논문 17-42-05-01 The Journal of Korean Institute of Communications and Information Sciences '17-05 Vol.42 No.05
https://doi.org/10.7840/kics.2017.42.5.951

채널 오류율 추정에 기반을 둔 길쌈부호의 개선된 재구성 알고리즘

성 진 우•, 정 하 봉°

An Improved Reconstruction Algorithm of Convolutional Codes Based on Channel Error Rate Estimation

Jinwoo Seong•, Habong Chung°

요 약

채널 재구성 기법이란 통신시스템에서 의도되지 않은 수신자가 수신 신호로부터 어떤 채널 부호가 사용되었는지, 주요 파라미터는 무엇인지를 알아내는 기법이다. 본 논문은 수신한 신호가 길쌈부호로 부호화된 경우, 사용된 길쌈부호의 주요파라미터인 입출력단의 비트수인 k와 n, 그리고 $k\times n$ 생성다항식행렬(Polynomial Generator Matrix, PGM)을 찾아내는 기법에 대해 다룬다. 본 논문은 M. Marazin 등이 제안한, 피버팅을 통한 가우스 조단 소거법(Gauss Jordan Elimination Through Pivoting, GJETP)을 사용한 길쌈부호의 채널 재구성 기법에서 채널오류율과 무관하게 임계값을 설정해주던 것과 달리, 수신한 시퀀스로부터 2진 대칭 채널(Bynary Symetric Channel, BSC)의 채널오류확률을 추정하고 이로부터 임계값을 설정하는 방식을 제안하고, S. Shaojing 등의 연판정(soft decision) 값을 이용한 기법을 적용시켜서 채널 재구성 기법의 성공률을 향상시켰다.

Key Words : Reconstruction, Convolutional Code, Gauss Elimination, BER Estimation, Threshold

ABSTRACT

In an attack context, the adversary wants to retrieve the message from the intercepted noisy bit stream without any prior knowledge of the channel codes used. The process of finding out the code parameters such as code length, dimension, and generator, for this purpose, is called the blind recognition of channel codes or the reconstruction of channel codes. In this paper, we suggest an improved algorithm of the blind recovery of rate k/n convolutional encoders in a noisy environment.

The suggested algorithm improves the existing algorithm by Marazin, et. al. by evaluating the threshold value through the estimation of the channel error probability of the BSC. By applying the soft decision method by Shaojing, et. al., we considerably enhance the success rate of the channel reconstruction.

Ⅰ. 서 론

디지털 통신 시스템에서 채널부호는 채널오류를 정정하기 위해서 필수적으로 사용된다. 길쌈부호는 채널부호의 한 종류이며 단독으로, 또는 RS 부호 등과의 연접부호로 이동통신이나 위성통신 시스템에서 많이

※ 본 연구는 한국연구재단 이공분야기초연구산업(NRF-2014R1A1A2059324) 지원 및 홍익대학교 산학협력단 관리로 수행되었습니다.
• First Author : Hongik University Department of Electronics, Information and Communication Engineering, adsads12@naver.com, 학생회원
° Corresponding Author : Hongik University Department of Electronic and Electrical Engineering, habchung@hongik.ac.kr, 종신회원
논문번호 : KICS2017-03-086, Received March 28, 2017; Revised April 17, 2017; Accepted April 25, 2017

사용되고 있다. 통신시스템에서 의도하지 않은 제 3의 수신자가 아무런 사전정보 없이 수신 신호로부터 해당 통신시스템에서 사용된 채널부호의 파라미터를 알아내는 기법을 채널재구성 기법이라 한다.

Communication Intelligence system(COMINT)란 미지의 수신신호로부터 복조, 복호, 암호해독을 거쳐서 중요한 정보를 얻게 해주는 시스템이며, 현대 정보전에서 중요한 역할을 한다. 채널재구성 기법은 COMINT의 복호과정에서 필수적이다. 시스템이 전파환경을 측정하여 이에 적합하게 통신 파라미터를 설정하여 동작하는 무선통신기술인 인지 무선통신 시스템(Cognitive Radio System, CRS)에서도 복호과정에서 부호의 파라미터를 알아내기 위한 채널재구성 기법이 필요하다.

지금까지 길쌈부호의 재구성기법은 다양한 연구자들에 의해 연구된 바 있다. B. Rice는 1995년 $(n,1)$ 길쌈부호의 재구성 기법을 제안하였다[1]. [1]은 최초의 길쌈부호의 재구성 기법이지만, 부호율이 $1/n$인 부호에 국한되었고, 상대적으로 짧은 메시지에 대해서만 고려하며, 오류가 있는 일반적인 채널상황에 대해서는 논의되지 않았다. E. Filiol과 J. Babier는 각각 1997년과 2005년에 B. Rice의 기법을 개선한 연구를 제안하였다[2,3]. 이들은 각각 [1]의 방법을 이용하여 기법의 적용을 부호율이 k/n인 경우로 확장하였다. 그 외에도 많은 연구자들이 길쌈부호의 재구성 기법과 그 응용분야에 대한 연구를 진행하였다[6-8].

2009년에 M. Marazin 등은 가우스 조단 소거법(Gauss Jordan Elimination Through Pivoting)을 이용한 길쌈부호의 재구성기법 (앞으로 GJETP 재구성 기법이라 줄여 쓰겠다)을 제안하였다[4]. [4]의 기법에서는 길이가 $M=lL$인 수신 시퀀스를 l개씩 행에 나열하여 만든 행렬 R_l을 이용한다. 특정 값의 l로 만든 R_l은 오류가 없는 경우, rank가 l 보다 작고, 이를 토대로 사용된 부호의 상보부호를 알아낼 수 있다는 사실로부터, 오류가 있는 일반적인 상황에서도 GJETP을 이용하여 행렬 R_l을 하삼각행렬(low triangular matrix) G_l로 만들면 1의 개수가 매우 작은 열이 나타나고 이 열이 오류가 없는 경우의 영벡터일 확률이 크다는 점을 이용한다. S. Shaojing 등은 [4]의 기법에서 R_l의 행배치를 연판정 값(soft value)으로부터 구한 신뢰도(reliability)가 높은 순으로 지정해주는 방법을 제시함으로써 기존 알고리즘의 반복수행을 배제하고 재구성 성공률까지 높였다[5].

[4]와 [5]에서는 G_l에서 1의 개수가 작은 열을 판정할 때, 채널에 무관하게 임계값을 설정해주었다. 본 논문은 채널오류율을 추정하여 이로부터 정확한 임계값을 설정해주는 방식을 추가하여 재구성 성공률을 향상시켰다.

논문의 구성은 다음과 같다. II 장에서는 [4]의 GJETP 재구성 기법과 [5]에서 제시된 연판정 값을 활용하여 GJETP 재구성 기법의 성능을 향상시키는 방법에 대해 소개한다. III 장에서는 본 논문에서 제안한 채널 오류율 추정에 기반한 임계값 설정 GJETP 재구성 기법을 제안하고 모의실험 결과를 제시한다. 최종적으로 IV 장에서 결론을 낸다.

Ⅱ. GJETP 재구성 기법

본 절에서는 논문 [4]의 GJETP 재구성 기법을 간단히 설명하겠다. 사용되는 길쌈부호는 생성다항식 행렬이

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

인 (n,k) 길쌈부호라 하고, 이 부호의 상보부호(dual code)의 PGM $H(D)$는 다음과 같다고 하자.

$$H(D)=\left[h_{i,j}(D)\,|\,i\in\{1,\cdots,n-k\},j\in\{1,\cdots,n\}\right]$$

2.1 행렬 R_l의 특성

본 소절에서는 GJETP 재구성 기법의 이해를 위해 길이가 $M=lL$인 오류가 없는 수신 시퀀스를 l개씩 행에 나열한 행렬 R_l의 특성에 대해 알아본다.

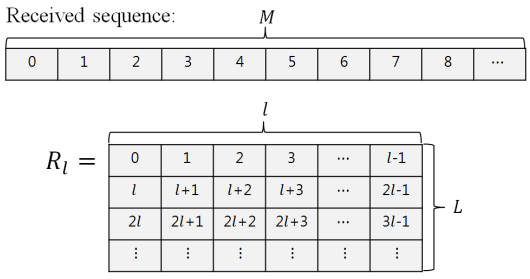

그림 1. 수신한 시퀀스로부터 만들어지는 행렬 R_l
Fig. 1. matrix R_l made from received sequence

$L \gg l$이라 가정한다. [4]에 의하면, 수신 시퀀스에 오류가 없는 경우, R_l의 행렬계수(rank)는 다음과 같다.

$$rank(R_l)=\begin{cases} l & \text{if } l\neq 0 \bmod n \text{ or } l<n_a \\ l\dfrac{k}{n}+\mu^{\perp} & \text{if } l=0 \bmod n \text{ and } l\geq n_a \end{cases} \quad (1)$$

여기서 $n_a=n\left\lfloor \frac{\mu^{\perp}}{n-k}+1 \right\rfloor$ 이고 $\mu^{\perp}$는 $h_{i,j}(D)$의 최대 차수를 의미한다. 즉, 적당한 l 값으로 R_l을 만들게 되면 행렬계수결핍(rank deficiency)이 발생해 행렬계수가 l보다 작아진다는 사실을 알 수 있다.

2.2 GJETP 재구성 기법

R_l을 GJETP를 이용하여 하삼각행렬 G_l로 만들면 다음과 같다.

$$G_l=A_lR_lB_l \quad (2)$$

식 (2)에서 A_l은 R_l의 행의 치환을 나타내는 $L\times L$ 행렬이고, B_l은 G_l의 각 열이 R_l의 어떤 열의 조합으로 만들어 졌는지를 나타내주는 $l\times l$ 행렬이다. 편의상 A_l로 인한 R_l의 행의 치환을 무시하고, B_l, G_l의 j번째 열을 각각 $\vec{b}_j$, $\vec{g}_j$ 라고 하자. 예를 들어, $\vec{b}_j=[101111]^T$ 이라면

$$\vec{g}_j=\vec{r}_1+\vec{r}_3+\vec{r}_4+\vec{r}_5+\vec{r}_6$$

가 된다. 채널오류가 없는 경우에는 식 (1)에서 보는 바와 같이 l이 n의 정수배일 때 G_l의 열들 중에 R_l의 행렬계수결핍 개수만큼의 영벡터가 나타나고, 해당 위치의 B_l의 열이 길쌈부호의 상보부호가 된다. 앞의 예에서처럼 $\vec{g}_j=\vec{0}$, $\vec{b}_j=[101111]^T$, $n=2$라면 $\vec{b}_j$의 홀수 번째와 짝수 번째 비트들로부터 $h_{i,1}(D)=1+D+D^2$, $h_{i,2}(D)=1+D$가 됨을 알 수 있다.

채널오류가 있을 때 GJETP 재구성 기법[4]의 수행 과정에 대해 알아보자. [4]의 기법은 채널오류가 심하지 않다면 G_l의 열 중 1의 개수가 현저히 작은 열이 오류가 없는 경우의 영벡터에 해당할 확률이 높다는 점에 착안하였다. G_l의 $l+1$행부터 L행까지의 부분 행렬을 G_l'이라 하자. $N_l(i)$를 G_l'의 i번째 열의 1의 개수라 하고, $Z(l)$을 다음과 같이 정의한다.

$$Z(l)=|\{i\in\{1,\ldots,l\}|N_l(i)\leq T\}| \quad (3)$$

[4]에서는 임계값을 $T=\frac{(L-l)\gamma}{2}$로 설정해 주었고, γ는 임계값을 최적화 하는 상수라고 언급했지만 구하는 방법에 대해서는 언급하지 않았고 고정된 값을 사용하였다. 식 (1)에 의해 $Z(l)$이 0이 아닌 최초의 l 값으로부터 $\hat{n}_a$를, 0이 아닌 수들의 간격으로부터 $\hat{n}$을 추정할 수 있다. $\hat{n}_a$와 $\hat{n}$으로부터 $\hat{k}$ 또한 추정할 수 있다. 그림 2는 $n=2$ 일 때의 $Z(l)$의 예를 나타내며, 이러한 경우 $\hat{n}_a=6$, $\hat{n}=2$로 추정한다.

l	2	3	4	5	6	7	8	9	…
$Z(l)$	0	0	0	0	1	0	2	0	…

그림 2. $n=2$일 때 $Z(l)$의 예
Fig. 2. Example of $Z(l)$ in case of $n=2$

G_l'의 j번째 열의 1의 개수가 임계값보다 작다면 $\vec{b}_j$가 상보부호의 기저일 것이라 추정할 수 있다. 독립적인 상보부호의 기저를 모두 찾을 때까지 l을 늘려가며 계속 수행한다.

2.3 연판정 값을 활용한 GJETP 재구성 기법

본 소절에서는 연판정 기법을 사용하여 기존 알고리즘의 복잡도를 줄인 [5]에서 제안한 방법을 설명하겠다. [4]에서는 식 (2)를 얻기 위해 R_l의 행의 위치를 무작위로 치환해가며 반복수행을 통해 모의실험을 한다고 밝혔다. 그들은 행의 위치를 치환하는 횟수가 늘어날수록 재구성 성공률이 올라가다 일정 횟수에 도달하게 되면 재구성 성공률이 포화된다고 주장하였다. GJETP 과정은 R_l을 열 사다리꼴 형태(column echelon form)로 변환시키는 과정이므로, 열의 조합을 나타내는 B_l의 생성에 가장 큰 영향을 주는 부분은 R_l의 가장 위쪽 $l\times l$ 행렬이다. 즉, 이 부분에 오류가 많은 경우에는 알고리즘이 실패할 확률이 높게 된다. [4]는 이 행들의 위치를 행의 치환을 통해 바꾸어 가면서 반복수행을 통해 이를 해결하려 하였지만 [5]에서는 연판정을 통해 신뢰도가 높은 행을 R_l의 위쪽에 차례로 배치함으로써 반복수행을 배제하였다. 즉, 연판정된 수신 시퀀스로 R_l을 만든 후, 각 행의 신뢰도를 계산하여 신뢰도가 높은 순으로 R_l의 행을 배열하고, 이를 경판정 값으로 바꾼 후 GJETP 재구성 기법을 수행한 것이다.

Ⅲ. 제안하는 기법과 모의실험 결과

II장에서 소개한 기존의 GJEPT 기법에서 G_l의 어떤 열이 오류 없는 경우의 영벡터에 해당하는 가를 판단하는 부분이 알고리즘의 성능을 가장 크게 좌우하는 부분이다. 채널의 상태가 좋은 경우라면 1의 개수가 작은 열이 영벡터에 해당할 확률이 높다. 그러나 채널 상태가 좋지 않은 경우라면 반드시 그렇지 않을 수도 있고, 또한 R_l의 몇 개의 열의 합이 영벡터가 되는가에 따라 1의 개수가 작다는 기준도 달라질 수 있다.

기존의 GJETP 기법은 임계값을 채널 상황과 $wt(\vec{b}_j)$에 무관하게 고정하였고, 이로 인해 채널 상황에 따라서는 잘못된 G_l의 열을 영벡터로 오인하여 잘못된 상보부호를 찾게 되고, 이는 곧 재구성 실패로 귀결된다. 본 논문에서 제안하는 기법은 채널오류율을 추정을 통해 각 열에 보다 정확한 임계값을 설정해줌으로써 재구성 성공률을 향상시킨다.

3.1 BSC 오류 확률을 추정하는 방법과 이를 이용한 임계값 설정방법

만약 BSC의 오류율 ϵ을 안다면, 오류가 없을 때 영벡터에 해당하는 열의 1의 개수의 기댓값을 구할 수 있다. 채널오류가 없을 때 영벡터가 되는 열이 G_l'의 j번째 열이라고 가정하고, $wt(\vec{b}_j)=w$ 라고 하자. 채널오류로 인하여 이 열의 임의의 한 비트가 1이 될 확률 p_j는 R_l의 w개의 열에서 해당 위치의 비트 중 홀수개의 오류가 발생할 확률이다. 따라서 다음 식으로 나타낼 수 있다.

$$p_j = \sum_{i=1}^{\left\lceil \frac{w}{2} \right\rceil} \binom{w}{2i-1} \epsilon^{2i-1} (1-\epsilon)^{(w-2i+1)} \tag{4}$$

이 열의 1의 개수의 기댓값은 $p_j(L-l)$이고, 표준편차는 $\sqrt{p_j(1-p_j)(L-l)}$ 이다. 이로부터 이 열에 대한 임계값 T_j는 다음과 같이 설정하였다.

$$T_j = p_j(L-l) + \alpha\sqrt{p_j(1-p_j)(L-l)} \tag{5}$$

적절한 α값은 모의실험의 상황에 따라 조금씩 달라지지만 $1 \le \alpha \le 7$에서 성능의 차이가 거의 없었고 그 이상 커지게 되면 성공률이 조금씩 떨어짐을 모의실험을 통해 확인하였다. 3.3 소절에서의 모의실험 결과는 $\alpha = 5$로 설정하고 수행하였다.

이제 채널 오류 확률 ϵ를 추정하는 방법에 대해 알아보자. 하나의 R_l을 만드는 동안 (본 모의실험에서는 20,000 비트의 수신 동안)에는 ϵ 값이 변하지 않는다고 가정하였다. 우선 G_l의 열 중 1의 개수가 현저히 작은 하나의 열을 선택한다. 이 열을 j번째 열이라고 하자. $G_l = A_l R_l B_l$에서 B_l의 j번째 열을 $\vec{b}_j$ 라고 하고, $wt(\vec{b}_j)=w$ 라고 하자. 식 (4)에 의해 $E\{N_l(j)\} = p_j(L-l)$ 이다. 이 식에 의해 ϵ에 대한 방정식을 도출할 수 있지만, 문제는 하나의 R_l로부터는 $E\{N_l(j)\}$를 얻을 수 없다는 점이다. 다만, L이 충분히 큰 경우, 이항분포인 $N_l(j)$의 값은 확률적으로 평균값에서 크게 벗어나지 않을 것이라는 점에 착안하여 ϵ에 대한 방정식을 다음과 같이 만들었다.

$$N_l(j) = \lceil p_j(L-l) \rceil \tag{6}$$

식 (6)에서 $\lceil \bullet \rceil$는 반올림을 의미한다. 식 (4)와 이항정리를 이용하면 식 (6)은 다음과 같이 정리된다.

$$N_l(j) = \left\lceil (l-L) \sum_{i=1}^{\left\lceil \frac{w}{2} \right\rceil} \binom{w}{2i-1} \sum_{t=0}^{w-2i+1} \binom{w-2i+1}{t} (-\epsilon)^{w-t} \right\rceil \tag{7}$$

식 (7)에서 반올림을 제거하고 최소 자승법을 사용했을 때 가장 근접한 해가 나오도록 하는 좌변의 값을 $L-l$로 나눈 것을 C라 하고, 식 (7)을 정리하면 다음과 같다.

$$-C = \frac{(1-2\epsilon)^w - 1}{2} \tag{8}$$

식 (8)로부터 ϵ을 아래와 같이 나타낼 수 있다.

$$\epsilon = \frac{1-(1-2C)^{\frac{1}{w}} e^{j\frac{2\pi}{w}k}}{2}, \quad k = 0, \cdots, w-1 \tag{9}$$

식 (9)에 의해 ϵ은 w가 홀수일 때

$$\epsilon = \frac{1-(1-2C)^{\frac{1}{w}}}{2},$$

w가 짝수일 때

$$\epsilon = \frac{1-(1-2C)^{\frac{1}{w}}}{2},\ \epsilon = 1-\frac{1-(1-2C)^{\frac{1}{w}}}{2}$$

만을 실수해로 가진다. G_l의 열 중 1의 개수가 현저히 작은 하나의 열을 선택하였기 때문에 $0 < C < 1/2$이고,

$$0 < \frac{1-(1-2C)^{\frac{1}{w}}}{2} < \frac{1}{2}$$

이다. 따라서 채널 오류 확률은 아래의 식을 이용하여 구할 수 있다.

$$\epsilon = \frac{1}{2}\left\{1-\left(1-2\frac{N_l(j)}{(L-l)}\right)^{\frac{1}{w}}\right\} \quad (10)$$

제안된 ϵ추정 기법의 타당성 검토를 위해서 모의실험을 수행하였다. 다음의 표는 (3,1,3) 길쌈부호 부호기로 생성되어 BSC를 통과한 길이 20,000의 시퀀스를, 제안한 ϵ추정 기법을 사용하여 1,000번의 모의실험 후 추정한 ϵ값의 평균과 표준편차를 나타내었다.

표 1. BSC 오류 확률 추정 모의실험
Table 1. Simulation result of BSC error probability estimation

BER	0.01	0.03	0.05	0.07	0.1
Mean	0.0099	0.0299	0.0499	0.07	0.0991
Dev	0.0006	0.0011	0.0015	0.0023	0.0027

3.2 추정한 BSC 오류 확률로부터 구한 임계값을 이용하는 기법

그림 3은 제안하는 기법의 순서도를 나타낸다. 기법이 길기 때문에 파트를 나눠서 설명하도록 한다. 첫 번째로 설명할 파트는 채널오류율을 추정하는 파트이다

① $l=2,\ \gamma=0.4,\ l_{\max}=20$으로 시작한다.
② 수신한 연판정 시퀀스로 R_l을 만든다.
③ R_l의 행을 높은 신뢰도 순으로 재정렬한다.
④ R_l을 복조한다.
⑤ GJETP를 이용하여 $G_l = A_l R_l B_l$을 만든다.

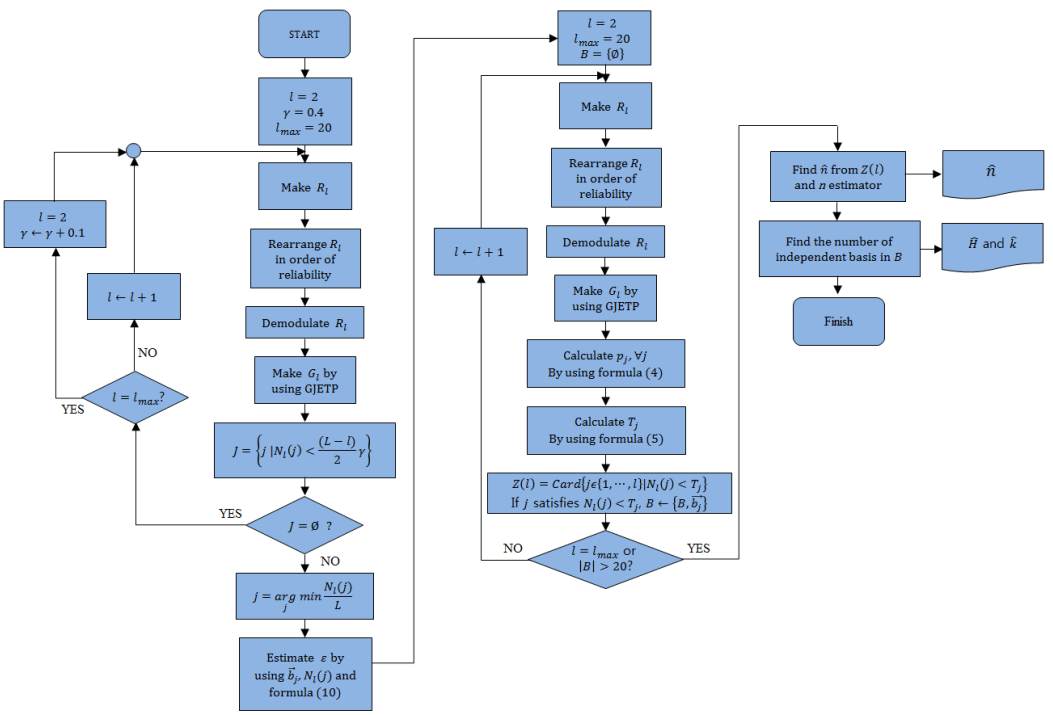

그림 3. 채널 오류율 추정에 기반 한 임계값 설정을 이용한 길쌈부호의 재구성 기법 알고리즘 순서도
Fig. 3. Flow chart of improved reconstruction algorithm of convolutional code based on channel error rate estimation

⑥ 집합 $J=\left\{j|N_l(j)<\frac{(L-l)}{2}\gamma\right\}$를 만든다.

⑦-(1) J가 공집합이면 $l\leftarrow l+1$하여 ②에서부터 반복한다.

⑦-(2) J가 공집합, $l=l_{\max}$라면 $l=2$, $\gamma\leftarrow\gamma+0.1$하여 ②로 돌아간다.

⑦-(3) J가 공집합이 아니라면 ⑧로 간다.

⑧ J의 원소 중 $N_l(j)$값의 비율($N_l(j)/L$값이 최소인 것을 선택, L은 l이 바뀔 때마다 달라진다)이 최소인 l, j를 선택하여, 이때의 $\vec{b}_j$, $N_l(j)$ 그리고 식 (10)을 이용하여 ϵ을 구한다.

다음으로 설명할 파트는 ϵ를 이용하여 G_l의 각 열마다 임계값을 설정해주고, 이를 이용하여 상보부호의 기저를 구하는 방법이다.

① $l=2$, $l_{\max}=20$, $B=\{\varnothing\}$으로 시작한다.

②~⑤ 앞 파트와 동일

⑥ 식 (4)를 이용하여 p_j를 구하고, 식 (5)를 이용하여 G_l'의 각 열에 대응하는 T_j를 구한다.

⑦ $Z(l)=Card\{j\in\{1,...,l\}|N_l(j)\leq T_j\}$을 기록하고, $N_l(j)\leq T_j$를 만족하는 j에 대해서 $B\leftarrow\left\{B,\vec{b_j}\right\}$.

⑧ $l=l_{\max}$ 또는 $|B|>20$ 이 아니라면 $l\leftarrow l+1$하여 ②로 돌아가서 반복한다.

⑨ $Z(l)$로부터 $\hat{n}$을 구한다.

⑩ B에 속한 j에 대해 독립적인 $\vec{b}_j$ 들이 상보부호의 기저가 되고, 그 개수가 $\hat{k}$가 된다.

⑪ 상보부호의 기저로부터 $\hat{H}$를 구한다.

⑫ 종료

3.3 모의실험결과

모의실험은 $l=2$에서 시작하여 $l_{\max}$까지 변화시키며 수행한다. $l_{\max}$가 부호의 구속장에 비해 너무 커지면 오류의 영향이 커져서 재구성에 실패할 확률이 높아지고, 구속장에 비해 너무 작아지면 상보부호의 기저를 모두 찾기 힘들다. 따라서 제안하는 기법을 사용하여 재구성을 하는 경우 $l_{\max}$를 20부터 10단위로 늘려가면서 $Z(l)$을 관찰하며 기법을 수행하는 것이 좋다. 또한 상보부호의 후보 집합인 B의 크기가 20 이하에서 독립적인 상보부호의 기저를 모두 찾아내는 것을 모의실험을 통해 확인하였기 때문에 그 이상 찾지 않는 것으로 하였다. B의 크기를 한정하는 이유는 재구성 기법의 불필요한 수행을 막기 위해서이다. 변조와 복조는 BPSK를 사용하였다. 모의실험은 1,000번의 기법 실행에서 완벽하게 재구성을 성공한 횟수를 기록하였고, 매번 다른, 길이 20,000의 수신 시퀀스를 사용하였다.

표 2. 제안하는 기법의 (2,1) 길쌈부호의 재구성 성능
Table 2. Reconstruction performances of (2,1) convolutional code with the proposed algorithm

Code / SNRdB	(2,1,3)	(2,1,5)	(2,1,7)
0	998	943	15
0.5	1,000	992	74
1	1,000	999	619
1.5	1,000	1,000	965
2	1,000	1,000	997
2.5	1,000	1,000	1,000
3	1,000	1,000	1,000

표 3. 기존의 기법의 (2,1) 길쌈부호의 재구성 성능
Table 3. Reconstruction performances of (2,1) convolutional code with the existing algorithm

Code / SNRdB	(2,1,3)	(2,1,5)	(2,1,7)
0	0	0	0
0.5	282	0	0
1	999	0	0
1.5	1,000	659	0
2	1,000	996	9
2.5	1,000	1,000	996
3	1,000	1,000	1,000

사용된 길쌈부호의 부호기를 표기의 편의를 위해 8진 표기법으로 나타내도록 한다. 표 2, 3에서 사용된 길쌈부호는 다음과 같다.

(2,1,3) 길쌈부호: [7 5], $l_{\max}=20$

(2,1,5) 길쌈부호: [23 33], $l_{\max}=20$

(2,1,7) 길쌈부호: [171 133], $l_{\max}=40$

표 4. 제안하는 기법의 (3,1) 길쌈부호의 재구성 성능
Table 4. Reconstruction performances of (3,1) convolutional code with the proposed algorithm

Code / SNRdB	(3,1,3)	(3,1,5)	(3,1,7)
0	1,000	1,000	927
0.5	1,000	1,000	974
1	1,000	1,000	997
1.5	1,000	1,000	1,000
2	1,000	1,000	1,000
2.5	1,000	1,000	1,000

표 5. 기존의 기법의 (3,1) 길쌈부호의 재구성 성능
Table 5. Reconstruction performances of (3,1) convolutional code with the existing algorithm

Code / SNRdB	(3,1,3)	(3,1,5)	(3,1,7)
0	1,000	0	0
0.5	1,000	407	0
1	1,000	999	340
1.5	1,000	1,000	991
2	1,000	1,000	999
2.5	1,000	1,000	1,000

표 4, 5에서 사용된 길쌈부호는 다음과 같다.
(3,1,3) 길쌈부호: [5 7 7], $l_{\max} = 20$
(3,1,5) 길쌈부호: [25 33 37], $l_{\max} = 20$
(3,1,7) 길쌈부호: [171 165 133], $l_{\max} = 20$

표 6. 제안하는 기법의 (3,2) 길쌈부호의 재구성 성능
Table 6. Reconstruction performances of (3,2) convolutional code with the proposed algorithm

Code / SNRdB	(3,2,3)	(3,2,5)
0	414	0
0.5	816	13
1	985	20
1.5	1,000	51
2	1,000	131
2.5	1,000	360
3	1,000	633
3.5	1,000	855
4	1,000	956
4.5	1,000	995

표 7. 기존의 기법의 (3,2) 길쌈부호의 재구성 성능
Table 7. Reconstruction performances of (3,2) convolutional code with the existing algorithm

Code / SNRdB	(3,2,3)	(3,2,5)
0	216	0
0.5	761	0
1	894	0
1.5	977	0
2	1,000	0
2.5	1,000	27
3	1,000	418
3.5	1,000	837
4	1,000	917
4.5	1,000	993

표 6, 7에서 사용된 길쌈부호는 다음과 같다.
(3,2,3) 길쌈부호: [1 2 0 ; 4 1 2], $l_{\max} = 30$
(3,2,5) 길쌈부호: [27 33 0 ; 0 5 13], $l_{\max} = 30$

이제 계산복잡도를 비교해보자. 제안하는 기법은 기존의 기법[5]보다 낮은 SNR에서 높은 재구성 성공률을 보이지만 계산복잡도가 높다는 단점이 존재한다. 이를 비교하기 위해 동일한 머신을 사용하여 두 기법이 한번 작동하는데 걸리는 평균 시간을 측정하여 아래의 표에 나타내었다.

표 8. 알고리즘의 수행시간 비교
Table 8. Time comparison of both algorithms

	Proposed algorithm(sec)	Existing algorithm(sec)
(2,1,3)	0.324	0.218
(2,1,5)	0.414	0.197
(2,1,7)	1.474	0.456
(3,1,3)	0.313	0.273
(3,1,5)	0.396	0.241
(3,1,7)	0.415	0.218
(3,2,3)	0.389	0.270
(3,2,5)	1.339	0.248

Ⅳ. 결 론

본 논문에서는 M. Marazin 등과 S, Shaojing 등의 기법[4,5]이 채널상황과 무관하게 임계값을 설정해 주는 것과 달리, 채널오류율을 추정하고 이로부터 임계값을 설정해주는 방법을 추가한 기법을 제안하였다. 제안한 기법은 3.3 소절에서 볼 수 있듯이 기존의 기법[4,5]과 비교해 볼 때 전체 SNR 구간에서 기존의 방법보다 우수한 성능을 보였다. 특히, 낮은 SNR 상황에서는 채널재구성 성공률을 월등히 향상시킨다. 따라서 COMINT 시스템과 같이 채널상태가 좋지 않은 경우라도 보다 정확한 정보를 필요로 하는 경우, 비록 알고리즘의 계산복잡도는 다소 증가하지만, 기존의 기법보다 활용도가 높을 것이다.

References

[1] B. Rice, “Determining the parameters of a rate 1/n convolutional encoder over GF(q),” in *Proc. 3rd Int. Conf. Finite Fields an App.*, 1995.

[2] E. Filiol, “Reconstruction of convolutional encoders over GF(q),” *LNCS, Crypt and Coding*, vol. 1355, pp. 101-109, Dec. 1997.

[3] J. Barbier, “Reconstruction of turbo-code encoders,” in *Proc. SPIE Security and Defense Space Commun. Tech. Symp.*, vol. 5819, pp. 463-473, 2005.

[4] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," *EURASIP J. Wirel. Commun. and Netw.*, vol. 2011, no. 168, pp. 1-9, 2011.

[5] S. Shaojing, J. Zhou, Z. Huang, C. Liu, and Y. Zhang, "Blind identification of convolutional encoder parameters," *The Scientific World J.*, vol. 2014, Article ID 798612, p. 6, 2014.

[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] H. B. Chung and J. W. Seong, "Sufficient conditions for the existence of an (n,1) mother code and its puncturing pattern to generating a given convolutional code," *J. KICS*, vol. 41, no. 04, pp. 379-386, Apr. 2016.

[8] 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.

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

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
1988~1991년 : 미국 뉴욕주립대 전기공학과 조교수
1991년~현재 : 홍익대학교 전자전기공학부 교수
<관심분야> 부호 이론, 조합수학, 시퀀스 설계, 협력통신, 시공간 부호