논문 17-42-12-08 The Journal of Korean Institute of Communications and Information Sciences '17-12 Vol.42 No.12
https://doi.org/10.7840/kics.2017.42.12.2270

BCH 부호의 유한체의 크기에 대한 암맹 판별 기법

권 순 희◆, 신 동 준°

Blind Detection Scheme for the Size of Galois Field of BCH Code

Soonhee Kwon◆, Dong-Joon Shin°

요 약

본 논문에서는 Chi-square goodness-of-fit 검정을 이용하여 BCH 부호가 정의된 유한체(Galois field) 크기를 암맹 판별할 수 있는 기법을 제안한다. 이진 대칭 채널의 다양한 채널 천이 확률(cross-over probability)에 따른 암맹 판별 성능을 시뮬레이션을 통하여 확인하고 제안된 기법의 유효성을 검증한다.

Key Words : BCH code, Blind detection, Galois field, Chi-square goodness-of-fit test, Galois field Fourier transform

ABSTRACT

In this paper, a blind detection scheme for the Galois field size of BCH code is proposed, which is based on Chi-square goodness-of-fit test. Through simulation, the performance of the proposed scheme is evaluated for various cross-over probability of the binary symmetric channel to confirm the validity of this scheme.

Ⅰ. 서 론

현대 디지털 통신 시스템에서는 채널에 의해 발생하는 오류를 정정하기 위한 오류정정부호의 사용이 필수적이다. 송신단과 수신단은 서로 약속된 오류정정부호를 사용하여 채널에 의해 발생하는 오류를 발견 또는 정정할 수 있다. 하지만 수신단이 송신단에서 사용한 오류정정부호의 파라미터를 알지 못한다면 데이터를 정확히 복호화(decoding) 할 수 없다. 이러한 경우 수신된 데이터만을 이용하여 송신단에서 사용한 오류정정부호의 파라미터를 찾아내야 한다. 특히, 이러한 상황은 미지의 적의 신호에서 정보를 알아내야 하는 군통신에서 매우 중요하다.

최근 들어, BCH 부호와 RS 부호와 같은 순회 부호의 파라미터를 모르는 경우 수신된 데이터만을 이용한 생성 다항식의 암맹 판별 기법 등이 연구되어 왔다[1-2]. 특히, 순회 부호는 유한체 푸리에 변환(Galois field Fourier transform, 이하 GFFT)을 하게 되면 유한체 상에서 공통근을 갖기 때문에, 수신된 데이터에 GFFT를 수행하여 송신단에서 부호화 할 때 사용한 생성다항식을 구할 수 있다[1]. 하지만 GFFT를 이용한 생성다항식의 암맹 판별 기법은 BCH 부호가 정의된 유한체 크기를 알고 있다고 가정하거나, BCH 부호 중 사용된 유한체의 크기와 확대체(extension field)의 크기가 같은 RS 부호로 가정하여 연구가 진행되어 왔다.

본 논문에서는 위와 같은 가정을 완화하여 이진 비트로 수신된 데이터만을 이용하여 BCH 부호의 유한체 크기를 암맹 판별할 수 있는 기법을 제안한다. 추정하고자 하는 유한체의 크기가 원래의 유한체 크기와 동일하지 않으면 수신된 부호어들의 GFFT 결과 값들이 랜덤하게 분포한다는 성질을 기반으로 확률 분포 검정 방법 중 널리 사용되는 Chi-square goodness-of-fit 검정을 이용한다. 그리고 시뮬레이션을 통하여 제안된 암맹 판별 기법의 성능을 확인한다.

Ⅱ. BCH 부호와 유한체의 크기 판별 기법

2.1 BCH 부호와 유한체

길이가 n이고 $2t$개의 오류를 정정할 수 있는 유한체 $GF(q)$ 상에서 정의된 BCH 부호는 다음과 같은 생성다항식 $g(x)$을 갖는다[3].

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

여기서 LCM은 최소공배수를 의미하며 α는 $GF(q)$의 확대체 $GF(q^l)$ 상의 원시 차수(order)가 n인 원소이다. 또한, b는 $(0, n)$의 임의의 자연수이고

※ 본 연구는 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호정보 특화연구센터 사업의 지원을 받아 수행되었음.
◆ First Author : Department of Electronic Engineering, Hanyang University, tnsgml1991@hanyang.ac.kr, 학생회원
° Corresponding Author : Department of Electronic Engineering, Hanyang University, djshin@hanyang.ac.kr, 종신회원
논문번호 : KICS2017-09-253, Received September 19, 2017; Revised November 1, 2017; Accepted November 15, 2017

$M_{\alpha^i}(x)$는 $GF(q^l)$상의 원소인 α^i의 최소 다항식(minimal polynomial)이다. 길이 n은 q^l-1의 약수이며 q값은 편의상 가장 많이 사용되는 2의 거듭제곱인 경우를 고려한다.

생성다항식은 $GF(q^l)$상의 α^b부터 α^{b+2t-1}까지 $2t$개의 모든 원소를 근으로 갖는다. BCH 부호의 부호어는 생성 다항식과 메시지 다항식의 곱으로 생성되므로 모든 부호어도 동일한 $2t$개의 원소를 근으로 갖는다. 이러한 특성을 기반으로 수신부호어에 GFFT를 하게 되면 $GF(q^l)$상의 α^b부터 α^{b+2t-1}에 대한 결과값은 0이 된다. 메시지 다항식 $m(x)$에 대한 부호어 다항식은 $c(x) = m(x)g(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$이고 α^i에 대한 GFFT 값은 $c(\alpha^i)$이 된다. 이러한 성질을 이용한 유한체 크기에 대한 암맹 판별 알고리즘을 다음과 같이 제안한다.

2.2 유한체 크기 암맹 판별 알고리즘

본 논문에서는 이진 대칭 채널(binary symmetric channel)을 통하여 M개의 부호어를 수신했다고 가정한다. 또한, 이진수로 변환된 부호어의 길이(mn)는 알고 있고(여기서 m은 BCH 부호가 정의된 $GF(q), q=2^m$의 m값임) 부호어의 동기가 완벽하다고 가정한다. 모든 부호어는 $GF(q^l)$상의 원소 α^b부터 α^{b+2t-1}에 대하여 GFFT 값이 0이라는 성질을 이용하여 송신단에서 사용한 BCH 부호의 유한체의 크기를 판별한다. 또한, 추정하고자 하는 유한체의 크기가 원래의 유한체의 크기와 다른 경우 GFFT 결과 값이 랜덤하게 나오는 성질을 이용하여 Chi-square goodness-of-fit 검정을 통한 판별 기법을 제안한다.

이진 대칭 채널을 통과하여 수신된 이진수로 표현된 M개의 부호어를 $r_j^{(2)}(x)$, $1 \leq j \leq M$, 로 정의하였을 때, 부호어의 길이에 대한 후보 $\hat{n}$을 mn의 약수 중 홀수인 수로 정하고 $\hat{m}=mn/\hat{n}$으로 정한다. 수신된 이진 부호어 $r_j^{(2)}(x)$를 $GF(2^{\hat{m}})$상의 원소로 변환하여 $r_j^{\hat{m}}(x)$로 만들고 $\hat{n}|(2^{\hat{m}\times\hat{l}}-1)$을 만족시키는 최소 $\hat{l}$ 값을 이용하여 확대체 $GF(2^{\hat{m}\times\hat{l}})$을 생성하고 각각의 $r_j^{\hat{m}}(x)$에 대한 GFFT를 하여 $C_j^{\hat{m}}(i) = r_j^{\hat{m}}(\beta_{\hat{m}}^i)$ 값을 구한다. 여기서 $\beta_{\hat{m}}$값은 $\alpha_{\hat{m}}^{(2^{\hat{m}\times\hat{l}}-1)/\hat{n}}$값과 동일하며 $\alpha_{\hat{m}}$값은 $GF(2^{\hat{m}\times\hat{l}})$상에서의 차수가 $\hat{n}$인 원소이다. 그런 후, i값에 따른 GFFT 결과 값들의 빈도수 $F_w^{\hat{m},i}$, $1 \leq w \leq \Gamma$,를 구한다. 여기서 Γ값은 아래에서 설명하는 $(2^{\hat{m}})^{rk(R_i^{\hat{m}})}$값과 동일하며 이는 $\beta_{\hat{m}}^i$에 대한 GFFT 결과 값으로 가질 수 있는 값들의 개수와 동일하다[1]. 자세히 설명하면, Chi-square goodness-of-fit 검정에서 사용될 평균값 $A_i^{\hat{m}}$는 $\beta_{\hat{m}}^i$의 랭크(rank)인 $rk(R_i^{\hat{m}})$에 의해 결정되며 랭크는 다음과 같이 계산한다.

첫째, $\alpha_{\hat{m}}$의 $GF(2^{\hat{m}})$상에서의 원시 다항식(primitive polynomial) $p^{\hat{m}}(x)$을 선택한다. 여기서 원시 다항식은 무엇을 선택해도 되고 다음의 과정을 모두 선택된 원시 다항식을 이용하여 수행한다.

둘째, 1, $\beta_{\hat{m}}^i$, $(\beta_{\hat{m}}^i)^2, \cdots$, $(\beta_{\hat{m}}^i)^s, \cdots$, $(\beta_{\hat{m}}^i)^{\hat{n}-1}$, $0 \leq i \leq \hat{n}-1$, 값들을 $p^{\hat{m}}(\alpha_{\hat{m}})$으로 나눈 나머지를 $GF(2^{\hat{m}})$상에서 정의된 계수들로 이루어진 벡터 $v_{i,s}^{\hat{m}}$, $0 \leq s \leq \hat{n}-1$,를 구한다. 그런 후, 각 행들이 $v_{i,s}^{\hat{m}}$로 이루어진 $\hat{n}\times\hat{l}$ 행렬 $R_i^{\hat{m}}$을 구성한다.

셋째, $GF(2^{\hat{m}})$상에서 정의된 $R_i^{\hat{m}}$의 랭크 $rk(R_i^{\hat{m}})$를 구한다. $rk(R_i^{\hat{m}})$은 $\beta_{\hat{m}}^i$의 랭크이며, $A_i^{\hat{m}} = M/(2^{\hat{m}})^{rk(R_i^{\hat{m}})}$이 된다. 이를 이용하여 Chi-square goodness-of-fit 검정의 통계값 $\chi_i^{\hat{m}}$을 다음과 같이 계산한다.

$$\chi_i^{\hat{m}} = \sum_{w=1}^{\Gamma} \frac{(F_w^{\hat{m},i} - A_i^{\hat{m}})^2}{A_i^{\hat{m}}} \tag{2}$$

또한, Chi-square goodness-of-fit 검정에서 사용되는 문턱값(threshold)은 $\chi_{i,th}^{\hat{m}} = \chi(1-v_{sig}, d_{free}^{\hat{m},i})$이며 $\chi(1-v_{sig}, d_{free}^{\hat{m},i})$는 자유도(degree of freedom)가 $d_{free}^{\hat{m},i}$이고 유의수준으로 v_{sig}를 갖는 카이제곱(Chi-square) 분포의 값이다. $d_{free}^{\hat{m},i} = (2^{\hat{m}})^{rk(R_i^{\hat{m}})}-1$이며 본 논문에서 0.05의 유의수준을 고려한다. 그런 후, $\chi_i^{\hat{m}} < \chi_{i,th}^{\hat{m}}$를 만족하면 주어진 데이터가 균등 분포(uniform distribution)를 따른다고 결정하며 그 외의 경우 균등 분포를 따르지 않는다고 결정한다. 추정하고자 하는 $GF(2^{\hat{m}})$가 실제 BCH 부호가 정의된 $GF(2^m)$과 동일한 경우 특정 i에 대하여 GFFT 값 중 0의 비중이 높아지게 되므로 균등 분포를 따르지 않게 된다. 따라서 모든 길이 후보 $\hat{n}$에 대하여 위와

알고리즘 1: 유한체 크기의 암맹 판별 기법

입력: 수신된 M개의 이진 표현 부호어 $r_j^{(2)}(x)$, (※ 이진 부호어의 길이$=mn$)

출력: 유한체 $GF(2^m)$의 지수 추정치 $\hat{m}$

1: for 모든 후보 $\hat{n}$에 대하여 do

2: $\hat{m}=mn/\hat{n}$

3: $\hat{l}$을 구함

4: 수신 부호어를 $r_j^{\hat{m}}(x)$로 모두 변환

5: for $\beta_{\hat{m}}^i$, $0 \le i \le \hat{n}-1$, do

6: $(\chi_i^{\hat{m}}/\chi_{i,th}^{\hat{m}})$ 값을 계산

7: if $(\chi_i^{\hat{m}}/\chi_{i,th}^{\hat{m}}) \ge 1$ then

8: 후보군에 $\hat{m}$값과 그에 대응되는 $(\chi_i^{\hat{m}}/\chi_{i,th}^{\hat{m}})$ 값을 같이 저장

9: end if

10: end for

11: end for

12: 후보군에 저장된 $(\chi_i^{\hat{m}}/\chi_{i,th}^{\hat{m}})$ 값 중 가장 큰 값에 해당하는 $\hat{m}$값 선택

13: $\hat{m}$ 값 출력

같은 계산법을 이용하여 Chi-square goodness-of-fit 검정을 실시 한 후 $(\chi_i^{\hat{m}}/\chi_{i,th}^{\hat{m}}) \ge 1$ 를 만족하는 $\hat{m}$값을 모두 구하여 $(\chi_i^{\hat{m}}/\chi_{i,th}^{\hat{m}})$ 값이 가장 큰 경우의 $\hat{m}$ 값을 BCH 부호가 정의된 $GF(2^m)$의 m값으로 결정한다. 제안하는 알고리즘의 개략도는 다음과 같다.

그림 1은 $n=21, m=2$인 BCH 부호, $n=21$, $m=3$인 BCH 부호, $n=63, m=1$인 BCH 부호에 대하여 각각 수신된 부호어의 개수가 $M=300$, $M=500$인 경우에 대해 제안된 암맹 판별 알고리즘의 시뮬레이션을 수행하여 성공 확률을 확인한 결과이다. 세 가지의 BCH 부호는 모두 $b=1$이고 $t=1$로 설정하였다. 이를 통하여 부호 길이가 길어지거나, 또는 길이가 같더라도 유한체의 크기가 커질수록 성능이 저하되지만 수신된 부호어의 개수가 많아질수록 성능이 좋아지는 것을 확인할 수 있었다.

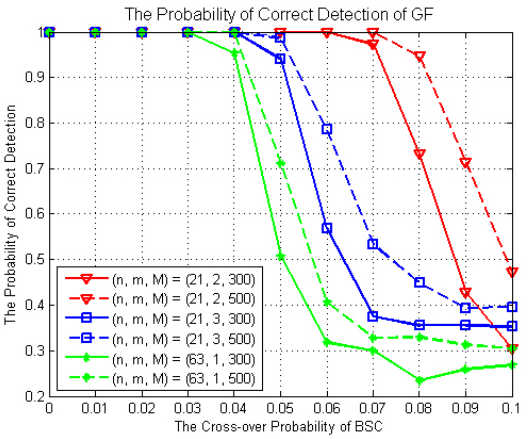

그림 1. 채널 천이 확률에 따른 유한체의 크기에 대한 판별 성공 확률.
Fig. 1. The probability of correct detection of the Galois field size for various cross-over probability of BSC.

Ⅲ. 결 론

본 논문에서는 이진 비트로 수신된 부호어들에 대한 GFFT 결과 값들의 빈도수를 이용하여 BCH 부호가 정의된 유한체를 암맹 판별할 수 있는 기법을 제안하였고 다양한 BCH 부호에 대한 컴퓨터 시뮬레이션을 통하여 본 기법의 성능을 확인하였다. 제안된 기법을 통하여 기존의 논문들에서 사용되었던 비현실적인 유한체 크기 정보를 알고 있다는 가정을 완화할 수 있다.

References

[1] G. Wu, B. Zhang, X. Wen, and D. Guo, "Blind recognition of BCH codes based on Galois field Fourier transform," in *Proc. 2015 Int. Conf. Wireless Commun. Sign. Process.*, pp. 1-4, Nanjing, China, Oct. 2015.

[2] H.-B. Chung, H.-S. Jang. W.-C. Cho, and C.-S. Park, "Reconstruction of linear cyclic codes," *J. KICS*, vol. 36, no. 10C, pp. 605-613, Oct. 2011.

[3] T. K. Moon, *Error Correction Coding: Mathematical methods and algorithms*, John Wiley & Sons Inc., 2005.