DBpia

논문 16-41-04-01 The Journal of Korean Institute of Communications and Information Sciences '16-04 Vol.41 No.04
http://dx.doi.org/10.7840/kics.2016.41.4.379

임의의 생성다항식 행렬을 갖는 길쌈부호도 $(n,1)$ 마더부호의 천공으로 생성 가능한가?

정 하 봉◆, 성 진 우°

Sufficient Conditions for the Existence of an $(n,1)$ Mother Code and Its Puncturing Pattern to Generating a Given Convolutional Code

Habong Chung◆, Jinwoo Seong°

요 약

천공이란 길쌈부호의 부호율을 증가시키는데 쓰이는 가장 보편적인 방법이며, 이때 천공하기 전의 길쌈부호를 마더부호라고 한다. 본 논문에서는 임의의 (N,K) 길쌈부호를 특정 $(n,1)$ 마더부호를 천공함으로써 만들 수 있는지 여부에 대하여 조사하였다. 동일한 부호어 집합을 갖는 두 개의 길쌈부호를 서로 동등(equivalent)하다고 할 때, 주어진 (N,K) 길쌈부호가 $(n,1)$ 마더부호를 천공하여 얻은 천공된 길쌈부호와 동등하기 위한 두 개의 충분조건을 소개한다.

Key Words : Punctured Convolutional Code, Mother Code, Puncturing Pattern, Polynomial Generator Matrix, Reconstruction Algorithm

ABSTRACT

Puncturing is the most common way of increasing the rate of convolutional codes. The puncturing process is done to the original code called the mother code by a specific puncturing pattern. In this article, we investigate into the question whether any convolutional code is obtainable by puncturing some $(n,1)$ mother codes. We present two sufficient conditions for the mother code and the puncturing pattern to satisfy in order that the punctured code is equivalent to the given (N,K) convolutional code.

Ⅰ. 서 론

천공은 길쌈부호에서 부호율을 조정하기 위한 기법 중 가장 보편적인 기법이다. 천공이란 길쌈부호로 부호화된 심벌들을 주어진 패턴에 따라 주기적으로 제거하는 것이다. 길쌈부호의 천공은 다양한 부호율의 채널부호들을 필요로 하는 시스템에서 자주 사용된다. 일반적으로 천공 전의 길쌈부호는 낮은 부호율$(1/n)$을 갖고 있으며, 이 길쌈부호를 마더부호라 한다. 그리고 심벌들을 주기적으로 제거하는 패턴을 천공패턴이라고 하며, 천공의 결과로 얻어지는 부호를 천공된 길쌈부호라 한다.

※ 본 연구는 한국연구재단 이공분야기초연구사업(NRF-2014R1A1A2059324) 지원 및 홍익대학교 산학협력단 관리로 수행되었습니다.
◆ First Author : Hongik University Department of Electronic and Electrical Engineering, habchung@hongik.ac.kr, 정회원
° Corresponding Author : Hongik University Department of Electronics, Information and Communication Engineering, adsads12@naver.com, 학생회원
논문번호 : KICS2016-01-017, Received January 25, 2016; Revised April 8, 2016; Accepted April 11, 2016

www.dbpia.co.kr

마더 부호로부터 천공된 길쌈부호를 만들어 내는 것은 단순한 천공과정을 거치면 되는 간단한 작업이지만, 그 반대로 임의의 주어진 (N,K) 길쌈부호가 어떤 마더부호를 어떤 천공패턴을 통해 만들 수 있는지를 알아내는 일은 그리 간단치만은 않은, 따라서 수학적으로 매우 흥미있는 문제일 것이다. 단순한 수학적 흥미 외에도 이 문제는 천공된 길쌈부호의 재구성 기법이라는 응용 분야를 가지고 있다. 채널부호의 재구성기법이란 통신시스템에서 의도되지 않은 수신자가, 사용된 채널부호에 대한 정보가 전무한 상황에서, 수신 심벌만으로 사용된 채널부호의 생성행렬 G를 알아내는 기법이다. 일반적인 재구성기법의 과정은 채널을 통과한 잡음이 낀 수신 심벌들로부터 부호어 집합이라고 판단된 벡터공간을 복원한 후, 그 벡터공간을 생성하는 G를 찾아내는 것이다.

채널부호의 재구성기법은 많은 연구자에 의해 연구된바 있다[1-8]. Cluzeau와 Finiasz[9]는 천공된 길쌈부호의 재구성기법을 제안하였다. 그들은 기존에 알려진 길쌈부호의 재구성기법을 통해 $K\times N$ 생성다항식행렬(PGM, Polynomial Generator Matrix)을 먼저 구한 후, K배 확장한 블록화 부호의 개념을 사용하여 이미 구한 PGM과 동등한 PGM을 갖는 $(n,1)$ 마더부호와 천공패턴을 찾는 알고리즘을 제안하였다.

이때 굳이 $K\times N$ PGM 대신 마더부호와 천공패턴을 찾으려는 이유는 하나의 비터비 복호기로 다양한 부호율의 부호들을 모두 복호할 수 있다는 장점 외에도 비터비 복호과정의 계산 복잡도를 줄일 수 있다는 장점이 있기 때문이다. 일반적으로 천공전의 마더부호의 부호기를 구성하는 시프트 레지스터의 개수와 천공된 (N,K) 길쌈부호의 $K\times N$ PGM을 구성하는 시프트 레지스터의 개수는 같게 된다. 이 시프트 레지스터의 개수를 m이라고 하면, (N,K) 길쌈부호의 비터비 복호과정의 계산 복잡도는 $O(2^K\times 2^{m+1})$인 반면 천공패턴을 이용한 $(n,1)$ 마더부호의 복호 계산 복잡도는 $O(2\times 2^{m+1})$이다. 따라서 $K>2$ 인 경우에는 천공패턴을 이용한 복호의 복잡도가 줄게 된다.

Cluzeau와 Finiasz의 알고리즘은 높은 성공률로 마더부호를 복원하지만, 알고리즘이 끝나기 전엔 특정 천공패턴에서의 마더부호의 존재 여부를 알 수 없다는 단점이 있고, 예컨대 다음의 일련의 질문들에 대한 답을 주지 못한다: "임의의 주어진 (N,K) 길쌈부호와 동일한 부호어 집합을 갖게 만드는 $(n,1)$ 마더부호와 해당 천공패턴은 항상 존재하는가?" 또는 "주어진 (N,K) 길쌈부호와 동등한 천공된 길쌈부호의 마더부호는 임의의 천공패턴에 대해서도 항상 존재하는가?" 또는 좀 더 구체적으로, "임의의 $(N,N-1)$ 길쌈부호도 항상 $(2,1)$ 마더부호의 천공으로 만들 수 있는가?"[11]

본 논문에서는 PGM의 동등성(equivalence)의 개념에 대한 수학적 접근을 통해 위의 질문들에 대한 답을 내놓고자 한다.

논문의 구성은 다음과 같다. 2.1소절에서는 길쌈부호의 기본 성질과 함께 천공된 길쌈부호의 분석을 위한 K배 확장한 블록화 부호의 개념[9]을 소개하고, 2.2소절에서는 주어진 (N,K) 길쌈부호의 PGM과 동등한 PGM을 갖기 위한 마더부호와 천공패턴의 조건을 분석한다. 3절에서는 결론을 이끌어 낸다.

Ⅱ. 본 론

2.1 천공된 길쌈부호

2.1.1 생성다항식행렬(PGM)

(n,k) 길쌈부호의 부호어 집합은 다음에서 보는 계수(rank) k인 $k\times n$ 행렬 $G(D)$에 의해 결정되며 이 행렬을 생성다항식 행렬이라고 한다.

$$G(D)=\left[g_{i,j}(D)\,|\,0\le i\le k-1, 0\le j\le n-1\right]$$

위 식에서 $g_{i,j}(D)$들은 다항식 환(polynomial ring) $F_2[D]$의 몫 체(quotient field)인 $F_2(D)$의 원소이며, D는 지연연산자(delay operator)이다. 만약 부호기에 피드백 루프가 없다면, $g_{i,j}(D)$는 $F_2[D]$의 원소로 표현이 가능하다. 본 논문의 정리 및 예제에서는 편의를 위해 $g_{i,j}(D)$들을 $F_2[D]$의 원소라고 가정하였으나 일반적으로 $F_2(D)$의 원소로 보아도 본 논문의 결과는 유효하다. 부호화의 과정은 다음과 같이 나타낼 수 있다.

$$c(D)=v(D)G(D), \tag{1}$$

위에서 $v(D)=\left(v_0(D),\cdots,v_{k-1}(D)\right)$ 는 메시지 다항식이며, $c(D)=\left(c_0(D),\cdots,c_{n-1}(D)\right)$ 는 부호어 다항식이다.

$G(D)$의 계수가 k이므로 (1)식으로부터 만들어지는 부호어들은 $(F_2(D))^n$의 k차원 부분 공간(subspace)을 생성한다. 동일한 부호어 집합을 생성하는 서로 다른 두개의 PGM (또는 해당 부호)를 동등(equivalent)하다고 한다. 동등성에 대한 정의는 다음

www.dbpia.co.kr

과 같다.

정의 1: $G_1(D)$와 $G_2(D)$가 각각 두 (n,k) 길쌈부호의 PGM이다. 만일 다음 식을 만족하는, $F_2[D]$ 상에서 정의된 $k\times k$ 다항식행렬 $T(D)$가 존재한다면, $G_1(D)$와 $G_2(D)$는 동등하다고 한다.

$$G_1(D) = T(D)\,G_2(D). \tag{2}$$

$G_1(D)$와 $G_2(D)$는 동등하다면, $G_1(D)$를 PGM으로 하여 생성한 부호어 집합과, $G_2(D)$를 PGM으로 하여 생성한 부호어 집합은 동일하다.

(n,k) 길쌈부호의 상보부호(dual code)는 $(n,n-k)$ 길쌈부호이고, 상보부호의 PGM은 다음 식을 만족하는 $(n-k)\times n$ $H(D)$로 나타낼 수 있다.

$$G(D)\,H(D)^T = [0]\,. \tag{3}$$

2.1.2 생성다항식행렬(PGM)

본 소절에서는 $(n,1)$ 마더부호를 천공하여 만든 (N,K) 천공된 길쌈부호의 PGM $G_P(D)$가 마더부호의 PGM $G_M(D)$로부터 유도되는 과정을 알아보겠다. 본 소절의 내용은 [9]에서 소개된 K배 블록화 부호의 개념을 이용한 것으로 [9]에서 생략된 과정을 유도한다.

우선 천공된 (N,K) 길쌈부호가 $(n,1)$ 마더부호의 천공으로 만들어 졌다고 가정하자. 이 경우, 천공패턴 P는 0과 1로 구성된 $n\times K$ 행렬이고 nK개의 심벌 중 1의 개수가 N인 행렬이 된다. 천공으로 인한 PGM의 변화를 쉽게 이해하기 위해서 천공하기 전의 nK 심벌을 출력하는 (nK,K) 부호인 K배 블록화 부호의 개념을 도입하자.

K배 블록화 부호란 $(n,1)$ 마더부호의 부호화기에 K개의 입력이 병렬로 들어갔을 때 nK개의 심벌이 출력되는 (nK,K) 길쌈부호를 말한다. 그림 1-(a)는 $(2,1)$ 마더부호의 부호화기이고 그림 1-(b)는 동일한 출력을 갖는 K배 블록화 부호($K=3$ 인 경우)를 나타낸 그림이다.

이제 편의를 위해 그림의 경우, 즉 $K=3$ 인 경우에 대해 마더부호의 PGM $G_M(D)$와 K배 블록화 구

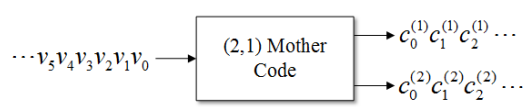

그림 1. (a) $(2,1)$ 마더부호
Fig. 1. (a) $(2,1)$ Mother Code

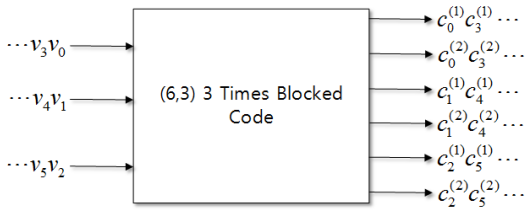

그림 1. (b) $(6,3)$ 3배 블록화 부호
Fig. 1. (b) $(6,3)$ 3 times Blocked Code

조의 PGM $G_B(D)$의 관계를 알아보자. 우선 그림 1-(a),(b)의 입출력을 각각 다음과 같이 정의한다.

$$v(D) = \sum_i v_i D^i$$
$$v^{(l)}(D) = \sum_i v_{3i+l} D^i\,,\ l=0,1,2$$
$$c^{(j)}(D) = \sum_i c_i^{(j)} D^i\,,\ j=1,2$$
$$c_m^{(j)}(D) = \sum_i c_{3i+m}^{(j)} D^i\,,\ j=1,2,\ m=0,1,2$$

그림 1-(b)의 블록구조로 인해

$$v(D) = \sum_{l=0}^{2} D^l v^{(l)}(D^3) \tag{4}$$

이고

$$c^{(j)}(D) = \sum_{m=0}^{2} D^m c_m^{(j)}(D^3) \tag{5}$$

임을 알 수 있다. $G_M(D)=\left[g^{(1)}(D)\quad g^{(2)}(D)\right]$라고 하면 식 (1)에 의해

$$c^{(j)}(D) = v(D)\,g^{(j)}(D)\,,\ j=1,2 \tag{6}$$

이 된다. 또한 그림 1-(b)에 의하면 3배 블록화 부호의 3×6 PGM $G_B(D)$의 홀수 열은 $g^{(1)}(D)$에, 짝수 열은 $g^{(2)}(D)$에 의해 결정되는 것을 알 수 있으므로 $G_B(D)$는 다음과 같다고 가정하자.

$$G_B(D) = \begin{bmatrix} g_{00}^{(1)} & g_{00}^{(2)} & g_{01}^{(1)} & g_{01}^{(2)} & g_{02}^{(1)} & g_{02}^{(2)} \\ g_{10}^{(1)} & g_{10}^{(2)} & g_{11}^{(1)} & g_{11}^{(2)} & g_{12}^{(1)} & g_{12}^{(2)} \\ g_{20}^{(1)} & g_{20}^{(2)} & g_{21}^{(1)} & g_{21}^{(2)} & g_{22}^{(1)} & g_{22}^{(2)} \end{bmatrix}. \tag{7}$$

www.dbpia.co.kr

식 (7)에서 $g_{im}^{(j)}$는 다항식 $g_{im}^{(j)}(D)$를 의미한다. 역시 식 (1)에 의해 $j=1,2,\ m=0,1,2$에 대해

$$c_m^{(j)}(D)=\sum_{l=0}^{2} v^{(l)}(D)\, g_{lm}^{(j)}(D)\ , \tag{8}$$

이다. 식 (8)을 식 (5)에 대입하면

$$c^{(j)}(D)=\sum_{l=0}^{2} v^{(l)}(D^3)\sum_{m=0}^{2} D^m g_{lm}^{(j)}(D^3) \tag{9}$$

가 되어 식 (4)를 식 (6)에 대입하여 얻은

$$c^{(j)}(D)=\sum_{l=0}^{2} v^{(l)}(D^3)\, D^l g^{(j)}(D) \tag{10}$$

과 비교하면 $l=0,1,2$에 대해

$$D^l g^{(j)}(D)=\sum_{m=0}^{2} D^m g_{lm}^{(j)}(D^3) \tag{11}$$

이 됨을 알 수 있다. 식 (11)에 의하면 $D^m g_{lm}^{(j)}(D^3)$은 다항식 $D^l g^{(j)}(D)$의 항들 중 차수를 3로 나눴을 때 나머지가 m인 성분만을 모은 것이다. 식 (11)을 이용하여 식 (7)의 $G_B(D)$의 홀수 번째 (또는 짝수 번째) 열을 계산하면 다음과 같다는 것을 알 수 있다.

$$\begin{bmatrix} g_{00}^{(j)} & g_{01}^{(j)} & g_{02}^{(j)} \\ g_{10}^{(j)} & g_{11}^{(j)} & g_{12}^{(j)} \\ g_{20}^{(j)} & g_{21}^{(j)} & g_{22}^{(j)} \end{bmatrix} = \begin{bmatrix} g_{00}^{(j)} & g_{01}^{(j)} & g_{02}^{(j)} \\ Dg_{02}^{(j)} & g_{00}^{(j)} & g_{01}^{(j)} \\ Dg_{01}^{(j)} & Dg_{02}^{(j)} & g_{00}^{(j)} \end{bmatrix} \tag{12}$$

즉, 다항식 $g_{lm}^{(j)}(D)$들은 모두 $g_{0m}^{(j)}(D)$로 표현 가능하다. 식 (12)에서 우변의 세 번째 열벡터를 $\vec{v}$라고 하면 두 번째 열은 $\begin{bmatrix} 0&1&0\\ 0&0&1\\ D&0&0 \end{bmatrix}\vec{v}$ 이고 첫 번째 열은 $\begin{bmatrix} 0&1&0\\ 0&0&1\\ D&0&0 \end{bmatrix}^2\vec{v}$ 가 됨을 주목하자.

이제 위의 논리를 일반화하자. 다항식 $g(D)$가 주어졌을 때, $D^m g_m(D^K)$, $0\le m\le K-1$를 $g(D)$의 항들 중 차수를 K로 나눴을 때 나머지가 m인 성분만을 모은 것이라고 하고, 이를 아래와 같이 벡터 형태로 표현한 $\overrightarrow{v_K}(g(D))$를 다항식 $g(D)$의 K-adic 벡터 표현이라 부르자.

$$\overrightarrow{v_K}(g(D))=(g_{K-1}(D),g_{K-2}(D),\cdots,g_0(D))^T \tag{13}$$

마더부호의 PGM $G_M(D)$가 다음과 같을 때,

$$G_M(D)=\left[g^{(1)}(D)\quad g^{(2)}(D)\quad\cdots\quad g^{(n)}(D)\right] \tag{14}$$

K배 블록화 부호의 PGM $G_B(D)$는 다음과 같이 나타낼 수 있다.

$$G_B(D)=\left(Z^{K-1}\times M\mid\cdots\mid Z\times M\mid M\right) \tag{15}$$

여기서 M은 j번째 열이 $\overrightarrow{v_K}(g^{(j)}(D))$인 $K\times n$ 행렬이고, Z는 다음과 같은 $K\times K$ 행렬이다.

$$Z=\begin{bmatrix} 0 & & \\ \vdots & & I_{K-1} \\ 0 & & \\ D & 0\ \cdots\ 0 & \end{bmatrix} \tag{16}$$

최종적으로, (N,K) 천공된 길쌈부호의 PGM $G_P(D)$는 천공패턴에 따라 $G_B(D)$의 열을 제거함으로써 구할 수 있다. 다음의 예제를 보자.

예제 1: $(4,3)$ 천공된 길쌈부호가 $(2,1)$ 마더부호를 천공패턴 $P=\begin{bmatrix}1&0&1\\0&1&1\end{bmatrix}$에 따라 천공함으로써 얻어졌다고 가정하자. 마더부호의 PGM $G_M(D)$는 다음과 같다고 가정한다.

$$\begin{aligned} G_M(D)&=\left[g^{(1)}(D)\quad g^{(2)}(D)\right]\\ &=\left[1+D+D^3+D^4+D^5+D^6\quad 1+D^5+D^6\right]. \end{aligned}$$

$g^{(1)}(D)$와 $g^{(2)}(D)$의 3-adic 벡터 표현을 구하면 다음과 같다.

$$\overrightarrow{v_3}(g^{(1)}(D))=\left(g_2^{(1)}\,g_1^{(1)}\,g_0^{(1)}\right)^T=(D\ 1+D\ 1+D+D^2)^T.$$
$$\overrightarrow{v_3}(g^{(2)}(D))=\left(g_2^{(2)}\,g_1^{(2)}\,g_0^{(2)}\right)^T=(D\ 0\ 1+D^2)^T.$$

따라서

www.dbpia.co.kr

$$M=\begin{bmatrix} D & D \\ 1+D & 0 \\ 1+D+D^2 & 1+D^2 \end{bmatrix}$$

이 되고, 3배 블록화 부호의 PGM $G_B(D)$는

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

이고 천공된 $(4,3)$ 부호의 PGM $G_P(D)$는 $G_B(D)$의 두 번째와 세 번째 열을 제거함으로써 구할 수 있다.

$$\begin{aligned} G_P(D) &= \begin{bmatrix} g_0^{(1)} & g_1^{(2)} & g_2^{(1)} & g_2^{(2)} \\ Dg_2^{(1)} & g_0^{(2)} & g_1^{(1)} & g_1^{(2)} \\ Dg_1^{(1)} & Dg_2^{(2)} & g_0^{(1)} & g_0^{(2)} \end{bmatrix} \\ &= \begin{bmatrix} 1+D+D^2 & 0 & D & D \\ D^2 & 1+D^2 & 1+D & 0 \\ D+D^2 & D^2 & 1+D+D^2 & 1+D^2 \end{bmatrix}. \end{aligned}$$

□

예제1의 결과로부터도 마더부호의 시프트 레지스터의 개수나 $G_P(D)$의 부호기의 시프트 레지스터의 개수나 모두 6개임을 관찰할 수 있다.

식 (11)에서도 알 수 있듯이 다항식의 K-adic 벡터 표현은 다음과 같은 성질을 갖는다.

성질 1: 다항식 $g(D)$의 K-adic 벡터 표현 $\overrightarrow{v_K}(g(D))$가 식 (13)과 같을 때, $Dg(D)$의 벡터 표현은 다음과 같다.

$$\begin{aligned} \overrightarrow{v_K}(Dg(D)) &= \big(g_{K-2}(D),\cdots,g_0(D),Dg_{K-1}(D)\big)^T \\ &= Z\overrightarrow{v_K}(g(D)). \end{aligned}$$

여기서 Z는 식 (16)에 정의된 행렬로 $Z^K = DI_K$를 만족한다. 이 성질을 이용하여 다음의 보조정리를 도출할 수 있다.

보조정리 1: 모든 $a(D)\in F_2[D]$에 대하여

$$\overrightarrow{v_K}(a(D)g(D)) = a(Z)\overrightarrow{v_K}(g(D)). \qquad (17)$$

2.2 $(n,1)$ 마더부호가 존재하기 위한 조건

본 절에서는 주어진 (N,K) 길쌈부호의 부호어 집합과 $(n,1)$ 마더부호를 천공함으로써 얻어지는 부호어 집합이 동일하기 위한 조건에 대해 알아보고자 한다.

(N,K) 길쌈부호의 $K\times N$ PGM을 $G_0(D)$라 하고, $G_0(D)$의 상보행렬을 $H_0(D)=[h_{i,j}(D)]$, $0\le i\le N-K-1$, $0\le j\le N-1$라 하자.

(N,K) 길쌈부호의 부호어 집합과 $(n,1)$ 마더부호를 주어진 천공패턴 P에 따라 천공한 길쌈부호의 부호어 집합이 같다는 것은 마더부호의 K배 블록화 부호의 PGM $G_B(D)$에서 선택된 열들로 이루어진 $G_P(D)$와 $G_0(D)$가 동등하다는 말이고, 정의 1에 의해 $G_P(D)$가 $G_0(D)$와 동등하기 위해서는 다음의 두 조건을 만족해야 한다.

(i) $G_P(D)\,H_0(D)^T=[0]$.
(ii) $rank(G_P(D))=K$.

먼저 조건 (i)을 생각해보자. $G_P(D)$의 j번째 열을 $\underline{c}_j(D)$라고 하면, 조건 (i)은 $0\le i\le N-K-1$에 대해서 다음과 같이 다시 쓸 수 있다.

$$\sum_{j=0}^{N-1} h_{i,j}(D)\,\underline{c}_j(D)=0. \qquad (18)$$

2.1에서 본 바와 같이 $G_P(D)$의 열들은 $Z^u\overrightarrow{v_K}(g^{(l)}(D))$의 형태로 나타낼 수 있다. 이때 u와 l은 천공패턴에 따라 $0\le u\le K-1$, $1\le l\le n$의 범위에서 값을 갖는다. 따라서 식 (18)에서 $\underline{c}_j(D)$들을 해당하는 $Z^u\overrightarrow{v_K}(g^{(l)}(D))$로 바꾸고 l에 대해 정리하면 다음과 같이 다시 쓸 수 있다.

$$\sum_{l=1}^{n} S_l^{(i)}(Z)\,\overrightarrow{v_K}(g^{(l)}(D))=0, \qquad (19)$$

$0\le i\le N-K-1$. 여기서 $S_l^{(i)}(Z)$는 계수가 $F_2[D]$의 원소인, 행렬 Z의 다항식이며, 차수는 K보다 작다. 식 (19)를 행렬로 표현하면 다음과 같다.

$$\begin{bmatrix} S_1^{(0)}(Z) & S_2^{(0)}(Z) & \cdots & S_n^{(0)}(Z) \\ S_1^{(1)}(Z) & S_2^{(1)}(Z) & \cdots & S_n^{(1)}(Z) \\ \vdots & \vdots & \vdots & \vdots \\ S_1^{(J)}(Z) & S_2^{(J)}(Z) & \cdots & S_n^{(J)}(Z) \end{bmatrix} \begin{bmatrix} \overrightarrow{v_K}(g^{(1)}(D)) \\ \vdots \\ \overrightarrow{v_K}(g^{(n)}(D)) \end{bmatrix} = \mathbf{0}$$

www.dbpia.co.kr

위에서 $J=N-K-1$이다. 만약 위에서 모든 0이 아닌 $S_l^{(i)}(Z)$들이 역행렬을 갖고, $(N-K)$개의 식들 중 독립적인 식의 개수가 n보다 작다면, $\overrightarrow{v_K}(g^{(l)}(D))$들을 모두 구할 수 있고, 이로부터 $(n,1)$ 마더부호의 PGM도 구할 수 있다. $S_l^{(i)}(Z)$의 역행렬의 존재성은 다음의 정리1로부터 확인할 수 있다.

정리 1: $F_2(D)$를 다항식환(polynomial ring) $F_2[D]$의 몫 체라 하자. 그러면 $F_2(D)[Z]$ (modulo Z^K+DI_K)는 체이다.

증명: 임의의 체 F에 대하여 $m(x)$가 기약다항식이라면 $F[x]$ (modulo $m(x)$)가 체라는 사실은 잘 알려져 있다. 따라서 증명을 위해서는 Z^K+DI_K가 체 $F_2(D)[Z]$ 위에서 기약다항식이라는 사실만 보이면 된다. 만일 Z^K+DI_K가 기약다항식이 아니라면 차수가 K 보다 작은 다항식 $Z^l+c_{l-1}(D)Z^{l-1}+\cdots+c_0(D)I$을 인수로 가져야 하고, 이는 행렬 I, Z, $Z^2\cdots$, Z^l이 선형 종속임을 의미한다. 그러나 행렬 I, Z, $Z^2\cdots$, Z^{K-1}들의 첫 번째 행을 보면 $[100\cdots0]$, $[010\cdots0]$, $[001\cdots0]$, $\cdots$, $[000\cdots1]$이므로 이 행렬들은 모두 선형독립이다. 따라서 Z^K+DI_K는 체 $F_2(D)[Z]$에서 기약다항식이다. □

$F_2(D)[Z]$ (modulo Z^K+DI_K)가 체이므로, 원소인 0이 아닌 임의의 $S_l^{(i)}(Z)$는 역원을 갖는다. 따라서 식 (19)의 영이 아닌 해의 존재 여부를 알기위해서는 독립적인 식의 개수만 생각해 주면 된다. 이러한 사실로 부터 우리는 다음의 충분조건을 얻을 수 있다.

정리 2: $n>N-K$라면, (N,K) 길쌈부호를 만드는 임의의 천공패턴에 대해서도 조건 (i), 즉

$$G_P(D)\,H_0(D)^T=[0]$$

을 만족시키는 $G_P(D)$가 존재한다.

이제 $G_P(D)$의 행렬계수(rank)에 대한 조건 (ii)에 대해서 고려해보자. 우선 다음의 예제를 보자.

예제 2: $(4,3)$ 길쌈부호의 PGM이 다음과 같이 주어졌다고 하자.

$$G_0(D)=\begin{bmatrix} D & 1 & 0 & 1+D \\ 1 & D & 1 & D \\ 0 & D & D & 0 \end{bmatrix}.$$

이 부호가 천공패턴 $P=\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix}$에 따라 어떤 $(2,1)$ 길쌈부호로부터 만들어 질 수 있을지에 대해 확인해 보자. $G_M(D)=[g^{(1)}(D)\ \ g^{(2)}(D)]$ 라 하면, $G_P(D)$는 다음과 같은 형태를 지닌다.

$G_P(D)=\left[Z^2\overrightarrow{v_3}(g^{(1)})\ Z\overrightarrow{v_3}(g^{(1)})\ Z\overrightarrow{v_3}(g^{(2)})\ \overrightarrow{v_3}(g^{(2)})\right]$

$H_0(D)=[1111]$이므로, $G_P(D)H_0(D)^T=[0]$로부터

$$(Z^2+Z)\overrightarrow{v_3}(g^{(1)}(D))=(Z+I)\overrightarrow{v_3}(g^{(2)}(D)).$$

을 얻고 위 식은 $\overrightarrow{v_3}(g^{(2)}(D))=Z\overrightarrow{v_3}(g^{(1)}(D))$ 으로 정리할 수 있으므로, $G_P(D)$의 행렬계수는 $g^{(1)}(D)$, $g^{(2)}(D)$와 무관하게 2임을 알 수 있다. 따라서 이 부호는 주어진 천공패턴으로는 생성될 수 없다. □

위의 예제에서 볼 수 있듯이, 조건 (i)을 만족하는 $G_P(D)$의 행렬계수는 천공패턴에 따라 결정된다. 조건 (i)을 만족하는 $G_P(D)$의 행렬계수가 K가 되려면, $G_P(D)$의 열들 중 K개의 열들이 선형독립이어야 한다. $G_P(D)$의 열들은 천공패턴과 마더부호에 따라 $Z^u\overrightarrow{v_K}(g^{(l)}(D))$의 형태를 가지므로, 이들의 독립성을 확인하는 것은 꽤나 복잡한 일이다. 여기서 우리는 $G_P(D)$의 행렬계수가 K가 되기 위한 간단한 충분조건 하나를 소개한다.

정리 3: 만약 천공패턴 P에서 원소가 모두 1인 행이 존재한다면, $(n,1)$ 마더부호와 무관하게 $G_P(D)$의 행렬계수는 K이다.

증명: 만약 P의 l번째 행의 원소가 모두 1이라면, $Z^u\overrightarrow{v_K}(g^{(l)}(D))$, $0\le u\le K-1$는 모두 $G_P(D)$의 열이다. Z^K+DI_K는 $F_2(D)$에서 Z의 최소다항식이므로, $Z^0,Z^1,\cdots,Z^{K-1}$의 임의의 선형조합은 0이 될 수 없고, 이는 K개의 열 $Z^u\overrightarrow{v_K}(g^{(l)}(D))$, $0\le u\le K-1$는 선형독립이라는 말과 같다. 따라서 $G_P(D)$의 행렬계수는 K임이 자명하다. □

다음의 예제를 끝으로 본 절을 마무리 짓도록 하겠다.

www.dbpia.co.kr

예제 3: $(4,3)$ 길쌈부호의 PGM이 다음과 같다.

$$G_0(D)=\begin{bmatrix}1+D & 1 & 0 & 0\\ 0 & 1+D & 1+D & 1\\ D & 0 & D & 1+D\end{bmatrix}$$

천공패턴은 $P=\begin{bmatrix}1&1&1\\0&1&0\end{bmatrix}$라 가정하자. 그러면 $G_P(D)$는 다음과 같이 표현되고

$$G_P(D)=\left[Z^2\overrightarrow{v_3}(g^{(1)})\ Z\overrightarrow{v_3}(g^{(1)})\ Z\overrightarrow{v_3}(g^{(2)})\ \overrightarrow{v_3}(g^{(1)})\right],$$

정리 3에 의해 이 천공패턴에 의한 $G_P(D)$의 행렬계수는 항상 3이 된다. $G_0(D)$의 상보 행렬인 $H_0(D)$는

$$H_0(D)=\left[1+D+D^2\ \ 1+D^3\ \ 1+D^2+D^3\ \ D^2+D^3\right]$$

이며 조건 (i)에 의해 다음을 얻는다.

$$\left\{(1+D+D^2)Z^2+(1+D^3)Z+(D^2+D^3)I\right\}\overrightarrow{v_3}(g^{(1)}(D))=(1+D^2+D^3)Z\,\overrightarrow{v_3}(g^{(2)}(D)).\tag{20}$$

이제

$$\overrightarrow{v_3}(g^{(2)}(D))=(0\ 0\ 1)^T$$

로 두면 식 (20)에 의해 다음을 얻을 수 있다.

$$\overrightarrow{v_3}(g^{(1)}(D))=\frac{1}{1+D+D^3}\begin{pmatrix}1+D+D^2\\1+D\\1+D^3\end{pmatrix}.$$

이로부터 M을 만들고, M에 $1+D^2+D^3$을 곱해주면 식 (21)이 된다.

$$M=\begin{bmatrix}1+D+D^2 & 0\\ 1+D & 0\\ 1+D^3 & 1+D+D^3\end{bmatrix}\tag{21}$$

(21)식으로부터 마더부호를 구할 수 있다.

$$g^{(1)}(D)=1+D+D^2+D^4+D^5+D^8+D^9$$
$$g^{(2)}(D)=1+D^3+D^9$$

이다. $g^{(1)}(D)$와 $g^{(2)}(D)$의 최대 공약수는

$$\gcd\left(g^{(1)}(D),g^{(2)}(D)\right)=D^6+D^5+D^4+D^2+1$$

이므로, 이를 나눠주면 결과적으로 마더부호를 다음과 같이 구할 수 있다.

$$G_M(D)=\left[g^{(1)}(D)\ g^{(2)}(D)\right]=\left[1+D+D^3\ \ 1+D^2+D^3\right].$$

□

Ⅲ. 결 론

본 논문에서는 임의의 (N,K) 길쌈부호가 $(n,1)$ 마더부호를 주어진 천공패턴에 따라 천공함으로써 구해질 수 있는가에 대한 답을 제시하고자 하였다. 이를 위해 $G_P(D)$가 만족해야 할 두 조건, (i) $G_P(D)\,H_0(D)^T=[0]$ 과 (ii) $rank\left(G_P(D)\right)=K$를 제시하였다. $n>N-K$이면 천공패턴에 따라서는 이 두 조건을 만족하는 $G_P(D)$가 존재하여, (N,K) 길쌈부호는 항상 $(n,1)$ 마더부호를 천공함으로써 얻어질 수 있음을 증명하였다. 조건 (i)을 만족하는 $G_P(D)$의 존재는 $F_2(D)[Z]$ (modulo Z^K+DI_K)가 체임을 보임으로써 증명하였고, 조건 (ii)를 만족하기 위한 천공패턴 P의 충분조건을 제시하였다. 결론적으로, 우리가 도입에서 제시하였던 세 가지 질문들은 "$n>N-K$인 경우 예", "아니오", 그리고 "예"로 대답할 수 있다.

References

[1] J. Barbier, G. Sicot, and S. Houcke, "Algebraic approach for the reconstruction of linear and convolutional error correcting codes," in *Proc. CISE'06*, pp. 66-71, Venice, Italia, Nov. 2006.

[2] A. Canteaut and F. Chabaud, "A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense BCH codes of length 511," *IEEE Trans. Inf. Theory,* vol. 44, no. 1, pp. 367-378, Jan. 1998.

[3] M. Côte and N. Sendrier, "Reconstruction of convolutional codes from noisy observation," in *Proc. IEEE ISIT'09*, pp. 546-550, Seoul, Korea, Jun. 2009.

www.dbpia.co.kr

[4] É. Filiol, "Reconstruction of convolutionnal encoders over GF(q)," *Lecture Notes in Com. Sci., Crypt. and Coding*, vol. 1355, pp. 101-109, Dec. 1997.

[5] É. Filiol, "Reconstruction of punctured convolutional encoders", in *Proc. ISITA'00*, Hawaii, USA, Nov. 2000.

[6] J. H. Lee, et al., "Recognition of convolutional code with performance analysis," *J. KICS,* vol. 37A, no. 04, pp. 260-268, Apr. 2012.

[7] M. Marazin, et al., "Blind recovery if *k/n* rate convolutional encoders in a noisy environment," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, pp. 1186-1687, Nov. 2011.

[8] S. Su, et al., "Blind identification of convolutional encoder parameters," *The Scientific World J.*, vol. 2014, no. 798612, p. 9, May 2014.

[9] M. Cluzeau and M. Finiasz, "Reconstruction of punctured convolutional codes," in *Proc ITW'09*, pp. 75-79, Taormina, Italy, Oct. 2009.

[10] G. Karpilovsky, *Topics in field theory*, 1st Ed., Elsevier, 1989.

[11] H. S. Jang, H. B. Chung, and J. W. Seong, "On the existence of the (2,1) mother code of (n,n−1) convolutional code," *J. KICS*, vol. 39A, no. 04, pp. 165-171, Apr. 2014.

정 하 봉 (Habong Chung)

1981년 2월 : 서울대학교 전자공학과 졸업

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

1988년 8월 : 미국 University of Southern California, 전기공학과 공학박사

1988년~1991년 : 미국 뉴욕주립대 전기공학과 조교수

1991년~현재 : 홍익대학교 전자전기공학부 교수

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

성 진 우 (Jinwoo Seong)

2012년 2월 : 홍익대학교 전자전기공학부 졸업

2014년 2월 : 홍익대학교 전자정보통신공학과 석사

2014년~현재 : 홍익대학교 전자정보통신공학과 박사과정

<관심분야> 부호 이론, 채널 코딩, 채널 재구성 기법, 머신 러닝

www.dbpia.co.kr