

수신 신호의 연관성 값을 이용한 길쌘부호의 파라미터 암맹 판별 기법

이지현*, 권순희*, 신동준^o

A Blind Detection Method of Convolutional Codes by Using Soft-Decision Values of Received Signals

Jihyeon Lee*, Soonhee Kwon*,
Dong-Joon Shin^o

요 약

본 논문에서는 길쌘부호로 부호화된 수신 신호의 연관성 값을 알고 있는 경우, 주요 파라미터인 부호기의 출력비트수 n 을 암맹판별할 수 있는 기법을 제안한다. 행 재배열에만 수신 신호의 연관성 값을 이용하는 기존기법과 달리, 본 논문에서는 행 재배열과 열의 재배열 및 Gauss-Jordan Elimination Through Pivoting 기법에서도 연관성 값을 이용한다. AWGN 채널 환경에서의 시뮬레이션 결과를 통해 제안한 암맹판별기법의 성능이 기존기법의 성능보다 우수함을 확인하고 유효성을 검증한다.

Key Words : Blind detection, Box-plus operation, Convolutional code, Gauss-Jordan elimination through pivoting, Log-likelihood ratio, Soft-decision values

ABSTRACT

In this paper, we propose a blind detection

method which estimates the number of encoder output bits n of convolutional code. Compared to the conventional method which uses the soft-decision values of received signal for rearranging rows of the matrix, we use the soft-decision values to rearrange both the rows and columns, and to do the Gauss-Jordan elimination through pivoting. Also, we evaluate the proposed algorithm by performing simulation in additive white gaussian noise (AWGN) channel to confirm the improved performance of the proposed algorithm compared with the conventional method.

1. 서 론

디지털 통신 시스템에서 오류정정부호는 채널에 의해 발생하는 오류를 정정하기 위해서 필수적으로 사용된다. 일반적으로 송신단과 수신단이 공통된 오류정정부호를 사용하기로 약속하지만, 만약 수신단이 오류정정부호의 파라미터 정보를 알 수 없다면 송신단에서 사용된 오류정정부호의 파라미터를 수신된 데이터만으로 찾아내야 한다. 이러한 기법을 오류정정부호의 암맹판별기법이라 한다. 길쌘부호는 오류정정부호의 한 종류로, 이동통신 및 위성통신 등 다양한 응용분야에서 광범하게 사용되고 있으며 길쌘부호의 암맹판별기법도 꾸준히 연구되어 왔다. 그 중에서도 Gauss-Jordan elimination through pivoting (GJETP) 기법을 이용한 길쌘부호의 파라미터 암맹판별기법이 활발하게 연구되고 있다¹⁻³. [1]은 채널 오류율을 안다는 상황에서 GJETP 기법에서의 임계값을 수식적으로 설정해주고, 만약 연관성 값을 안다면, 연관성 값의 절댓값으로 각 행에서 오류라고 추정되는 개수가 적은 순서대로 행을 재배열하여 길쌘부호에서 사용된 인터리버의 크기, 인터리버의 시작점, 길쌘부호의 부호율 등의 여러 파라미터들을 암맹판별하는 기법을 제안하였다. [2]는 오류가 존재하는 환경에서 GJETP 기법을 사용하여 길쌘부호의 입력비트수, 출력비트수, 그리고 상보부호의 메모리개수 등의 파라미터 및 생다항식행렬을 암맹 판별하는 방법을 제시하였다. 또

※ 본 연구는 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호정보 특화연구센터 사업의 지원을 받아 수행되었음.

• First Author : (ORCID:0000-0003-3768-3813)Department of Electronic Engineering, Hanyang University, jhlee95@hanyang.ac.kr, 학생회원

o Corresponding Author : (ORCID:0000-0002-5017-5314)Department of Electronic Engineering, Hanyang University, djshin@hanyang.ac.kr, 종신회원

* (ORCID:0000-0002-8204-5311)Department of Electronic Engineering, Hanyang University, tmsgml1991@hanyang.ac.kr, 학생회원
논문번호 : 201908-166-A-LU, Received August 21, 2019; Revised September 11, 2019; Accepted September 16, 2019

한 [3]에서는 채널 오류율을 모른다는 상황에서 수신된 시퀀스로부터 2진 대칭 채널의 채널오류확률을 추정하고 이를 토대로 GJETP 기법에서의 임계값을 설정해 주어 길쌈부호의 입력비트수와 출력비트수, 그리고 상보부호의 생성다항식행렬의 재구성 성공률을 향상시켰다. 특히, Su 등은 수신된 비트의 연관성 값을 알고 있는 경우 그 값을 이용해 만들어진 행렬의 행을 재배열하여 길쌈부호의 파라미터 암맹판별 성능을 향상시켰다^[4].

본 논문에서는 연관성 값을 이용한 행렬의 행과 열의 재배열을 통해 길쌈부호의 파라미터 암맹판별 성능을 더욱 향상시킬 수 있는 GJETP 기법을 제안한다. 그리고 시뮬레이션을 통하여 제안된 암맹판별기법의 성능을 확인한다.

II. 길쌈부호와 부호기의 출력비트수 판별 기법

2.1 길쌈부호와 GJETP 기법

길쌈부호에서 k 를 부호기의 입력 비트 수, n 을 부호기의 출력비트 수라고 하면, k 개의 메시지 입력 스트림은 $m_i = (m_i^{(1)}, m_i^{(2)}, \dots, m_i^{(k)})$ 으로 나타나고, 생성다항식에 의해서 n 개의 부호화된 데이터 스트림 $c_i = (c_i^{(1)}, c_i^{(2)}, \dots, c_i^{(n)})$ 가 만들어진다. 이렇게 생성된 부호어는 변조과정을 거친 후 채널을 통해 전송되는데, 이 때 원치 않는 신호인 잡음이 추가되어 수신된 신호에 오류가 발생한다. 여기서 수신 신호를 복조할 때, 수신 값의 부호에 따라 양수면 0으로, 음수면 1로 표현하는 경관정과, 수신 값을 두 레벨을 초과하여 양자화하는 연관정의 두 형태로 출력을 얻을 수 있고, 해당 값으로 수신 신호의 복호를 진행한다. 또한 연관정 시, 값들의 신뢰도를 나타내기 위해 주로 Log-likelihood ratio (LLR)가 사용되는데, y 를 수신 값이라고 할 때, 한 비트 x 의 LLR 값은 $\lambda(x) = \log(P(x=0|y)/P(x=1|y))$ 로 나타낼 수 있다. 두 비트 x_1 과 x_2 의 modulo-2 합 연산에 대한 LLR값은 box-plus연산으로, 계산의 복잡도를 줄이기 위해 다음과 같이 근사될 수 있다^[4].

$$\lambda(x_1 \oplus x_2) = \lambda(x_1) \boxplus \lambda(x_2) \approx \text{sign}(\lambda(x_1)) \times \text{sign}(\lambda(x_2)) \min(|\lambda(x_1)|, |\lambda(x_2)|) \quad (1)$$

여기서 \oplus 는 modulo-2 합 연산, $\text{sign}(X)$ 은 X 의 부호, $\min(A, B)$ 는 A 와 B 중 최솟값을 나타낸다. 기존 연관성 값을 이용한 GJETP 기법은 다음과 같

다^[4]. BPSK 변복조를 사용하였고, AWGN 채널을 통하여 M 개의 비트를 수신했다고 가정한다. 또한, 채널 오류 확률 P_e 을 알고 있고 부호어의 동기가 완벽하다고 가정한다.

먼저, 열의 개수의 최솟값 l_{\min} 과 최댓값 l_{\max} 를 정해주고 l_{\min} 으로 l 을 초기화해준 뒤, l 을 l_{\max} 까지 1씩 늘리면서 다음의 과정을 수행한다. 길이가 M 인 수신 시퀀스를 한 행에 l 개씩 나열하여 행의 길이가 $L = \lfloor M/l \rfloor$ 인 $L \times l$ 행렬 R_l 을 만든다. 그림 1을 통해 수신 시퀀스로부터 행렬 R_l 이 만들어지는 과정을 자세히 알아볼 수 있다. 주어진 행렬 R_l 의 i 번째 열을 R_l^i 라고 하고, $i=1$ 에서 $i=l$ 까지 다음의 과정을 수행한다.

만약, R_l^i 의 i 번째 값이 0이면, 처음으로 i 번째 값이 1이 나오는 $R_l^{i'}$ ($i' > i$)을 R_l^i 과 치환한다. $R_l^{i'}$ 의 i 번째 값들이 모두 0이면, 처음으로 i 번째 값이 1이 나오는 i' 번째 행을 i 번째 행과 치환한다. 이제 R_l^i 의 i 번째 값이 1이면, i 번째 행에서 값이 1인 모든 $R_l^{i'}$ 을 R_l^i 과 modulo-2 합 연산한다.

결과적으로 R_l 은 윗부분을 하삼각행렬로 만들 수 있고 그 때의 행렬을 G_l 이라 하면, $G_l = A_l R_l B_l$ 로 나타낼 수 있다. 이 때, A_l 은 R_l 의 행 재배열을 나타내는 $L \times L$ 행렬이고 B_l 은 R_l 의 열들 사이의 조합을 나타내는 $l \times l$ 행렬이다. G_l 의 하삼각행렬 아래의 $(l+1)$ 행부터 L 행까지의 $(L-l) \times l$ 행렬을 J_l 이라고 하고, $N_l(i)$ 은 J_l 의 i 번째 열의 1의 개수라고 하면, Z_l 은 다음과 같이 정의된다.

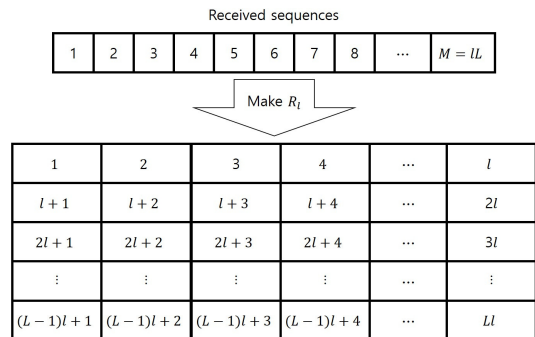


그림 1. 수신 시퀀스로 만들어지는 행렬 R_l
Fig. 1. matrix R_l generated by received sequences

$$Z(l) = \text{Card} \left\{ i \in (1, \dots, l) \mid N_i(i) \leq \frac{L-l}{2} \gamma_{opt} \right\} \quad (2)$$

여기서 γ_{opt} 은 임계값을 최적화 하는 상수로, 채널 오류 확률 P_e 과 열 조합 행렬 B_l 을 이용하여 구할 수 있다^[2]. l 의 값이 n 의 배수이면 R_l 의 특정 열들은 다른 열들에 종속적이게 되어 rank 값이 줄어드는 현상이 발생한다. 따라서 길쌈부호의 출력비트수 \hat{n} 은 $Z(l)$ 이 0이 아닌 경우의 l 값들의 간격으로부터 추정할 수 있다.

GJETP 기법은 상단부분 $l \times l$ 행렬의 대각성분을 기준으로 열 조합이 발생하기 때문에 해당 부분의 신뢰도가 암맹판별 성능에 큰 영향을 준다. 그래서 [4]에서는 수신 신호의 연관정 값으로 만든 행렬 R_l 에서 각 행의 연관정 값들을 이용하여 행의 신뢰도를 추정한 후 행을 재배열해주고 다시 경관정 값으로 복호시켜 GJETP 기법을 진행하였다. 본 논문에서는 암맹판별 성능을 더욱 향상시키기 위해 행 재배열과 열 재배열, 그리고 GJETP 기법에 연관정 값을 이용하는 알고리즘을 다음과 같이 제안한다.

2.2 제안하는 GJETP 기반 암맹판별기법

본 논문에서는 기존 논문과 동일하게 BPSK 변복조를 사용하고, AWGN 채널을 통하여 M 개의 비트를 수신하며, 채널 오류 확률 P_e 을 알고 있고 부호어의 동기가 완벽하다고 가정한다. 이를 기반으로 다음과 같은 GJETP 기반 암맹판별기법을 제안한다.

기존 기법과 같이 열의 최솟값 l_{min} 과 최댓값 l_{max} 을 지정하고, 모든 가능한 열의 값 l 에 대해서 다음을 수행한다. M 개 수신 신호의 LLR값으로 l 개의 열과 L 개의 행을 갖는 $L \times l$ 행렬 $R_{l,soft}$ 을 생성하고, 이를 복조시켜 경관정 값을 갖는 행렬 $R_{l,hard}$ 을 생성한다. $R_{l,soft}$ 의 각 행에서 LLR값의 절댓값이 가장 작은 값을 행의 신뢰도라고 하며, 행의 신뢰도가 큰 순서대로 두 행렬, $R_{l,soft}$ 과 $R_{l,hard}$ 의 모든 행을 동일한 순서로 재배열해준다. 다음으로, 주어진 행렬 $R_{l,soft}$ 의 상단 $l \times l$ 에 해당하는 행렬을 $K_{l,soft}$ 라고 하고, $K_{l,soft}$ 의 i 번째 행을 $K_{l,soft}^{i,row}$ 라고 하자. $i=1$ 에서 $i=l$ 까지 다음의 과정을 수행한다. 연관정 값들로 GJETP 기법을 사용하기 위해선 대각성분의 값들을 음수로 만들어주어야 한다. 따라서 $K_{l,soft}^{i,row}$ 의 i 번째 값이 양수이면 $K_{l,soft}^{i,row}$ 에서 i' 번째 값들($i' > i$)중 음수인 값들을 찾

알고리즘 1: 부호기의 출력비트 수 암맹판별기법

- 입력: M 개 수신비트의 경관정과 연관정 값, $l_{min}l_{max}$
 출력: 부호기의 출력비트 수 추정치 \hat{n}
- 1: for 모든 후보 l 에 대하여 do
 - 2: $R_{l,soft}$, $R_{l,hard}$ 생성
 - 3: $R_{l,soft}$ 행의 신뢰도값 기준, 행 재배열
 - 4: for 모든 l 에 대하여 do
 - 5: if $K_{l,soft}$ 의 l 번째 행 > 0
 - 6: $l < l'$ 중 음수 값 있는 첫 l' 찾아 치환
 - 7: end if
 - 8: $K_{l,soft}^{i,row}$ 에서 열의 신뢰도기준, 열 재배열
 - 9: $G_{l,hard} = A_l R_{l,hard} B_l$
 - 10: end for
 - 11: end for
 - 12: $G_{l,hard}$ 에서 각 열의 1의 개수 = N_l
 - 13: $N_l \leq (L-l)\gamma_{opt}/2$ 만족하는 l 값 저장
 - 14: 저장된 l 값들의 차이 값 중 가장 많이 나오는 값에 해당하는 \hat{n} 값 선택
 - 15: \hat{n} 값 출력

는다. 만약 모두 양수라면, $K_{l,soft}^{i,row}$ 중에서 i 와 i' 번째 값들에 음수 값이 존재하는 가장 가까운 행을 찾아 $K_{l,soft}^{i,row}$ 와 치환해 준다. $K_{l,soft}^{i,row}$ 의 i' 번째 값들 중 음수 값을 갖는 값들이 속해있는 열에서 i' 번째 원소들에 대해 LLR값의 절댓값이 가장 작은 값을 열의 신뢰도라고 하고, 열의 신뢰도가 가장 큰 열을 i 번째 열과 치환한다. 그 후, $R_{l,soft}^{i,row}$ 에서 i' 번째 값이 음수인 모든 열들과 i 번째 열에 대해서 $R_{l,soft}$ 에서는 box-plus연산을, $R_{l,hard}$ 에서는 modulo-2 합 연산을 시행한다. 열의 최댓값 l_{max} 까지 모든 과정이 완료되면 $R_{l,hard}$ 의 하삼각행렬 $G_{l,hard}$ 에 대해서 식 (2)를 통해 기존 기법과 동일한 방법으로 부호기의 출력비트 수 \hat{n} 을 추정한다.

III. 시뮬레이션

그림 2는 수신 신호의 길이가 $M=1000, 2000, 4000$ 인 경우에 대해 수신 신호의 연관정 값을 행 재배열에만 사용한 기존의 연관정 기반 GJETP 기법^[4]과 수신 신호의 LLR 값을 행과 열의 재배열 그리고 GJETP 기법에 사용하는 것을 제안한 본 논문의 암맹판별 알고리즘의 채널 값에 대한 길쌈부호 부호기의 출력비트 수 추정 실패 확률을 자체적으로 시뮬레이션을 수행하여 확인한 결과이다. 사용된 길쌈부호의

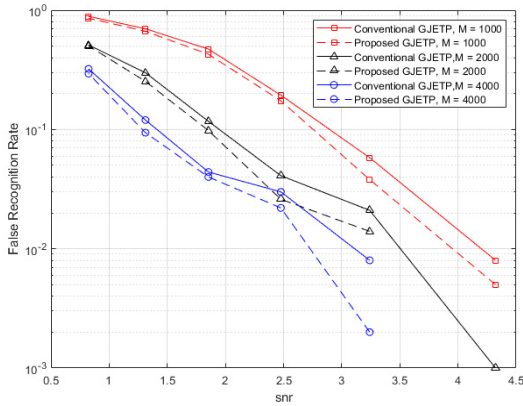


그림 2. 다양한 수신 신호의 길이와 채널 값에 대한 길쌈부호 부호기의 출력비트 수 추정 실패 확률
 Fig. 2. False recognition rate of the number of output bits of the convolutional code for various number of received bits and SNR.

(n, k) 값은 $(2, 1)$ 이며, 생성다항식은 8진법으로 나타냈을 때 $(23, 35)_8$ 이다. 그림 2를 통해서 모든 SNR과 모든 수신 신호의 길이에 대해 제안하는 기법이 기존의 기법보다 부호기의 출력비트 수 추정 실패 확률이 낮은 것을 확인할 수 있다. 즉, 기존의 기법에 비해 제안한 기법의 암맹판별 성능이 향상된다는 것을 확인할 수 있었다. 이는 기존기법에서는 GJETP 기법을 시행하기 전의 행 재배열에만 수신 신호의 연관정 값을 사용하였기 때문에 GJETP 기법을 진행하면서 행렬 K_i 의 신뢰도가 감소하였지만, 본 논문에서 제안하는 기법은 행과 열의 재배열 및 GJETP 기법에도 수신 신호의 LLR 값을 사용함으로써 행렬 K_i 의 신뢰도를 향상시켰기 때문에 암맹판별 성능이 향상된 것으로 보인다.

IV. 결 론

본 논문에서는 길쌈부호로 부호화된 신호가 AWGN 채널을 통해 수신되었을 경우, 수신 신호의 LLR값으로 행과 열의 신뢰도를 측정하여 재배열하고 LLR연산을 수행함으로써 길쌈부호의 주요 파라미터인 부호기의 출력비트 수 n 을 암맹판별하는 기법을 제안하였다. 제안한 기법을 복잡도 측면에서 기존기법과 비교하였을 때에는 유사한 성능을 보이지만, 본 기법의 암맹판별 성능에 대해서는 기존기법의 성능보다 향상되었음을 다양한 수신 신호의 길이와 채널 값에 대한 시뮬레이션을 통하여 확인하였다.

References

- [1] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters," *Sign. Process.*, vol. 89, no. 4, pp. 450-462, Apr. 2009.
- [2] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," *EURASIP J. Wireless Commun. and Netw.*, vol. 2011, no. 168, pp. 1-9, 2011.
- [3] J. Seong and H. Chung, "An improved reconstruction algorithm of convolutional codes based on channel error rate estimation," *J. KICS*, vol. 42, no. 5, pp. 951-958, Apr. 2017.
- [4] S. Su, J. Zhou, Z. Huang, C. Liu, and Y. Zhang, "Blind identification of convolutional encoder parameters," *Scientific World J.*, vol. 2014, pp. 1-9, 2014.
- [5] T. K. Moon, *Error correction coding: Mathematical methods and algorithms*, John Wiley & Sons Inc., 2005.