논문 2010-47TC-7-14

고속 M-Gold-Hadamard 시퀀스 트랜스폼

(On Fast M-Gold Hadamard Sequence Transform)

이 미 성*, 이 문 호**, 박 주 용***

(Mi Sung Lee, Moon Ho Lee, and Ju Yong Park)

요 약

본 논문에서는 GF(2)에서의 두 생성다항식에 의해 생성된 M-sequence로 Gold-Sequence를 생성한 후, Permutation을 해줌으로써 Hadamard 행렬의 특성을 가지게 됨을 살펴보았다. M-sequence는 선형 귀환 천이 레지스터 부호 생성기(Linear feedback shift register code generator)에 의해 생성되었으며, 두 개의 M-sequence에 의해 생성된 Gold-sequence의 첫 열에 8x1의 영행렬을 추가하고 Permutation을 시켜줌으로써 Hadamard 행렬의 주요 성질인 직교성(Orthogonal)과 한 행렬과 이 행렬의 Transpose시킨 행렬의 결과가 단위행렬이 되고, 역행렬은 element-wise Inverse가 되며, 고속 Jacket행렬의 성질을 만족한다. 또한 선형 귀환 축차 생성기를 통하여 생성된 M-sequence의 1행과 1열을 추가함으로써 위에서 언급한 Hadamard 행렬의 주요 성질을 만족하고 L-matrix 와 S-matrix 를 통하여 고속변환이 가능함을 보인다.

Abstract

In this paper we generate Gold-sequence by using M-sequence which is made by two primitive polynomial of GF(2). Generally M-sequence is generated by linear feedback shift register code generator. Here we show that this matrix of appropriate permutation has Hadamard matrix property. This matrix proves that Gold-sequence through two M-sequence and additive matrix of one column has one of major properties of Hadamard matrix, orthogonal. and this matrix show another property that multiplication with one matrix and transpose matrix of this matrix have the result of unit matrix. Also M-sequence which is made by linear feedback shift register gets Hadamard matrix property mentioned above by adding matrices of one column and one row. And high-speed conversion is possible through L-matrix and the S-matrix.

Keywords : M-sequence, 고속변환, Gold sequence, Hadamard Transform, Orthogonal

I. 서 론

의사잡음수열(Pseudo Noise Sequence or M Sequence)은 첫째, 디지털 통신에서 의사 잡음 수열은 통계적인 무작위성에 대한 표준 검사 중 하나 이상을 충족시키는 잡음과 비슷한 신호의 한 종류가 의사 잡음이다. 의사 잡음 수열이나 의사 잡음 부호 수열을 이용하여 잡음처럼 보이는 광대역 확산 대역 신호를 생성한다. 둘째, 암호에서는 하나의 키로 의사 잡음 형태를 결정하는데 의사 잡음의 반복 주기는 수 백 만년이 될 수 있을 정도로 매우 길다. 의사 잡음기는 일부 전자 음악 악기에 감산 합성의 입력 형태나 의사 잡음 자체로 사용되며 다른 백색 잡음 기계에 사용 된다. 셋째, 이동통신에서는 직접 확산 방식 시스템에서 의사 잡음 확산 파형은 의사 잡음 수열의 시간 함수이다. 주파수 도약 방식의 시스템에서 의사 잡음 부호는 주파수 도약 형태를 생성한다. 주의할 점은 확산 대역 통신 링크 사이에 유용한 정보 교환이 이루어지도록 의사 잡음 수열은 결정적으로 생성되어야 한다. 의사 잡음 수열은 일반 사용자에게 난수 수열처럼 보이도록 설계해야 하고 또한 의사 잡음처럼 보이는 시간 파형을 생성한다. 의사 잡

* 학생회원, ** 정회원, 전북대학교 전기전자컴퓨터공학부
(Chonbuk National University)
*** 정회원, 신경대학교 인터넷정보통신학과
(Shingyeong University)
※ 본 논문은 WCU R32-2009-000-200 14-0에 의하여 이뤄졌음
접수일자:2009년11월12일 수정완료일자:2010년6월21일

음 부호는 난수 수열과 비슷한 대역을 가지지만 결정적으로 생성된다.

넷째, 직접 확산 방식 시스템에 가장 많이 쓰이는 수열은 최대 길이 수열, Gold 부호, Kasami 부호, Barker 부호 등이다. 선형 귀환 축차 생성기를 이용하여 의사 잡음 수열은 0과 1로 구성되어 있기에 이진 의사 잡음 수열이다. 따라서 M-sequence는 선형 귀환 축차 생성기에 의해 발생되기 때문에 이진수열(Binary Sequence)로 의사잡음수열(Pseudo-Noise Sequences)이다.

이에 대한 연구는 M시퀀스에 대해 1960년대부터 연구가 되어 왔는데 상호 상관과 자기 상관이 좋은 상관 관계 시퀀스를 찾는데 노력해왔다. 1967년 Golomb는 $\{a_n\}$과 $\{b_n\}$이 상이한 원시 다항식에서 3개 값을 갖는 상호상관 관계를 밝혔고, 1967년 Gold는 3개의 Recursive 상호 상관 관계값을 찾았다. 1969년 Kasami는 Multiple access통신을 위한 3개 이상의 상호 상관 시퀀스를, 국내에서는 1989년 서울대 노종선 교수가 No Sequence를 발표했는데 Kasami 시퀀스와 같은 종류의 많은 선형 스펜(Span) 시퀀스를 갖는다.

본 논문은 Ⅱ장에서 M-Sequence (or Pseudo Sequence) 에 대해 소개하고 Ⅲ장에서는 이의 생성방법과 생성된 sequence의 변환을 통해 중요 성질과 고속의 변환을 보이고, Ⅳ장에서는 Gold sequence에 대한 대략적인 소개와 이 행렬의 변환으로 Hadamard 행렬의 성질을 가짐을 보이며, Ⅴ장에서는 고속 Hadamard 변환에 관한 내용을 다루었고 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. M(or Pseudo Noise) Sequence

M-sequence는 선형 귀환 천이 레지스터에 의해 발생되는 이진수열로 TR(transmitted reference) 대역 확산 방식은 다른 대역에서 부호 신호와 변조된 데이터 부호 신호를 동시에 전송하기 때문에 확산(spreading)과 복원(despreading)에 실제 랜덤 코드 신호를 이용할 수 있다. 그러나 SR(stored reference) 방식에서는 부호가 수신단에서 발생되거나 저장될 필요가 없기 때문에 실제 랜덤 신호를 사용할 수 없다. 따라서, SR방식은 가상잡음 즉, PN 신호를 사용하여 송수신 상호간에 동일 코드를 발생할 수 있는 기준을 제공해야 한다.

PN 신호를 외관적으로 랜덤한 것처럼 만드는 랜덤 특성을 알아보면, 임의의 주기적인 2진 수열에 적용될

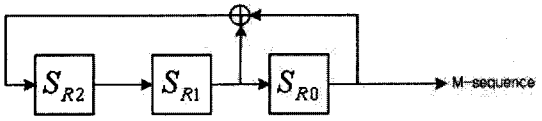


그림 1. $f(x)=x^3+x+1$ 대한 피드백 생성기
Fig. 1. Feedback generators for $f(x)=x^3+x+1$.

수 있는 3가지 기본 특성이 있다. 기본 특성은 평형(balance), 동작(run), 상관(correlation)등으로 다음과 같다. 여기서 평형특성은 각 수열의 한주기에서 이진 1의 개수는 0의 개수보다 최대 1개 많다는 것을 말한다. 런(run)이란 같은 형태의 이진수열이고, 런의 길이란 런에서의 숫자(digit)의 개수이다. 수열내에 다른 숫자가 나타나면 새로운 런을 시작한다. 각 주기에서 런의 개수의 1/2는 길이가 1이고 1/4는 길이가 2, 1/8은 길이가 3 등으로 나타난다.

상관 특성은 한 주기의 수열이 그 자체의 순환 이전된 수열의 한 주기마다 비교되어질 때 일치하는 숫자(number of agreements)와 일치하지 않는 숫자(number of disagreement)의 차이가 한 개 이하이면 가장 좋은 경우이다.

위의 그림 1의 선형 피드백 3단 천이 레지스터의 연산은 클럭 펄스열로서 제어한다. 각 클럭 펄스마다 레지스터 각단의 내용은 오른쪽으로 한 단씩 천이되고 단의 내용 레지스터 S_{R1}와 레지스터 S_{R0}은 modulo-2 가산이 되어 레지스터 S_{R2}로 피드백된다. 그림 1에서 천이 레지스터열은 마지막 단 레지스터 S_{R0}의 출력으로 정의된다. 레지스터 초기 상태가 100일 때 연속적인 레지스터 상태는 다음의 표 1과 같다.

초기 상태에 대응되는 마지막 상태가 100으로 레지스터가 7클럭 펄스 후에 이전의 수열이 다시 반복한다는 것을 알 수 있다. 출력 수열은 매 클럭마다 레지스터 S_{R0}의 내용을 표시함으로 얻을 수 있고 출력 수열은 다

표 1. $f(x)=x^3+x+1$ 대한 피드백 생성기의 출력값
Table 1. Output of Feedback generators for $f(x)=x^3+x+1$.

Shift	S_{R2}	S_{R1}	S_{R0}
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1

음 (1)과 같다.

출력 : 0 0 1 0 1 1 1 (1)

위에서 얻은 레지스터 S_{R0}로 부터의 출력에 대해 위에서 언급했던 수열의 랜덤 특성을 테스트해 보면, 먼저 수열 내에 3개의 0과 4개의 1이 있다. 따라서 평형 조건을 만족한다. 그리고 런특성은 수열의 길이가 짧아서 최소 15자리의 출력에서부터 확인할 수 있다. 이 후로 더 늘려가며 체크해 보면 런 특성도 만족됨을 확인할 수 있다. 위의 경우 수열의 길이가 짧지만 표 1을 보면 상관특성 또한 만족함을 알 수 있다. 출력수열은 최대 길이(maximal length)와 비최대 길이(nonmaximal length)로 분류된다. 최대 길이 수열은 n단 선형 피드백 천이 레지스터에 대해 클럭 펄스에서 다음과 같은 수열 반복 주기를 갖는다.

$$p=2^n-1 \tag{2}$$

그러므로 그림 1의 천이 레지스터열은 최대 길이 수열이다. 수열의 길이가 (2^n-1)보다 적으면 이 수열은 비최대 길이 수열로 구분된다.

PN시퀀스의 가장 주요한 성질중에 한가지로 자기상관 특성을 말할 수 있다. T_0의 주기적인 파형을 갖는 $x(t)$의 자기 상관 함수는 다음과 같이 나타낼 수 있다.

$$R_x(\tau)=\frac{1}{K}\left(\frac{1}{T_0}\right)\int_{-\frac{T_0}{2}}^{\frac{T_0}{2}}x(t)x(t-\tau)dt(\text{for } -\infty<\tau<\infty) \tag{3}$$

$$K=\frac{1}{T_0}\int_{-\frac{T_0}{2}}^{\frac{T_0}{2}}x^2(t)dt \tag{4}$$

$x(t)$가 PN 코드를 표현하는 주기적인 펄스 파형이라고 할 때, 각 기본 펄스를 PN 코드 심볼 또는 칩으로 간주한다. 이와 같은 단위 칩 구간과 주기의 p의 PN

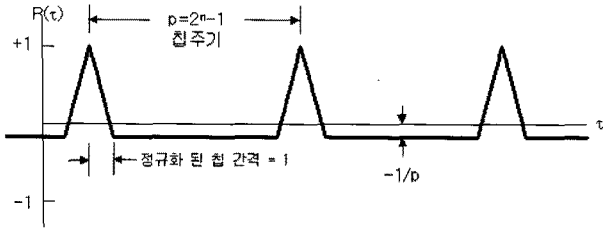


그림 2. PN 상관 함수
Fig. 2. PN correlation function.

수열에 대해 최대 길이 수열에 대한 정규화된 자기 상관 함수 $R_x(\tau)$는 그림 2처럼 나타낼 수 있다.

$\tau=0$이면 $R(\tau)=1$이나 $(1\le\tau$ <p)에서 $x(t)$와 $x(t-\tau)$에 대해서 -1/p이다. p가 커질 경우 수열은 가상적으로 하나의 칩의 천이에 대해서는 비상관이다. 임의의 PN수열의 랜덤 특성-상관 관계를 살펴보면 일치하는 숫자는 a(=3), 일치하지 않는 숫자는 d(=4)로 할 때 다음과 같다.

$$R(\tau=1)=\frac{1}{7}(3-4)=-\frac{1}{7} \tag{5}$$

완벽한 비정합성을 가지는 순환 이동은 동일한 자기상관값 -1/p를 가짐을 알 수 있다. 그러므로 이 수열은 랜덤 특성의 상관 특성을 만족한다. 이러한 점이 천이 레지스터 부호를 사용하는 중요한 이유이다.

Ⅲ. M-sequence 생성 방법

앞 장에서 생성다항식 $f(x)=x^3+x+1$를 사용하여 구한 출력값 0 0 1 0 1 1 1을 이용하여 M-sequence를 생성하고, 1 -> -1, 0 ->.1로 표현하면 출력값은 1 1 -1 1 -1 -1 -1로 나타낼 수 있다. 이 출력값을 첫 번째 행으로 놓고, Shift Registor를 이용하여 6번 Shift시키면 다음 7 x 7의 M행렬을 얻을 수 있다.

$$M=\begin{bmatrix} 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 \end{bmatrix} \tag{6}$$

위의 과정을 통해 얻은 M-sequence의 각 첫 번째 column과 첫 번째 row에 1 1 1 1 1 1 1 1을 삽입하여 Hadamard 행렬의 특성을 가짐을 보인다.

$$\hat{H}_8=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \end{bmatrix} \Rightarrow$$

$$\hat{H}_8^{-1}=\frac{1}{8}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \end{bmatrix} \tag{7}$$

위의 (7)과 같이 추가된 column과 row에 의해 앞장에서 언급한 여러 성질들을 만족하며 Hadamard 행렬의 주요한 성질인 직교성과 $\hat{H}_8\hat{H}_8^{-1}=nI_8$의 관계가 성립함을 볼 수 있다. 또한 위에서 구한 출력값 0 0 1 0 1 1 1 에 의해 생성된 M-sequence에 각 첫 번째 column과 첫 번째 row에 1 1 1 1 1 1 1 1을 삽입함으로써 이 행렬의 고속변환 또한 가능하다.

예를 들어 n=3인 경우, 생성다항식이 $f(x)=x^3+x+1$ 일 때, 출력 시퀀스는 0 0 1 0 1 1 1이다. 이를 이용해 M-sequence를 생성한 후, 각각의 첫 번째 column과 row에 1 1 1 1 1 1 1 1을 삽입해주면 다음의 행렬 M_c를 얻을 수 있다.

$$M_c=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&0&0&1&0&1&1&1\\1&0&1&0&1&1&1&0\\1&1&0&1&1&1&0&0\\1&0&1&1&1&0&0&1\\1&1&1&1&0&0&1&0\\1&1&1&0&0&1&0&1\\1&1&0&0&1&0&1&1\end{bmatrix}=LS=S'L' \tag{8}$$

(8)에서 L은 $(p+1)\times(n+2)$의 2진 행렬을, S는 M_c의 첫 번째 행부터 다섯 번째 행까지의 $(n+2)\times(p+1)$ 행렬을, '(prime)은 matrix transposition을 나타낸다. 여기에서 L과 S의 index를 변환하여 계산을 수행하였고 이를 통해 불규칙하게 1행렬을 추가시켰음에도 고속변환공식을 사용할 수 있음을 보인다.

이제, σ를 S의 첫 번째 $n+2$열들로 구성되어진 $n+2$ 차의 정방 행렬이라고 놓으면 (8)로부터,

$$L\sigma=S' \tag{9}$$

(9)식을 얻을 수 있다. 0이 아닌 모든 이진 n 벡터는 양 L, S'에서 행으로서 나타난다. 따라서 행렬 σ는 필수적으로 nonsingular이다.

$$L=S'\sigma^{-1} \tag{10}$$

이로써 (11)을 얻을 수 있다.

$$S=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&0&0&1&0&1&1&1\\1&0&1&0&1&1&1&0\\1&1&0&1&1&1&0&0\\1&0&1&1&1&0&0&1\end{bmatrix}\quad\sigma=\begin{bmatrix}1&1&1&1&1\\1&0&0&1&0\\1&0&1&0&1\\1&1&0&1&1\\1&0&1&1&1\end{bmatrix}$$

$$\sigma^{-1}=\begin{bmatrix}0&1&1&0&1\\1&0&0&0&1\\1&0&0&1&0\\0&0&1&0&1\\1&1&0&1&1\end{bmatrix}$$

$$L=\underbrace{\begin{bmatrix}1&1&1&1&1\\1&0&0&1&0\\1&0&1&0&1\\1&1&0&1&1\\1&0&1&1&1\\1&1&1&1&0\\1&1&1&0&0\\1&1&0&0&1\end{bmatrix}}_{S'}\underbrace{\begin{bmatrix}0&1&1&0&1\\1&0&0&0&1\\1&0&0&1&0\\0&0&1&0&1\\1&1&0&1&1\end{bmatrix}}_{\sigma^{-1}}=\underbrace{\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&1&0&1&1\\0&1&1&1&0\\0&0&1&1&1\end{bmatrix}}_{L} \tag{11}$$

(11)의 행렬에서 $L=(l_{ij})$라 하고, i = 1, 2, 3, ... , p에 대해 다항식은 아래와 같다.

$$g_i(x)=\sum_{j=1}^{n} l_{i,j}\,x^{j-1} \tag{12}$$

$$g_i(x)=x^{i-1}\ (\text{modulo f(x)}),\ \text{i = 1, 2, ... , p.} \tag{13}$$

(13)의 관계를 증명하기 위해 원시다항식을 수식화한 $f(x)=x^n+\sum_{j=0}^{n-1}c_jx^j$의 양변에 x^{k-n}을 곱하면 (14)가 되고

$$x^{k-n}f(x)=x^k+\sum_{j=0}^{n-1}c_jx^{j+k-n} \tag{14}$$

(14)의 좌변은 modulo $f(x)$에서 0이 되므로 (15)와 같이 쓸 수 있다.

$$x^k=\sum_{j=0}^{n-1}c_jx^{j+k-n}\ (\text{modulo } f(x)) \tag{15}$$

위의 가정을 이용하여 (15)를 다시 쓰면 (16)과 같다.

$$x^k=\sum_{j=0}^{n-1}c_jg_{j+k-n+1}\ (\text{modulo } f(x)) \tag{16}$$

여기에 (12)를 대입하면,

$$x^k=\sum_{j=0}^{n-1}\sum_{r=1}^{n}c_jl_{j+k-n+1,r}x^{r-1}\ \text{modulo } f(x) \tag{17}$$
$$=\sum_{r=1}^{n}x^{r-1}\sum_{j=0}^{n-1}c_jl_{j+k-n+1,r}$$

(10)에 의하면 L의 column은 S'의 선형적인 결합이다. 따라서 L의 각 column은 M-sequence의 기본식을 만족한다. 그러므로

$$\sum_{j=0}^{n-1}c_jl_{j+k-n+1,r}=l_{k+1,r} \tag{18}$$

(17)를 (18)에 대입하면, (19)를 얻을 수 있고,

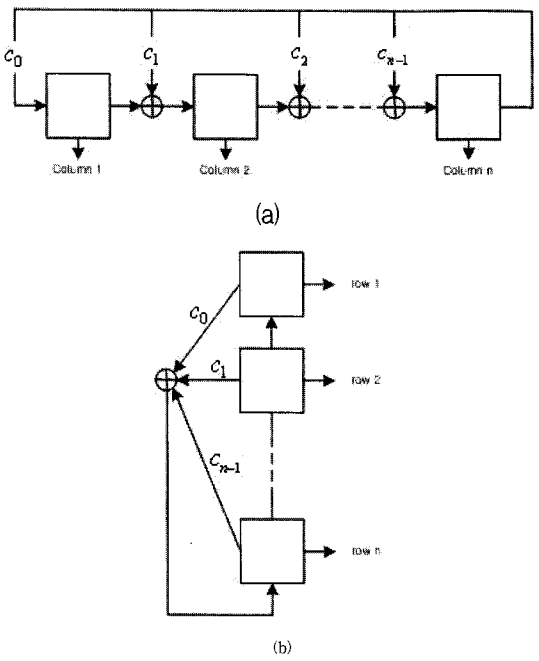


그림 3. 행렬 L과 S에 대한 피드백 생성기.
Fig. 3. Feedback generators for the matrices L and S.

$$x^k = \sum_{r=1}^{n} l_{k+1,r} x^{r-1} = g_{k+1}(x) (\text{modulo f(x)}) \qquad (19)$$

이로써 (13)이 증명된다. 예를 들어, n=5인 경우는 $f(x)=x^5+x^4+x^3+x$을 사용함으로써 (20)과 같고 (11)에서 구한 L과 같음을 볼 수 있다.

$$\begin{aligned}
g_i(x) &= \sum_{j=1}^{5} l_{i,j} x^{j-1} \\
g_1(x) &= l_{1,1}x^0 + l_{1,2}x^1 + l_{1,3}x^2 + l_{1,4}x^3 + l_{1,5}x^4 \\
g_2(x) &= l_{2,1}x^0 + l_{2,2}x^1 + l_{2,3}x^2 + l_{2,4}x^3 + l_{2,5}x^4 \\
&\vdots \\
g_8(x) &= l_{8,1}x^0 + l_{8,2}x^1 + l_{8,3}x^2 + l_{8,4}x^3 + l_{8,5}x^4
\end{aligned} \qquad (20)$$

$$\begin{aligned}
x^0 &= 1 \\
x^1 &= x \\
x^2 &= x^2 \\
x^3 &= x^3 \\
x^4 &= x^4 \\
x^5 &= x + x^3 + x^4 \\
x^6 &= x + x^2 + x^3 \\
x^7 &= x^2 + x^3 + x^4
\end{aligned} \qquad (\text{modulo} f(x))$$

따라서 L과 S matrix에 대한 feedback generator는 그림 3과 같다.

Ⅳ. Gold Sequence

Gold sequence는 두 개의 생성다항식을 이용하여 만들어진 각각의 M sequence의 출력 2개를 조합하여 만들어진 수열로 그림 4와 같다.

처음에 주어지는 초기값 001을 사용하여 각각의 생성다항식에 의해 생성되는 sequence들을 구한 후, 이들의 연산을 통해 Gold sequence를 구할 수 있다.

GF(2)에서 3차의 원시다항식은 위의 그림 4 에서 이용한 $f_1(x)=x^3+x+1$과 $f_2(x)=x^3+x^2+1$, 이 두 개뿐이다. 이 두 개의 3차 원시다항식을 생성다항식으로 이용하여 얻은 M-시퀀스를 X, Y라 할 때, 그림 4의 회로에 초기값 $a=[0\,0\,1]$를 넣어줌으로써 다음과 같은 출력값 X, Y를 얻을 수 있다.

$$\begin{aligned}
&\text{X=[1 0 0 1 0 1 1]} \\
&\text{Y=[1 0 0 1 1 1 0]}
\end{aligned} \qquad (21)$$

이 두 M-시퀀스를 이용해 Gold-시퀀스를 생성하기 위해 우리는 위의 과정에서 얻은 출력값 Y를 이용하여 다음의 값을 얻을 수 있다.

$$\begin{aligned}
Y &= 1\,0\,0\,1\,1\,1\,0 \\
T^{-1}Y &= 0\,0\,1\,1\,1\,0\,1 \\
T^{-2}Y &= 0\,1\,1\,1\,0\,1\,0 \\
T^{-3}Y &= 1\,1\,1\,0\,1\,0\,0 \\
T^{-4}Y &= 1\,1\,0\,1\,0\,0\,1 \\
T^{-5}Y &= 1\,0\,1\,0\,0\,1\,1 \\
T^{-6}Y &= 0\,1\,0\,0\,1\,1\,1
\end{aligned} \qquad (22)$$

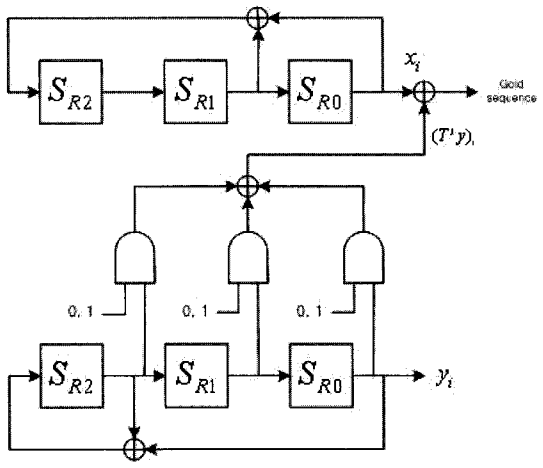


그림 4. 생성다항식 $f_1(x)=x^3+x+1$, $f_2(x)=x^3+x^2+1$에 대한 Gold sequence 생성기
Fig. 4. Gold sequence generator for the preferred-pair $f_1(x)=x^3+x+1$ and $f_2(x)=x^3+x^2+1$.

위의 표현식 중 $T^{-j}Y$는 Y를 왼쪽으로 j자리 순환 이동시키는 것을 나타낸다. 생성다항식 $f(x)=x^3+x+1$을 이용하여 얻은 X와 생성다항식 $f(x)=x^3+x^2+1$을 이용하여 얻은 Y의 shift value를 이용하여 다음의 Gold-시퀀스를 얻을 수 있다.

$$\begin{aligned}
X+\quad 0 &= 1\,0\,0\,1\,0\,1\,1\\
X+\quad Y &= 0\,0\,0\,0\,1\,0\,1\\
X+T^{-1}Y &= 1\,0\,1\,0\,1\,1\,0\\
X+T^{-2}Y &= 1\,1\,1\,0\,0\,0\,1\\
X+T^{-3}Y &= 0\,1\,1\,1\,1\,1\,1\\
X+T^{-4}Y &= 0\,1\,0\,0\,0\,1\,0\\
X+T^{-5}Y &= 0\,0\,1\,1\,0\,0\,0\\
X+T^{-6}Y &= 1\,1\,0\,1\,1\,0\,0
\end{aligned} \tag{23}$$

위의 계산의 결과와 첫 번째 column에 8x1의 0행렬을 넣어줌으로 우리는 다음의 (24)식의 행렬을 얻을 수 있다. 여기서 생성된 행렬 (24)는 불규칙하게 생성되었지만 PN시퀀스의 좋은 상관특성을 그대로 가지고 있다.

$$\hat{M}_{8\times 8}=\begin{bmatrix}
0&1&0&0&1&0&1&1\\
0&0&0&0&0&1&0&1\\
0&1&0&1&0&1&1&0\\
0&1&1&1&0&0&0&1\\
0&0&1&1&1&1&1&1\\
0&0&1&0&0&0&1&0\\
0&0&0&1&1&0&0&0\\
0&1&1&0&1&1&0&0
\end{bmatrix} \tag{24}$$

(24)에 생성된 시퀀스의 자기상관 특성은 일반적인 PN시퀀스와 같이 자기 자신과의 신호와의 관계를 제외한 모든 경우에 일정하게 나타난다. 그리고 이에 대한 상호상관 특성은 그림 5에서 나타내었다.

위의 (24)의 $\hat{M}$행렬을 0→1로, 1→-1로 표현하면, 다음의 (25)식과 같이 Hadamard 행렬의 특성을 가지는 $\tilde{H}$행렬을 얻을 수 있다.

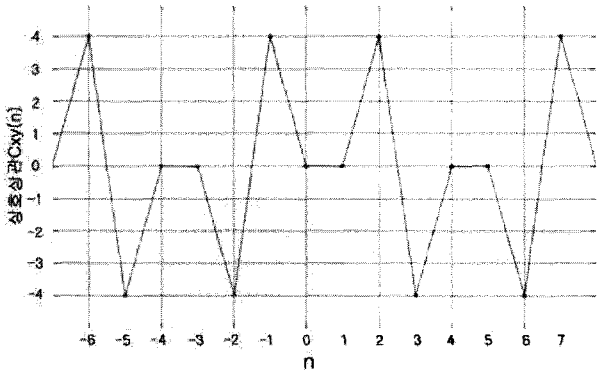


그림 5. Gold sequence에 대한 상호상관관계
Fig. 5. Cross-Correlation for Proposed Gold sequence.

$$\tilde{H}_{8\times 8}=\begin{bmatrix}
1&-1&1&1&-1&1&-1&-1\\
1&1&1&1&1&-1&1&-1\\
1&-1&1&-1&1&-1&-1&1\\
1&-1&-1&-1&1&1&1&-1\\
1&1&-1&-1&-1&-1&-1&-1\\
1&1&-1&1&1&1&-1&1\\
1&1&1&-1&-1&1&1&1\\
1&-1&-1&1&-1&-1&1&1
\end{bmatrix}$$

$$\tilde{H}_{8\times 8}=\begin{bmatrix}
1&-&1&1&-&1&-&-\\
1&1&1&1&1&-&1&-\\
1&-&1&-&1&-&-&1\\
1&-&-&-&1&1&1&-\\
1&1&-&-&-&-&-&-\\
1&1&-&1&1&1&-&1\\
1&1&1&-&-&1&1&1\\
1&-&-&1&-&-&1&1
\end{bmatrix} \tag{25}$$

여기서 구한 (25)식, $\tilde{H}$행렬의 첫 번째 row과 두 번째 row, 여섯 번째 column과 여덟 번째 column을 permutation해주면, 위에서 구한 permutation행렬과 그의 transpose행렬의 연산이 단위행렬의 결과를 얻음을 (30)식을 통해 확인할 수 있다. 위에서 구한 (25)식의 permutation을 위한 permutation행렬 P_r, P_c는 다음과 같다.

$$P_r=\begin{bmatrix}
0&1&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1
\end{bmatrix} \tag{26}$$

$$P_c=\begin{bmatrix}
1&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&0
\end{bmatrix} \tag{27}$$

한편 위에서 언급한 permutation을 사용하기 위해서 (25)식과 permutation행렬 (26)식과 (27)식을 이용하여

$$P_r\,\tilde{H}_8\,P_c=\check{H}_8 \tag{28}$$

다음의 (28)식과 같이 8 x 8 Hadamard 행렬의 특성을 갖는 $\check{H}_8$을 얻을 수 있다.

$$\begin{bmatrix}01000000\\10000000\\00100000\\00010000\\00001000\\00000100\\00000010\\00000001\end{bmatrix}\begin{bmatrix}1&-1&1&1&-1&1&-1&-1\\1&1&1&1&1&-1&1&-1\\1&-1&1&-1&1&-1&-1&1\\1&-1&-1&-1&1&1&1&-1\\1&1&-1&-1&-1&-1&-1&-1\\1&1&-1&1&1&1&-1&1\\1&1&1&-1&-1&1&1&1\\1&-1&-1&1&-1&-1&1&1\end{bmatrix}\begin{bmatrix}10000000\\01000000\\00100000\\00010000\\00001000\\00000001\\00000010\\00000100\end{bmatrix}$$

$$\check{H}_{8\times8}=\begin{bmatrix}1&1&1&1&1&-1&1&-1\\1&-1&1&1&-1&-1&-1&1\\1&-1&1&-1&1&1&-1&-1\\1&-1&-1&-1&1&-1&1&1\\1&1&-1&-1&-1&-1&-1&-1\\1&1&-1&1&1&1&-1&1\\1&1&1&-1&-1&1&1&1\\1&-1&-1&1&-1&1&1&-1\end{bmatrix} \quad (29)$$

마지막으로 위에서 구한 $\check{H}_8$행렬과 $\check{H}_8$행렬의 transpose 행렬을 연산하면 다음의 결과 (30)을 얻을 수 있다. 이 식에서 사용된 $\check{H}_8^T$는 $\check{H}_8$행렬의 transpose 행렬을 나타낸다.

$$\check{H}_{8\times8}\times\check{H}_{8\times8}^T=$$

$$\begin{bmatrix}1&1&1&1&1&-&1&-\\1&-&1&1&-&-&-&1\\1&-&1&-&1&1&-&-\\1&-&-&-&1&-&1&1\\1&1&-&-&-&-&-&-\\1&1&-&1&1&1&-&1\\1&1&1&-&-&1&1&1\\1&-&-&1&-&1&1&-\end{bmatrix}\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-&-&-&1&1&1&-\\1&1&1&-&-&-&1&-\\1&-&-&-&1&-&-&1\\1&-&1&1&-&1&-&-\\-&-&1&-&-&1&1&1\\1&-&-&1&-&-&1&1\\-&1&-&1&-&1&1&-\end{bmatrix}$$

$$=\begin{bmatrix}8&0&0&0&0&0&0&0\\0&8&0&0&0&0&0&0\\0&0&8&0&0&0&0&0\\0&0&0&8&0&0&0&0\\0&0&0&0&8&0&0&0\\0&0&0&0&0&8&0&0\\0&0&0&0&0&0&8&0\\0&0&0&0&0&0&0&8\end{bmatrix}=8I_8 \quad (30)$$

이로써 위에서 보인 결과가 일반적인 Hadamard행렬의 성질인 직교성(orthogonal), 임의의 두 행의 내적과 두 열의 내적이 0임을 만족하고, Hadarmard행렬의 또 다른 성질인 $AA^T=A^TA=nI$ 의 만족함을 보였다.

V. 고속 Hadamard Transform

Pseudo Hadamard 행렬은 한개의 $[bit]_N$행렬과 그의 transpose행렬인 $[bit]_N^T$ 로 만들 수 있다. 즉,

$$[bit]_N[bit]_N^T\simeq\overline{H}_N \quad (31)$$

예를 들어 2bit인 경우, $[bit]_N$ 을 B라고 하고 $[bit]_N^T$ 을 B'라고 하면

$$\overline{H}=B\bullet B'$$

$$B\bullet B'=\begin{bmatrix}0&0\\0&1\\1&0\\1&1\end{bmatrix}\begin{bmatrix}0&0&1&1\\0&1&0&1\end{bmatrix}=\begin{bmatrix}0&0&0&0\\0&1&0&1\\0&0&1&1\\0&1&1&0\end{bmatrix}$$

$$\therefore H_4=\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{bmatrix} \quad (32)$$

(32)와 같이 4 x 4의 Hadamard 행렬을 만들 수 있다. 위의 수식에서 $\hat{L}$와 $\hat{S}$는 permutation을 통해 B와 B'으로 나타낼 수 있다. 이들은 permutation을 적용하여 순차적인 차이만 있을 뿐이다. $\hat{L}$은 B의 row2와 row3을 바꾸어 줌으로써 구할 수 있고, $\hat{S}$는 B'의 column3과 column4를 바꿔줌으로써 구할 수 있다. 이에 적용된 permutation 행렬은 다음의 P_L , P_S 와 같다.

$$P_L=\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$$

$$P_S=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \quad (33)$$

위의 permutation을 통해 다음의 (34), (35) 두개의 식이 성립함을 알 수 있다.

$$\hat{L}=P_LB$$

$$\begin{bmatrix}0&0\\1&0\\0&1\\1&1\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}0&0\\0&1\\1&0\\1&1\end{bmatrix} \quad (34)$$

$$\hat{S}=B'P_S$$

$$\begin{bmatrix}0&0&1&1\\0&1&1&0\end{bmatrix}=\begin{bmatrix}0&0&1&1\\0&1&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \quad (35)$$

8 x 8의 Hadamard 행렬인 (36)도 다음 식 (37)을 만족한다.

$$\begin{array}{c}\\index\\\\000\\001\\010\\011\\100\\101\\110\\111\end{array}\begin{array}{c}\begin{matrix}0&0&0&0&1&1&1&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\end{matrix}\\\begin{bmatrix}0&0&0&0&0&0&0&0\\0&1&0&1&0&1&0&1\\0&0&1&1&0&0&1&1\\0&1&1&0&0&1&1&0\\0&0&0&0&1&1&1&1\\0&1&0&1&1&0&1&0\\0&0&1&1&1&1&0&0\\0&1&1&0&1&0&0&1\end{bmatrix}\end{array} \quad (36)$$

$$\hat{M}=\hat{L}\hat{S}=P_LBB'P_S=P_LHP_S \quad (37)$$

이러한 방식을 이용하여 고속 변환 알고리즘이 실현될 수 있다. 다음의 (39)은 8 x 8 Hadamard행렬로 $\log_2 8=3$이므로 3단의 Sparse Matrix를 갖는다. (39)을 이용하여 Butterfly Diagram을 그리기 위해 Sparse Matrix로 1단, 2단, 3단을 표현하였다.

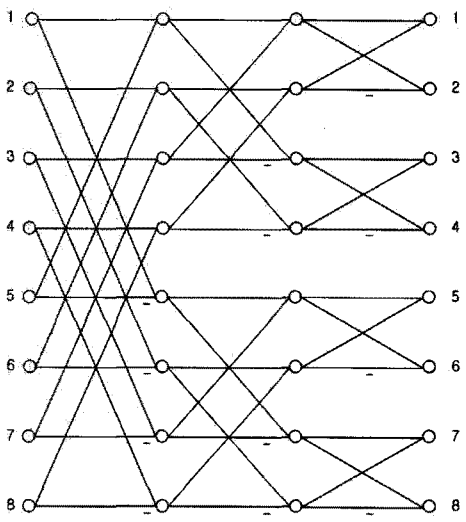


그림 6. 8 x 8 Hadamard 행렬의 버터플라이도
Fig. 6. Butterfly diagram for 8 by 8 Hadamard matrix.

$$[H]_8 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix} \tag{39}$$

$$= \begin{bmatrix} + & 0 & 0 & 0 & + & 0 & 0 & 0 \\ 0 & + & 0 & 0 & 0 & + & 0 & 0 \\ 0 & 0 & + & 0 & 0 & 0 & + & 0 \\ 0 & 0 & 0 & + & 0 & 0 & 0 & + \\ + & 0 & 0 & 0 & - & 0 & 0 & 0 \\ 0 & + & 0 & 0 & 0 & - & 0 & 0 \\ 0 & 0 & + & 0 & 0 & 0 & - & 0 \\ 0 & 0 & 0 & + & 0 & 0 & 0 & - \end{bmatrix} \begin{bmatrix} + & 0 & + & 0 & 0 & 0 & 0 & 0 \\ 0 & + & 0 & + & 0 & 0 & 0 & 0 \\ + & 0 & - & 0 & 0 & 0 & 0 & 0 \\ 0 & + & 0 & - & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & + & 0 & + & 0 \\ 0 & 0 & 0 & 0 & 0 & + & 0 & + \\ 0 & 0 & 0 & 0 & + & 0 & - & 0 \\ 0 & 0 & 0 & 0 & 0 & + & 0 & - \end{bmatrix} \begin{bmatrix} + & + & 0 & 0 & 0 & 0 & 0 & 0 \\ + & - & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & + & + & 0 & 0 & 0 & 0 \\ 0 & 0 & + & - & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & + & + & 0 & 0 \\ 0 & 0 & 0 & 0 & + & - & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & + & + \\ 0 & 0 & 0 & 0 & 0 & 0 & + & - \end{bmatrix}$$

위의 (39)를 이용하여 그림 6과 같이 3단의 Sparse 행렬단을 Butterfly 형태로 나타내었다. 이때 덧셈기 수는 $N\log_2 N$으로 8 x 8 일 경우 $8\log_2 8 = 24$이다.

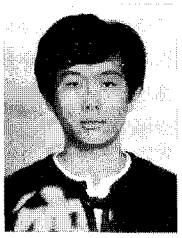
VI. 결 론

본 논문에서는 생성 다항식으로 원시 다항식을 이용하여 이진 선형 천이 레지스터 부호 생성기를 구성하는 경우 한 생성기를 통해 생성된 M-sequence를 구한후 이에 1행과 1열을 추가함으로써 8 x 8의 Hadamard 행렬의 주요한 특성인 직교성(각 행열의 내적이 0인 성질)과 $AA^T = A^TA = nI$ 의 만족함을 볼 수 있었고, L matrix와 S matrix를 통해 이의 고속변환이 가능함을 확인하였다. 또한 두 생성기를 통해 생성된 Gold Sequence를 permutation함으로써 위에서 언급한 Hadamard 행렬의 주요한 특성이 만족함을 확인할 수 있었다. 이를 통하여 통신 공학 분야에서 널리 쓰이는 Sequence들을 기존의 응용 분야뿐만 아니라 Hadamard 행렬의 특성을 가짐으로 더 많은 응용 분야에 이용할 수 있는 계기를 마련할 수 있었다.

참 고 문 헌

[1] P. Fan and M. Darnell, Sequence Design for Communications Applications, Research Studies Press LTD, 1996.
[2] Cohn. M, and Lempel. A, "On Fast M-Sequence Transforms," IEEE Trans. Information Theory, vol. IT-23, pp. 135-137, January, 1977.
[3] Solomon W. Golomb, Shift Register Sequences, Holden-Day, Inc., San Francisco, 1967.
[4] Solomon W. Golomb, Shift Register Sequences, Revised Edition, Aegean Park Press, May, 1982.
[5] M. H. Lee and M. Kaveh, "Fast Hadamard Transform Based on a Simple Matrix Factorization," IEEE Transactions on Acoustic. Speech. and Signal Processing, vol. Assp-34, no. 6, Dec. 1986.
[6] M. H. Lee and Y. Yasuda, "Simple systolic array for hadamard transform," Electron. Lett., vol. 26, no. 18, pp. 1478-1480, Aug. 30. 1990.
[7] http://en.wikipedia.org/wiki/Pseudorandom_binary_sequence.
[8] http://en.wikipedia.org/wiki/Hadamard_matrix.
[9] http://en.wikipedia.org/wiki/Jacket_matrix.
[10] http://en.wikipedia.org/wiki/Pseudo-noise_code.

저 자 소 개



이 미 성(학생회원)
2009년 전북대학교 전자공학 학사
2009년 전북대학교 전자정보 공학부 석사 과정
<주관심분야 : 무선이동통신>

이 문 호(정회원)
1967년 전북대학교 전자공학과 학사
1984년 전남대학교 전기공학과 박사
1990년 동경대학교 정보통신공학과 박사
1980년 10월~현재 전북대학교 전기전자컴퓨터 공학부 교수
<주관심분야 : 무선이동통신>

박 주 용(정회원)
1982년 전북대학교 전자공학과 학사
1994년 전북대학교 전자공학과 박사
1991년 3월~2006년 2월 서남대학교 전자공학과부 교수
2007년 3월~현재 신경대학교 인터넷정보통신 학과 부교수
<주관심분야 : 무선이동통신>