^T$이라 하자. 이 때, 다음과 같이 주어지는 주기가 $M=3^{3k}-1$인 3진 시퀀스 $b_u(t_1)$은 이상적인 자기상관특성을 갖는다.

$$b_u(t_1) = \sum_{a \in I} tr_1^{3k}(\beta^{at_1})$$

단, 앞 식에서 계수들의 집합 I는 $\{1, 3^{2k}-3^k+1\}$이고, J는 $\{1, 3^{6ek}-3^{3ek}+1\}$이다. 또한 계수들의 집합 J의 모든 원소 s에 대해 $s \equiv 1 \bmod 3^{3k}-1$이 성립하는 것과 $d=1$이 $3^{3k}-1$과 서로 소인 것은 자명하다. 따라서 다음과 같이 주어지는 주기가 $3^{9ek}-1$인 3진 시퀀스 $c(t)$는 이상적인 자기상관특성을 갖는다.

$$c(t) = \sum_{s \in J} tr_1^{9ek}(\alpha^{st}) \tag{13}$$

또한, $3^{3k}-1$과 서로 소인 $1 \le r \le 3^{3k}-2$인 정수 r과 $s=3^{6ek}-3^{3ek}+1$, $a=3^{2k}-3^k+1$에 대해 다음과 같이 정의된 주기가 $3^{9ek}-1$인 3진 통합시퀀스 $c(t)$는 이상적인 자기상관특성을 갖는다.

$$\begin{aligned} c_u(t) \\ = \ & tr_1^{3k}\{[tr_{3k}^{9ek}(\alpha^t) + tr_{3k}^{9ek}(\alpha^{st})]^r\} \\ & + tr_1^{3k}\{[tr_{3k}^{9ek}(\alpha^t) + tr_{3k}^{9ek}(\alpha^{st})]^{ar}\} \end{aligned} \tag{14}$$

□

현재까지는 정리 10에서 주어진 이상적인 자기상관특성을 갖는 3진 통합시퀀스가 이진과 비이진을 포함하여 이상적인 자기상관특성을 갖는 유일한 통합시퀀스이다. 이 때, (15)에서 $J=\{1\}$로 대신하면 통합시퀀스는 다음과 같은 이상적인 자기상관 값을 갖는 3진 확장 시퀀스가 된다.

$$\begin{aligned} c_u(t) = \ & tr_1^{3k}\{[tr_{3k}^{9ek}(\alpha^t)]^r\} \\ & + tr_1^{3k}\{[tr_{3k}^{9ek}(\alpha^t)]^{(3^{2k}-3^k+1)r}\} \end{aligned}$$

단, 위 식에서 r은 $3^{3k}-1$과 서로 소인 $1 \le r \le 3^{3k}-2$인 정수이다.

본 논문에서는 이상적인 자기상관특성을 갖는 새로운 p시퀀스를 생성하는 방법을 제안하고 여러 가지 예를 제시하였다. 이러한 새로운 시퀀스는 차집합의 생성 및 통신시스템의 여러분야에서 활용될 수 있을 것이다.

참 고 문 헌

[1] L.D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathmatics, Springer Verlag, 1991.

[2] S.W. Golomb, *Shift-Register Sequences*, Revised Ed., Aegean Park Press San Francisco, 1982.

[3] R. Lidl and H. Neiderreiter, *Finite Fields*, vol. 20 of Encyclopedia of Mathmatics and Its applications, Addision-Wesley, Reading, MA, 1983.

[4] A.H. Chan and R. Games, "On the linear span of binary sequences from finite geometries, q odd," in *Proc. Crypto 1986*, Santa Barbara, CA, pp. 405-417, 1986.

[5] M. Goresky, A.H. Chan and A. Klapper, "Cross-correlation of linearly and quadratically related geometric sequences and GMW sequences," *Discrete Appl. Math.*, vol. 46, no. 1, pp. 1-20, 1993.

[6] A. Klapper, "*d*-form sequences: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423-431, Mar 1995.

[7] A. Klapper, A.H. Chan, and M. Goresky, "Cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 177-183, Jan. 1993.

[8] G. Gong, "Q-ary cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 263-267, Jan. 1996.

[9] T. Helleseth, P.V. Kumar, and H.M. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation function," *Proceedings of International Symposium on Information Theory*, pp. 328, Jun 2000.

[10] 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. 35, no. 2, pp. 371-379, Mar 1989.

[11] J.S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. Dissertation, University of Southern California, May, 1988.

[12] 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*

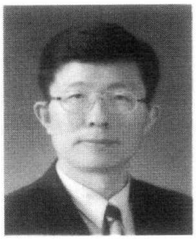
'96), pp. 837-840, Victoria, B.C., Canada, Sept. 17-20, 1996.

[13] J.S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 1, pp. 260-262, Jan. 1996.

[14] R.A. Scholtz and L.R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory,* vol. IT-30, no. 3, pp. 548-553, May 1984.

[15] M.K. Simon, J.K. Omura, R.A. Sholtz, and B.K. Levitt, *Spread Spectrum Communications,* vol. 1, Computer Science Press, Rockville, MD, 1985.

노 종 선(Jong-Seon No) 종신회원



1981년 2월 : 서울대학교 전자공학과 공학사

1984년 2월 : 서울대학교 대학원 전자공학과 공학석사

1988년 5월 : University of Southern California, 전기공학과 공학박사

1988년 2월~1990년 7월 : Hughes Network Systems, Senior MTS

1990년 9월~1999년 7월 : 건국대학교 전자공학과 부교수

1999년 8월~현재 : 울대학교 전기 · 컴퓨터공학부 부교수

<주관심 분야> 시퀀스, 오류정정부호, 암호학, 이동통신