논문 13-38A-02-03

한국통신학회논문지 '13-02 Vol.38A No.02
http://dx.doi.org/10.7840/kics.2013.38A.2.156

BCH 부호 식별 및 생성 파라미터 추정 기법

이 현◆, 박 철 순*, 이 재 환**, 송 영 준°

Classification and Generator Polynomial Estimation Method for BCH Codes

Hyun Lee◆, Cheol-sun Park*, Jae-hwan Lee**, Young-joon Song°

요 약

잡음이 존재하는 채널을 통하여 디지털 통신을 하는 경우 일반적으로 채널 부호를 사용한다. 만약 수신측에서 채널 부호의 생성 파라미터를 모르는 경우, 채널 부호의 복호는 매우 어렵다. 이러한 경우에 수신데이터의 정확한 복호를 위해서는 채널부호의 종류 및 생성 파라미터를 알아내는 방법이 필요하다. 본 논문에서는 BCH(Bose-Chaudhuri-Hocquenghem) 부호의 생성 파라미터인 생성다항식을 추정하는 기법을 소개한다. 이 방법은 생성다항식이 최소다항식으로 구성된다는 특징과 순회부호의 특성을 이용한 방법이다. 그리고 종래 방법에 비해 생성다항식 추정 성능을 향상 시킬 수 있는 결정 확률 변수 보상 기법을 제안한다. 제안한 기법은 랜덤데이터 패턴이 생성다항식을 구성하는 최소다항식으로 나누어지는 특성을 이용한 기법이다. 또한 컴퓨터 시뮬레이션을 통해 제안한 알고리즘의 우수성을 검증한다.

Key Words : BCH codes, generator polynomial, minimal polynomial, parameter estimation, compensation

ABSTRACT

The use of an error-correcting code is essential in communication systems where the channel is noisy. When channel coding parameters are unknown at a receiver side, decoding becomes difficult. To perform decoding without the channel coding information, we should estimate the parameters. In this paper, we introduce a method to reconstruct the generator polynomial of BCH(Bose-Chaudhuri-Hocquenghem) codes based on the idea that the generator polynomial is compose of minimal polynomials and BCH code is cyclic code. We present a probability compensation method to improve the reconstruction performance. This is based on the concept that a random data pattern can also be divisible by a minimal polynomial of the generator polynomial. And we confirm the performance improvement through an intensive computer simulation.

Ⅰ. 서 론

일반적인 통신 시스템에서는 오류를 검출하고 정정하는 채널 부호의 사용은 필수적이다. 채널 부호를 사용할 때 통신 시스템의 송·수신단에서는 사전에 오류 정정 부호의 종류 및 생성 파라미터를 결정하고 결정된 파라미터를 이용하여 채널 부호화 및 복호를 수행한다[1,2]. 그러나 만약 수신측에 이러한 정보를 모르는 경우에는 복호를 수행하는데 어려움을 겪을 것이다. 이러한 경우 수신데이터의 정확한 복호를 위해서는 오류정정부호의 종류 및 생성 파라미터를 알아내는 방법이 필요하다. 예를 들어 전자전

◆ 주저자 : LIG넥스원, jdlgus@gmail.com, 정회원
° 교신저자 : 금오공과대학교 전자공학부 모바일 통신 및 부호 연구실, yjsong@kumoh.ac.kr, 종신회원
* 국방과학연구소, 정회원, ** 금오공과대학교 전자공학부 모바일 통신 및 부호 연구실, 준회원
논문번호 : KICS2012-10-507, 접수일자 : 2012년 10월 24일, 최종논문접수일자 : 2013년 1월 21일

(Electronic Warfare)분야의 전자전 지원(Electronic Warfare Support)에서는 적에 의해 방사되는 전자파 에너지를 탐색→감청→방향 탐지→식별하여 필요한 정보를 생산하거나, 생산한 정보를 전자공격 활동에 제공하는 활동을 수행하는데, 이러한 활동을 위해서는 먼저 적의 전파 신호를 수신하고 수신된 신호를 디코딩하는 기술이 필요하다. 수신된 신호를 정확하게 복호하기 위해서는 수신 신호에 적용된 기법들에 대해 분석하고 분류할 수 있어야 한다. 여기서 채널 부호화 된 위협신호에 대해 정확하게 복호를 수행하기 위해서는 채널 부호의 생성 파라미터를 찾아내는 것이 중요하다. 이처럼 수신 데이터로부터 사용된 채널부호의 파라미터를 추출하여 채널 부호를 복원하는 기법을 채널 부호의 복원 기법이라 한다. 본 논문에서는 블록부호의 한 종류인 BCH 부호의 식별 및 생성 파라미터 추정 기법에 대해서 소개하고 생성 파라미터 추정 성능을 향상시키는 결정 확률 보상 기법을 제안한다. 현재 블록 부호의 식별 및 파라미터 추정 방법에 대해서는 많은 연구가 진행되고 있다[3-7]. BCH 부호는 생성다항식 기반으로 생성되는 순회부호이므로 순회부호의 특성을 이용하면 생성 파라미터 복원이 가능하다. 부호어는 생성다항식과 메시지다항식의 곱으로 구성되고, 생성다항식은 최소다항식들의 최소공배다항식으로 구성되기 때문에 최소다항식들과 부호 데이터의 모듈로(modulo)연산 수행을 통해 생성다항식 복원이 가능하다. 즉, 모듈로 연산 결과가 0인 최소다항식들을 분류하여 서로 곱함으로써 생성다항식을 복원할 수 있다. 만약 부호데이터에 오류가 포함되어 있는 경우에는 여러 개의 부호데이터에 대해 모듈로 연산을 수행하고 연산 결과에 적절한 임계치를 적용하여 생성다항식을 복원할 수 있다. 그러나 랜덤 데이터에 대해서도 동일한 방법으로 모듈로 연산을 수행하였을 때에도 0이 되는 특성이 존재하는데 이러한 특성은 생성다항식을 복원하는데 영향을 준다. 본 논문에서 제안하는 결정 확률 보상 기법은 이러한 특성을 보상해 줌으로써 모듈로 연산 결과에 임계치를 적용할 때 종래 방법에 비해 더 낮은 임계치를 적용할 수 있고, 이를 통해 종래 방법에 비해 열악한 채널 환경에서도 정확한 생성 파라미터 추정이 가능하다.

본 논문의 구성은 다음과 같다. 먼저 Ⅰ장에 서론을 나타내고 Ⅱ장에서는 BCH 부호의 구성과 순회부호 특성을 이용한 BCH 부호의 생성 파라미터 추정 방법을 소개한다. 그리고 Ⅲ장에서는 종래 기법과 비교하여 부호 인식 성능이 향상되는 확률 보상 기법을 제안하고 컴퓨터 시뮬레이션을 통해 부호 식별 및 생성다항식 알고리즘에 대한 검증 및 성능을 확인한다. 마지막으로 Ⅳ장에서는 본 논문의 결론에 대하여 기술한다.

Ⅱ. BCH 부호의 생성 파라미터 추정 기법

BCH 부호는 다음과 같이 정의할 수 있다. 부호의 길이가 n이고 오류정정 능력을 t라고 할 때, 유한체 $GF(q)$ 상의 생성다항식 $g(x)$에 의하여 생성된 순회부호를 BCH 부호라 한다. 여기서 부호 길이 n은 q^m-1을 나누게 된다. BCH 부호의 생성다항식 $g(x)$는 식 (1)과 같이 구성된다[1-2,8].

$$g(x)=LCM[M_{\beta^b}(x), M_{\beta^{b+1}}(x),\cdots,M_{\beta^{b+2t-1}}(x)] \quad (1)$$

식 (1)에서 LCM은 최소공배다항식을 의미하고, $M_{\beta^i}(x),(0\le i\le q^m)$ 는 $GF(q)$ 상에서 β^i의 최소다항식을 의미한다. 여기서 β는 $GF(q^m)$ 상의 위수(order)가 n인 원소이며, b는 생성다항식 $g(x)$를 구성하는 최소다항식의 시작 위치를 의미하는 임의의 정수이다. 만약 $n=q^m-1$ 이면 이 부호를 원시 BCH 부호 (primitive BCH code)라 한다.

블록 부호의 식별 및 생성 파라미터 추정 방법은 여러 가지가 존재하지만 본 논문에서는 BCH부호의 부호인식에 대하여 다루므로, 순회부호의 특성을 이용한 추정 기법에 대해 알아본다.

2.1. 순회 부호의 특성

임의의 순회부호의 부호벡터 c와 정보어 m은 다음과 같이 다항식으로 표현이 가능하다[8].

$$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1} \quad (2)$$

$$m(x)=m_0+m_1x+\cdots+m_{k-1}x^{k-1} \quad (3)$$

여기서 부호 다항식 $c(x)$는 식 (4)와 같이 생성다항식 $g(x)$와 $m(x)$의 곱을 통해 비조직적 형태로 생성 가능하다.

$$c(x)=m(x)g(x) \quad (4)$$

만약 조직적 형태로 생성하면 식(5)과 같다.

$$c(x)=a(x)g(x)=x^{n-k}m(x)+b(x) \quad (5)$$

여기서 $a(x)$와 $b(x)$는 $x^{n-k}m(x)$를 $g(x)$로 나누었을 때의 몫과 나머지 이다. 따라서 순회부호에서 $c(x)$와 $g(x)$의 사이에는 다음과 같은 관계가 성립한다.

$$c(x) \bmod g(x) = 0 \tag{6}$$

식 (6)에서 mod는 모듈로(modulo) 연산을 의미한다. BCH 부호의 생성다항식 $g(x)$는 연속적인 $2t$개의 최소다항식의 최소공배다항식으로 구성된다. 따라서 임의의 최소다항식 M_{β^i}가 $g(x)$의 구성성분인 최소다항식이라면 식 (7)과 같이 $c(x)$를 나눌 수 있다.

$$c(x) \bmod M_{\beta^i} = 0 \tag{7}$$

따라서 $g(x)$를 구성하는 최소다항식들은 모든 $c(x)$대해 식 (7)을 항상 만족할 것이다. 그러나 임의의 최소다항식이 $g(x)$의 구성성분이 아니라면 식 (7)을 항상 만족하지 않을 것이다[8].

2.2. 생성다항식 추정 알고리즘

BCH 부호는 생성다항식을 기반으로 생성되는 순회부호이므로 순회부호의 특성을 이용하면 생성다항식 복원이 가능하다[9]. 단, 추정하려는 BCH 부호는 원시 BCH 부호이며 부호의 길이를 알고 있다고 가정한다. 만약 부호의 길이를 알고 있다면 그 부호 길이에 대한 모든 최소다항식들을 생성할 수 있다. 추정하려는 대상이 원시 BCH 부호이므로 $n = q^m - 1$의 관계가 성립한다. 따라서 부호 길이 n을 이용하여 m을 추정 할 수 있고 $GF(q^m)$에 대한 최소다항식들도 생성이 가능하다. $GF(q^m)$의 생성 가능한 모든 원소의 수는 q^m개이기 때문에 $GF(q^m)$에 대한 영을 제외한 모든 최소다항식들의 수는 $q^m - 1$이며, 최소다항식들을 다음과 같이 M_a로 정의한다.

$$M_a = \left\{ M_{\beta^0}(x), M_{\beta^1}(x), \cdots, M_{\beta^{q^m-2}}(x) \right\} \tag{8}$$

즉 $GF(q^m)$의 모든 원소가 β^0부터 β^{q^m-2}로 구성되기 때문에 최소다항식 역시 M_{β^0}부터 $M_{\beta^{q^m-2}}$까지 생성 할 수 있다. BCH 부호의 생성다항식 $g(x)$는 M_a중에서 연속적인 $2t$개가 선택되어 최소공배다항식 연산으로 구성된다. 이 때 선택되는 최소다항식들은 오류 정정 능력 t와 선택되는 최소다항식의 시작 지점인 b에 따라 결정된다. 여기서 $g(x)$를 구성하는 최소다항식들은 다음과 같이 M_g로 정의한다.

$$M_g = \left\{ M_{\beta^b}(x), M_{\beta^{b+1}}(x), \cdots, M_{\beta^{b+2t-1}}(x) \right\} \tag{9}$$

순회부호의 특성에 의하면 M_g는 $c(x)$를 나눌 수 있기 때문에 이러한 특성을 이용하면 M_a중에서 M_g를 분류할 수 있고 분류된 M_g를 이용하여 $g(x)$를 재구성할 수 있다. 즉, 분석하려는 데이터에 대해서 식 (7)과 같이 모듈로 연산을 수행 했을 때 그 결과가 항상 0이 되는 최소다항식들이 바로 M_g가 된다. 이와 같은 과정을 수식으로 표현하면 다음과 같다.

$$v_{(i,j)} = \begin{cases} 1, & c_j(x) \bmod M_{\beta^i} = 0 \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

식 (10)에서 $v_{(i,j)}$는 결정 변수(decision variable)라 정의한다. 이때 i는 최소다항식에 대한 순번이고, j는 부호어에 대한 순번이다. 수신된 부호어의 총 개수를 N이라 한다면 j의 범위는 $(1 \le j \le \mathrm{N})$이다. $c_j(x)$는 j번째 부호어를 의미하고 $v_{(i,j)}$는 j번째 부호어에 대한 i번째 최소다항식 M_{β^i}의 결정 변수를 의미한다. 결정 변수는 임의의 부호어 $c_j(x)$와 임의의 최소다항식 M_{β^i}에 대하여 모듈로 연산을 수행하였을 때 결과가 0이라면 1, 아니면 0으로 정의한다.

다음은 부호길이가 15인 BCH부호에 대한 결정 변수 시뮬레이션 결과를 나타내고 있다.

표 1. 부호 길이가 15인 BCH 부호에 대한 결정 변수
Table 1. Decision variable for BCH codes of code length 15

code / i	BCH(15,5)	BCH(15,7)	BCH(15,11)
0	0.5074	0.5079	0.4924
1	1	1	1
2	1	1	1
3	1	1	0.0622
4	1	1	1
5	1	0.2463	0.2552
6	1	1	0.0622
7	0.0654	0.0654	0.0666
8	1	1	1
9	1	1	0.0622
10	1	0.2463	0.2552
11	0.0654	0.0654	0.0666
12	1	1	0.0622
13	0.0654	0.0654	0.0666
14	0.0654	0.0654	0.0666

총 10,000개의 부호어를 대상으로 시뮬레이션을 수행하였고 각 부호어에 대한 결정 변수의 평균을 계산한 값이다. 가로축은 최소다항식에 대한 순번을 나타내고 있고 세로축은 BCH 부호의 종류를 나타내고 있다. 표 1에서 오류정정능력 t가 1인 BCH(15,11)부호의 경우 최소다항식 1, 2, 4, 8의 결정 변수가 1을 나타내고 있다. 그러나 생성다항식을 구성할 때 $2t$개의 연속적인 최소다항식으로 구성되기 때문에 생성다항식을 구성하는 최소다항식은 연속적인 2개의 최소다항식이다. 따라서 최소다항식 1에서 2까지 연속적으로 1값을 가지기 때문에 생성다항식은 최소다항식 1과 2의 최소공배다항식으로 구성되어 있음을 알 수 있다. 그러므로 최소다항식 1은 x^4+x+1이고 최소다항식 2도 x^4+x+1이므로 최소다항식 1과 2를 최소공배다항식을 취하면 x^4+x+1이 되기 때문에 생성다항식은 x^4+x+1 된다. BCH(15,7), BCH(15,5)부호도 동일한 방법으로 생성다항식을 추정하면 각각 $x^8+x^7+x^6+x^4+1$과 $x^{10}+x^8+x^5+x^4+x^2+x+1$ 가 된다.

따라서 이러한 특성을 이용하면 M_g를 알 수 있고, 이를 이용한다면 BCH부호의 식별 및 생성 파라미터 추정이 가능하다. 또한 위와 같은 연산을 수행했을 때 결정변수가 1인 값이 존재하지 않는다면, 그 데이터는 BCH부호가 아니기 때문에 이러한 특성을 이용하여 BCH 부호의 식별이 가능하다. $e(x)$가 오류다항식이고, 수신 데이터 $r(x)$가 $c(x)+e(x)$라 하면 다음과 같은 관계가 성립한다.

$$r(x) \bmod M_g = c(x) \bmod M_g + e(x) \bmod M_g = e(x) \bmod M_g \quad (11)$$

이와 같이 데이터에 에러가 존재하는 경우에는 통계적으로 접근한다면 부호 추정 기법을 적용할 수 있으며, 수식으로 표현하면 다음과 같다.

$$\mathrm{P}(v_i = 1) = \frac{\sum_{j=1}^{N} v_{(i,j)}}{N} \quad (12)$$

식 (12)의 $\mathrm{P}(v_i = 1)$는 N개의 부호어에 대해서 최소다항식 M_{β^i}의 결정변수가 1이 되는 확률을 의미한다. 즉, N개의 부호어에 대한 결정 변수 $v_{(i,j)}$의 평균값을 의미한다. 식 (12)의 $\mathrm{P}(v_i = 1)$를 최소다항식 M_{β^i}에 대한 결정 확률 변수(decision probability variable)이라 정의한다. 따라서 수신 데이터에 대해서 $\mathrm{P}(v_0 = 1)$ 부터 $\mathrm{P}(v_{q^m-2} = 1)$까지 계산한 후 결정 확률 변수가 1에 가까울수록 M_g일 가능성이 크므로 적절한 임계치를 설정하여 최소다항식들을 분류하면 M_g를 추정할 수 있게 된다. 그림 1은 위의 과정을 흐름도로 나타낸 것이다.

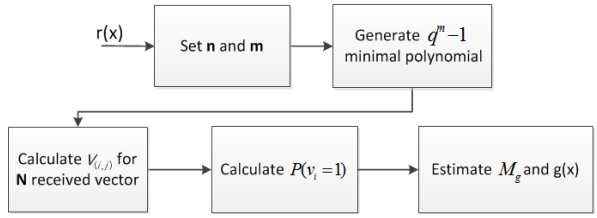

그림 1. 생성 다항식 추정 알고리즘
Fig 1. Algorithm for the estimation of generator polynomials

먼저 부호 길이 n과 m을 가정한 후 이에 대한 최소다항식을 생성한다. 그리고 각 부호어에 대한 결정변수를 계산하고 이 결과를 이용하여 결정 확률 변수를 계산한다. 그리고 계산한 결정 확률 변수를 이용하여 M_g를 추정하고 추정한 M_g를 이용하여 $g(x)$를 계산한다.

2.3. 시뮬레이션

그림 2는 BCH(15,11)에 대한 채널 상태에 따른 결정 확률 변수의 분포를 나타내고 있다. 여기서 minpoly1부터 minpoly5는 서로 다른 최소다항식 5개를 의미한다. 시뮬레이션 환경은 AWGN채널에서 수행하였다. 부호 길이가 15인 BCH부호의 경우에는 모든 최소다항식의 개수가 15이지만 중복되는 최소다항식들을 제거하면 서로 다른 최소다항식은 5개이다. 따라서 서로 다른 5개의 최소다항식을 대상으로 시뮬레이션을 수행하였다. 그래프에서 채널 상태가 좋을 때는 최소다항식 2의 결정 확률 변수가 1인 것을 알 수 있다. 따라서 BCH(15,11)의 생성다항식은 최소다항식 2로 구성되는 것을 알 수 있다. 그러나 채널 상태가 안 좋아 짐에 따라 최소다항식 2의 결정 확률 변수가 작아지는 것을 알 수 있다. 그러나 좋은 채널 환경에서는 다른 최소다항식들의 결정 확률 변수 값 보다 큰 값을 갖기 때문에 적절한 임계치를 적용하면 오류가 존재하는 데이터에 대해서도 생성다항식 추정이 가능함을 알 수 있다.

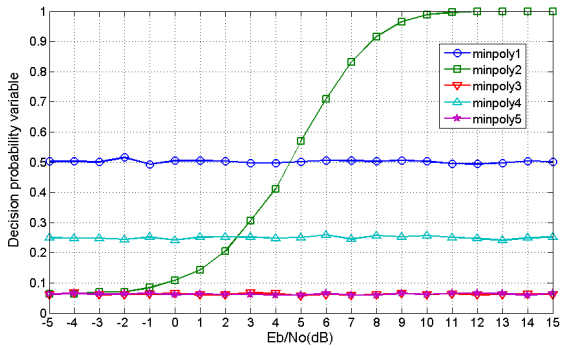

그림 2. BCH(15,11)부호의 결정 확률 변수
Fig 2. Decision probability variable of BCH(15,11)

Ⅲ. 결정 확률 변수 보상 기법

3.1. 제안하는 기법

Ⅱ장의 순회 부호 특성에 의하면 M_g는 $c(x)$를 항상 나눌 수 있다. 그러나 M_g가 아닌 최소다항식으로도 $c(x)$를 나누는 경우도 존재한다. 이와 같은 특성은 Ⅱ장의 표 1과 그림 2에서 확인할 수 있다. 표 1의 데이터를 보면 i가 0인 결정 변수는 약 0.5를 나타내고 있다. 즉, i가 0인 경우의 최소다항식은 M_g가 아님에도 불구하고 약 0.5의 확률로 $c(x)$를 나눈다. 이러한 특성을 설명하면 다음과 같다.

임의의 수신 벡터를 $r(x)$라 하고, $r(x)$를 차수가 d인 임의의 다항식 $a(x)$로 나누었을 때, 나머지를 $b(x)$라 하자. 그러면 $b(x)$는 d개의 계수로 구성된 차수가 $d-1$인 다항식이 된다. 그리고 $b(x)$의 d개의 계수가 모두 0일 확률은 $GF(q)$인 경우 $\sigma = q^{-d}$이 된다. 따라서 σ 값은 M_g에 속하지 않는 차수가 d인 최소다항식이 $r(x)$를 나눌 확률과 동일하다. 예를 들어 차수가 1인 $x+1$이 차수가 1 이상인 임의의 다항식을 나누는 확률은 0.5가 된다. 이와 같은 방법으로 d와 q값에 따라 σ를 계산하면 표 2와 같다.

표 2. 다항식의 차수 d와 유한체 $GF(q)$ 상의 q에 따른 σ값
Table 2. σ for polynomial degree d and q of $GF(q)$

q \ d	2	4	8	16	32
1	0.5	0.25	0.125	0.0625	0.03125
2	0.25	0.0625	0.015625	0.00390625	0.000976563
3	0.125	0.015625	0.001953125	0.000244141	3.05176E-05
4	0.0625	0.00390625	0.000244141	1.52588E-05	9.53674E-07
5	0.03125	0.000976563	3.05176E-05	9.53674E-07	2.98023E-08
6	0.015625	0.000244141	3.8147E-06	5.96046E-08	9.31323E-10
7	0.0078125	6.10352E-05	4.76837E-07	3.72529E-09	2.91038E-11
8	0.00390625	1.52588E-05	5.96046E-08	2.32831E-10	9.09495E-13
9	0.001953125	3.8147E-06	7.45058E-09	1.45519E-11	2.84217E-14
10	0.000976563	9.53674E-07	9.31323E-10	9.09495E-13	8.88178E-16

따라서 2장에서 설명된 n이 15인 BCH 부호의 경우 생성가능한 모든 최소다항식에 대한 σ값은 표 3과 같다.

표 3. 부호 길이가 15인 BCH 부호의 최소다항식에 대한 σ
Table 3. σ for BCH codes of code length 15

Minimal polynomial	σ
$x+1$	0.5
x^4+x+1	0.0625
$x^4+x^3+x^2+x+1$	0.0625
x^2+x+1	0.25
x^4+x^3+1	0.0625

위의 설명과 같이 σ값이 항상 존재하기 때문에 생성다항식 추정에 영향을 주게 된다. 이러한 문제점을 해결하기 위해서 최소다항식 마다 σ값을 미리 계산하고 생성다항식을 추정하기 전에 결정 확률 변수에 대해 보상을 수행하고 추정한다면 σ의 영향을 최소화 할 수 있다. 이 과정을 수식으로 나타내면 다음과 같다.

$$P_c(v_i=1) = (P(v_i=1)-\sigma) \times \left(\frac{1}{1-\sigma}\right) \quad (13)$$

식 (13)에서 $P_c(v_i=1)$는 보상후의 결정 확률 변수이다. 먼저 기존의 결정 확률 변수에 σ를 빼주고 $1/(1-\sigma)$를 곱하여 정규화를 시켜준다. 이와 같이 정규화를 수행하면 보상 후에도 결정 확률 변수의 최대값이 1이 되므로 각 확률 변수마다 동일한 임계

치를 적용할 수 있게 된다. 이러한 과정을 확률 보상 기법이라 정의한다. 다음 그림은 확률 보상 기법을 포함한 생성다항식 추정 과정의 흐름도이다. 기존의 생성다항식 추정 알고리즘에서 σ의 계산 및 보상 과정이 추가 되었다.

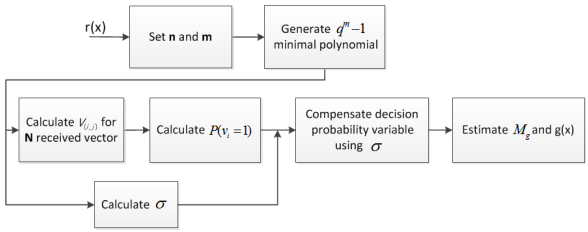

그림 3. 결정 확률 보상 기법 기반의 생성다항식 추정 알고리즘
Fig 3. Generator polynomial estimation algorithm using decision probability compensation method

3.2. 시뮬레이션

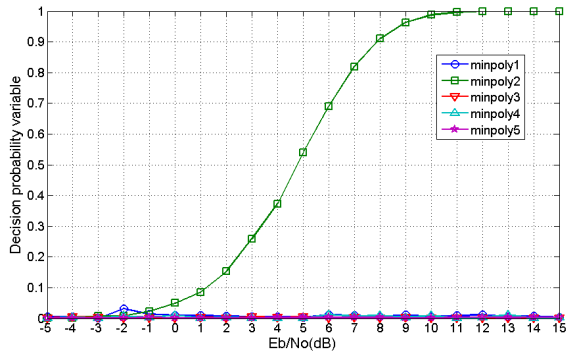

그림 4. 확률보상기법을 적용한 BCH(15,11)부호의 결정확률 변수
Fig 4. Decision probability variable of BCH(15,11) using compensation method

그림 4는 확률 보상 기법 적용 후의 BCH(15,11) 부호의 결정 확률 변수 분포를 나타내고 있다. 그림 2의 보상전의 결정 확률 변수를 살펴보면 M_g가 아닌 최소다항식임에도 불구하고 σ가 0이 아닌 일정한 상수에 가까운 값을 가짐을 알 수 있다. 그러나 보상 후에는 M_g를 제외한 최소다항식의 결정 확률 변수가 모두 0에 가까운 값으로 변한 것을 알 수 있다. 따라서 확률 변수 보상 기법을 적용하면 부호 식별 및 생성다항식 추정 시 더 낮은 임계치를 적용할 수 있기 때문에 부호 인식 성능이 적용 전보다 향상 될 수 있다.

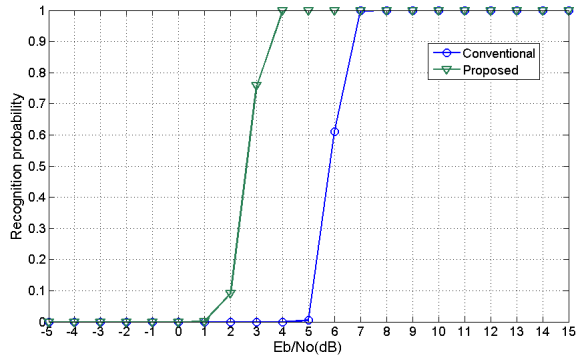

그림 5. BCH(15,11)에 대한 확률보상기법 적용 전후의 부호 인식 확률
Fig 5. Recognition probability for BCH(15,11) code before and after using probability compensation method

그림 5는 BCH(15,11) 부호에 대한 제안한 기법 적용 전후의 부호 인식 확률 비교 데이터이다. 제안한 기법을 적용하기 전에는 E_b/N_o가 6~7dB 이상 되어야 정확한 생성다항식 추정이 가능하였지만 확률 보상 기법 적용 후에는 약 3~4dB 이상만 되어도 정확한 생성다항식 추정이 가능한 것을 확인 할 수 있다. 여기서 결정 확률 변수 보상 기법 적용 전의 모듈에는 임계치를 0.65로 설정 하였고 적용 후의 모듈에는 임계치를 0.23으로 설정하였다. 이 임계치는 오류가 없는 데이터를 수신했을 때 항상 부호를 인식할 수 있는 임계치를 각각 시뮬레이션을 통해 구한 값이다. 따라서 결정 확률 보상 기법의 적용으로 인해 약 3dB의 부호 인식 및 생성다항식 추정 성능 개선 효과를 얻을 수 있다.

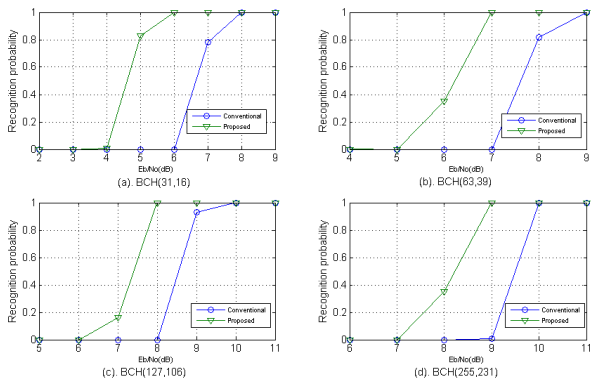

그림 6. BCH(31,16), BCH(63,39), BCH(127,106), BCH(255,231) 부호에 대한 확률보상기법 적용 전후의 부호 인식 확률
Fig 6. Recognition probability for BCH(31,16), BCH(63,39), BCH(127,106), BCH(255,231) code before and after using probability compensation method

그림 6은 다양한 BCH 부호에 대한 제안한 기법 적용 전후의 부호 인식 확률 비교 데이터이다. 그림과 같이 BCH 부호 길이가 31, 63, 127, 255의 다양한 경우에도 제안된 기법을 적용하였을 때 부호 인식 및 생성다항식 추정 성능 개선 효과를 확인할 수 있다. 따라서 일반적인 BCH 부호에 대해서도 결정 확률 보상 기법을 적용을 통해 부호 인식 확률의 향상을 얻을 수 있다.

Ⅳ. 결 론

본 논문에서는 파라미터가 알려지지 않은 미지의 데이터로부터 BCH 부호의 인식 및 생성 파라미터인 생성다항식을 추정하는 기법에 대해서 소개하였다. BCH 부호의 생성 파라미터를 추정하는 방법은 여러 가지가 존재하나 그중 한 방법인 순회부호의 특성을 이용한 방법을 소개하였다. 또한 시뮬레이션을 통해 분석이 가능함을 보였고 에러가 있는 데이터에 대해서도 확률적 접근방법을 이용하여 생성다항식 추정이 가능한 것을 보였다. 그리고 본 논문에서는 결정 확률 변수 보상 기법을 제안하였다. 확률 보상 기법은 생성다항식 추정 과정 중에서 보상할 확률 변수를 계산하여 보상하는 기법이다. BCH(15,11)에 대해 부호 인식 확률에 대한 시뮬레이션을 수행한 결과, 확률 변수 보상 기법을 적용하기 전에는 E_b/N_o가 6~7dB이상 되어야 정확하게 생성다항식을 추정하였지만 확률 변수 보상 기법 적용 후에는 3~4dB이상만 되어도 정확하게 추정되어 약 3dB의 성능 향상이 있음을 확인하였다. 그리고 BCH 부호 길이가 다른 다양한 부호에 대해서도 시뮬레이션을 통해 부호 인식 성능 향상을 확인하였다. 확률 보상 기법은 단순한 연산으로 구성되어 있기 때문에 생성다항식 추정과정에 복잡도가 크게 증가하지 않는다. 본 연구에서는 부호의 동기가 완료된 것으로 가정하였으나 본 논문에서의 기법이 실제적으로 사용되기 위해서는 부호 동기에 대한 연구가 필수적이다. 따라서 앞으로도 다양한 채널 부호의 복원 기법에 대한 연구와 더불어 부호 동기에 대한 연구도 같이 진행되어야 할 것이다.

References

[1] S. Lin and D. J. Costello Jr, *Error Control Coding*, Pearson Prentice Hall, 2004.

[2] R. H. Morelos-Zaragoza, *The Art of Error Correcting Coding*, John Wiley & Sons, 2007.

[3] J. Wang, Y. Yue and J. Yao, "Statistical recognition method of binary BCH Code", in *Proc. Scientific Research on Commun. and Netw.*, pp. 17-22, Feb. 2011.

[4] I. S. Kang, H. Lee, S. J. Han, C. S. Park, J. H. Soh, and Y. J. Song, "Reconstruction method for reed-muller codes using fast hadamard transform", in *Proc. ICACT 2011*, pp. 793-796, Feb. 2011.

[5] M. Cluzeau, "Block code reconstruction using iterative decoding techniques", in *Proc. Int. Symp. Inform. Theory (ISIT '06)*, pp. 2269-2273, July 2006.

[6] C. Chabot, "Recognition of a code in a noisy environment", in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 2211-2215, June 2007.

[7] M. Cluzeau and M. Finiasz, "Recovering a code's length and synchronization from a noisy intercepted bit stream", in *Proc. Int. Symp. Inform. Theory (ISIT '09)*, pp. 2737-2741, July 2009.

[8] Y. J. Song, *Coding Theory for Communication Engineering*, Infinity Books, 2008.

[9] H. Lee, C. S. Park, J. H. Lee, and Y. J. Song, "Reconstruction of BCH codes using probability compensation", in *Proc. APCC 2012*, pp. 591-594, Oct. 2012.

이 현 (Hyun Lee)

2010년 2월 금오공과대학교 전자공학과 학사

2012년 2월 금오공과대학교 전자공학과 석사

2011년~현재 LIG 넥스원 기술 6팀 연구원

<관심분야> 이동통신 시스템, 부호이론

박 철 순 (Cheol-sun Park)

1989년 2월 경기대학교 전자계산학과 학사
1991년 2월 인하대학교 전자계산공학과 석사
1991년~현재 국방과학연구소 선임연구원
1997년 전자계산 조직응용 기술사
2007년 충남대학교 정보통신공학과 박사
<관심분야> 신호처리, 통신응용

이 재 환 (Jae-hwan Lee)

2011년 2월 금오공과대학교 전자공학과 학사
2011년 2월~현재 금오공과대학교 전자공학과 석사과정
<관심분야> 이동통신 시스템, 부호 이론

송 영 준 (Young-joon Song)

1987년 2월 한양대학교 전자통신공학과 공학사
1994년 2월 한양대학교 전자통신공학과 공학석사
1999년 2월 한양대학교 전자통신공학과 공학박사
2006년 1월~2007년 1월 미국 하와이 주립대학교방문학자
2002년 3월~현재 금오공과대학교 전자공학부 부교수
<관심분야> 이동통신 시스템, 부호 이론