논문 14-39A-04-01 The Journal of Korea Information and Communications Society '14-04 Vol.39A No.04
http://dx.doi.org/10.7840/kics.2014.39A.4.165

$(n,n-1)$ 길쌈부호에 대한 $(2,1)$ 마더부호의 존재

장 환 석•, 정 하 봉°, 성 진 우*

On the Existence of the $(2,1)$ Mother Code of $(n,n-1)$ Convolutional Code

Hwan-seok Jang•, Ha-bong Chung°, Jin-woo Seong*

요 약

모든 채널부호는 다양한 방법에 따라 부호율의 조절이 가능하다. 부호율을 높이는 방법들 중 하나가 천공이며, 이 때, 천공에 사용되는 채널부호를 마더부호라 부른다. 임의의 (n,k) 길쌈부호는 항상 어떤 마더부호를 천공함으로써 만들 수 있을 것이고, 이때 천공패턴에 따른 마더부호를 구하는 과정은 최적의 복호화기를 설계하는데 필요하다. 본 논문에서는 주어진 천공패턴에서 $(2,1)$ 길쌈부호가 $(n,n-1)$ 길쌈부호의 마더부호이기 위한 조건과 마더부호로 가능한 길쌈부호들 사이의 동등 관계에 대하여 살펴본다.

Key Words : Punctured Convolutional Code, Mother Code, Blocked Polynomial Generator Matrix

ABSTRACT

The rate of the channel code can be controlled by various methods. Puncturing is one of the methods of increasing the code rate, and the original code before puncturing is called the mother code. Any (n,k) convolutional code is obtainable by puncturing some mother codes, and the process of finding the mother code is necessary for designing the optimum channel decoder. In this paper, we proved that any $(n,n-1)$ convolutional code has $(2,1)$ mother codes regardless of the puncturing pattern and showed that they must be equivalent.

Ⅰ. 서 론

채널부호는 채널을 통과하면서 발생하는 심벌의 오류를 정정하기 위해 사용되며, 전송하고자 하는 메시지 시퀀스에 패러티 시퀀스를 추가함으로써 만들어진다. 패러티 시퀀스를 이용하여 심벌의 오류를 정정하며, 패러티 시퀀스의 길이가 길어짐에 따라 정정할 수 있는 오류의 개수(오류정정능력)가 증가하게 된다. 메시지 시퀀스와 패러티 시퀀스를 합하여 부호어 시퀀스라 하며, (n,k) 채 널부호는 부호어 시퀀스의 길이가 n, 메시지 시퀀스의 길이가 k인 채널부호를 말한다.

길쌈부호는 블록부호와는 다르게 부호화 과정에서 시프트 레지스터를 이용한다. 이 때, (n,k) 길쌈부호란 동시에 입력되는 비트의 개수가 k개, 동시에 출력되는 비트의 개수가 n개인 길쌈 부호를 말한다. 따라

※ 이 논문은 2011년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임. (No.2011C10272702)
• First Author : Department of Electronics, Information and Communication Engineering, Hongik University, hsjang@hongik.ac.kr, 정회원
° Corresponding Author : Department of Electronics, Information and Communication Engineering, Hongik University, habchung@hongik.ac.kr, 종신회원
* 홍익대학교 전자정보통신공학과 통신연구실, adsads12@naver.com
논문번호 : KICS2014-01-004, Received January 8, 2014; Revised March 7, 2014; Accepted March 26, 2014

서 (n,k) 길쌈부호의 부호율은 k/n이다.

모든 채널부호는 다양한 방법에 의해 부호율을 조절하는 것이 가능하며, 이러한 방법들 중, 부호어의 패러티 비트 일부를 제거하여 부호율을 높이는 방법을 천공이라 한다. 천공되기 이전의 채널부호를 마더부호라 한다. 천공은 정해진 천공 패턴에 따른 해당 비트의 제거로 이루어지며, 마더부호로는 주로 $k=1$인 길쌈부호를 사용한다.

하나의 마더부호로부터 동일한 부호율의 천공된 길쌈부호를 만드는 방법(천공패턴)에는 여러 가지가 있으며, 각각의 천공패턴에 따라 부호의 성능은 서로 달라진다[1].이러한 이유로 효율적인 천공을 위한 천공패턴에 관한 연구는 과거부터 많이 진행되어 왔다[2-4]. 그러나 천공된 길쌈부호와 마더부호 간의 관계를 분석하는 연구는 거의 진행되지 않았으며, 최근 M. Cluzeau가 이에 대하여 연구하였다[5]. [5]에서는 부호율 $1/n$인 마더부호를 천공한 길쌈부호의 생성다항식 행렬을 마더부호의 생성다항식 행렬로부터 구하였다. 본 논문에서는 [5]와는 반대로, 임의의 주어진 길쌈부호가 어떤 마더부호의 어떤 천공으로 만들어질 수 있는가를 연구한다.

가능한 모든 k 값에 대해 주어진 길쌈부호와 마더부호와의 관계를 분석하는 것은 상당히 복잡한 작업이기 때문에, 본 논문에서는 k 값을 $n-1$로, 마더부호를 $(2,1)$ 길쌈부호로 가정하였으며, 이러한 가정 하에, 기존의 연구를 좀 더 수학적으로 정립하였고, $(n,n-1)$ 길쌈부호의 마더부호를 구하는 방법을 제시한다.

본 논문의 구조는 다음과 같다. 2장에서는 길쌈부호와 천공된 길쌈부호에 대하여 살펴보고, 3장에서는 $(n,n-1)$ 길쌈부호가 $(2,1)$ 길쌈부호를 마더부호로 가지기 위한 조건과 마더부호로 가능한 길쌈부호들 사이의 동등 관계에 대하여 살펴본다. 마지막으로 4장에서 결론 및 향후 연구 과제에 대하여 논한다.

Ⅱ. 본 론

2.1 길쌈부호와 길쌈부호의 상보부호

선형블록부호가 생성행렬을 이용하여 부호어 집합이 결정되듯이, 길쌈부호는 생성다항식행렬로 부호어 집합이 결정된다. (n,k) 길쌈부호의 경우 생성다항식 행렬 $G(D)$는 $k\times n$ 행렬로 아래와 같이 표현된다.

$$G(D)=\begin{bmatrix} g_{1,1}(D) & g_{1,2}(D) & \cdots & g_{1,n}(D) \\ g_{2,1}(D) & g_{2,2}(D) & \cdots & g_{2,n}(D) \\ \vdots & \vdots & \ddots & \vdots \\ g_{k,1}(D) & g_{k,2}(D) & \cdots & g_{k,n}(D) \end{bmatrix}$$

여기서 $g_{i,j}(D)\in F_2[D]$, $\forall\ i,j$ 이다.

동일한 부호어 집합을 갖는 두 개의 (n,k) 길쌈부호를 서로 동등(equivalent)하다고 하며, 각각 $G_1(D)$와 $G_2(D)$를 생성다항식 행렬로 갖는 두 개의 (n,k) 길쌈부호가 동등하기 위해서는 다음의 조건이 만족되어야 한다.

$$G_1(D)=T(D)\,G_2(D) \tag{1}$$

여기서 $T(D)$를 변환행렬이라 부르며 $T(D)$는 비특이(nonsingular) $k\times k$ 다항식행렬이다.

선형 채널부호의 상보부호 (dual code)는 주어진 채널부호의 모든 부호어 시퀀스와 내적하여 0이 되는 시퀀스들을 부호어로 갖는 부호이다. 생성다항식 행렬이 $G(D)$인 (n,k) 길쌈부호의 상보부호의 생성다항식 행렬 $H(D)$는 $(n-k)\times n$ 다항식 행렬로 아래와 같이 나타낼 수 있고

$$H(D)=\begin{bmatrix} h_{1,1}(D) & h_{1,2}(D) & \cdots & h_{1,n}(D) \\ h_{2,1}(D) & h_{2,2}(D) & \cdots & h_{2,n}(D) \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1}(D) & h_{n-k,2}(D) & \cdots & h_{n-k,n}(D) \end{bmatrix}$$

$G(D)$와 $H(D)$ 사이에는 다음 식이 성립한다.

$$G(D)\,H(D)^T=[0]$$

즉, $G(D)$의 임의의 행과 $H(D)$의 임의의 행을 내적하면, 그 결과는 항상 0이 된다.

2.2 천공된 길쌈부호

$(2,1)$ 마더부호의 천공으로 얻은 (n,k) 천공된 길쌈부호의 생성다항식 행렬 $G_P(D)$는 마더부호의 생성다항식행렬 $G_M(D)$를 k배 확장한 $(2k,k)$ 블록화 길쌈부호의 $k\times(2k)$ 생성다항식행렬 $G_B(D)$로부터 얻을 수 있다[5]. 본 절에서는 이후 논의의 편이를 위해 [5]의 내용을 간단히 살펴보겠다. 지금부터 $G_B(D)$를 $G_M(D)$의 블록화 생성다항식행렬이라 부르도록 하자.

주어진 다항식 $g(D)=\sum_i a_i D^i$ 에서 차수가

$l \bmod k$인 항 만을 모은 다항식을 $D^l g_l(D^k)$, $0 \le l \le k-1$, 이라 하자. 그러면 다항식 $g(D)$는 식 (2)와 같이 표현할 수 있고

$$g(D) = \sum_{l=0}^{k-1} D^l g_l(D^k) \ , \tag{2}$$

이 때, $\underline{g}(D) = \left(g_{k-1}(D), g_{k-2}(D), \cdots, g_0(D)\right)^T$ 를 $g(D)$의 벡터표현이라 하고 $\vec{v}(g(D)) = \underline{g}(D)$ 로 표기하자. 예를 들어 $g(D) = 1 + D^2 + D^3 + D^4 + D^7$ 이라고 하고 $k=3$이라고 하면, $g_0(D^3) = 1 + D^3$, $Dg_1(D^3) = D(D^3 + D^6)$, $D^2 g_2(D^3) = D^2$이 되어 $g_2(D) = 1$, $g_1(D) = D + D^2$, $g_0(D) = 1 + D$ 이 된다. 따라서 $\vec{v}(g(D)) = \underline{g}(D) = \begin{pmatrix} 1 \\ D+D^2 \\ 1+D \end{pmatrix}$ 이 된다. 또한 다항식 $Dg(D)$의 벡터표현은

$$\vec{v}\left(Dg(D)\right) = \left(g_{k-2}(D), \cdots, g_0(D), Dg_{k-1}(D)\right)^T$$

가 되므로 다음 식으로 정의된 $k \times k$ 행렬 Z에 의해 $Z\underline{g}(D)$가 됨도 알 수 있다.

$$Z = \begin{bmatrix} 0 & \\ \vdots & I_{k-1} \\ 0 & \\ D\,0 & \cdots \ 0 \end{bmatrix} \tag{3}$$

위에서 I_{k-1}은 $(k-1) \times (k-1)$ 항등행렬을 의미하며, $Z^k = DI_k$ 이다. 이를 일반화하면 다음의 보조정리를 얻을 수 있다.

보조정리 1: 다항식 $a(D) \in F_2[D]$일 때,

$$\vec{v}\left(a(D)\, g(D)\right) = a(Z)\, \vec{v}(g(D)) \ . \tag{4}$$

보조정리 1의 증명은 자명하므로 생략한다. 그리고 식 (4)는 $a(D) \in F_2(D)$ 일 때도 성립함을 알 수 있다.

이제 $G_M(D)$가 다음과 같이 주어졌다고 하자.

$$G_M(D) = \left[g^{(1)}(D) \quad g^{(2)}(D)\right]$$

[1]에 따르면 $G_B(D)$는 행렬 Z와 생성다항식 $g^{(1)}(D)$와 $g^{(2)}(D)$의 벡터표현인 $\underline{g}^{(1)}(D)$와 $\underline{g}^{(2)}(D)$ 로부터 식 (5)와 같이 표현된다.

$$G_B(D) = \left[Z^{k-1}B(D) \ \cdots \ ZB(D) \ \ B(D)\right] \tag{5}$$

여기서 $B(D) = \left[\underline{g}^{(1)}(D) \quad \underline{g}^{(2)}(D)\right]$ 이다.

천공된 길쌈부호의 생성다항식 행렬 $G_P(D)$는 천공 패턴에 따라 $G_B(D)$의 열을 제거함으로써 얻어진다. 천공패턴 P는 0과 1로 이루어진 이진 $2 \times k$ 행렬로, P의 i번째 행, j번째 열에 해당하는 $p_{i,j}$가 0이면, $G_B(D)$의 $(2(j-1)+i)$번째 열을 제거하게 된다. $(2,1)$ 길쌈부호를 천공하여 $(n,n-1)$ 길쌈부호를 생성하기 위해서는 $k = n-1$ 이고, 천공패턴 내의 0의 개수는 $n-2$개이어야 한다.

예를 들어 $k=3$인 경우라면, 3×6 블록화 생성다항식행렬 $G_B(D)$는

$$G_B(D) = \begin{bmatrix} g_0^{(1)} & g_0^{(2)} & g_1^{(1)} & g_1^{(2)} & g_2^{(1)} & g_2^{(2)} \\ Dg_2^{(1)} & Dg_2^{(2)} & g_0^{(1)} & g_0^{(2)} & g_1^{(1)} & g_1^{(2)} \\ Dg_1^{(1)} & Dg_1^{(2)} & Dg_2^{(1)} & Dg_2^{(2)} & g_0^{(1)} & g_0^{(2)} \end{bmatrix}$$

이고 만일 천공패턴이 $P = \begin{bmatrix} 1\,0\,1 \\ 0\,1\,1 \end{bmatrix}$이라면 $G_P(D)$는 다음과 같다.

$$G_P(D) = \begin{bmatrix} g_0^{(1)} & g_1^{(2)} & g_2^{(1)} & g_2^{(2)} \\ Dg_2^{(1)} & g_0^{(2)} & g_1^{(1)} & g_1^{(2)} \\ Dg_1^{(1)} & Dg_2^{(2)} & g_0^{(1)} & g_0^{(2)} \end{bmatrix}$$

2.3 $(n,n-1)$ 길쌈부호의 $(2,1)$ 마더부호의 생성다항식행렬

본 장에서는 $(n,\, n-1)$길쌈부호의 생성행렬 $G_0(D)$가 주어졌을 때, 천공을 통해 $G_0(D)$와 동등한 $G_P(D)$를 만들어 낼 수 있는 $(2,1)$ 마더부호가 존재하기 위한 조건 및 그 도출 방법에 대하여 논의하겠다.

$G_0(D)$의 상보부호의 생성다항식행렬을 $H_0(D)$라 하고, 천공패턴 P은 정해졌다고 가정하자. $H_0(D)$는 $1 \times n$ 행렬이므로, 아래와 같이 나타낼 수 있다.

$$H_0(D) = \left[h_1(D)\; h_2(D) \cdots h_n(D)\right]$$

$G_P(D)$가 다음과 같다면,

$$G_P(D) = [\boldsymbol{c}_1(D)\, \boldsymbol{c}_2(D) \cdots \boldsymbol{c}_n(D)],$$

$G_P(D)$ 역시 $H_0(D)$와 상보관계이므로,

$$\sum_{i=1}^{n} h_i(D)\boldsymbol{c}_i(D) = \underline{0} \qquad (6)$$

이 성립한다. 앞 장에서 본 바와 같이 $G_P(D)$의 열들은 $Z^l g^{(j)}(D)$, $j=1,2$, 형태로 표현되므로, 식 (6)은 다음과 같이 바꾸어 쓸 수 있다.

$$S_1(Z)g^{(1)}(D) + S_2(Z)g^{(2)}(D) = \underline{0} \qquad (7)$$

여기서 $S_j(Z), j=1,2,$는 식 (6)에서 $\underline{c_i}(D)$를 해당하는 $Z^l g^{(j)}(D)$로 치환한 뒤 식 (7)처럼 정리했을 때 $g^{(j)}(D)$의 계수에 해당하며, $F_2[D]$ 상에서 계수를 갖는 행렬 Z의 다항식으로 볼 수 있다. 따라서 만약, 식 (7)을 만족하는 $g^{(j)}(D)$들이 존재한다면, 주어진 P에 대하여 $G_0(D)$의 마더부호가 존재한다고 할 수 있다.

보조정리 2: Z는 식 (3)으로 정의된 $k \times k$ 행렬이고 $F_2(D)$는 다항식 환 $F_2[D]$의 분수체 (quotient field)이다. 다항식 $p(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$을 계수가 $F_2(D)$ 상에 있는 $(k-1)$차 이하의 임의의 다항식이라고 하면 $p(Z)$는 항상 역행렬을 가진다.

증명 : 부록 참조.

식 (7)의 $S_j(Z), j=1,2,$는 $F_2[D]$ 상에서 계수를 갖는 행렬 Z의 다항식이므로 보조정리 2에서 본 $p(Z)$에 해당한다. 따라서 보조정리 2의 결과로부터 식 (7)은 다음과 같이 쓸 수 있고

$$\begin{aligned} g^{(1)}(D) &= S_1^{-1}(Z)S_2(Z)g^{(2)}(D) \\ &= S(Z)\, g^{(2)}(D), \end{aligned} \qquad (8)$$

임의로 정한 $g^{(2)}(D)$와 식 (8)에 의해 $g^{(1)}(D)$가 결정되면 식 (2)에 의해 마더부호의 생성다항식 행렬 $G_M(D)$을 구할 수 있다. 이는 다음과 같이 정리된다.

정리 1: $(n, n-1)$ 길쌈부호는 가능한 어떤 천공패턴에 대해서도 항상 $(2,1)$ 길쌈부호를 천공한 부호와 동등할 수 있다.

식 (8)의 $g^{(2)}(D)$에는 0이 아닌 임의의 값을 대입하여도 되기 때문에, 무수히 많은 $G_M(D)$가 존재한다. 이제 그러한 $G_M(D)$들이 서로 동등해야 하는 가에 대해 알아보겠다.

우선 식 (8)에 정의된 $S(Z)\left(= S_1^{-1}(Z)\,S_2(Z)\right)$의 구조를 알아보기 위해 다음의 보조정리가 필요하다.

보조정리 3: $S_j(Z)$의 역행렬 $S_j^{-1}(Z)$ 역시 $F_2(D)$ 상에서 계수를 갖는 $(k-1)$차 이하의 Z의 다항식으로 표현할 수 있다.

증명: $S_j(Z)$와 $S_j^{-1}(Z)$를 다음과 같이 가정하자.

$$\begin{aligned} S_j(Z) &= \sum_{i=0}^{k-1} a_i(D)\, Z^i \\ S_j^{-1}(Z) &= \sum_{i=0}^{k-1} b_i(D)\, Z^i \end{aligned} \qquad (9)$$

$Z^k = DI_k$이므로 $S_j(Z)\,S_j^{-1}(Z)$ 역시 $(k-1)$차 이하의 Z의 다항식으로 표현할 수 있고, 따라서

$$S_j(Z)\,S_j^{-1}(Z) = \sum_{l=0}^{k-1} c_l(D)\, Z^l = I_k \qquad (10)$$

가 성립한다. 위에서 계수 $c_l(D)$는

$$c_l(D) = \sum_{i=0}^{l} a_{l-i}(D)b_i(D) + D\sum_{i=l+1}^{k-1} a_{k+l-i}(D)b_i(D)$$

이다. 보조정리 2에 의해 식 (10)이 성립하기 위한 필요충분조건은 $c_l(D) = 0$ for $1 \le l \le k-1$, $c_0(D) = 1$ 이다. 이를 행렬을 이용하여 표현하면, 식 (11)과 같이 표현할 수 있다.

식 (11)의 $k \times k$ 행렬의 전치행렬은 보조정리 2의 $S_j(Z)$와 같은 구조를 가지므로 항상 역행렬을 가진다. 따라서 식 (9)를 만족하는 다항식 계수들인

$$\begin{bmatrix} a_0 & Da_{k-1} & Da_{k-2} & \cdots & Da_1 \\ a_1 & a_0 & Da_{k-1} & \cdots & Da_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k-2} & a_{k-3} & a_{k-4} & \cdots & Da_{k-1} \\ a_{k-1} & a_{k-2} & a_{k-3} & \cdots & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{k-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad (11)$$

$b_i(D)$ 들이 존재하게 되므로 식 (9)의 표현이 정당하다.

보조정리 3으로부터 $S(Z)$ 역시 $(k-1)$차 이하의 Z의 다항식으로 표현됨을 알 수 있다. 이는 다음의 두 따름정리로 요약된다.

따름정리 1: $S(Z)$는 $F_2(D)$ 상에서 계수를 갖는 $(k-1)$차 이하의 Z의 다항식으로 표현할 수 있다.

따름정리 2:
$S(Z) = S_1^{-1}(Z)S_2(Z) = S_2(Z)S_1^{-1}(Z)$

이제 주어진 $(n,n-1)$ 길쌈부호로부터 천공패턴 P에 대해 구한 서로 다른 마더부호들이 서로 동등해야 하는 가에 대해 알아보자.

정리 2: 정해진 천공패턴 P에 따른 $G_0(D)$의 모든 가능한 마더부호는 서로 동등하다.

증명 : $(n,n-1)$ 길쌈부호 $G_0(D)$로부터 구한 서로 다른 두 마더부호를 $G_M(D) = [g^{(1)}(D)\ \ g^{(2)}(D)]$, $G_M'(D) = [f^{(1)}(D)\ \ f^{(2)}(D)]$라 하자. 두 마더부호가 동등하다는 것은

$$G_M'(D) = T(D)\, G_M(D) \qquad (12)$$

을 만족하는 다항식 $T(D)$가 존재한다는 의미이다. 다시 말해,

$$f^{(2)}(D) = T(D)\, g^{(2)}(D) \qquad (13)$$

일 때

$$f^{(1)}(D) = T(D)\, g^{(1)}(D) \qquad (14)$$

도 성립함을 보이면 된다.

식 (13)은 보조정리 1에 의해

$$\underline{f}^{(2)}(D) = T(Z)\, \underline{g}^{(2)}(D)$$

이므로

$$\begin{aligned} \underline{f}^{(1)}(D) &= S(Z)\, \underline{f}^{(2)}(D) \\ &= S(Z)\, T(Z)\, \underline{g}^{(2)}(D) \\ &= T(Z) S(Z)\, \underline{g}^{(2)}(D) = T(Z)\, \underline{g}^{(1)}(D) \end{aligned} \qquad (15)$$

가 되어 식 (14)가 성립한다. 따라서 두 마더부호는 동등하다.

정리 2에 의해, 정해진 천공패턴에 대해서 오직 하나의 마더부호만 구하여도 무방하다는 것을 알 수 있다.

이해를 돕기 위하여, (4,3) 길쌈부호가 주어졌을 때, 주어진 천공 패턴에 해당하는 (2,1) 마더부호를 찾는 예제를 아래에 나타내었다.

예제) $G_0(D) = \begin{bmatrix} D+1 & D & 1 & 1 \\ 1 & 1 & D+1 & D \\ 0 & D+1 & 0 & D+1 \end{bmatrix}$이고, 천공패턴은 $P = \begin{bmatrix} 1\,0\,1 \\ 0\,1\,1 \end{bmatrix}$이다.

먼저, P에 해당하는 $G_P(D)$의 구조는 다음과 같다.

$$G_P(D) = \left[Z^2 \underline{g}^{(1)}(D)\ \ Z\underline{g}^{(2)}(D)\ \ \underline{g}^{(1)}(D)\ \ \underline{g}^{(2)}(D) \right]$$

그리고, $G_0(D)$의 상보부호 생성다항식행렬 $H_0(D)$는 다음과 같다.

$$H_0(D) = \left[D^3 + D\ \ D^3 + D^2\ \ D^3 + D^2\ \ D^3 + D^2 \right]$$

$G_P(D)$와 $H_0(D)$는 상보관계여야 하므로, 다음의 식을 만족하여야 한다.

$$\begin{aligned} &\left((D^3 + D) Z^2 + (D^3 + D^2) I \right) \underline{g}^{(1)}(D) \\ &= \left((D^3 + D^2) Z + (D^3 + D^2) I \right) \underline{g}^{(2)}(D) \end{aligned}$$

여기서 $\underline{g}^{(2)}(D) = \begin{bmatrix} 0 \\ 0 \\ D^{11} + D^8 + D^6 + D^5 \end{bmatrix}$로 두면 $\underline{g}^{(1)}(D)$을 구할 수 있으며, 이로부터 $g_1(D)$와 $g_2(D)$를 구할 수 있다. 마지막으로 $g_1(D)$와 $g_2(D)$의 최대 공약수로 각각을 나누어준 뒤, $G_M(D)$를 구성하면 결

과는 다음과 같다.

$$G_M(D) = \left[D^2+D \;\; D^3+D+1\right]$$

본 예제에서는 역행렬 계산 과정에서 발생하는 분수를 제거하기 위하여 $g^{(2)}(D)$를 위와 같이 결정하였지만, 다른 값을 가정하더라도 $G_M(D)$는 동일한 결과가 나온다.

Ⅲ. 결 론

$(n,n-1)$ 길쌈부호는 어떤 천공패턴에 대해서도 (2,1) 길쌈부호를 마더부호로 가지며, 천공패턴이 결정되면 모든 마더부호는 서로 동등함을 확인하였다.

본 논문에서는 다루지 않았지만 일반적인 (n,k) 길쌈부호는 항상 (2,1) 길쌈부호를 마더부호로 가지지는 않는다. 그러나 본 논문의 접근 방법을 활용한다면, (2,1) 길쌈부호를 마더부호로 가지는 조건을 규명할 수 있을 것으로 예상하며, 향후 범위를 확장하면서 이에 대한 연구를 진행하고자 한다.여기서는 소단원에 관한 내용을 간단히 살펴본다. 여기서는 소단원에 관한 내용을 간단히 살펴본다.

부록 (보조정리 2의 증명)

경우 1 : k가 홀수인 경우.

Z의 특성 방정식 $\phi_Z(\lambda)$은 다음과 같다.

$$\phi_Z(\lambda) = \det\begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & & 0 & 0 \\ 0 & 0 & \lambda & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & \lambda & 1 \\ D & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix} = \lambda^k + D \qquad (16)$$

$k|2^l-1$을 만족하는 가장 작은 l 값을 r이라 하고, $2^r-1=ek$라고 하자. Z의 고유값은 $u, u\alpha^e, u\alpha^{2e}, \cdots, u\alpha^{(k-1)e}$이며, 이 때 $u^k=D$, α는 $GF(2^r)$ 상에서의 원시소(primitive element)이다. Z의 모든 고유값들이 서로 다르므로, Z는 대각행렬로 변환할 수 있으며, $Z=S\Lambda S^{-1}$로 나타낼 수 있다.

$$\Lambda = \begin{bmatrix} u & 0 & 0 & \cdots & 0 \\ 0 & u\alpha^e & 0 & & 0 \\ 0 & 0 & u\alpha^{2e} & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & u\alpha^{(k-1)e} \end{bmatrix}$$

$$p(Z) = a_0 I_w + a_1 Z + \cdots + a_{k-1} Z^{k-1}$$
$$= S\left(a_0 I_k + a_1 \Lambda + \cdots + a_{k-1}\Lambda^{k-1}\right) S^{-1}$$

따라서 $\det(p(Z))$는 아래와 같다.

$$\det p(Z) = \det\left(a_o I + a_1\Lambda + \cdots + a_{k-1}\Lambda^{k-1}\right)$$
$$= \det\begin{bmatrix} p(u) & 0 & \cdots & 0 \\ 0 & p(u\alpha^e) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & p\left(u\alpha^{(k-1)e}\right) \end{bmatrix}$$

$u, u\alpha^e, u\alpha^{2e}, \cdots, u\alpha^{(k-1)e}$ 중 어떠한 값도 $p(x)$의 근이 될 수 없으므로, $\det(p(Z)) \neq 0$이다.

경우 2 : $k=2^m$인 경우.

$\phi_Z(\lambda) = \lambda^{2^m} + D = (\lambda+u)^{2^m}$이 되며, 이 때, $u^k = D$이다. 이 경우, Z의 고유값은 중복도가 k인 u이다. 고유벡터 $\underline{x}$는 $\left[1\; u\; u^2 \cdots u^{k-1}\right]^T$이며, 모든 고유벡터들은 서로 종속(dependent)이다. 즉, 고유벡터 공간의 차원은 1이 된다. 따라서 Z의 Jordan canonical form은

$$U = \begin{bmatrix} u & 1 & 0 & \cdots & 0 \\ 0 & u & 1 & & 0 \\ 0 & 0 & u & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & u \end{bmatrix}$$

이며, $Z=SUS^{-1}$이 된다.

유사하게 $p(Z) = Sp(U)S^{-1}$이고, $\det(p(Z))$는 $\det(p(U)) = \det(a_0 I + a_1 U + a_2 U^2 + \cdots + a_{k-1}U^{k-1})$이 된다. U는 윗삼각형행렬이므로, U^i 또한 윗삼각형행렬이 되며, 대각 성분 값은 u^i가 된다. 따라서, $p(U)$ 역시 윗삼각형행렬이 되고, 대각 성분은 0이 될 수 없으므로, $\det(p(Z)) \neq 0$이다.

경우 3 : $k=2^r q$, q는 홀수인 경우

$\lambda^k + D = (\lambda^q + v)^{2^r}$이다. 이 때, $u^q = v$, $v^{2^r} = D$라 하자. Z의 고유값은 중복도가 2^r인 $u, u\beta, \cdots, u\beta^{q-1}$이 되며, 이 때, β는 $GF(2^q)$ 상의 원시소이다. 경우 2와 유사하게, U는 다음과 같이 나타내어진다.

$$U = \begin{bmatrix} U_0 & & & 0 \\ & U_1 & & \\ & & \ddots & \\ 0 & & & U_{q-1} \end{bmatrix}$$

여기서 $U_i = \begin{bmatrix} u\beta^i & 1 & 0 & \cdots & 0 & 0 \\ 0 & u\beta^i & 1 & & & \\ 0 & 0 & u\beta^i & & & \vdots \\ \vdots & & & \ddots & & \\ 0 & & & & u\beta^i & 1 \\ 0 & & \cdots & & 0 & u\beta^i \end{bmatrix}$는 윗삼각형 행렬이며, 대각 성분들로 $u^i, (u\beta)^i, \cdots, (u\beta^{q-1})^i$ 을 포함한다. 이 때, $p(U)$에서 U_i에 해당하는 블록의 대각 성분은 모두 $p(u\beta^i)$이 된다. 따라서, 경우 2에서와 같이, $\det(p(Z)) \neq 0$이다.

References

[1] L. Sari, "Effects of puncturing patterns on punctured Convolutioal Codes," *TELKOMNIKA*, vol. 10, no. 4, pp. 752-762, Aug. 2012.

[2] M. A. Kousa and A. H. Mugaibel, "Puncturing effects on turbo codes," in *Proc. IEE Commun.*, vol. 149, no. 3, pp. 132-138, Jun. 2002.

[3] R. M. Deshmukh and S. A. Ladhake, "Analysis of various puncturing patterns and code rates: Turbo code," *Int. J. Electronic Engineering Research*, vol. 1, no. 2, pp. 79-88, 2009.

[4] J. Lee, H. Lee, I.-S. Kang, S. Yun, C. Park, and Y. Song, "Recognition of convolutional code with performance analysis," *J. KICS*, vol. 37, no. 4, pp. 260-268, Apr. 2012.

[5] M. Cluzeau and M. Finiasz, "Reconstruction of punctured convolutional codes," in *Proc. IEEE ITW*, pp. 75-79, Taormina, Oct. 2009.

장 환 석 (Hwan-seok Jang)

2008년 2월 : 홍익대학교 전자전기공학부 졸업

2010년 2월 : 홍익대학교 전자정보통신공학과 석사

2010년 3월~현재 : 홍익대학교 전자통신공학과 박사과정

<관심분야> 부호 이론, 채널 코딩, 소스 코딩

정 하 봉 (Ha-bong Chung)

1981년 2월 : 서울대학교 전자공학과 공학사

1985년 2월 : 미국 University of Southern California, 전기공학과 공학석사

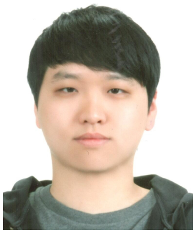
1988년 : 미국 University of Southern California, 전기공학과 공학박사

1988~1991년 : 미국 뉴욕주립대 전기공학과 조교수

1991년~현재 : 홍익대학교 전자전기공학부 교수

<관심분야> 부호 이론, 조합수학, 시퀀스 설계, 협력통신, 시공간 부호

성 진 우 (Jin-woo Seong)



2012년 2월 : 홍익대학교 전자전기공학부 졸업

2014년 2월 : 홍익대학교 전자정보통신공학과 석사

2014년 3월~현재 : 홍익대학교 전자통신공학과 박사과정

<관심분야> 부호 이론, 채널 코딩