通信情報保護學會論文誌
第 8 卷 第 1 號, 1998. 3

Extended Legendre 시퀀스의 선형스팬

노 종 선*, 정 채 홍*

Linear Span of Extended Legendre Sequences

Jong-Seon No, Chea-Hong Jeong

요 약

본 논문에서는 2^m-1의 머센소수 주기를 갖는 Legendre 시퀀스에 확장이론을 적용하여 유도되는 주기가 $2^{em}-1$인 extended Legendre 시퀀스를 decimated m-시퀀스들의 합으로 표현하였으며 이를 이용하여 extended Legendre 시퀀스의 선형스팬의 상한식 및 선형스팬에 관한 conjecture를 유도하였다.

Abstract

In this paper, extended Legendre sequences of period $2^{em}-1$ which are drived from extension of Legendre sequences of Mersenne prime period of 2^m-1 are expressed by summation of decimated m-sequences and upper bound for linear span of extended Legendre sequences and conjecture for linear span are derived.

키워드: Legendre 시퀀스, 선형스팬, extended Legendre 시퀀스, 의사불규칙시퀀스, 자기상관특성

I. 서 론

의사불규칙시퀀스(pseudorandom sequence)들은 확산스펙트럼통신시스템 및 스트림암호화시스템 등에서 많은 응용분야를 갖고 있다.[5] 지금까지 발견된 주기가 2^n-1이고 이상적인 자기상관특성을 갖는 의사불규칙시퀀스들을 보면 m-시퀀스, GMW 시퀀스, generalized GMW 시퀀스, Legendre 시퀀스, extended 시퀀스 등이 있다.[1,2,3,5,6,7,10,11] 특히 최근 들어서 시퀀스의 확장(extension)이론에 의해 이상적인 자기상관특성을 갖는 짧은 주기의 의사불규칙시퀀스로부터 이상적인 자기상관특성을 갖는 긴 주기의 의사불규칙시퀀스를 유도할 수 있다는

본 논문은 1996년도 건국대학교 지원에 의한 논문임.

* 건국대학교 전자공학과

사실이 알려졌다.[7] 이를 이용하여 이상적인 자기상관특성을 갖는 주기가 $2^m - 1$인 Legendre 시퀀스로부터 주기가 $2^{em} - 1$인 extended Legendre 시퀀스를 만들 수 있다.[6,7]

그런데 이러한 의사불규칙시퀀스들의 성질 중에서 선형스팬(linear span)은 그 시퀀스의 복잡도를 나타내는 것으로 일반적으로 암호학 및 확산스펙트럼통신시스템에서 사용되는 시퀀스에서 매우 중요한 성질로 평가되고 있다. 의사불규칙시퀀스의 현재 값은 과거 몇개의 값들의 선형 결합에 의해서 다음과 같이 표현될 수 있다.[5]

$$s(t) = \sum_{i=1}^{L} a_i \cdot s(t-i) \qquad (1)$$

여기서 a_i는 0 또는 1의 값을 갖는 계수이다. 위의 수식을 만족시키는 최소의 L을 시퀀스의 선형스팬이라고 정의한다. 또한 선형스팬은 의사불규칙시퀀스를 유한체상의 원소들의 합으로 표현하는 경우 그 원소들의 개수로 정의될 수 있는데 의사불규칙시퀀스가 decimated m-시퀀스들의 합으로 표현될 수 있다면 이를 이용하여 쉽게 선형스팬을 구할 수 있을 것이다.

이상적인 자기상관특성을 갖는 의사불규칙시퀀스들 중, m-시퀀스는 선형스팬이 매우 짧아서 높은 보안성 요구되는 여러 응용분야에서의 활용에 많은 제약을 받고 있다. 그러나 GMW 시퀀스 및 generalized GMW 시퀀스는 선형스팬이 매우 큰 시퀀스로서 앞의 응용분야에 있어서 유용한 시퀀스로 알려져 있다.[8,9] 그리고 최근에 발견된 Legendre 시퀀스와 extended Legendre 시퀀스가 있는데 Legendre 시퀀스의 경우에는 선형스팬이 알려져 있으나 extended Legendre 시퀀스의 경우에는 선형스팬에 관한 구체적인 값이 알려져 있지 않다.[6, 7]

본 논문에서는 이상적인 자기상관특성을 갖는 주기가 $2^n - 1$인 extended Legendre 시퀀스의 성질 중 매우 중요한 선형스팬에 대한 특성을 규명하고자 한다. Ⅱ장에서는 Legendre 시퀀스의 trace 표현 및 선형스팬과 extended Legendre 시퀀스의 정의 등을 기술하였다. Ⅲ장에서는 extended Legendre 시퀀스를 decimated m-시퀀스들의 합으로 표현하는 식을 구하고 그에 따른 예를 들었다. 그리고 extended Legendre 시퀀스의 선형스팬의 상한식을 구하고 선형스팬에 관한 conjecture를 제안하였다. IV장에서는 conjecture에 관한 예를 들었고 V장에서 결론을 논하였다.

Ⅱ. Extended Legendre 시퀀스

a를 정수라 하고 p는 $p > 2$인 소수라 하면, Legendre symbol $(\frac{a}{p})$는 다음과 같이 0, +1, -1로서 정의된다.[6]

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ +1, & \text{if } a : \text{quadratic residue } mod\ p \\ -1, & \text{if } a : \text{quadratic nonresidue } mod\ p \end{cases} \qquad (2)$$

이러한 Legendre symbol에 있어서 0은 1로, +1은 0으로 -1은 1로 대치함에 의해서 주기가 p인 Legendre 시퀀스를 얻을 수 있다.

어떤 양의 정수를 이진수로 표현하였을 경우 그 이진수에서 1의 개수를 Hamming weight라 한다.

Trace함수 $tr_1^m(x)$은 유한체 $GF(2^m)$으로부터 다음과 같이 주어지는 부분체 $GF(2) = \{0, 1\}$로의 매핑(mapping)을 나타낸다.[4]

$$tr_1^m(x) = \sum_{i=0}^{m-1} x^{2^i} \qquad (3)$$

주기가 $M = 2^m - 1$이고 머센소수(Mersenne prime)인 경우 유한체상에서 정의되는 trace 함수를 이용하여 Legendre 시퀀스를 표현하면

다음과 같다.[6]

$$s(t) = \sum_{i=0}^{\frac{M-1}{2m}-1} tr_1^m(\beta^{u^{2i}t}) \quad (4)$$

여기서 u는 modulo M을 취한 정수들의 집합인 Z_M의 원시원(primitive element)이며, β는 $GF(2^m)$의 원시원이다. 위에서 정의된 Legendre 시퀀스는 이상적인 자기상관특성을 갖으며 선형스팬은 $(M-1)/2$이라고 알려져 있다.

최근에 발견된 시퀀스 확장이론에 의해서 이상적인 자기상관특성을 갖는 짧은 주기 2^m-1의 의사불규칙시퀀스로부터 이상적인 자기상관특성을 갖는 긴 주기의 의사불규칙시퀀스를 만들수 있다. 즉, 주기가 $M=2^m-1$인 Legendre 시퀀스를 이용하여 이상적인 자기상관특성을 갖는 주기가 $N=2^n-1$인 extended Legendre 시퀀스를 생성할 수 있는데 이를 trace 함수를 이용하여 표현하면 다음과 같다.[7]

$$c(t) = \sum_{i=0}^{\frac{M-1}{2m}-1} tr_1^m\{[tr_m^n(\alpha^r)]^{r\cdot u^{2i}}\} \quad (5)$$

여기서 α는 $GF(2^n)$의 원시원이고, $n=em$이고 e는 양의 정수이며 r은 $1 \le r \le 2^m-2$, $gcd(2^m-1, r)=1$이다.

Ⅲ. Extended Legendre 시퀀스의 선형스팬

일반적으로 의사불규칙시퀀스의 선형스팬은 그 시퀀스를 유한체 $GF(2^n)$상의 원소들의 합으로 표현하였을 때 서로 다른 원소의 개수로 정의될 수 있다. 따라서 비선형의사불규칙시퀀스의 선형스팬을 구하기 위해 그 시퀀스들을 decimated m-시퀀스들의 합으로 표현하는 것은 매우 중요하다. 따라서 식(5)에서 정의된 extended Legendre 시퀀스의 선형스팬을 구하기 위해 이 시퀀스들을 decimated m-시퀀스들의 합으로 표현하는 것은 의미가 있는 일이 될 것이다. 우선 extended Legendre 시퀀스의 정의식에서 지수인 $r\cdot u^{2i}$는 이진수로 다음과 같이 표현된다고 가정하자.

$$r\cdot u^{2i} = 2^{l_{i_0}} + 2^{l_{i_1}} + \cdots + 2^{l_{i_{w_i-1}}} \quad (6)$$

여기서 $l_{i_0} = 0 < l_{i_1} < l_{i_2} < \cdots < l_{i_{w_i-1}}$이고 w_i는 $r\cdot u^{2i}$을 이진수로 표현한 경우의 Hamming weight에 해당된다. GMW 시퀀스의 decimated m-시퀀스들의 합에 의한 표현식을 이용하면 다음과 같이 extended Legendre 시퀀스는 decimated m-시퀀스들의 합으로 표현될 수 있다.[7,8]

Theorem 1 : m, $n=em$, e는 각각 양의 정수이고, $M=2^m-1$이며, u는 modulo M을 취한 정수들의 집합인 Z_M의 원시원이라 하고 α는 $GF(2^n)$의 원시원이라 하자. $1\le r\le M-1$이며, M과 서로소인 정수 r에 대해, $N=2^n-1$의 주기를 갖는 시퀀스 $\{c(t), t=0, 1, \ldots, N-1\}$는 이상적인 자기상관특성을 갖으며 다음과 같이 decimated m-시퀀스들의 합으로 표현된다.

$$c(t) = \sum_{i=0}^{\frac{M-1}{2m}-1} tr_1^m\left\{[tr_m^n(\alpha^r)]^{\sum_{j=0}^{w_i-1}2^{l_{ij}}}\right\}$$

$$= \sum_{i=0}^{\frac{M-1}{2m}-1} \sum_{k_{i_1}=0}^{e-1} \sum_{k_{i_2}=0}^{e-1} \cdots \sum_{k_{i_{w_i-1}}=0}^{e-1} tr_1^n\left(\alpha^{(\sum_{j=0}^{w_i-1}2^{l_{ij}+k_{ij}\cdot m})t}\right) \quad (7)$$

여기서 $e=n/m$이고, w_i는 $r\cdot u^{2i}$을 이진수로 표현한 경우의 Hamming weight에 해당된다.

Example : $m=5$, $n=10$, $M=31$이고 Z_{31}의 원시원 $u=3$이라 하고, α는 $GF(2^{10})$의 원시원이라 하자. $1\le r\le 30$이며, 31과 서로 소인

정수 $r = 1$에 대해, $N = 1023$의 주기를 갖는 시퀀스 $\{c(t), t = 0, 1, ..., 1022\}$는 이상적인 자기상관특성을 갖으며 다음과 같이 decimated m-시퀀스들의 합으로 표현된다

$$c(t) = \sum_{i=0}^{\frac{31\cdot 1}{2\cdot 5}-1} tr_1^5\left\{[tr_5^{10}(\alpha^t)]^{\sum_{j=0}^{w_j-1}2^{i_{ij}}}\right\}$$

$$= \sum_{i=0}^{2} tr_1^5\left\{[tr_5^{10}(\alpha^t)]^{\sum_{j=0}^{w_j-1}2^{i_{ij}}}\right\}$$

$$= tr_1^5\left\{[tr_5^{10}(\alpha^t)]^{\sum_{j=0}^{w_0-1}2^{i_{0j}}}\right\}$$

$$+ tr_1^5\left\{[tr_5^{10}(\alpha^t)]^{\sum_{j=0}^{w_1-1}2^{i_{1j}}}\right\} + tr_1^5\left\{[tr_5^{10}(\alpha^t)]^{\sum_{j=0}^{w_2-1}2^{i_{2j}}}\right\}$$

$$= \sum_{i=0}^{2}\sum_{k_{i1}=0}^{1}\sum_{k_{i2}=0}^{1}\cdots\sum_{k_{iw_2-1}=0}^{1} tr_1^{10}\left(\alpha^{(\sum_{j=0}^{w_j-1}2^{(i_{ij}+k_{ij}\cdot m)})t}\right)$$

여기서 $e = n/m = 10/5 = 2$이고, w_i는 $1 \cdot 3^{2i}$을 이진수로 표현한 경우의 Hamming weight에 해당된다.

위의 표현에서 $\alpha^{(\sum_{j=0}^{w_j-1}2^{(i_{ij}+k_{ij}\cdot m)})}$이 모든 i, k_{ij}에 대해 유한체 $GF(2^n)$상의 서로 다른 coset에 속하는 경우에 시퀀스의 선형스팬이 최대값을 갖는다. 만일 서로 다른 coset에 속하지 않으면, 즉 α의 서로 다른 지수 값이 $GF(2^n)$상의 같은 coset에 속한다면 trace 항이 서로 상쇄되어 trace 함수의 개수가 적어지므로 선형스팬은 최대값보다 작아질 것이다. 그리고 고정된 i에 대해 $\alpha^{(\sum_{j=0}^{w_j-1}2^{(i_{ij}+k_{ij}\cdot m)})}$의 지수는 모든 k_{ij}에 대해 $GF(2^n)$상에서 서로 다른 coset에 속한다는 것은 알려져 있다.[5, 8] 따라서 extended Legendre 시퀀스의 선형스팬은 다음과 같은 경계식으로 나타낼 수 있다.

Theorem 2 : 식 (5)에서 정의된 주기가 $N = 2^n - 1$인 extended Legendre 시퀀스 $c(t)$의 선형스팬에 관한 경계식은 다음과 같이 나타낼 수 있다.

$$L \le \sum_{i=0}^{\frac{M\cdot 1}{2m}-1} n \cdot \left(\frac{n}{m}\right)^{w_i - 1} \tag{8}$$

위의 선형스팬의 상한식은 몇몇 변수들을 바꾸면 일반적인 extended 시퀀스에도 적용될 수 있다. 식 (7)에서 $\alpha^{(\sum_{j=0}^{w_j-1}2^{(i_{ij}+k_{ij}\cdot m)})}$의 지수가 모든 i, k_{ij}에 대해 $GF(2^n)$의 서로 다른 coset에 속한다고 가정하면 식 (8)의 선형스팬에 관한 수식은 등호가 성립될 수 있다. 따라서 extended Legendre sequence의 선형스팬에 관하여 다음과 같은 conjecture를 유도할 수 있다.

Conjecture 1 : 식 (5)에서 정의된 주기가 $N = 2^n - 1$인 extended Legendre 시퀀스 $c(t)$의 선형스팬은 다음과 같다.

$$L = \sum_{i=0}^{\frac{M\cdot 1}{2m}-1} n \cdot \left(\frac{n}{m}\right)^{w_i - 1} \tag{9}$$

Ⅳ. Example

먼저, $m = 5, n = 10, r = 1, u = 3$인 경우 $r \cdot u^{2i}$를 각각이 속해있는 coset leader를 보면 1(00001), 5(00101), 7(00111)이므로 식 (7)에서 α의 서로 다른 지수들은 $GF(2^{10})$상에서 같은 coset에 속할 수 없다. 왜냐하면 Hamming weight가 각각 1, 2, 3으로 서로 다르기 때문이다. $n = 10, r = 3$인 경우도 역시 $r \cdot u^{2i}$이 속해있는 coset leader를 보면 3(00011), 15(01111), 11(01011)인데 여기서도 Hamming weight가 서로 다르다. 결국 $m = 5$일 때는 식 (7)에서 $\alpha^{(\sum_{j=0}^{w_j-1}2^{(i_{ij}+k_{ij}\cdot m)})}$이 모든 i, k_{ij}에 대해 $GF(2^{10})$의 서

로 다른 coset에 속하므로 식 (8)에서 등호가 성립됨을 알 수 있다.

그리고 $M = 127$이고, $m = 7$, Z_{127}의 원시원 $u = 3$이라 하며, α는 $\alpha^7 + \alpha^4 + 1 = 0$을 만족하는 $GF(2^7)$의 원시원이라 하면 주기가 127인 Legendre 시퀀스는 다음과 같이 표현될 수 있다.

$$s(t) = \sum_{i=0}^{8} tr_1^7(\alpha^{3^i t}) = \sum_{i=0}^{8} tr_1^7(\alpha^{9^i t}) \qquad (10)$$

그러면 식 (5)에서 정의된 extended Legendre 시퀀스는 다음과 같은 식으로 나타낼 수 있다.

$$\begin{aligned} c(t) &= \sum_{i=0}^{8} tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^i}\right\} \\ &= tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^0}\right\} + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^1}\right\} \\ &\quad + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^2}\right\} + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^3}\right\} \\ &\quad + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^4}\right\} + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^5}\right\} \\ &\quad + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^6}\right\} + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^7}\right\} \\ &\quad + tr_1^7\left\{[tr_7^n(\alpha^t)]^{r\cdot 9^8}\right\} \qquad (11) \end{aligned}$$

위식을 decimated m-시퀀스들의 합으로 표현하기 위해 $r = 1$이고, n이 14인 경우를 고려하자. 그러면 위식의 세번째 trace 함수에서 $9^2 \cdot r$은 81이 되는데 유한체 $GF(2^7)$상에서 이값의 coset leader는 13이 되고 이를 유한체 $GF(2^{14})$상에서 이진수로 표현하면 아래와 같다. 여기서 빈칸은 모두 0이다.

2^0	2^1	2^2	2^3	2^4	2^5	2^6
1		1	1			
2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}

식 (7)에서 표현된 바와 같이 맨 왼쪽 첫 비트는 고정시키고 다른 비트들을 아래로 천이시키면 다음과 같은 값들을 얻을 수 있다.

1		1				
			1			

1			1			
		1				

1						
		1	1			

여기서 각 경우의 숫자들이 속해 있는 coset leader를 구하면 각 81, 289, 35가 된다. 따라서 식 (11)에서 세번째 trace 함수는 다음과 같이 decimated m-시퀀스들의 합으로 표현된다.

$$\begin{aligned} tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^2}\right\} &= tr_1^{14}\{\alpha^{13t}\} + tr_1^{14}\{\alpha^{35t}\} + \\ &\quad tr_1^{14}\{\alpha^{81t}\} + tr_1^{14}\{\alpha^{289t}\} \end{aligned}$$

이와 같은 방법으로 식 (11)의 각 항들을 decimated m-시퀀스들의 합으로 표현하면 다음과 같다.

$$\begin{aligned} tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^0}\right\} &= tr_1^{14}\{\alpha^t\} \\ tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^1}\right\} &= tr_1^{14}\{\alpha^{9t}\} + tr_1^{14}\{\alpha^{17t}\} \\ tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^2}\right\} &= tr_1^{14}\{\alpha^{13t}\} + tr_1^{14}\{\alpha^{35t}\} \\ &\quad tr_1^{14}\{\alpha^{81t}\} + tr_1^{14}\{\alpha^{289t}\} \\ tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^3}\right\} &= tr_1^{14}\{\alpha^{47t}\} + tr_1^{14}\{\alpha^{61t}\} \\ &\quad tr_1^{14}\{\alpha^{87t}\} + tr_1^{14}\{\alpha^{107t}\} \\ &\quad tr_1^{14}\{\alpha^{117t}\} + tr_1^{14}\{\alpha^{301t}\} \\ &\quad tr_1^{14}\{\alpha^{341t}\} + tr_1^{14}\{\alpha^{361t}\} \\ &\quad tr_1^{14}\{\alpha^{555t}\} + tr_1^{14}\{\alpha^{569t}\} \\ &\quad tr_1^{14}\{\alpha^{595t}\} + tr_1^{14}\{\alpha^{625t}\} \\ &\quad tr_1^{14}\{\alpha^{809t}\} + tr_1^{14}\{\alpha^{849t}\} \\ &\quad tr_1^{14}\{\alpha^{1123t}\} + tr_1^{14}\{\alpha^{1317t}\} \\ tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^4}\right\} &= tr_1^{14}\{\alpha^{21t}\} + tr_1^{14}\{\alpha^{37t}\} \\ &\quad tr_1^{14}\{\alpha^{41t}\} + tr_1^{14}\{\alpha^{529t}\} \end{aligned}$$

$$tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^5}\right\} = tr_1^{14}\{\alpha^{31t}\} + tr_1^{14}\{\alpha^{79t}\} + tr_1^{14}\{\alpha^{103t}\} + tr_1^{14}\{\alpha^{115t}\} + tr_1^{14}\{\alpha^{121t}\} + tr_1^{14}\{\alpha^{285t}\} + tr_1^{14}\{\alpha^{333t}\} + tr_1^{14}\{\alpha^{357t}\} + tr_1^{14}\{\alpha^{369t}\} + tr_1^{14}\{\alpha^{539t}\} + tr_1^{14}\{\alpha^{587t}\} + tr_1^{14}\{\alpha^{611t}\} + tr_1^{14}\{\alpha^{793t}\} + tr_1^{14}\{\alpha^{841t}\} + tr_1^{14}\{\alpha^{1095t}\} + tr_1^{14}\{\alpha^{1301t}\}$$

$$tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^6}\right\} = tr_1^{14}\{\alpha^{19t}\} + tr_1^{14}\{\alpha^{25t}\} + tr_1^{14}\{\alpha^{73t}\} + tr_1^{14}\{\alpha^{273t}\}$$

$$tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^7}\right\} = tr_1^{14}\{\alpha^{11t}\} + tr_1^{14}\{\alpha^{49t}\} + tr_1^{14}\{\alpha^{69t}\} + tr_1^{14}\{\alpha^{265t}\}$$

$$tr_1^7\left\{[tr_7^{14}(\alpha^t)]^{1\cdot 9^8}\right\} = tr_1^{14}\{\alpha^{15t}\} + tr_1^{14}\{\alpha^{71t}\} + tr_1^{14}\{\alpha^{99t}\} + tr_1^{14}\{\alpha^{113t}\} + tr_1^{14}\{\alpha^{269t}\} + tr_1^{14}\{\alpha^{325t}\} + tr_1^{14}\{\alpha^{353t}\} + tr_1^{14}\{\alpha^{579t}\}$$

만일 여기서 α의 지수가 유한체 $GF(2^{14})$ 상에서 같은 coset에 속하는 것이 있다면 trace 함수는 같은 것이므로 서로 상쇄될 것이다. 하지만 여기서는 α의 서로 다른 지수가 같은 coset에 속하는 것이 없으므로 상쇄되는 항이 없어 extended Legendre 시퀀스의 선형스팬은 식 (9)로부터 아래와 같이 구할 수 있다.

$$L = 14\left(\frac{14}{7}\right)^{1-1} + 14\left(\frac{14}{7}\right)^{2-1} + 14\left(\frac{14}{7}\right)^{3-1} + 14\left(\frac{14}{7}\right)^{5-1} + 14\left(\frac{14}{7}\right)^{3-1} + 14\left(\frac{14}{7}\right)^{5-1} + 14\left(\frac{14}{7}\right)^{3-1} + 14\left(\frac{14}{7}\right)^{3-1} + 14\left(\frac{14}{7}\right)^{4-1} = 826$$

앞서 언급한 두 경우의 예는 앞의 conjecture가 맞는다는 것을 나타낸다.

V. 결 론

본 논문에서는 머센소수 주기를 갖는 Legendre 시퀀스를 확장한 extended Legendre 시퀀스를 decimated m-시퀀스들의 합으로 표현하였고 이를 이용하여 extended Legendre 시퀀스의 선형스팬에 대한 상한식을 구하였고 또한 선형스팬에 관한 conjecture를 세워 컴퓨터 시뮬레이션을 통해 주기가 짧은 경우의 extended Legendre 시퀀스들에 대해 검증하였다. 그리고 추후로 수행되어야 할 연구내용으로는 본 논문에서 제안된 conjecture를 증명하는 것이 될 것이다.

참 고 문 헌

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

[2] 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.

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

[4] R. Lidl and H. Niederreiter, Finite Fields, vol. 20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.

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

[6] 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. 3, pp.2254-2255, Nov. 1996.

[7] 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.

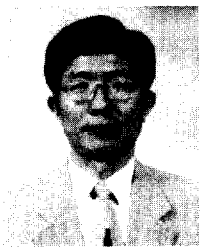
[8] J.-S. No, "Generalization of GMW sequences and No sequences," IEEE Trans. Inform. Theory, vol. IT-42, no. 1, pp 260-262, Jan. 1996.

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

[10] 노종선, "의사불규칙 시퀀스들 사이의 관계, 통신정보보호학회지 제 2권, 제2호, pp. 81-87, 1992년 6월.

[11] 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.

□ 著者紹介



노 종 선

1981년 2월 서울대학교 공과대학 전자공학과 (공학사)
1984년 2월 서울대학교 대학원 전자공학과 (공학석사)
1988년 5월 미국 남가주대학교 대학원 전기공학과 (공학박사)
1988년 2월 - 1990년 7월 미국 Hughes Network Systems 책임연구원
1990년 9월 - 현재 건국대학교 공과대학 전자공학과 부교수

※ 주관심분야: 오류정정부호, 시퀀스, 이동통신, IMT-2000

정 채 홍

1995년 2월 건국대학교 공과대학 전자공학과 (공학사)
1997년 2월 건국대학교 대학원 전자공학과 (공학석사)
1997년 7월 - 현재 현대전자산업 정보통신연구소 연구원

※ 주관심분야 : IMT-2000, 이동통신