커버링 다항식을 이용한 골레이 부호의 연판정 복호

정회원 성 원 진*

Soft-Decision Decoding of the [23,12] Golay Code Using Covering Polynomials

Wonjin Sung* *Regular Member*

요 약

커버링 다항식을 이용한 복호는 오류 포착 복호의 확장된 형태로써, 순환 부호에 적용되어 간단하고도 효율적인 복호기 구현을 가능하게 한다. 커버링 다항식은 한계 거리 이상의 복호와 연판정 복호에도 사용될 수 있으며, 구현 복잡도는 사용되는 커버링 다항식의 개수에 비례하게 된다. 본 논문에서는 커버링 다항식을 이용한 연판정 복호 방법을 제시하고 이를 [23,12] 골레이 코드에 적용하였다. 적용을 위하여 새로운 커버링 다항식 집합을 일반화된 공식으로 유도하고, 이 집합이 골레이 부호를 비롯한 다수의 순환 부호에 효율적으로 활용될 수 있음을 보였다. 또한 제시된 방법을 사용한 복호기의 성능 평가 모의 실험을 수행하여 복잡도와 성능의 trade-off 관계를 보였다. 유도된 커버링 다항식을 사용한 골레이 부호의 연판정 복호 시, 최대 유사도 복호가 갖는 최적 오율과 비교하여 전체 실험 구간에서 0.2dB 이내의 성능을 보였으며, 유사한 성능을 갖는 Chase 알고리듬 2와 경판정 복호가 결합된 경우에 비해 복잡도가 감소함을 확인하였다.

ABSTRACT

The decoding method using covering polynomials is an extended form of error-trapping decoding, and is a simple and effective means to implement decoders for cyclic codes. Covering polynomials can be used for soft-decision decoding as well as for decoding beyond the bounded distance of the code. The implementation complexity is proportional to the number of covering polynomials employed. In this paper, the soft-decision decoding procedure using covering polynomials is described, and the procedure is applied to the [23,12] Golay code. A new set of covering polynomials is derived for the procedure, which is presented as a generalized closed-form solution. The set can be efficiently utilized for decoding a class of cyclic codes including the Golay code. Computer simulation of the described procedure is performed to show the trade-offs between the decoder performance and complexity. It is demonstrated that soft-decision decoding of the Golay code using the derived set of covering polynomials has less than 0.2dB deviation from the optimal performance of maximum-likelihood decoding, with a reduced complexity when compared to the Chase Algorithm 2 combined with hard-decision decoding that has nearly identical performance.

Ⅰ. 서 론

부호어(codeword)와 정보 데이터 비트의 길이가 각각 n비트와 k비트인 $[n,k]$ 순환 부호 (cyclic code)의 복호 방법 중 하나인 오류 포착 복호 (error-trapping decoding)는 연집 오류 (burst error)를 효율적으로 정정할 수 있는 방법으로, 신드롬 계산을 수행하는 쉬프트 레지스터 회로

* 서강대학교 전자공학과 디지털전송연구실 (wsung@sogang.ac.kr)
논문번호 : 020016-0115, 접수일자 : 2002년 1월 15일
※ 본 연구는 한국과학재단 목적기초연구 R01-2001-00542 지원으로 수행되었음.

를 사용하여 간단히 구현할 수 있다[1][2]. 오류 포착 복호를 사용하여 정정할 수 있는 오류 패턴 (error pattern)에는 오류가 없는 k개의 연속적인 비트가 존재하여야 하며, 이 때 연속적인 비트 위치는 오류 패턴의 양쪽 끝에서 순환적으로 이어지는 경우 (wrap-around case)를 포함한다. 일반적으로, 최대 s개까지의 오류 비트를 오류 포착 복호로 정정하기 위해서는 부호율(code rate) $R = k/n$ 이 $R < 1/s$ 를 만족하여야 하며[2], 이 조건을 만족하지 않는 경우에 대한 복호를 위해 커버링 다항식 (covering polynomial)을 사용하는 방법이 Kasami에 의해 제안되었다[3]. 커버링 다항식은 주어진 k개의 연속적인 비트 위치에서 존재하는 오류를 "커버"하는 역할을 하며, 복호 원리 및 절차는 많은 참고문헌에 설명되어 있는 바와 같다[1-4].

커버링 다항식에서 항의 개수는 부호율 R과 정정하려는 오류의 최대 개수 s에 의해 결정되며, $R < 2/s$ 인 경우는 단항식(monomial)만이, $R \geq 2/s$ 인 경우는 단항식 및 이항식(binomial) 이상이 필요하게 된다. 커버링 다항식 복호기의 복잡도는 사용하는 다항식의 개수에 비례하므로, 주어진 오류 개수를 모두 정정할 수 있는 최소 개수의 다항식 집합을 사용하는 것이 중요하다. 부호 파라미터 n, k, s에 대한 최소 다항식 집합의 일반해는 알려져 있지 않으며[4], 제한된 경우에 대한 다항식 집합이 연구되어 왔다. Kasami의 논문[3]에서는 몇몇 부호에 대한 커버링 다항식 집합 구성 예가 주어졌으며, 단항식이 사용되는 경우 ($R < 2/s$)에 대해 단항식 집합 크기의 상한값이 제시되었다[5]. 최소 단항식 집합은 $s = 2$와 $s = 3$일 때[6]와 $s < 9$을 만족하는 모든 s에 적용되는 경우[7]에 대해 연구되었다. 이항식 이상이 필요한 경우 ($R \geq 2/s$)에 대해서는 $s = 3$일 때의 최소 다항식 집합이 연구되었다[8].

커버링 다항식을 이용한 복호의 장점 중에는 부호의 한계 거리 (bounded distance) 이상의 복호가 가능하다는 점과 연판정 복호 (soft-decision decoding)로의 확장이 용이하다는 점이 있다. 커버링 다항식 복호가 골레이 부호를 비롯한 순환 부호의 경판정 복호 (hard-decision decoding) 방법으로 적용된 사례는 많으나, 연판정 복호 절차 및 수행 시 성능 평가, 또한 연판정 복호를 위한 커버링 다항식 집합에 대한 보고는 미미한 편이다. 본 논문에서는 커버링 다항식을 이용한 연판정 복호를 골레이 부호에 적용하고, 모의 실험을 통한 복호 성능 평가를 하였다. 커버링 다항식 개수의 변화에 따른 성능 변화를 분석하고, 최대 유사도 복호 (maximum-likelihood decoding) 성능과의 비교를 수행하였다. 특히 정정하려는 오류의 개수가 $s = 4$이고 $R \geq 2/s$의 부호율을 갖는 경우에 요구되는 최소 다항식 집합을 일반화된 형태의 공식으로 유도하고 집합의 최적성을 평가하였으며, 유도된 공식이 골레이 부호의 연판정 복호를 비롯한 다수의 순환부호의 복호에 적용됨을 보였다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 커버링 다항식 복호 절차 및 연판정 복호 방법을 설명하고, Ⅲ장에서는 새로운 다항식 집합을 제시하고 집합의 필요충분조건을 분석적으로 증명하였다. 제시된 복호 방법 및 다항식 집합을 사용하여 얻어지는 성능 평가 결과를 Ⅳ장에서 보이고, Ⅴ장에서 논문의 결론을 맺는다.

Ⅱ. 커버링 다항식을 이용한 복호

1. 구간 벡터와 커버링 다항식

길이 n을 갖는 부호어의 전송과정에서 발생하는 오류 패턴은 0과 1로 구성된 원소 n개로 이루어진 벡터로써, 0은 오류가 없는 비트를, 1은 오류가 발생한 비트 위치를 나타낸다. 길이 $n = 9$를 갖는 오류 패턴의 한 예인 [001100100]의 경우 첫 번째와 두 번째 오류 비트 사이의 거리는 1, 두 번째와 세 번째 오류 비트 사이의 거리는 3, 세 번째와 첫 번째 오류 비트 사이의 순환적 거리는 5이다. 이 때 오류 비트 사이의 구간 거리를 나타내는 새로운 벡터 [1,3,5]를 "구간 패턴"라 부르기로 하고, 구간 패턴 내의 원소들을 순환적으로 이동한 형태도 동일한 구간 패턴으로 간주한다. 즉 위의 예에서 [1,3,5], [3,5,1], [5,1,3]은 모두 동일한 구간 패턴이다. 일반적으로 오류 비트의 개수가 s인 오류 패턴은 s개의 원소를 갖는 구간 패턴 $[u_1, u_2, \ldots, u_s]$로 나타내어지고, 구간 패턴 원소 값들의 합은 오류 패턴의 길이 n과 동일하게 된다. 단일 오류의 경우 구간 패턴은 [n]이 된다.

커버링 다항식은 최대 차수가 k인 다항식으로써, 각 항의 지수는 다항식이 커버하는 오류 비트의 위치를 나타내게 된다. 그림 1에서 비트 인덱스 1,2,...,k는 부호어의 정보 비트 (information bits)를, k+1,...,n은 패리티 비트 (parity bits)를 표시하고, 단

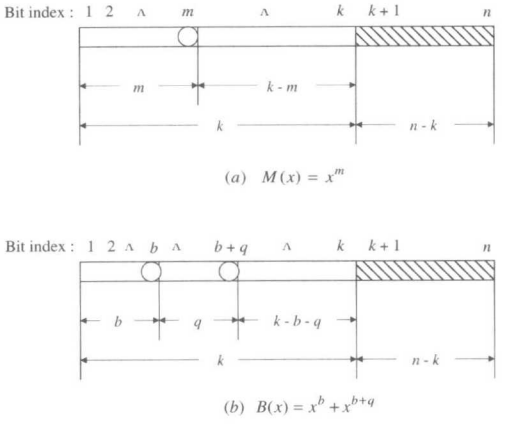

그림 1. [n,k] 순환 부호에 사용되는 커버링 다항식: (a) 단항식 (b) 이항식

항식을 나타내는 그림 1(a)의 $M(x)=x^m$은 m번째 정보 비트에 위치한다. 그림 1(b)에 표시된 이항식 $B(x)=x^b+x^{b+q}$의 두 항은 b번째와 $b+q$번째 정보 비트에 위치하고, 두 항 사이의 거리 q를 이항식의 "분리간격"이라 부른다.

구간 패턴 $[u_1, u_2, \ldots, u_s]$에서 $u_i \geq m$과 $u_{i+1} \geq k+1-m$의 조건을 만족하는 연속된 두 원소 (u_i, u_{i+1})이 존재할 때 단항식 x^m이 그 구간 패턴을 커버한다고 말하고, 이 때 연속된 두 원소는 순환적으로 연속된 (u_s, u_1)을 포함한다. 또한 $u_i \geq b$, $u_{i+1}=q$, $u_{i+2} \geq k+1-b-q$의 조건을 만족하는 연속된 세 원소 (u_i, u_{i+1}, u_{i+2})가 존재할 때 이항식 $B(x)=x^b+x^{b+q}$이 그 구간 패턴을 커버한다고 말하고, 이 때 연속된 세 원소는 순환적으로 연속된 (u_{s-1}, u_s, u_1)과 (u_s, u_1, u_2)를 포함한다. 구간 패턴을 커버하는 커버링 다항식의 예를 그림 2에 나타내었다. 그림 2(a)에서는 단항식 x^3이 구간 패턴 [5,1,3]을 커버함을 도시하였다. 세 개의 오류 비트 중 두 개는 패러티 비트 위치에 있고 한 개는 단항식에 의해 커버되었다. 오류 비트의 순환적 이동 (cyclic shift)을 통해 같은 구간 패턴이 이항식 $x+x^4$에 의해서도 커버될 수 있음을 그림 2(b)에서 나타내었다. 일반적으로 a 개의 항을 갖는 커버링 다항식이 s ($>a$) 개의 원소를 갖는 구간 패턴을 커버함을 다음과 같이 정의할 수 있다.

정의: 커버링 다항식 $Q(x)=x^{l_1}+x^{l_2}+\ldots+x^{l_a}$ $(1 \leq l_1 < l_2 < \ldots < l_a \leq k)$가 주어졌을 때, 구간 패턴

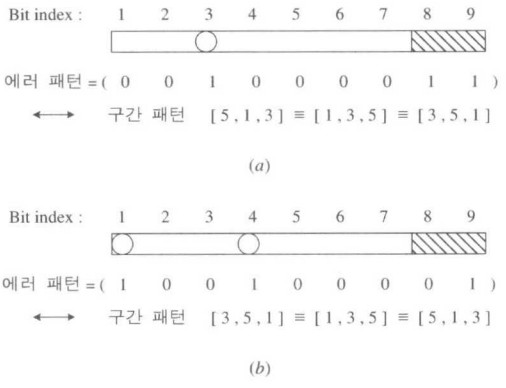

그림 2. [9,7] 부호에서 구간 패턴을 커버하는 커버링 다항식의 예

$[u_1, u_2, \ldots, u_s]$에서 $a+1$개의 연속된 (또는 순환적으로 연속된) 원소 $(u_i, u_{i+1}, \ldots, u_{i+a})$가 $u_i \geq l_1$, $u_{i+1}=l_2-l_1$, $u_{i+2}=l_3-l_2$, ..., $u_{i+a-1}=l_a-l_{a-1}$, $u_{i+a} \geq k+1-l_a$의 조건을 모두 만족하면, $Q(x)$가 그 구간 패턴을 커버한다고 말한다. (이때 순환적으로 연속된 경우 구간 패턴의 원소 u_{i+j}, $i \in \{1,2,\ldots,s\}$, $j \in \{1,2,\ldots,a\}$의 표기에서 $i+j>s$이면 $u_{i+j}=u_{i+j-s}$를 의미한다.)

2. 경판정 복호 절차

순환 부호의 전송 중 발생한 s개의 오류를 정정하기 위해서는 s개의 원소를 갖는 모든 구간 패턴들이 적어도 하나의 다항식에 의해 커버되도록 다항식 집합을 구성하여야 한다. 구간 패턴 중 최대 원소의 크기가 $k+1$ 이상인 경우는 커버링 다항식 0에 의해서, 즉 커버링 다항식을 사용하지 않고 커버되며, 이는 오류 포착 복호에서 정정할 수 있는 구간 패턴에 해당한다. 적절히 구성된 커버링 다항식 집합을 $\{Q_0(x), Q_1(x), \ldots, Q_N(x)\}$으로 나타낼 때, 복호 절차를 요약하면 아래와 같다. 아래에서 $r(x)$는 수신된 비트 열을 다항식으로 나타낸 것이고, $wt[\cdot]$의 표기는 주어진 다항식의 해밍 무게 (Hamming weight), 즉 다항식의 항 수를 의미한다.

(1) 생성 다항식 $g(x)$를 이용하여 각 커버링 다항식에 대해 $z_j(x)=x^{n-k-1}Q_j(x) \bmod g(x)$ $(j=0,1,\ldots,N)$를 미리 계산하여 저장한다.

(2) 수신 다항식 $r(x)$를 i번 순환적 이동시킨 $r^i(x)$의 신드롬 $s^i(x)=r^i(x) \bmod g(x)$를 $i=0,1,\ldots,n-1$에 대해 구하고 해밍 무게

$wt[s^i(x)+z_0(x)]+wt[Q_0(x)]$를 계산한다.

(3) 위 (2)번 과정을 커버링 다항식 $Q_j(x)$, $j=0,1,\ldots,N$에 대해 수행한 뒤 해밍 무게 $wt[s^i(x)+z_j(x)]+wt[Q_j(x)]$를 최소화하는 i,j를 찾는다.

(4) 최소화하는 $i=i_1, j=j_1$으로 결정되는 다항식 $s^{i_1}(x)+z_{j_1}(x)+x^{n-k-1}Q_{j_1}(x)$를 i_1번 역방향으로 순환적 이동시킴으로써 오류 다항식 $e(x)$와 복호된 다항식 $\hat{c}(x)=r(x)+e(x)$를 얻는다.

3. 연판정 복호 절차

일반적으로 연판정 복호는 경판정 복호와 비교하여 더 많은 수의 경판정 오류를 정정할 수 있으며, 따라서 커버링 다항식을 이용하여 연판정 복호를 수행할 때는 정정 오류의 개수인 s의 값이 커지게 되고 요구되는 커버링 다항식의 개수 N도 증가한다. 연판정 복호 절차는 앞에서 설명된 경판정 복호 절차와 매우 유사하나, 해밍 무게 대신 Euclidean 거리가 복호 메트릭(metric)으로 사용되는 점이 가장 큰 차이이다. 연판정 복호는 오류 포착 복호에 적용된 바 있으며[9], 이를 커버링 다항식을 이용한 복호에도 일반화하여 적용할 수 있다. 연판정 계수를 갖는 수신 다항식 $\tilde{r}(x)$는 양자화 과정을 거쳐 경판정 계수 (0 또는 1)를 갖는 수신 다항식 $r(x)$로 먼저 변환된다. 또한 $\tilde{r}^j(x)$와 $r^i(x)$는 각각 $\tilde{r}(x)$와 $r(x)$의 계수를 i번씩 순환적 이동하여 얻어진 다항식을 의미한다.

비트 0과 비트 1이 각각 +1과 -1을 이용한 BPSK 변조를 통해 가우시안 잡음 채널로 전송되는 경우, $\tilde{r}(x)$의 계수들로 이루어지는 벡터는 $\tilde{\boldsymbol{r}}=[\tilde{r}_0,\tilde{r}_1,\ldots,\tilde{r}_{n-1}]$로 표현이 되고, 각각의 계수는 모든 실수 구간에서의 값을 갖는다. 경판정 수신 다항식 $r(x)$의 계수들로 이루어지는 벡터 $\boldsymbol{r}=[r_0,r_1,\ldots,r_{n-1}]$에서 각각의 계수는 $\tilde{r}_i>0$일 때 $r_i=0$, 또 $\tilde{r}_i<0$일 때 $r_i=1$로 양자화된 값들이다. 두 다항식 $\tilde{r}(x)$와 $r(x)$ 간의 Euclidean 거리는

$$\mu[\tilde{r}(x),r(x)]=\sum_{j=0}^{n-1}|\tilde{r}_j-(1-2r_j)|^2$$

로 정의되고, 여기서 $1-2r_j$는 +1 또는 -1의 값을 갖는다. 수신다항식의 순환적 이동 형태인 $\tilde{r}^j(x)$와 아래 복호 절차에서 정의된 이진 계수를 갖는 다항식 $r^i(x)+e_j^i(x)$ 간의 Euclidean 거리도 유사하게 계산될 수 있다. 즉 $\tilde{r}^j(x)$의 계수로 이루어진 벡터 $\tilde{\boldsymbol{r}}^j=[\tilde{r}_0^j,\tilde{r}_1^j,\ldots,\tilde{r}_{n-1}^j]$와 $r^i(x)+e_j^i(x)$의 이진 계수로 이루어진 벡터 $\boldsymbol{b}=[b_0,b_1,\ldots,b_{n-1}]$가 주어졌을 때, 두 다항식 $\tilde{r}^j(x)$와 $r^i(x)+e_j^i(x)$ 간의 Euclidean 거리는

$$\mu[\tilde{r}^j(x),r^i(x)+e_j^i(x)]=\sum_{j=0}^{n-1}|\tilde{r}_j-(1-2b_j)|^2$$

를 이용하여 계산된다. 연판정 복호 절차는 다음과 같다.

(1) $z_j(x)=x^{n-k-1}Q_j(x) \bmod g(x)$ $(j=0,1,\ldots,N)$를 미리 계산하여 저장한다.

(2) 양자화 된 수신 다항식 $r(x)$를 i번 순환적 이동시킨 $r^i(x)$, $i=0,1,\ldots,n-1$에 대해 $e_0^i(x)=s^i(x)+z_0(x)+x^{n-k-1}Q_0(x)$를 구하고 Euclidean 거리 $\mu[\tilde{r}^j(x),r^i(x)+e_0^i(x)]$를 계산한다.

(3) 위 (2)번 과정을 커버링 다항식 $Q_j(x)$, $j=0,1,\ldots,N$에 대해 수행하여 $e_j^i(x)=s^i(x)+z_j(x)+x^{n-k-1}Q_j(x)$를 구하고, Euclidean 거리 $\mu[\tilde{r}^j(x),r^i(x)+e_j^i(x)]$를 최소화하는 i,j를 찾는다.

(4) 최소화하는 $i=i_1, j=j_1$으로 결정되는 다항식 $e_{j_1}^{i_1}(x)=s^{i_1}(x)+z_{j_1}(x)+x^{n-k-1}Q_{j_1}(x)$를 i_1번 역방향으로 순환적 이동시킴으로써 오류 다항식 $e(x)$와 복호된 다항식 $\hat{c}(x)=r(x)+e(x)$를 얻는다.

[23,12] 골레이 부호의 경판정 복호의 경우 $s=3$개의 오류를 정정하게 되며, 이 때 $R=12/23<2/s$의 조건이 만족되므로 단항식으로 구성된 커버링 다항식 집합으로 모든 구간 패턴을 커버하는 것이 가능하다. 골레이 부호의 경판정 복호를 위한 최적 커버링 다항식 집합은 2개의 단항식이 포함된 $\{Q_0(x),Q_1(x),Q_2(x)\}=\{0,x^6,x^7\}$이며[3], 최적 집합의 구성은 유일하지 않고 다수가 존재한다[7]. 연판정 복호의 경우는 경판정 복호에 사용되는 커버

링 다항식과 동일한 집합을 사용할 수도 있으나, 복호 성능의 향상을 위해서는 s = 4개 이상의 경판정 오류를 커버하는 커버링 다항식이 사용되어야 한다. s = 4의 경우 $R \geq 2/s$ 이므로 이항식이 포함된 집합이 필요하며, 이 조건을 만족하는 집합은 알려져 있지 않다. 다음 장에서는 골레이 부호의 연판정 복호에 사용될 수 있는 커버링 다항식 집합을 유도하고, 복호에 적용한 성능 평가 결과를 Ⅴ장에서 보인다.

Ⅲ. 커버링 다항식 집합의 유도

정리 1: $k=\lceil n/2 \rceil$를 만족하는 $[n,k]$ 순환 부호에서 s = 4개의 원소를 가지는 모든 구간 패턴은 커버링 다항식 집합 $\{0, x^{\lceil (k+1)/2 \rceil}, x(1+x), x(1+x^2), \ldots, x(1+x^{\lceil (k+1)/2 \rceil -1})\}$에 의해 커버된다.

증명: 제시된 다항식 집합에 의해 커버되지 않는 구간 패턴 $[u_1, u_2, u_3, u_4]$이 존재한다고 가정하여 보자. 일반화에 대한 오류 없이 (without loss of generality) 구간 패턴 $[u_1, u_2, u_3, u_4]$에서 최대값을 갖는 원소를 u_2라 하면, 아래의 보조정리 1 로부터 $u_2 \geq \lfloor (k+1)/2 \rfloor$의 조건이 성립한다. 또한 아래의 보조정리 2 로부터, 연속된 두 원소 (u_1, u_2)는 $u_1+u_2 \leq k-1$를 만족하여야 한다. 연속된 두 원소 (u_2, u_3)의 경우, 만일 $u_3 \geq \lfloor (k+1)/2 \rfloor$, 즉 $u_3 \geq k+1-\lceil (k+1)/2 \rceil$이면 단항식 $x^{\lceil (k+1)/2 \rceil}$에 의해 커버될 수 있으므로 $u_3 \leq \lfloor (k+1)/2 \rfloor -1$의 조건이 만족되어야 한다. 원소 u_4를 두 가지 구간으로 나누어 고려할 때, 첫 번째로 $u_4 \leq \lfloor (k+1)/2 \rfloor -1$이면 u_3의 조건과 결합하여 $u_3+u_4 \leq k-1$가 된다. 두 번째로 $u_4 \geq \lfloor (k+1)/2 \rfloor$이면 보조정리 2 로부터 $u_3+u_4 \leq k-1$이 되므로, 연속된 두 원소 (u_3, u_4)는 항상 $u_3+u_4 \leq k-1$의 조건을 만족한다. 따라서 모든 원소의 합은

$$n=(u_1+u_2)+(u_3+u_4) \leq 2(k-1) \qquad (1)$$

이 되고, $k=\lceil n/2 \rceil < n/2+1$의 조건과 부등식 (1)을 결합하면 $n \leq 2(k-1) < n$ 의 모순이 도출된다. 즉 커버되지 않는 구간 패턴이 존재한다는 가정은 오류이고, 제시된 다항식 집합이 4개의 원소를 가지는 모든 구간 패턴을 커버함을 알 수 있다. □

보조정리 1: $k=\lceil n/2 \rceil$일 때 구간 패턴 $[u_1, u_2, u_3, u_4]$의 최대 원소 $u_{\max}$는 $u_{\max} \geq \lfloor (k+1)/2 \rfloor$를 만족한다.

증명: 최대 원소가 $u_{\max} \leq \lfloor (k+1)/2 \rfloor -1$ 라고 가정하면, 모든 원소의 합은

$$\begin{aligned} n &= u_1+u_2+u_3+u_4 \\ &\leq 4\{\lfloor (k+1)/2 \rfloor -1\} = 2(k+1-\delta_k)-4 \end{aligned}$$

의 조건이 성립하고, δ_k는 k가 짝수일 때는 1, 홀수일 때는 0의 값을 갖는다. 또한 n이 짝수일 때는 0, 홀수일 때는 1의 값을 갖는 δ_n을 사용하여 $k=\lceil n/2 \rceil = (n+\delta_n)/2$로 표현할 수 있으므로, 위의 원소 합에 대한 관계식은

$$n \leq n-2+\delta_n-2\delta_k \leq n-1$$

이 된다. 이는 명백한 모순이므로, 최대 원소가 $u_{\max} \leq \lfloor (k+1)/2 \rfloor -1$이라는 가정은 오류이고 따라서 $u_{\max} \geq \lfloor (k+1)/2 \rfloor$이다. □

보조정리 2: 정리 1의 다항식 집합에 의해 커버되지 않는 구간 패턴 $[u_1, u_2, u_3, u_4]$의 연속된 두 원소 (u_i, u_{i+1})에서 $u_{i+1} \geq \lfloor (k+1)/2 \rfloor$일 때, $u_i+u_{i+1} \leq k-1$의 조건이 성립한다.

증명: $u_i \geq \lceil (k+1)/2 \rceil$이면 (u_i, u_{i+1})이 단항식 $x^{\lceil (k+1)/2 \rceil}$에 의해 커버되므로 $u_i \leq \lceil (k+1)/2 \rceil -1$의 조건이 만족되어야 한다. $u_i=j$, $j=1,2,\ldots,\lceil (k+1)/2 \rceil -1$일 때 u_i는 이항식 $x(1+x^j)$의 분리간격과 일치하고, 연속된 세 원소 (u_{i-1}, u_i, u_{i+1})가 이항식 $x(1+x^j)$에 의해 커버되지 않기 위해서는 $u_{i+1} \leq k-j-1$의 조건이 성립하여야 하므로, 가능한 모든 u_i 값에 대해 $u_i+u_{i+1} \leq k-1$임을 알 수 있다. □

정리 2: 정리 1의 커버링 다항식 집합은 $[n,k]$ 순환 부호에서 $s \leq 4$개의 원소를 가지는 모든 구간 패턴을 커버한다.

증명: 원소가 1개인 모든 구간 패턴은 다항식 0에 의해, 원소가 2개인 모든 구간 패턴은 다항식 0 또는 단항식 $x^{\lceil (k+1)/2 \rceil}$에 의해 커버된다. 제시된

다항식 집합에 의해 커버되지 않는 원소가 3개인 구간 패턴 $[u_1, u_2, u_3]$가 존재한다고 가정하고 최대값을 갖는 원소를 u_2라 하면, 정리 1의 증명에서와 마찬가지 방법으로 $u_1+u_2 \le k-1$와 $u_3 \le \lfloor (k+1)/2 \rfloor -1$의 조건이 만족되어야 함을 보일 수 있다. 이 때 세 원소의 합은

$$n = u_1+u_2+u_3 \le k-1+\lfloor (k+1)/2 \rfloor -1 \le \frac{3}{2}(k-1) < \frac{3}{4}n$$

이 되고 이는 모순이다. 따라서 정리 1의 커버링 다항식 집합은 원소의 개수가 s = 1,2,3,4개인 모든 구간 패턴을 커버한다. □

정리 3: 정리 1의 커버링 다항식 집합은 $k=n/2$를 만족하는 $[n,k]$ 순환 부호에서 $s \le 4$개의 원소를 가지는 모든 구간 패턴을 커버하는 단항식과 이항식으로 구성된 집합 중 최소 집합이다.

증명: 정리 1에서 $k=\lceil n/2 \rceil$의 조건은 n이 짝수인 경우 $k=n/2$가 되고, $\lceil (k+1)/2 \rceil -1$개의 구간 패턴 $[k-j, j, k-j, j]$, $j=1,2,\ldots, \lceil (k+1)/2 \rceil -1$ 이 존재한다. 이들 구간 패턴은 연속한 두 원소의 합이 항상 k 이므로 단항식으로는 커버되지 않으며, 각각의 구간 패턴은 분리간격이 j 또는 $k-j$ 인 이항식에 의해서만 커버된다. 따라서 적어도 $\lceil (k+1)/2 \rceil -1$ 개의 이항식이 필요하게 된다. 두 번째로 고려되는 $k-2$개의 구간 패턴은 $[k, j, 1, k-j-1]$, $j=1,2,\ldots, k-2$로써, 추가로 한 개 이상의 단항식을 사용하여 이들 구간 패턴을 커버하는 경우 사용하는 다항식의 총 개수는 적어도 $\lceil (k+1)/2 \rceil$이 된다. 만일 단항식이 사용되지 않는다면 각각의 구간패턴은 이항식 $x^{k-j}(1+x^j)$ 또는 $x(1+x^{k-j-1})$에 의해 커버되고, 총 $k-2$ 개의 이항식이 필요하게 된다. ($u_2+u_3+u_4 \le k$ 이므로 분리간격이 1인 이항식은 사용될 수 없다.) $k > 4$의 조건하에서 $k-2 > \lceil (k+1)/2 \rceil -1$ 이므로, 필요한 이항식의 개수는 $\lceil (k+1)/2 \rceil$ 이상이 된다. 즉 두 번째로 고려된 구간 패턴을 커버하기 위해 단항식을 사용하는 경우와 이항식을 사용하는 경우 공히, 필요한 다항식의 총 개수는 적어도 $\lceil (k+1)/2 \rceil$ 이며, 이 수는 정리 1에서 제시된 커버링 다항식 집합에서 단항식과 이항식 개수의 합과 일치한다. □

정리 1에서 제시된 다항식 집합은 다양한 부호의 커버링 다항식 복호에 적용될 수 있다. [n,k]-d 가 최소 거리 (minimum distance)가 d인 [n,k] 부호를 나타낼 때, 한계거리 t = 3인 [23,12]-7, [31,16]-7, [45,23]-7 순환 부호, 한계거리 t = 4인 [33,12]-10, [41,21]-9, [51,26]-10 순환 부호, 한계거리 t = 5인 [47,24]-11, [63,32]-12 순환 부호 등에서 4개까지의 오류를 정정하는 경우가 적용 예이다. 제시된 집합이 4개의 오류뿐 아니라 그 이하의 오류 개수도 정정할 수 있음은 정리 2에서 보인 바와 같다. 정리 3에서는 짝수인 n에 대해 제시된 집합이 최적 집합임을 보였다. 홀수 n을 포함한 경우의 최적성 증명은 어려운 문제로 보이나, 제시된 집합은 모든 경우에 대해 최적일 것으로 추론(conjecture)된다. 실제로 컴퓨터 탐색(search)을 통해 조사해 본 결과, 부호어의 길이가 n $\le$ 41을 만족하는 모든 순환 부호의 경우에 대해 최적임을 확인하였다. 골레이 부호를 비롯한 순환 부호에서 사용할 수 있는 커버링 다항식 집합의 예는 다음과 같다.

적용 예: [23,12]-7 골레이 부호에서 원소의 개수가 4개까지의 모든 구간 패턴을 커버하는 최적 커버링 다항식 집합은

$$\{0, x^7, x(1+x), x(1+x^2), \ldots, x(1+x^6)\}$$

으로 주어진다. [31,16]-7 BCH 부호의 경우 집합

$$\{0, x^9, x(1+x), x(1+x^2), \ldots, x(1+x^8)\}$$

또한 [41,21]-9 순환 부호의 경우 집합

$$\{0, x^{11}, x(1+x), x(1+x^2), \ldots, x(1+x^{10})\}$$

이 원소 개수 4개까지의 모든 구간 패턴을 커버하는 최적 커버링 다항식 집합이다. □

위 적용 예 중 [41,21]-9 순환 부호의 한계거리 복호기 구현을 위한 커버링 다항식 집합은 [3]에서 제시된 바 있으며 총 14개의 다항식을 포함하고 있다. 최적 집합은 위의 12개의 다항식으로 이루어진 집합이다.

Ⅳ. 골레이 부호의 복호

커버링 다항식을 사용한 골레이 부호의 경판정 및 연판정 복호기를 구현하고 성능 평가를 수행하였다. AWGN 채널에서 BPSK 변조를 이용하여 모의 실험으로 얻어지는 비트 오율 (BER)과 부호어 오율 (WER)을 비트 신호 대 잡음비 E_b/N_0의 함

수로 구하였다. 경판정 복호의 경우 Ⅱ장에서 언급된 바와 같이 3개까지의 오류 정정을 위해 3개의 다항식이 사용하여 성능 평가를 하였으며 그 결과를 그림 1에 도시하였다. 골레이 부호는 한계 거리와 커버링 반경 (covering radius)이 동일한 perfect code이므로 그 이상의 다항식을 추가로 사용하는 것이 경판정 복호 성능 향상을 가져오지는 않는다. 같은 3개의 다항식을 사용하여 연판정 복호를 하는 경우 (그림에서 soft-decision decoding s = 3, 이하 SD3), 1e-3 BER 값에서 약 0.6dB 성능 이득을 보였다. 연판정 복호의 성능 향상을 위해서는 더 많은 수의 경판정 오류 개수 (또는 구간 패턴의 원소 개수)를 커버할 수 있는 다항식 집합이 필요하며, Ⅲ장에서 유도된 8개의 다항식으로 이루어진 집합을 적용한 결과 (그림에서 soft-decision decoding s = 4, 이하 SD4), 1e-3 BER에서 약 0.8dB의 추가 성능 이득, 즉 경판정 복호 시와 비교할 때 약 1.4dB의 이득이 발생하였다. 연판정 복호 시 얻어지는 성능의 하한 값인 최대 유사도 복호의 성능을 그림 1에 도시하고 비교하였다. 본 실험에서의 최대 유사도 복호는 복잡도를 고려하지 않은 성능 비교만을 위해 1024개의 모든 부호어와 수신 다항식 계수의 Euclidean 거리를 계산하고 최소 거리를 갖는 부호어를 선택하는 방법을 사용하였다. 비교 결과 8개 다항식을 이용한 연판정 복호는 최적 성능에서 0.2dB 이내의 차이를 보였으며, 따라서 커버링 다항식 복호의 특징인 간단한 복호 과정을 통하여 연판정 복호 최적 성능에 매우 가까운 성능을 얻음을 알 수 있다. s = 4 보다 큰 개수의 오류를 커버하는 다항식 집합을 사용하는 경우, 필요한 다항식의 수는 빠르게 증가하는 반면 얻을 수 있는 성능 이득은 크지 않게 된다.

그림 2에서는 각 경우에 대한 WER을 도시하였고 유사한 성능 비교 결과를 얻었다. 또한 연판정 복호를 위해 널리 사용되는 Chase 알고리듬[10][11]의 성능을 그림 2에서 나타내었다. 잘 알려진 바와 같이 Chase 알고리듬 1, 2, 3은 $[n,k]$-d 인 부호에 대해 각각 $\binom{n}{\lfloor d/2 \rfloor}$, $2^{\lfloor d/2 \rfloor}$, $\lfloor (d/2)+1 \rfloor$ 개의 테스트 패턴을 사용하며, 테스트 패턴 개수만큼의 경판정 복호를 반복하게 된다. 일반적으로 알고리듬 1은 알고리듬 2와 비교해 성능 이득이 미미한 반면 계산수가 많음으로 인해 널리 사용되지 않는다. 골레이 부호의 경우 Chase 알고리듬 2 (CA2)는 8번의 경판정 복호가 필요하며, 정확한 복잡도는 사용하는 경판정 복호기의 복잡도에 의해 결정되게 된다. 경판정 복호를 위해 커버링 다항식 복호가 사용되는 경우, 총 8×3 = 24개의 커버링 다항식에 대해 복호 절차가 수행되는 것과 동일한 계산량을 갖게된다. 그림 2에서의 나타낸 Chase 알고리듬 성능은 [12]의 결과를 사용한 것이고, 그림에서 보여지는 바와 같이 CA2와 SD4의 성능은 매우 유사하다. SD4의 경우 8개의 커버링 다항식에 대해 복호 절차가 수행되는 복잡도를 가지며, 사용되는 다항식 개수의 측면에서 감소된 복잡도를 가지게 된다. Chase 알고리듬 3 (CA3)는 4번의 경판정 복호가

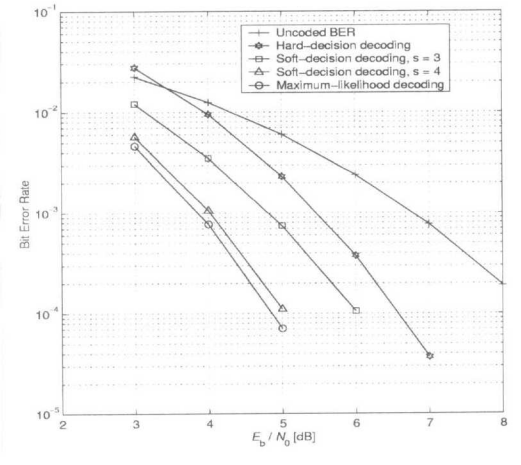

그림 3. 커버링 다항식 복호를 이용한 골레이 부호의 Bit Error Rate

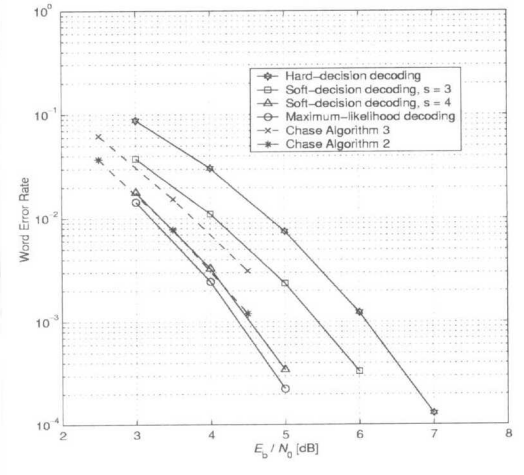

그림 4. 커버링 다항식 복호를 이용한 골레이 부호의 Word Error Rate

필요하며, 커버링 다항식을 사용한 경판정 복호의 경우 4×3 = 12개의 다항식 사용에 해당한다. 성능 곡선은 SD3와 SD4의 사이에 위치한다. Chase 알고리듬과 연판정 커버링 다항식 복호의 WER 성능 비교 결과는 $P_{BER} \approx (d/n) P_{WER}$의 근사식[11]을 이용하면 BER 측면에서의 유사한 성능 비교로 전환될 수 있다.

V. 결 론

본 논문에서는 $\lceil (k+1)/2 \rceil - 1$개의 이항식과 한 개의 단항식을 포함하는 새로운 커버링 다항식 집합을 제시하였고, 이 집합이 골레이 부호의 연판정 복호를 비롯하여 다양한 순환 부호의 복호에 활용될 수 있음을 보였다. [41,21] 부호의 한계 거리 복호에 적용 시 Kasami의 집합[3]과 비교하여 커버링 다항식 2개에 해당하는 복잡도를 감소시키게 된다. 골레이 부호의 연판정 복호에 적용하는 경우 8개의 커버링 다항식이 필요하고, 3개의 커버링 다항식일 이용한 경판정 복호와 비교하여 1e-3 WER 값에서 약 1.6dB 성능 이득을 갖는다. 모의 실험 전구간에서의 BER과 WER은 최적 하한값에서 0.2dB 이내의 성능을 갖음을 확인하였다.

참 고 문 헌

[1] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications.* Englewood Cliffs, NJ: Prentice-Hall, 1983.

[2] A. Benyamin-Seeyar, S. G. S. Shiva, and V. K. Bhargava, "Capability of the error- trapping technique in decoding cyclic codes," *IEEE Trans. Inform. Theory,* vol. 32, no. 2, pp. 166-180, Mar. 1986.

[3] T. Kasami, "A decoding procedure for multiple-error-correcting cyclic codes," *IEEE Trans. Inform. Theory,* vol. 10, no. 2, pp. 134-138, Apr. 1964.

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.

[5] Y. Kangyou and L. Liang, "An upper bound on the number of covering poly- nomials for a class of cyclic codes," *Acta Electronica Sinica,* vol. 20, no. 4, pp. 25- 31, Apr. 1992.

[6] V. K. Wei, "An error-trapping decoder for nonbinary cyclic codes," *IEEE Trans. Inform. Theory*, vol. 30, no. 3, pp. 538-541, May. 1984.

[7] W. Sung and J. T. Coffey, "Decoding short binary cyclic codes via covering polynomials," *European Transaction on Telecommunications,* vol. 5, no. 6, pp. 653-664, Nov./Dec. 1994.

[8] W. Sung and J. T. Coffey, "Optimal covering polynomial sets correcting three errors for binary cyclic codes," *IEEE Trans. Inform. Theory,* Vol. 48, no. 4, pp. 985-991, Apr.2002.

[9] V. C. da Rocha, "Soft error-trapping decoding of cyclic codes," *Electronics Lett.,* vol. 25, no. 3, pp. 293-294, Feb. 1989.

[10] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Inform. Theory.,* vol. 18, no. 1, pp. 170-182, Jan. 1972.

[11] G. C. Clark, Jr. and J. B. Cain, *Error-Correction Coding for Digital Communications.* New York, NY: Plenum Press, 1981.

[12] H. Tanaka and K. Kakigahara, "Simplified correlation decoding by selecting possible codewords using erasure information," *IEEE Trans. Inform. Theory,* vol. 29, no. 5, pp. 743-748, Sept. 1983.

성 원 진(Wonjin Sung) 정회원

1990년 2월 : 서울대학교 전자공학과 학사

1992년 5월 : University of Michigan 전기공학과 석사

1995년 12월 : University of Michigan 전기공학과 박사

1996년 1월~2000년 8월 : Hughes Network Systems사 책임연구원

2000년 9월~현재 : 서강대학교 전자공학과 조교수

<주관심 분야> 디지털통신 이론 및 응용