論文 98-23-5-3

# 다항식 $z^d+(z+1)^d$에 의해 발생된 이상적인 자기상관을 갖는 주기 $2^m-1$의 이진 의사불규칙 시퀀스

正會員 노 종 선*, 정 하 봉**, 윤 민 선*

# Binary Pseudorandom Sequences of Period $2^m-1$ with Ideal Autocorrelation Generated by the Polynomial $z^d+(z+1)^d$

Jong-Seon No*, Habong Chung**, Min-Seon Yun* *Regular Members*

※본 연구는 정보통신부 대학기초연구지원 사업 연구비에 의한 결과임.(과제번호 : 96003-RT-11 및 96190-CT-12)

요 약

본 논문에서는 다항식 $z^d+(z+1)^d$를 이용하여 이상적인 자기상관특성을 갖는 주기 $2^m-1$의 이진 의사불규칙 시퀀스를 구성하는 것을 보였다. 다항식으로부터 얻어진 시퀀스는 어떤 $d$값에서는 m-시퀀스가 된다. 또한 $k$가 양의 정수이고 $m$이 $3k\pm1$일 때 이상적인 자기상관특성을 갖는 새로운 이진 시퀀스를 산출하는 몇몇의 $d$값을 발견했다. 이들 새로운 시퀀스는 trace함수를 이용하여 표현하였으며 그 결과들을 표로 나타내었다.

ABSTRACT

In this paper, we present a construction for binary pseudorandom sequences of period $2^m-1$ with ideal autocorrelation property using the polynomial $z^d+(z+1)^d$. We show that the sequence obtained from the polynomial becomes an m-sequence for certain values of $d$. We also find a few values of $d$ which yield new binary sequences with ideal autocorrelation property when $m$ is $3k\pm1$, where $k$ is a positive integer. These new sequences are represented using trace function and the results are tabulated.

## Ⅰ. 서 론

주기가 $N=2^m-1$인 이진(0 or 1) 시퀀스 $\{a(t), t=0, 1, \cdots, N-1\}$는 만일 주기적 자기상관함수 $R_a(\tau)$가 다음과 같이 주어진다면 이상적인 자기상관특성을 갖는다고 말한다[1, 6].

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

여기서 $R_a(\tau)$은 다음과 같이 정의된다.

*건국대학교 전자공학과
**홍익대학교 전기전자공학부
論文番號:97360-1008
接受日字:1997年 10月 8日

$$R_a(\tau)=\sum_{t=0}^{N-1}(-1)^{a(t+\tau)+a(t)} \tag{2}$$

그리고 $t+\tau$은 modulo $N$으로 계산된다.

주기가 $2^m-1$인 몇몇의 잘 알려진 이진 시퀀스는 m-시퀀스, GMW 시퀀스, 일반화된(generalized) GMW 시퀀스, Legendre시퀀스, Hall's sextic residue 시퀀스, 확장된(extended) 시퀀스, 그리고 생성방법이 아직 알려 있지 않은 기타 시퀀스(miscellaneous sequence)를 포함한다[1, 3-14]. 이들 시퀀스는 유한체(finite field) 상의 trace 함수의 항들로 표현된다[2]. $2^m$개의 원소를 갖는 유한체를 $GF(2^m)$라 하자. 몇몇 양의 정수 $e$와 $n$에 대해 $m=en>1$이라 하자. 그러면 trace 함수 $tr_n^m(\cdot)$은 $GF(2^m)$에서 그것의 부분유한체(subfield) $GF(2^n)$으로의 매핑(mapping)으로 다음과 같이 주어진다[2].

$$tr_n^m(x)=\sum_{i=0}^{e-1}x^{2^{ni}}. \tag{3}$$

본 논문에서는, 시퀀스를 생성하는 새로운 방법으로서 다항식 $z^d+(z+1)^d$를 이용하여 이상적인 자기상관특성을 갖는 주기 $2^m-1$의 m-시퀀스 및 새로운 이진 시퀀스를 구성하는 것을 보였다. 이들 시퀀스는 컴퓨터 search에 의해 발견하였다. Ⅱ절에서는 m-시퀀스가 어떤 $d$값에서 이 방법에 의해 얻어질 수 있음을 보였다. Ⅲ절에서는 또한 $k$가 양의 정수이고 $m$이 $3k\pm1$일 때 이상적인 자기상관특성을 갖는 새로운 이진 시퀀스를 산출하는 몇몇의 $d$값을 발견하였다. 이들 새로운 시퀀스는 trace함수를 이용하여 표현하였으며 그 결과들을 표로 나타내었다.

## Ⅱ. 다항식 $z^d+(z+1)^d$를 이용한 m-시퀀스의 구성

$I_d$를 다음과 같은 $GF(2^m)$의 집합이라 정의하자.

$$I_d=\{u \mid u=z^d+(z+1)^d,\ z\in GF(2^m)\}. \tag{4}$$

집합 $I_d$와 관련된 시퀀스 $a_d(t)$, $t=0, 1, 2, \cdots, 2^m-2$를 다음과 같이 정의하자.

ⅰ) $m$이 홀수인 경우;

$$a_d(t)=\begin{cases}1 & \text{if } \alpha^t\in I_d,\\ 0 & otherwise,\end{cases} \tag{5}$$

ⅱ) $m$이 짝수인 경우;

$$a_d(t)=\begin{cases}0 & \text{if } \alpha^t\in I_d,\\ 1 & otherwise,\end{cases} \tag{6}$$

여기서 $\alpha$는 $GF(2^m)$의 원시원(primitive element)이다. 다음에 오는 이론들은 시퀀스 $a_d(t)$가 $d$와 $m$의 어떤 조건하에서는 m-시퀀스임을 보인다.

**정리 1**: $m$을 양의 홀수인 정수라 하자. 만일 $d$가 $d=2^i+1$이고 $i$가 $m$과 서로 소라면, 식 (5)의 시퀀스 $a_d(t)$는 $a_d(t)=tr_1^m(\alpha^t)$로 주어진 m-시퀀스이다.

증명: $a_d(t)=tr_1^m(\alpha^t)$라는 것을 증명하기 위해서는 $I_d$가 trace값이 1인 $GF(2^m)$의 모든 원소들의 집합임을 보이는 것으로 충분하다. $I_d$의 어떤 원소 $u$는 다음과 같이 표현될 수 있다.

$$u=z^d+(z+1)^d=z^{2^i}+z+1. \tag{7}$$

따라서, $tr_1^m(u)=1$이다.

또한, 만일 $z=z_1$와 $z_2$가 주어진 $u$에 대한 식 (7)의 해라면, $z_1+z_2$은 $z^{2^i}+z=0$의 해이다. $\gcd(m, i)=1$이므로, $z_1+z_2$의 가능한 두 값은 단지 0 또는 1이다. 이 값들은 $tr_1^m(u)=1$가 되는 어떤 주어진 $u$에 대해 식 (7)에 적용되는 정확한 두 개의 해이다. 따라서 $|I_d|=2^{m-1}$인 즉, $I_d$는 trace값이 1인 $GF(2^m)$의 모든 원소들의 집합이다. □

**정리 2**: $m$을 양의 짝수인 정수라 하자. 만일 $d$가 $d=2^i+1$이고 $i$가 $m$과 서로 소라면, 식 (6)의 시퀀스 $a_d(t)$는 $a_d(t)=tr_1^m(\alpha^t)$로 주어진 m-시퀀스이다.

증명: $a_d(t)=tr_1^m(\alpha^t)$라는 것을 증명하기 위해서는 $I_d$가 trace값이 0인 0을 제외한 $GF(2^m)$의 모든 원소들의 집합임을 보이는 것으로 충분하다. 이것은 정리 1의 증명과 비슷한 논거를 사용하여 쉽게 증명될 수 있다. □

다음 정리는 $a_d(t)$와 $a_{d^{-1}}(t)$사이의 흥미 있는 관계를

말한다.

정리 3: $d$를 양의 정수라 하고 $s$를 $Z_{2^m-1}$에서의 $d$의 역원이라 하자. 즉,

$$d\cdot s\equiv 1 \pmod{2^m-1}. \tag{8}$$

그러면,

$$a_s(t)=a_d(-dt). \tag{9}$$

증명: $(I_d)^r$를 다음과 같이 정의하자

$$(I_d)^r=\{u^r \mid u\in I_d\}. \tag{10}$$

그러면 식 (5) 또는 (6)처럼 유사하게 집합 $(I_d)^r$와 관련된 시퀀스는 시퀀스 $a_d(t)$를 $r^{-1}$ 만큼 데시메이션한 것이다. $I_d$의 어떤 원소 $u(=z^d+(z+1)^d)$은 $z$를 $\frac{1}{x+1}$로 치환하는 것에 의해 다음과 같이 표현될 수 있다.

$$u=\left(\frac{1}{1+x}\right)^d+\left(\frac{x}{1+x}\right)^d=\frac{1+x^d}{(1+x)^d}. \tag{11}$$

그러면, $I_d$는 다음과 같이 쓸 수 있다.

$$I_d=\left\{u \mid u=\frac{1+x^d}{(1+x)^d},\ x\in GF(2^m)/\{1\}\right\}. \tag{12}$$

$x=1$을 제외하는 것은 $I_d$에 영향을 주지 않는다. 왜냐하면 $z=0$과 $z=1$은 같은 $u$를 산출하기 때문이다. 식 (11)에 $-s$승하면,

$$u^{-s}=\frac{(1+x)^{ds}}{(1+x^d)^s}=\frac{1+x}{(1+x^d)^s}. \tag{13}$$

그리고 $x^d$를 $y$로 치환하면,

$$u^{-s}=\frac{1+y^s}{(1+y)^s}. \tag{14}$$

그러면, 집합 $I_s$은 다음과 같이 다시 쓸 수 있다.

$$I_s=\left\{u \mid u=\frac{1+y^s}{(1+y)^s},\ y\in GF(2^m)/\{1\}\right\}$$

$$=\{u \mid u^{-s}\in I_d\}=(I_d)^{-s}. \tag{15}$$

따라서, $a_s(t)=a_d\left(-\frac{t}{s}\right)=a_d(-dt)$. □

$m$이 홀수인 경우에는 다항식 $z^d+(z+1)^d$에 의해 얻어지는 주기 $2^m-1$의 m-시퀀스는 정리 1과 정리 3에 의해 설명될 수 있다. $m$이 짝수 일 때는, $d$의 Hamming weight가 2인 다항식으로부터 발생된 어떤 m-시퀀스의 이진 표현은 정리 2에 의해 또한 설명될 수 있다. 그러나, $d=2^{m-1}-1$인 다항식으로부터 얻어진 m-시퀀스는 다음 이론에 의해 설명될 수 있다.

정리 4: $m$를 양의 짝수인 정수라 하고 $d=2^{m-1}-1$이라 하자. 그러면 식 (6)의 시퀀스 $a_d(t)$는 $a_d(t)=tr_1^m(\alpha^t)$로 주어지는 m-시퀀스이다.

증명: $a_d(t)=tr_1^m(\alpha^t)$라는 것을 증명하기 위해서는 $(I_d)^d$가 trace값이 0인 0을 제외한 $GF(2^m)$의 모든 원소들의 집합임을 보이는 것으로 충분하다. $(I_d)^d$의 어떤 원소 $w$는 다음과 같이 쓸 수 있다.

$$w=u^d=(z^d+(z+1)^d)^d. \tag{16}$$

$z=0$ 또는 1인 경우에, $w$는 1이고 $tr_1^m(1)=0$이다. 식 (16)에서 0 또는 1과 다른 $z$의 값들은 다음과 같이 쓸 수 있다.

$$w=\frac{\left\{\frac{z^{2^{m-1}}}{z}+\frac{(z+1)^{2^{m-1}}}{(z+1)}\right\}^{2^{m-1}}}{\left\{\frac{z^{2^{m-1}}}{z}+\frac{(z+1)^{2^{m-1}}}{(z+1)}\right\}}. \tag{17}$$

그러면

$$w^2=\frac{1}{\left\{\frac{z^{2^{m-1}}}{z}+\frac{(z+1)^{2^{m-1}}}{(z+1)}\right\}} \tag{18}$$

그리고

$$w^4=\frac{1}{\left\{\frac{1}{z}+\frac{1}{(z+1)}\right\}}=z+z^2. \tag{19}$$

그러면, $tr_1^m(w)=0$이다. 식 (19)은 어떤 주어진 $w$가 $tr_1^m(w)=0$, $|(I_d)^d|=2^{m-1}-1$인 경우에 정확히 $z$의 두 개의 해를 갖는다. 그러므로, $(I_d)^d$는 trace 값이 0인 $GF(2^m)$의 0이 아닌 모든 원소들을 포함하는 집합이다. □

## Ⅲ. 다항식 $z^d+(z+1)^d$에 의해 얻어진 새로운 이진 의사불규칙 시퀀스

$k$가 양의 정수이고 $m$이 $3k\pm1$일 때 이상적인 자기상관특성을 갖는 새로운 이진 시퀀스를 산출하는 $d$의 몇몇 값을 컴퓨터 search에 의해 발견했다. 이들 결과는 다음의 추측정리들로 요약되었다.

추측정리 5: $k(\geq 2)$를 양의 정수라 하고 $m=3k-1$이라 하자. 만일 $d$가 다음과 같이 주어진다면

$$d=2^{2k-1}+2^k-1. \tag{20}$$

식 (5) 또는 (6)에 의해 주어진 시퀀스 $a_d(t)$는 이상적인 자기상관특성을 갖는 주기가 $2^m-1$인 이진 의사불규칙 시퀀스이다. □

$k=2$일 때 주기 $N$이 31인 시퀀스는 $d$가 11이고 그 결과 시퀀스는 m-시퀀스와 같다. $k\geq3$일 때, 새로운 시퀀스 $a_d(t)$는 trace 표현을 이용하여 다음과 같이 표현할 수 있다.

$$a_d(t)=\sum_{i\in I} tr_1^m(\alpha^{it}), \tag{21}$$

각 $k$에 따른 집합 $I$는 다음과 같이 주어진다.

$k=3$, $m=8$, $d=39$:
$I=\{13, 19, 21, 29, 39\}$

$k=4$, $m=11$, $d=143$:
$I=\{25, 35, 41, 57, 69, 71, 73, 89, 105, 121, 139, 141, 143\}$

$k=5$, $m=14$, $d=543$:
$I=\{49, 67, 81, 113, 133, 135, 145, 177, 209, 241, 265, 267, 269, 271, 273, 305, 337, 369, 401, 433, 465, 497, 531, 533, 535, 537, 539, 541, 543\}$

$k=6$, $m=17$, $d=2111$:
$I=\{97, 131, 161, 225, 261, 263, 289, 353, 417, 481, 521, 523, 525, 527, 545, 609, 673, 737, 801, 865, 929, 993, 1041, 1043, 1045, 1047, 1049, 1051, 1053, 1055, 1057, 1121, 1185, 1249, 1313, 1377, 1441, 1505, 1569, 1633, 1697, 1761, 1825, 1889, 1953, 2017, 2083, 2085, 2087, 2089, 2091, 2093, 2095, 2097, 2099, 2101, 2103, 2105, 2107, 2109, 2111\}$

$k=7$, $m=20$, $d=8319$:
$I=\{193, 259, 321, 449, 517, 519, 577, 705, 833, 961, 1033, 1035, 1037, 1039, 1089, 1217, 1345, 1473, 1601, 1729, 1857, 1985, 2065, 2067, 2069, 2071, 2073, 2075, 2077, 2079, 2113, 2241, 2369, 2497, 2625, 2753, 2881, 3009, 3137, 3265, 3393, 3521, 3649, 3777, 3905, 4033, 4129, 4131, 4133, 4135, 4137, 4139, 4141, 4143, 4145, 4147, 4149, 4151, 4153, 4155, 4157, 4159, 4161, 4289, 4417, 4545, 4673, 4801, 4929, 5057, 5185, 5313, 5441, 5569, 5697, 5825, 5953, 6081, 6209, 6337, 6465, 6593, 6721, 6849, 6977, 7105, 7233, 7361, 7489, 7617, 7745, 7873, 8001, 8129, 8259, 8261, 8263, 8265, 8267, 8269, 8271, 8273, 8275, 8277, 8279, 8281, 8283, 8285, 8287, 8289, 8291, 8293, 8295, 8297, 8299, 8301, 8303, 8305, 8307, 8309, 8311, 8313, 8315, 8317, 8319\}$

$k=8$, $m=23$, $d=33023$:
$I=\{385, 515, 641, 897, 1029, 1031, 1153, 1409, 1665, 1921, 2057, 2059, 2061, 2063, 2177, 2433, 2689, 2945, 3201, 3457, 3713, 3969, 4113, 4115, 4117, 4119, 4121, 4123, 4125, 4127, 4225, 4481, 4737, 4993, 5249, 5505, 5761, 6017, 6273, 6529, 6785, 7041, 7297, 7553, 7809, 8065, 8225, 8227, 8229, 8231, 8233, 8235, 8237, 8239, 8241, 8243, 8245, 8247, 8249, 8251, 8253, 8255, 8321, 8577, 8833, 9089, 9345, 9601, 9857, 10113, 10369, 10625, 10881, 11137, 11393, 11649, 11905, 12161, 12417, 12673, 12929, 13185, 13441, 13697, 13953, 14209, 14465, 14721, 14977, 15233, 15489, 15745, 16001, 16257, 16449, 16451, 16453, 16455, 16457, 16459, 16461, 16463, 16465, 16467, 16469, 16471, 16473, 16475, 16477, 16479, 16481, 16483, 16485, 16487, 16489, 16491, 16493, 16495, 16497, 16499, 16501, 16503, 16505, 16507, 16509, 16511, 16513, 16769, 17025, 17281, 17537, 17793, 18049, 18305, 18561,

18817, 19073, 19329, 19585, 19841, 20097, 20353, 20609, 20865, 21121, 21377, 21633, 21889, 22145, 22401, 22657, 22913, 23169, 23425, 23681, 23937, 24193, 24449, 24705, 24961, 25217, 25473, 25729, 25985, 26241, 26497, 26753, 27009, 27265, 27521, 27777, 28033, 28289, 28545, 28801, 29057, 29313, 29569, 29825, 30081, 30337, 30593, 30849, 31105, 31361, 31617, 31873, 32129, 32385, 32641, 32899, 32901, 32903, 32905, 32907, 32909, 32911, 32913, 32915, 32917, 32919, 32921, 32923, 32925, 32927, 32929, 32931, 32933, 32935, 32937, 32939, 32941, 32943, 32945, 32947, 32949, 32951, 32953, 32955, 32957, 32959, 32961, 32963, 32965, 32967, 32969, 32971, 32973, 32975, 32977, 32979, 32981, 32983, 32985, 32987, 32989, 32991, 32993, 32995, 32997, 32999, 33001, 33003, 33005, 33007, 33009, 33011, 33013, 33015, 33017, 33019, 33021, 33023}

이 추측정리 5는 컴퓨터 시뮬레이션에 의해 $m \le 23$까지 검증되었다.

**추측정리 6**: $k$를 양의 정수라 하고 $m=3k+1$이라 하자. 만일 $d$가 다음과 같이 주어진다면

$$d=2^{2k}-2^k+1, \tag{22}$$

식 (5) 또는 (6)에 의해 주어진 시퀀스 $a_d(t)$는 이상적인 자기상관특성을 갖는 주기가 $2^m-1$인 이진 의사불규칙 시퀀스이다. □

$k=1$일 때 주기 $N$이 15인 시퀀스는 $d$가 3이고 그 결과 시퀀스는 m-시퀀스와 같다. $k\ge 2$일 때, 새로운 시퀀스 $a_d(t)$는 trace 표현을 이용하여 다음과 같이 표현할 수 있다.

$$a_d(t)=\sum_{i\in I} tr_1^m(\alpha^{it}), \tag{23}$$

각 $k$에 따른 집합 $I$는 다음과 같이 주어진다.

$k=2, m=7, d=13$:

$I=\{1, 3, 7, 19, 29\}$

$k=3, m=10, d=57$:

$I=\{1, 3, 5, 7, 11, 13, 15, 35, 69, 71, 89, 105, 121\}$

$k=4, m=13, d=241$:

$I=\{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 67, 133, 135, 265, 267, 269, 271, 305, 337, 369, 401, 433, 465, 497\}$

$k=5, m=16, d=993$:

$I=\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 131, 261, 263, 521, 523, 525, 527, 1041, 1043, 1045, 1047, 1049, 1051, 1053, 1055, 1121, 1185, 1249, 1313, 1377, 1441, 1505, 1569, 1633, 1697, 1761, 1825, 1889, 1953, 2017\}$

$k=6, m=19, d=4033$:

$I=\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 259, 517, 519, 1033, 1035, 1037, 1039, 2065, 2067, 2069, 2071, 2073, 2075, 2077, 2079, 4129, 4131, 4133, 4135, 4137, 4139, 4141, 4143, 4145, 4147, 4149, 4151, 4153, 4155, 4157, 4159, 4289, 4417, 4545, 4673, 4801, 4929, 5057, 5185, 5313, 5441, 5569, 5697, 5825, 5953, 6081, 6209, 6337, 6465, 6593, 6721, 6849, 6977, 7105, 7233, 7361, 7489, 7617, 7745, 7873, 8001, 8129\}$

$k=7, m=22, d=16257$:

$I=\{$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199, 201, 203, 205, 207, 209, 211, 213, 215, 217, 219, 221, 223, 225, 227, 229, 231, 233, 235, 237, 239, 241, 243, 245, 247, 249, 251, 253, 255, 515, 1029, 1031, 2057, 2059, 2061, 2063, 4113, 4115, 4117, 4119, 4121, 4123, 4125, 4127, 8225, 8227, 8229, 8231, 8233, 8235, 8237, 8239, 8241, 8243, 8245, 8247, 8249, 8251, 8253, 8255, 16449, 16451, 16453, 16455,

16457, 16459, 16461, 16463, 16465, 16467, 16469,
16471, 16473, 16475, 16477, 16479, 16481, 16483,
16485, 16487, 16489, 16491, 16493, 16495, 16497,
16499, 16501, 16503, 16505, 16507, 16509, 16511,
16769, 17025, 17281, 17537, 17793, 18049, 18305,
18561, 18817, 19073, 19329, 19585, 19841, 20097,
20353, 20609, 20865, 21121, 21377, 21633, 21889,
22145, 22401, 22657, 22913, 23169, 23425, 23681,
23937, 24193, 24449, 24705, 24961, 25217, 25473,
25729, 25985, 26241, 26497, 26753, 27009, 27265,
27521, 27777, 28033, 28289, 28545, 28801, 29057,
29313, 29569, 29825, 30081, 30337, 30593, 30849,
31105, 31361, 31617, 31873, 32129, 32385, 32641}

이 추측정리 6은 컴퓨터 시뮬레이션에 의해 $m \leq 22$까지 검증되었다. 추측정리 5와 6에 의해 구성되는 시퀀스는 최근에 Golomb과 Gong에 의해 추측되어진 시퀀스와 같은 종류의 것이다[14]. 그러나 그들의 구성방법은 본 논문에서의 방법과는 전적으로 다른 방법이다. 정리 3은 $m$이 홀수인 경우에 추측정리 5와 6의 시퀀스에도 적용될 수 있다.

다항식 $z^d + (z+1)^d$에 의해 발생된 이상적인 자기상관특성을 갖는 이진 시퀀스는 다음에 오는 表에 실렸다. 이들 시퀀스들은 m-시퀀스와 $d$값에 의해 새로 발견된 시퀀스로 분류된다. 表에서, 괄호 안의 숫자는 그것의 앞에 있는 값의 $Z_{2^m-1}$에서의 역원을 가리킨다. 또한, m은 m-시퀀스를 나타내고 MIS는 앞의 두 추측정리들에 의해 구성된 기타 시퀀스를 나타낸다. m-$i$ 또는 MIS-$i$ 표시법은 그 시퀀스를 $i$ 만큼 데시메이션한 시퀀스에 상응하는 시퀀스를 나타낸다.

## 참 고 문 헌

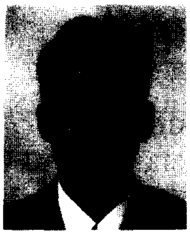

1. L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Springer-Verlag, 1971.
2. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, the Netherlands: North-Holland, 1977.
3. L. D. Baumert and Fredrickson, "The cyclotomic numbers of order 18 with applications to difference sets," *Math. Comp.*, vol. 21, pp. 204-219, 1967.
4. U. Cheng, "Exhaustive construction of (255, 127, 63) cyclic difference sets," *J. Combinatorial Theory*, vol. A-35, pp. 115-125, 1983.
5. R. Drier, "(511, 255, 127) cyclic difference sets," IDA talk, July 1992.
6. S. W. Golomb, *Shift-Register Sequences*, Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA 1982.
7. 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.
8. 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.
9. R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548-553, May 1984.
10. J. -S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 260-262, Jan. 1996.
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, K. Yang, C. Chung, and H. -Y. Song, "Extension of binary sequences with ideal autocorrelation property," preprint, Mar. 1996.
13. J. -S. No, K. Yang, H. Chung, and H. -Y. Song, "A new family of binary sequences with optimal correlation properties," *IEEE Trans. Inform. Theory*, vol. 43, No. 5, pp. 1596-1602, Sept. 1997.
14. S. W. Golomb and G. Gong, "Five suspected New infinite classes of permutation polynomials from $GF(2^n)$ to $GF(2)$," preprint, July 1997.

표 1. 다항식 $z^d+(z+1)^d$에 의해 발생된 의사불규칙 시퀀스

| $N$ | $d$ | 시퀀스 |
|---|---|---|
| $2^4-1=15$ | 3 | m-1 |
| | 7 | m-7 |
| $2^5-1=31$ | 3,5 | m-1 |
| | 7(5) | m-11 |
| | 11(3) | m-7 |
| $2^6-1=63$ | 3 | m-1 |
| | 31 | m-31 |
| $2^7-1=127$ | 3,5,9 | m-1 |
| | 11 | MIS-23 |
| | 13(11) | MIS-1 |
| | 15(9) | m-55 |
| | 27(5) | m-47 |
| | 43(3) | m-31 |
| $2^8-1=255$ | 3,9 | m-1 |
| | 39 | MIS-1 |
| | 127 | m-127 |
| $2^9-1=511$ | 3,5,17 | m-1 |
| | 31(17) | m-239 |
| | 103(5) | m-191 |
| | 171(3) | m-127 |
| $2^{10}-1=1023$ | 3,9 | m-1 |
| | 57 | MIS-1 |
| | 511 | m-511 |
| $2^{11}-1=2047$ | 3,5,9,17,33 | m-1 |
| | 43 | MIS-119 |
| | 143(43) | MIS-1 |
| | 63(33) | m-991 |
| | 231(9) | m-895 |
| | 365(17) | m-959 |
| | 411(5) | m-767 |
| | 683(3) | m-511 |
| $2^{12}-1=4095$ | 3,33 | m-1 |
| | 2047 | m-2047 |
| $2^{13}-1=8191$ | 3,5,9,17,33,65 | m-1 |
| | 171 | MIS-479 |
| | 241(171) | MIS-1 |
| | 127(65) | m-4031 |
| | 911(9) | m-3583 |
| | 1243(33) | m-3967 |
| | 1453(17) | m-3839 |
| | 1639(5) | m-3071 |
| | 2731(3) | m-2047 |

| $N$ | $d$ | 시퀀스 |
|---|---|---|
| $2^{14}-1=16383$ | 3,9,33 | m-1 |
| | 543 | MIS-1 |
| | 8191 | m-8191 |
| $2^{15}-1=32767$ | 3,5,17,129 | m-1 |
| | 255(129) | m-16255 |
| | 1935(17) | m-15359 |
| | 6555(5) | m-12287 |
| | 10923(3) | m-8191 |
| $2^{16}-1=65535$ | 3,9,33,129 | m-1 |
| | 993 | MIS-1 |
| | 32767 | m-32767 |
| $2^{17}-1=131071$ | 3,5,9,17,33,65,129,257 | m-1 |
| | 683 | MIS-2015 |
| | 2111(683) | MIS-1 |
| | 511(257) | m-65279 |
| | 7711(17) | m-61439 |
| | 14567(9) | m-57343 |
| | 19309(129) | m-65023 |
| | 19867(33) | m-63487 |
| | 22197(65) | m-64511 |
| | 26215(5) | m-49151 |
| | 43691(3) | m-32767 |
| $2^{18}-1=262143$ | 3,33,129 | m-1 |
| | 131071 | m-131071 |
| $2^{19}-1=524287$ | 3,5,9,17,33,65,129,257,513 | m-1 |
| | 2731 | MIS-8063 |
| | 4033(2731) | MIS-1 |
| | 1023(513) | m-261631 |
| | 15903(33) | m-253951 |
| | 52851(129) | m-260095 |
| | 58255(9) | m-229375 |
| | 75483(257) | m-261119 |
| | 88757(65) | m-258047 |
| | 92525(17) | m-245759 |
| | 104859(5) | m-196607 |
| | 174763(3) | m-131071 |
| $2^{20}-1=1048575$ | 3,9,129,513 | m-1 |
| | 8319 | MIS-1 |
| | 524287 | m-524287 |

| $N$ | $d$ | 시퀀스 |
|---|---|---|
| $2^{21}-1=2097151$ | 3,5,9,17,33,65,129,257,513,1025 | m-1 |
| | 2047(1025) | m-1047551 |
| | 16257(129) | m-1040383 |
| | 63551(33) | m-1015807 |
| | 204007(257) | m-1044479 |
| | 224841(513) | m-1046527 |
| | 225849(65) | m-1032191 |
| | 233017(9) | m-917503 |
| | 370093(17) | m-983039 |
| | 419431(5) | m-786431 |
| | 699051(3) | m-524287 |
| $2^{22}-1=4194303$ | 3,9,33,129,513 | m-1 |
| | 16257 | MIS-1 |
| | 2097151 | m-2097151 |
| $2^{23}-1=8388607$ | 3,5,9,17,33,65,129,257,513,1025,2049 | m-1 |
| | 10923 | MIS-32639 |
| | 33023(10923) | MIS-1 |
| | 4095(2049) | m-4192255 |
| | 129087(65) | m-4128767 |
| | 493455(17) | m-3932159 |
| | 845427(129) | m-4161535 |
| | 932071(9) | m-3670015 |
| | 1203053(1025) | m-4190207 |
| | 1271003(33) | m-4063231 |
| | 1357229(513) | m-4186111 |
| | 1387221(257) | m-4177919 |
| | 1677723(5) | m-3145727 |
| | 2796203(3) | m-2097151 |



윤 민 선(Min-Seon Yun) 정회원
1996년 2월 : 건국대학교 전자공학과 졸업(공학사)
1998년 2월 : 건국대학교 대학원 전자공학과 졸업(공학석사)
1997년 11월~현재 : 단암전자통신(주) 전자통신기술연구소 연구원

노 종 선(Jong-Seon No) 정회원
제 22권 6호 통신학회논문지 참조

정 하 봉(Habong Chung) 정회원
제 22권 6호 통신학회논문지 참조