Hall's Sextic Residue 시퀀스 및 기타 시퀀스의 Trace 함수에 의한 표현[1)]

이 환 근*, 노 종 선*, 정 하 봉**, 양 경 철†, 송 홍 엽‡
* 건국대학교 전자공학과, ** 홍익대학교 전기전자학부
† 한양대학교 전자통신공학과, ‡ 연세대학교 전자공학과

Trace Representation of Hall's Sextic Residue Sequences and Miscellaneous Sequences

Hwan-Keun Lee*, Jong-Seon No*, Habong Chung**, Kyeongcheol Yang†, Hong-Yeop Song‡
* Dept. of Electronic Engineering, Konkuk University
** School of Electronics and Electrical Engineering, Hong-Ik University
† Dept. of Electronic Communication Engineering, Hanyang University
‡ Dept. of Electronic Engineering, Yonsei University

요 약

이상적인 자기상관특성을 갖는 주기가 2^m-1인 이진 의사불규칙(pseudo noise, PN) 시퀀스인 m-시퀀스, GMW 시퀀스, Legendre 시퀀스, 그리고 extended 시퀀스 등에 관한 많은 연구가 이루어져 왔다. 이러한 시퀀스들 이외에도 이상적인 자기상관특성을 갖는 이진 시퀀스로서 Hall's sextic residue 시퀀스가 있고 그리고 구체적인 생성방법이 알려지지 않은 이상적인 자기상관특성을 갖는 많은 이진 시퀀스가 발견되었다. 그러나, 지금까지는 이들 시퀀스들을 trace 함수를 이용하여 표현하는 방법은 아직 알려져 있지 않았다. 본 논문에서는 이상적인 자기상관특성을 갖는 Hall's sextic residue 시퀀스와 생성방법이 알려져 있지 않은 기타 시퀀스들을 trace 함수를 이용하여 표현하였다. 그리고 컴퓨터 search에 의해서 이상적인 자기상관특성을 갖는 새로운 이진시퀀스를 발견하고 이들을 trace 함수를 이용하여 표현하였다.

ABSTRACT

Pseudonoise sequences of period 2^m-1 with ideal autocorrelation have been researched such as m-sequences, GMW sequences, Legendre sequences, and extended sequences. The m-sequences, the GMW sequences, the Legendre sequences, and the extended sequences are best described in terms of the trace function by previous works. Besides, there are Hall's sextic residue sequences and miscellaneous sequences with ideal autocorrelation, whose general constructions are not known so far. However, there are no explicit description of the Hall's sextic residue sequences and the miscellaneous sequences in terms of the trace function. In this paper, the Hall's sextic residue sequences and the miscellaneous sequences of period 2^m-1 are expressed as a sum of trace functions. The miscellaneous sequences with ideal autocorrelation, which are newly found by computer search, are also expressed as a sum of trace functions.

1. 본 연구는 정보통신연구관리단의 대학기초연구지원사업의 연구비지원에 의한 결과입니다.

I. 서 론

최근 수십년동안 PN 시퀀스(pseudo noise sequence)라고도 불리는 의사불규칙 시퀀스(pseudorandom sequence)는 통신분야 뿐만 아니라 그 외의 여러 분야에서 그의 사용영역을 넓혀 왔다. 즉, 주로 군용통신시스템으로 사용되어 왔던 확산스펙트럼 통신시스템(spread spectrum communication system)에서 메세지데이터 신호의 스펙트럼을 확산 및 역확산 시키기 위한 확산 부호로 사용되어 왔다. 또한, 최근 들어서 정보통신관련 분야의 중추적인 역할을 하고 있는 시스템으로 이동통신시스템(digital cellular system), 개인휴대통신시스템(personal communication system: PCS) 및 차세대이동통신시스템(future public land mobile telecommunication system: FPLMTS) 등이 있는데, 이러한 시스템들은 다원접속방식으로 부호분할 다원접속방식(code division multiple access: CDMA)을 표준으로 채택하였거나 채택을 고려하고 있다. 이 CDMA 방식에서 가장 중요한 핵심요소기술은 사용자간의 간섭이 최소화 되도록 여러 사용자 신호의 스펙트럼을 확산시키는데 사용되는 서명(signature) 시퀀스인데, 이것으로 의사불규칙 시퀀스가 사용된다. 그리고, 의사불규칙 시퀀스는 그의 중요도 및 관심도가 점증하고 있는 암호분야에서 스트림 암호화시스템의 핵심기술인 키스트림(key stream)으로 사용될 수 있으며 또한 CATV 신호의 스크램블링 및 GPS(global positioning system)에서도 핵심기술로 사용되고 있다.

주기가 v인 이진 시퀀스 $\{a_i\}$, $a_i \in \{+1, -1\}$를 $\tau = 0, 1, 2, \cdots, v-1$에 대해 주기적 자기상관함수(periodic autocorrelation function) $R(\tau)$는 다음과 같이 정의할 수 있다.

$$R(\tau) \triangleq \sum_{i=0}^{v-1} a_i \cdot a_{i+\tau} \tag{1}$$

여기서, 모든 아래첨자는 mod v로 연산된다. 여러 분야의 통신시스템에서는 아래에서 정의된 바와 같이 자기상관함수가 2-level을 갖는 즉, 이상적인 자기상관특성을 갖는 이진 시퀀스를 필요로 한다 [2],[3].

$$R(\tau) = \begin{cases} v \ , \ \text{for } \tau = 0 \bmod v \\ -1 \ , \ \text{otherwise} \end{cases} \tag{2}$$

일반적으로 시퀀스의 성질 규명 및 생성기의 구현을 위하여 이진 시퀀스를 trace 함수를 이용하여 표현하는 것이 필요하다고 알려져 있다. 따라서 시퀀스들을 trace 함수로 표현하기 위해 trace 함수에 대해 알아보면 다음과 같다.

Trace 함수는 finite field로부터 그의 subfield로의 선형매핑으로서 의사불규칙 시퀀스의 디자인과 분석을 위한 중요한 수학적 도구로써 널리 사용되고 있다.

즉, $m|n$에 대해 trace 함수 $tr_m^n(x)$는 $GF(2^n)$의 원소 x로부터 subfield $GF(2^m)$의 원소로의 매핑인데 다음의 관계식으로 표현할 수 있다.

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

위에서 정의된 trace 함수는 다음과 같은 유용한 성질들을 갖고 있다.

① 기약다항식(irreducible polynomial) over $GF(2^m)$의 $GF(2^n)$ 상에서의 모든 해는 동일한 trace 함수 값을 갖는다. 즉, 모든 i와 기약다항식의 해 $\alpha \in GF(2^n)$에 대해서

$$tr_m^n(\alpha) = tr_m^n(\alpha^{2^{mi}}) \tag{4}$$

를 만족한다.

② Trace 함수는 선형함수이다. 즉, 모든 $a, b \in GF(2^m)$와 $\alpha, \beta \in GF(2^n)$에 대해

$$tr_m^n(a\alpha + b\beta) = a\, tr_m^n(\alpha) + b\, tr_m^n(\beta) \tag{5}$$

가 성립한다.

③ $GF(2^m)$내의 모든 고정된 원소 b에 대하여, $tr_m^n(x) = b$를 만족하는 $GF(2^n)$ 상에서의 x는 정확히 2^{n-m}개이다.

④ $GF(2^n)$내의 모든 원소 x에 대해서 다음과 같은 관계를 만족한다.

$$tr_1^n(x) = tr_1^m\{tr_m^n(x)\} \tag{6}$$

이러한 trace 함수를 이용하여 주기가 $2^n - 1$인 이진 m-시퀀스를 표현하면 다음과 같다.

$$s(t) = tr_1^n(\alpha^t) \tag{7}$$

여기서 α는 $GF(2^n)$의 원시원(primitive element)이다.

본 논문에서 II절은 cyclic Hadamard difference set의 개요를 설명하고 특정한 주기에서 이상적인 자기상관특성을 갖는 Hall's sextic residue 시퀀스를 trace 함수를 이용하여 표현하였다. III절에서는 이상적인 자기상관특성을 갖는 생성방법이 알려져 있지 않은 기타 시퀀스들과 컴퓨터 search에 의해 발견된 새로운 이진시퀀스를 trace 함수를 이용하여 표현하였다. 그리고 IV절에서는 결론으로 본 논문의 끝을 맺었다.

II. Hall's Sextic Residue 시퀀스

1. Cyclic Hadamard Difference Set

서로 다른 k개의 residue $d_1, d_2, \cdots, d_k \bmod v$의 집합에서 모든 residue $b \not\equiv 0 \pmod v$에 대해 $b \equiv d_i - d_j \pmod v$의 관계식을 만족시키는 (d_i, d_j)가 λ개 존재한다면, 이 집합을 (v, k, λ)-difference set D라 한다. 여기서 각 파라미터들은 다음의 관계식을 만족한다.

$$\lambda(v-1) = k(k-1) \tag{8}$$

(v, k, λ)-difference set이 $(4n-1, 2n-1, n-1)$인 경우를 Hadamard difference set이라 하는데 정수 n에 대해 $4n$의 order를 갖는 Hadamard 행렬을 구성할 수 있다.

또한, v의 길이를 갖는 balanced binary two-level autocorrelation 시퀀스로 $v+1$의 order를 갖는 cyclic Hadamard 행렬들을 만들 수 있으므로, 이들 시퀀스를 cyclic Hadamard 시퀀스라고 부르기도 한다. 지금까지 알려진 Hadamard difference set들은 다음과 같은 4가지이다.

① $GF(p)$내의 quadratic residue로 이루어지는 Paley-Hadamard difference set의 시리즈가 있다. 이것을 이용하여 $v=4n-1$이 소수일 경우에 v의 길이를 갖는 Legendre 시퀀스를 구성할 수 있다[8].

② 모든 prime power q와 $d \geq 2$인 모든 정수에 대해 cyclic (v, k, λ)-difference set D가 존재하며, 이를 Singer difference set이라 하는데, 여기서 $q=2$의 경우에 다음과 같은 파라미터를 갖는 cyclic Hadamard difference set을 만든다.

$$(2^{d+1}-1,\ 2^d-1,\ 2^{d-1}-1) \tag{9}$$

③ p와 $p+2$가 odd prime이라면 order가 $v=p(p+2)$인 Hadamard difference set을 만들 수 있는데, 이를 twin prime construction이라 한다. 이를 이용하여 Jacobi 시퀀스를 구성할 수 있다.

④ p를 $p=4x^2+27$ 형태의 prime이라면 sextic residue의 어떤 coset들을 이용함으로써 $GF(q)$내의 cyclic Hadamard difference set을 구성할 수 있다. 이것을 이용하여 Hall's sextic residue 시퀀스를 구성할 수 있다.

Mersenne prime p와 $p=4x^2+27$의 형태가 같은 경우는 $p=31, 127, 131071$의 3가지인데, 이

들 중에 $v=31$일 때만이 ④의 sextic residue와 Singer difference set이 일치한다. 또, $v=15$일 때 Paley 시리즈와 ③의 twin prime construction은 일치한다.

Finite field내의 cyclotomic class들로부터 abelian difference set의 요소를 결정하는 것에 대해 고려하도록 하자. Prime power q를 고정시키고 $GF(q)^*$의 원소 ω와 $q-1=ef$를 만족하는 $e, f \neq 1$인 양의 정수를 발생시키면, e번째 cyclotomic classes $C_0, C_1, \cdots, C_{e-1}$은 다음과 같다.

$$C_i = \{\omega^{es+i} : s=0,1,\cdots,f-1\} \text{ for } i=0,1,\cdots,e-1 \tag{10}$$

다시 말하면, 이것들은 $GF(q)^*$내의 e번째 멱승의 집합 C_0의 multiplicative coset이다.

또한, 이것은 q가 소수라면 C_0의 원소의 e-th power residue라 한다. $e=2,3,4,5,6,8$의 경우에 대해 각각 quadratic, cubic, quartic 또는 biquadratic, quintic, sextic, octic residue라고 한다. 본 논문에서 다루고 있는 Hall's sextic residue 시퀀스는 $e=6$에 대해서 생성할 수 있다. 또한, e를 order로 갖는 cyclotomic number들은 다음과 같이 정의한다.

$$(i,j)_e = |\{(x,y) : x \in C_i,\ y \in C_j,\ x+1=y\}| \tag{11}$$

Cyclotomic number들은 cyclotomic class들의 적절한 합집합으로써, $GF(q)$의 additive group G 내의 difference set을 만드는데 중요하다.

$q=ef+1$가 odd prime이라고 가정하고, order e의 cyclotomic class들의 합집합이 difference set을 형성한다면, f는 홀수이고 e는 짝수이다.

D를 sextic residue를 multiplier로 갖고 곱셈형식으로 표현되는 group $G=\mathrm{E}A(q)$내의 difference set이라 하자. 여기서 $q \equiv 1 \pmod 6$을 만족하는 prime power라 하면, D는 다음과 같은 2가지 경우 중에 하나이다.

① $q \equiv 3 \pmod 4$이고 D는 quadratic residue로 구성된다.

② $q=4x^2+27$의 형태를 가지며, $D=C_0 \cup C_1 \cup C_3$이다.

Hall's sextic residue 시퀀스는 이와 같은 difference set D를 이용하여 생성할 수 있다.

다음절에서는 앞에서 언급한 cyclic Hadamard 시퀀스들 중에 Hall's sextic residue 시퀀스와 생성방법이 알려지지 않은 여러 가지의 기타 시퀀스들을 trace 함수를 이용하여 표현하였다.

2. Hall's Sextic Residue 시퀀스의 Trace 함수로의 표현

일반적으로 의사불규칙 시퀀스는 trace 함수를 이용하여 표현함으로써 그 시퀀스의 성질규명 및 생성기의 구현을 용이하게 할 수가 있다. 따라서 본 절에서는 이상적인 자기상관특성을 갖는

Hall's sextic residue 시퀀스를 trace 함수를 이용하여 표현하였다. Mersenne prime p가 $p=4x^2+27=2^m-1$을 만족시키는 수는 다음과 같이 $p=31, 127, 131071$가 있고 이들의 주기에 대해서 Hall's sextic residue 시퀀스가 존재하는데, 이들은 다음과 같이 trace 함수를 이용하여 표현할 수 있다.

$$h(t) = \sum_{i=0}^{\frac{p-1}{6m}-1} tr_1^m(\alpha^{u^{6i}t}) \tag{12}$$

여기서 u는 modulo p연산을 한 정수들의 집합인 Z_p의 원시원(primitive element)이며, α는 $GF(2^m)$의 원시원이다.

앞에서 정의한 식으로 $p=31, 127, 131071$일 때, Hall's sextic residue 시퀀스를 trace 함수를 이용하여 표현하면 다음과 같다.

먼저, $p=2^m-1=2^5-1=31$인 경우에 Hall's sextic residue 시퀀스는 trace 함수를 이용하여 다음과 같이 표현할 수 있다.

$$h(t) = \sum_{i=0}^{\frac{p-1}{6m}-1} tr_1^m(\alpha^{u^{6i}t}) = tr_1^5(\alpha^t) \tag{13}$$

따라서, $p=31$인 경우에는 Hall's sextic residue 시퀀스는 m-시퀀스와 동일함을 알 수 있다.

$p=2^m-1=2^7-1=127$인 경우에 Z_{127}의 원시원은 3이므로, Hall's sextic residue 시퀀스를 trace 함수를 이용하여 표현하면 다음과 같다.

$$h(t) = \sum_{i=0}^{\frac{p-1}{6m}-1} tr_1^m(\alpha^{u^{6i}t}) = \sum_{i=0}^{2} tr_1^7(\alpha^{3^{6i}t})$$

$$= tr_1^7(\alpha^t)+tr_1^7(\alpha^{19t})+tr_1^7(\alpha^{47t}) \tag{14}$$

$p=2^m-1=2^{17}-1=131071$인 경우에도 Z_{131071}의 원시원이 3이므로, Hall's sextic residue 시퀀스를 trace 함수를 이용하여 표현하면 다음과 같다.

$$h(t) = \sum_{i=0}^{\frac{p-1}{6m}-1} tr_1^m(\alpha^{u^{6i}t}) = \sum_{i=0}^{1284} tr_1^{17}(\alpha^{3^{6i}t}) \tag{15}$$

이때, 같은 주기를 갖는 cyclically different한 Hall's sextic residue 시퀀스는 모두 6개가 존재한다.

III. 기타 시퀀스들의 Trace 함수로의 표현

몇몇의 특정한 주기에서 아직은 생성방법이 알려지지 않았지만, 이상적인 자기상관특성을 갖는 기타 시퀀스들이 존재한다는 것이 알려져 왔다. 본 논문에서는 그 중에서 컴퓨터에 의한 모의실험에 의하여 발견한 이상적인 자기상관특성을 갖는 기타 시퀀스들을 trace 함수로 표현하였다.

$2^7-1=127$의 주기에서는 이상적인 자기상관특성을 갖는 이진 시퀀스가 모두 6종류가 존재한다. 즉, m-시퀀스, Legendre 시퀀스, Hall's sextic residue 시퀀스외에 3종류의 기타 시퀀스가 존재한다[4]. 그러나 이들의 3종류의 기타 시퀀스는 아직 trace 함수를 이용하여 표현되지 못하였는데 본 논문에서는 이들을 아래의 수식과 같이 trace 함수를 이용하여 표현하였다.

$$s_1(t) = tr_1^7(\alpha^t)+tr_1^7(\alpha^{3t})+tr_1^7(\alpha^{7t})+tr_1^7(\alpha^{19t})+tr_1^7(\alpha^{29t}) \tag{16}$$

$$s_2(t) = tr_1^7(\alpha^t)+tr_1^7(\alpha^{5t})+tr_1^7(\alpha^{7t})+tr_1^7(\alpha^{11t})+tr_1^7(\alpha^{31t}) \tag{17}$$

$$s_3(t) = tr_1^7(\alpha^t)+tr_1^7(\alpha^{9t})+tr_1^7(\alpha^{13t}) \tag{18}$$

여기서 α는 $GF(2^7)$의 원시원이다.

$2^8-1=255$의 주기에서는 이상적인 자기상관특성을 갖는 이진 시퀀스가 4종류가 존재한다. 즉, m-시퀀스, GMW 시퀀스외에 2종류의 기타 시퀀스가 존재한다[5]. 이들의 기타 시퀀스를 trace 함수를 이용하여 표현하면 각각 다음과 같다.

$$s_1(t) = tr_1^8(\alpha^t)+tr_1^8(\alpha^{3t})+tr_1^8(\alpha^{11t})+tr_1^8(\alpha^{43t})+tr_1^8(\alpha^{111t}) \tag{19}$$

$$s_2(t) = tr_1^8(\alpha^t)+tr_1^8(\alpha^{7t})+tr_1^8(\alpha^{9t})+tr_1^8(\alpha^{47t})+tr_1^8(\alpha^{63t}) \tag{20}$$

여기서 α는 $GF(2^8)$의 원시원이다.

그리고 $2^9-1=511$의 주기에서는 255의 주기에서와 같이 이상적인 자기상관특성을 갖는 이진 시퀀스가 현재까지 발견된 것은 모두 4종류이다. 즉, m-시퀀스, GMW 시퀀스 그리고 그 외에 2종류의 기타 시퀀스가 존재한다는 것이 알려져 있다[6]. 이들의 기타 시퀀스를 trace 함수를 이용하여 표현하면 각각 다음과 같다.

$$s_1(t) = tr_1^9(\alpha^t)+tr_1^9(\alpha^{3t})+tr_1^9(\alpha^{39t})+tr_1^9(\alpha^{55t})+tr_1^9(\alpha^{107t})+tr_1^9(\alpha^{125t})+tr_1^9(\alpha^{191t}) \tag{21}$$

$$s_2(t) = tr_1^9(\alpha^t) + tr_1^9(\alpha^{17t}) + tr_1^9(\alpha^{25t}) \tag{22}$$

여기서 α는 $GF(2^9)$의 원시원이다.

$2^{10}-1=1023$의 주기에서는 이상적인 자기상관특성을 갖는 이진 시퀀스가 m-시퀀스, GMW 시퀀스, 그리고 extended Legendre 시퀀스 등이 있는데 본 논문에서는 컴퓨터 search를 통하여 이상적인 자기상관특성을 갖고 있으나 그의 생성방법이 구체적으로 알려지지 않은 하나의 새로운 기타 시퀀스를 발견하였는데, 이것을 trace 함수를 이용하여 표현하면 다음과 같다.

$$s(t) = tr_1^{10}(\alpha^t) + tr_1^{10}(\alpha^{9t}) + tr_1^{10}(\alpha^{57t}) + tr_1^{10}(\alpha^{73t}) + tr_1^{10}(\alpha^{121t}) \tag{23}$$

여기서 α는 $GF(2^{10})$의 원시원이다.

그리고 $2^{13}-1=8191$의 주기에서도 지금까지 알려진 이상적인 자기상관특성을 갖는 이진 시퀀스들 외에 하나의 새로운 기타 시퀀스를 컴퓨터 search를 통하여 발견하였다. 이것을 trace 함수를 이용하여 표현하면 다음과 같다.

$$s(t) = tr_1^{13}(\alpha^t) + tr_1^{13}(\alpha^{65t}) + tr_1^{13}(\alpha^{97t}) \tag{24}$$

여기서 α는 $GF(2^{13})$의 원시원이다.

IV. 결 론

본 논문에서는 특정한 주기에서 이상적인 자기상관특성을 갖는 Hall's sextic residue 시퀀스를 trace 함수로 표현하였으며, 또한 특정한 주기에서 이상적인 자기상관특성을 갖는다고 알려진 주기가 127, 255, 및 511에서의 기타 시퀀스들을 trace 함수를 이용하여 표현하였으며 또한 주기가 1023 및 8191의 경우에는 아직은 구체적인 생성방법이 알려지지 않은 기타 시퀀스들을 새로 발견하였고 이들을 trace 함수를 이용하여 표현하였다. 따라서, 다른 의사불규칙 시퀀스들과 마찬가지로 생성방법이 알려지지 않은 기타 시퀀스들을 finite field상에서 trace 함수를 이용하여 표현함으로써 이들 시퀀스들의 성질 규명 및 생성기의 구현이 용이하게 되었다.

[참고문헌]

[1] M.Hall.Jr., "A survey of difference sets," Proc. Amer. Math. Soc., vol. 7, pp. 975-986, 1596.

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

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

[4] L.D.Baumert and H.Fredricksen, "The Cyclotomic Numbers of Order Eighteen with Applications to Difference Sets," *Math. Computation*, 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] R.A.Sholtz and L.R.Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 3, pp. 548-553, 1984.

[8] 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.