特別寄稿

Reed-Solomon 부호의 원리와 응용

전북대 정보통신공학과 이 문 호

차 례

1. 서 론

부호이론(Coding Theory)은 정보화 사회에 대응하여 정보의 신뢰성(reliability)을 다루는 학문이다. 전송 및 기록되는 정보량이 증가하면 할수록 또한 정보 시스템이 경제적이며 편리하게 되면 될수록 오류가 발생할 여지가 높아진다. 이 때문에 오류에 대한 대책은 향후 정보화 사회를 좌우하는 것이라 말해도 과언은 아니다.

정보의 신뢰성 향상의 대책은 부품의 품질관리에서 Man-Machine 인터페이스에 이르기까지 다양하지만, 특히 부호화(coding)에 의한 오류의 검출/정정(error detection/correction)은 중요한 분야를 차지하고 있다. 부호화에 의한 오류 검출/정정의 원리는 간단하다. 0 또는 1 을 전송(기록)하고자 할 때, 예를 들면 2회 연속 보내기로 정하여 00 또는 11 을 보낼 때 오류가 발생하면 01 또는 10 이 수신된다. 이것은 미리 정해둔 00 도 11 도 아니므로 오류가 발생한 것으로 알게 된다. 오류를 정정하고자 할 경우, 0 또는 1 을 3회 연속적으로 보내면 된다. 예를 들면 0 이라는 정보를 전달하고자 할 때 000 을 보낸다. 이때, 오류가 1개 발생하여 010 이 수신되었다 하여도 0 이 2개 남기 때문에 다수결 원리(Majority rule)에 의해 000 이 송신되었다고 판단할 수 있다. 이것은 1개의 오류를 정정한 것과 같다.

부호화에 의한 오류 검출/정정은 디지털 정보에 대하여 조직적으로 처리하기 쉬운 형태로 중복성 즉, 군더더기를 부가하여 신뢰성의 향상을 도모하는 기술이다. 이 군더더기를 부가한 것을 부호(code)라 하고 오류검출에 이용되는 부호가 오류검출부호(Error Detection Code) 이고, 정정에 이용되는 부호는 오류정정부호(Error Correction Code) 이다.

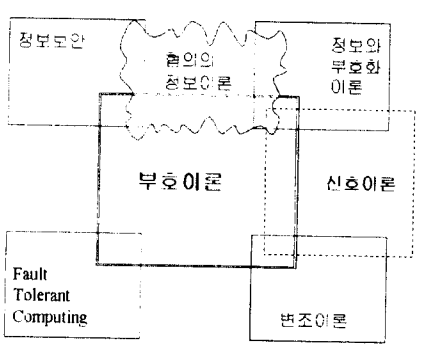
부호이론은 이와 같은 EDC/ECC의 구성법, 그 부호화·복호화, 부호에 의한 오류검출 및 정정의 한계, 신뢰성의 해석 등을 취급하는 이론이다. 부호이론은 대수학을 기초로 한 정연한 이론체계를 가지고 있다. 부호이론의 또 다른 특징은 그것이 공학적으로 널리 응용되어 오늘날의 정보시스템의 신뢰성 향상에 큰 공헌을 이루어 온 점이다[1][4][6][7][14].

1.1 부호이론의 관련분야

부호이론은 넓은 의미에서의 정보이론의 한 분야이다. 넓은 의미의 정보이론의 가장 중요한 테마는 부호화(coding)이다. 부호화는 여러 가지 목적으로 수행되는데 정보이론의 주요 대상은 정보의 전달이나 기록의 효율 향상을 위한 부호화, 신뢰성 향상을 위한 부호화, 정보보안을 위한 부호화의 세 가지이다. 효율 향상을 위한 부호화는 정보원 부호화(source coding)라 불리는 것으로 원 정보의 군더더기를 제거하여 압축하는 과정이다. 신뢰성 향상을 위한 부호화는 채널 부호화(channel coding)라 불리는 것으로 오류 정정부호를 위한 부호화가 중심이다. 안전성 향상을 위한 부호화는 비밀을 지키는 것, 정보의 위조 및 부정조작 등을 목적으로 한 암호(cryptography)가 주역을 담당하고 있다.

신뢰성 향상을 위한 부호화는 좁은 의미의 정보이론(Shannon Theory)에서도 취급하는 것으로, 중심이 되는 것은 부호화에 의해 신뢰성이 어디까지 향상될 것인가에 대한 한계에 관한 이론이다(1993년에는 샤논이론에 거의 근접하는 Turbo 부호가 발견되었다). 이것에 대하여 부호이론에서는 오류 정정부호의 구성 및 부호화 · 복호화 이론의 중심으로 되어 있는 것을 〔그림 1〕에 보이고 있다.

[그림 1] 부호이론과 관련분야



부호이론과 정보원 부호화 이론은 어떤 의미에서 쌍대성(Duality)이 성립하는 점이 있다. 즉, 정보원 부호화에서는 군더더기를 제거하기 때문에 오류에 대하여 약해질 수 있다. 이 때문에 오류정정부호를 설계하는 경우 어떤 정보원 부호화가 이루어졌는지를 고려해야 한다. 최근에 정보부호에 대한 연구는 정보원의 source는 압축을 하고 정보 채널 부호에는 군더더기 즉 중복도를 첨가하여 전송하는가 하면, 변조와 채널 부호화를 합쳐 최적 설계를 해서 샤논 정보이론에 접근하는 방법에 대한 연구를 하고 있다〔6〕〔7〕.

1.2 부호이론의 역사

1948년 C. E. Shannon은 어떤 조건이 만족되면 부호화에 의해 얼마든지 높은 신뢰성으로 정보를 전달할 수 있다는 놀라운 결과를 제시하였다. 이것은 구체적인 부호화 구성법을 제시하지는 않지만 부호 구성 연구의 길을 제시한 것으로 볼 수 있다. 구체적인 부호 구성 이론의 시작은 1950년의 Hamming부호인데, 컴퓨터 기억장치의 오류정정을 목적으로 1개의 오류를 정정하는 부호였다. 오류정정부호는 블록부호(block code)와 길쌈부호(convolutional code)로 나누어지는데, 블록부호는 일정 길이의 계열로 부호화하는 것이고, 길쌈부호는 부호화는 순차적으로 이루어져 이론적으로 무한 길이의 계열로 부호화 되는 것이다. 블록부호가 간단하여 연구가 급히 이뤄질 것 같았으나, 부호이론의 초기에는 오히려 길쌈부호가 먼저 이루어졌다. 1955년 P. Elias에 의해 길쌈부호가 제안되고, 2년후에 J. M. Wozencraft에 의해 길쌈부호의 순차복호법이 발견되었는데, 그 후 R. M. Fano 등에 의해 개선되어 현재 길쌈부호의 중요한 복호법의 하나로 자리잡고 있다. 나아가, 1959년에는 연집오류(burst error)를 정정하는 길쌈부호로서 Hagelbarger부호가 구성되어 오늘에 이르기까지 사용되고 있다.

그러나, 1950년대 말에는 블록부호에 관한 연구가 활발하여 1957년 E. Prange는 블록부호의 한 종류인 순회부호를 제안하였다. 이 부호는 정연한 구조를 가지며 수학적으로 취급하기 쉽기 때문에 이후 연구의

많은 곳에서 그 대상으로 하게 되었다. 1959년에서 1961년의 3년간은 부호이론 연구에서 특별히 기록할 시기이다. 우선, 1959년과 1960년에 다중오류를 정정하는 강력한 부호로서 BCH(Bose-Chaudhuri-Hocguenghem)부호와 RS(Reed-Solomon)부호가 발명되었다. 이들 부호는 지금에 이르기까지 부호이론에 있어서 이론적, 실용적으로 가장 중요한 위치를 차지하고 있다. 또한, 1951년에 연집오류를 정정하는 부호로서 Fire부호가 나타났고 1967년 Viterbi 알고리즘이, 1980년에는 Ungerboeck이 Trellis부호 변조기법을[11], 1993년에는 Berrou등에 의해서 Turbo부호가 발표되었다[13].

Shannon과 Hamming에 의한 문제 제기로부터 45년동안 오늘날 이용되고 있는 많은 부호가 발견된 것이다. 더욱이, 이 시기에서 잊어서는 안 되는 것이 W. W. Peterson의 "Error-Correcting Codes"의 출판이다. 이 책에서는 오류정정부호의 장치 알고리즘과 BCH부호, RS부호 등의 부호화 및 오늘날 Peterson법으로 불리는 복호법이 멋지게 체계화되었다. 이 책은 그후 오랫동안 부호이론 연구자의 바이블로 자리잡아 현재 부호이론의 기초를 이루었다. 1960년대는 부호이론의 제1기 황금시대라 해도 과언이 아니다. 1963년 J. L. Massey의 "Threshold Decoding"이 출판되었다. 이것은 Massey교수가 MIT에서 박사논문을 정리한 것으로 오류정정부호의 가장 간단한 복호법인 다수결 논리 복호법의 기초를 확고히 한 저서이다. 이 복호법이 적용될 수 있는 뛰어난 부호로서 E. J. Weldon이 1966년에 차집합 논리부호를 제안하였다. 이 부호는 현재 디지털 방송 관계를 중심으로 널리 응용되고 있다.

Massey교수(최근 스위스 공대교수 정년퇴임)와 같이 MIT의 박사논문을 정리한 것을 출판한 G. D. Forney(현재 모토로라 부사장)의 연접부호(concatenated codes)는 간단한 오류정정 부호를 조합하여 강력한 오류정정 부호를 구성하는 중요한 기법이다. 또한, Forney는 이 저서에서 통신로의 정보를 보다 유효하게 이용하여 얻을 수 있는 복호법으로서 일반화와 최소거리 복호를 제창하여 이후의 복호법 연구에 큰 영향을 주었다. 1960년대 후반의 중요한 연구성과는 1967년 Viterbi 복호법과 그 이듬해의 Berlekamp-Massey (BM) 알고리즘이다. Viterbi 복호법은 길쌈부호의 강력한 복호법이며, BM법은 BCH부호나 RS부호의 효율적인 복호법이 되고 있다.

1970년대에는 부호이론의 이론적 연구성과는 침체기였다. "부호이론은 죽었다"("Coding is dead")라고 까지 여겨졌다. 그러나, 그러한 가운데 러시아의 Gopper부호는 연구자에게 희망을 주었다. Gopper부호는 1980년대의 대수기하학적 부호로 이어졌는데, 1970년대 후반에는 응용의 면에서 요청된 부호이론과 다른 분야와의 경계영역의 연구가 왕성하게 되었고, 그 중에서 특히 중요한 것은 Ungerboeck부호와 일본 동경대 Imai-Hirakawa부호를 중심으로 하는 부호화 변조의 연구이다. 이것은 현재 부호이론의 가장 액티브한 연구분야로 되어 있다. 1980년대에 있어서 전통적 이론연구의 중심이 되는 것은 앞에서 기술한 대수기하학적 부호일 것이다. 그러나, 1980년대를 특징 지우는 것은 응용연구이다. 이러한 응용연구를 포함하는 오늘날의 부호이론은 제2의 황금시대에 있다고 말해도 과언이 아니다.

1990년대에 들어서는 1993년 불란서 Bretagne 지방의 Ecole 국립 Superieure 대학 C. Berrou 교수 등이 독일 뮌헨대학 J. Hagenauer와 P. Hoeher 논문[12]에서의 비터비 알고리즘에서 연판정 복호기가 신호대잡음비(SNR) 증폭기로서 인식될 수 있다는 생각을 근간으로 전자회로의 피드백(feedback)에서 착안, Turbo부호가 발명[13]이 되었다. Turbo부호는 인터리버의 크기가 충분히 크고 반복적 복호가 충분히 수행되었을 때, BER(Bit Error Rate)의 관점에서 샤논한계(-1.59dB)에 근접하는 우수한 성능을 보여 주어, 앞으로 채널부호에서 Turbo부호의 황금시대를 예고하고 있는데, 샤논(1948)의 정보이론을 발표한 후 50년이 지난 금년(1998)에 MIT에서 정보이론 및 응용 워크샵을 성황리에 끝냈다. 한편, 국내는 한양대 부총장을 지낸 원로학자 이만영 교수가 "Error Correcting Coding Theory" McGraw-Hill(1988),

"Cryptography and Secure Communications" McGraw-Hill(1994) 역저를 발표하였고, 건국대 노종선 교수는 No Sequence를, 한양대 양경철 교수는 Z4 부호를 각각 IEEE. Information Theory에 발표하였다.

2. RS(Reed-Solomon) 부호기

[그림 2] Irving S. Reed and Gustave Solomon

RS부호는 SIAM Journal on Applied Mathematics에 1960년도에 Reed와 Solomon(위의 〔그림 2〕)에 의해 처음으로 소개되었는데, 연집오류(burst error) 정정능 력이 뛰어나다. 이 논문에서 소개되고 있는 것은 RS부 호라 불리는 매우 강력한 비이진(non-binary) 부호로, 후에 Gorenstein과 Zierler에 의해 RS부호와 BCH 부호 가 밀접하게 연관이 있다는 것이 발견되었고, 미연합전략정보망(JTIDS)에 (31, 15) RS부호가, 미공군위성통신(AFSATCOM)에는 (7, 2) RS부호가 사용되었다.

RS 부호는 한마디로 확대된 BCH(Bose-Chaudhuri- Hocquenghem) 부호라 할 수 있다. 즉, BCH 부호와 마찬가지로 길이가 q^m-1인 q^m-ary 부호어라는 점이다. 따라서 GF(q^m)에서 정의된다는 점등은 BCH 부호의 특성을 그대로 보여주고 있다. 더불어 생성 다항식 $g(x)=(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t})$, ('narrow sense' 가정)로 정의된다. 따라서 BCH 부호의 경우 오류의 위치만 알면 그 부분을 '1'은 '0'으로, '0'는 '1'로 바꾸어 주기만 함으로서 오류를 정정할 수 있는 반면에 RS 부호의 경우 오류의 위치뿐만 아니라 오류의 크기까지 존재하여 이것을 알아야 오류를 정정할 수 있다.

일반적인 RS 부호는 (n, k, t)로 표현되는데,

n : 부호어 길이

k : 정보어 길이

t : 에러 정정능력

$$t = \frac{n-k}{2} = \frac{d_{\min}-1}{2},$$

최대거리분리 정정능력(maximum-distance separable)

$d_{min} \le n-k+1$: Singleton bound

의 매개변수를 갖게 된다.

GF(Galois Field)에서는 모듈 성질이 적용되기 때문에 순환하는 특성을 보여주는 데, 이는 원시다항식(Primitive Polynomial)을 통해 표현이 되며, 소수 다항식이면서 x^n+1는 나누지만 $x^l+1(1\le l< 2^m-1)$은 나누지 못하는 다항식이 원시다항식이다. 부호화에 있어서 각 부호 심볼은 m-bit로 구성되어 있는 비이진을 생각하고, 부호어는 $x^{n-k}m(x)+r(x)$로 만들어지는데, 식 (2.1)로 주어진다.

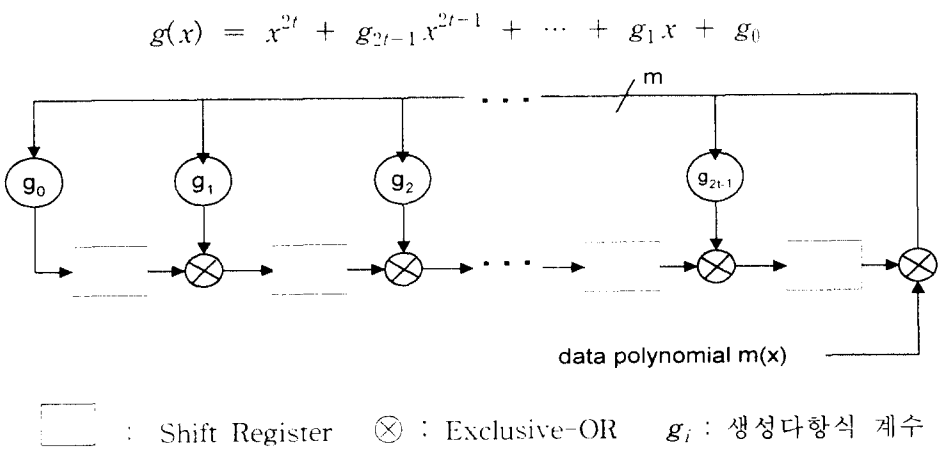
$$\frac{x^{n-k}m(x)}{g(x)} = q(x) + r(x) \quad (2.1)$$

부호기는 g(x)에 따라 궤환(feedback)이 연결된 LFSR(Linear Feedback Shift Register)이고, 각각의 궤환 연결부분에 생성 다항식 g(x)의 계수를 곱하기 때문에 〔그림 3〕과 같은 회로가 구성된다.

3. RS 복호화

1960년에 Peterson이 처음으로 BCH부호에 대한 복호 알고리즘으로 직접복호법을 제안했다. Peterson의 알 고 리 즘 은 Gorenstein과 Zierler(1961), Chien(1964), Forney(1965)에 의해 비이진 계열인 RS 부호로 확장되어 졌는데, 1967년에 Berlekamp가 BCH 부호와 RS 부호에

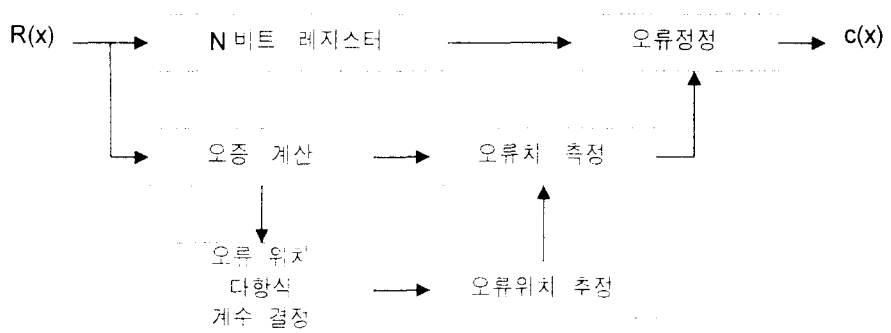
[그림 3] LFSR을 이용한 일반적인 RS 부호기



대한 매우 효율적인 복호 알고리즘을 제시했고, 1969년에 Massey가 RS 부호의 복호 문제는 어떤 주어진 순서열을 생성해내는 LFSR을 찾는 문제와 같다는 것을 증명했다. 한편, 1975년에 Sugiyama 등은 Euclid 알고리즘이 BCH부호와 RS부호를 복호하는데 사용될 수 있다는 것을 보였다[15]. 위의 여러 복호 알고리즘 중에 많이 사용되는 Berlekamp-Massey 알고리즘에 대해 간단히 살펴보면, 복호화는 다음의 일련의 순서에 의해 이루어지는데 [그림 4]와 같은 블록도로 표현된다.

[그림 4] Reed-Solomon 부호의 복호화 과정 계통도

1. 신드롬을 계산한다.
2. 오류위치 다항식을 구한다.
3. 오류위치 다항식의 근(에러 위치)을 구한다.
4. Forney 알고리즘을 이용하여 오류의 크기를 계산한다.
5. 3,4에서 구한 오류위치와 오류크기를 가지고 오류를 수정한다.



3.1 신드롬 계산

신드롬의 계산은 수신심볼 다항식에 생성다항식의 근 α, α^2, ···, α^{2t}을 대입하여 구한다. 오류 정정 가능한 t혹은 그 이하의 오류가 발생했다고 가정하고, 오류값 Y_1, Y_2, ···, Y_v가 α^{e1}, α^{e1}, ···, α^{ev}위치에 생겼다고 가정하면, 식 (3.1)로 표현된다.

$$e(x) = Y_1 x^{e_1} + Y_2 x^{e_2} + \cdots + Y_v x^{e_v} \quad (3.1)$$

오류위치번호 α^{ev}를 X_v로 간단히 표기하면, 오증(syndrome) S_i는

$$\begin{aligned} S_i &= r(x)|_{x=\alpha^i} = [c(x) + e(x)]|_{x=\alpha^i} = e(x)|_{x=\alpha^i} \\ &= Y_1(\alpha^i)^{e_1} + Y_2(\alpha^i)^{e_2} + \cdots + Y_v(\alpha^i)^{e_v} \\ &= Y_1 X_1^i + Y_2 X_2^i + \cdots + Y_v X_v^i = \sum_{j=1}^{v} Y_j X_j^i \end{aligned} \quad (3.2)$$

수신심볼 다항식 r(x)는

$$\begin{aligned} r(x) &= r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0 \\ &= ((\cdots((r_{n-1}x + r_{n-2})x + r_{n-3})x + \cdots + r_2)x + r_1)x + r_0 \end{aligned} \quad (3.3)$$

과 같이 Hornor's rule에 의해 시스톨릭 어레이(Systolic Array)로 표현될 수 있으며 [그림 5]와 같이 신드롬을 계산하는 회로가 설계된다[8].

3.2 오류위치 다항식과 Berlekamp-Massey 알고리즘

앞에서와 같이 신드롬이 계산이 되면 그 정보로부터 오류위치 다항식을 구할 수 있다. 오류위치 다항식 $\Lambda(x)$는 오류위치인 X_1, X_2, ···, X_v를 근으로 갖는다. v개의 오류를 갖는 v차수의 오류위치 다항식은 식 (3.4)처럼 표현된다.

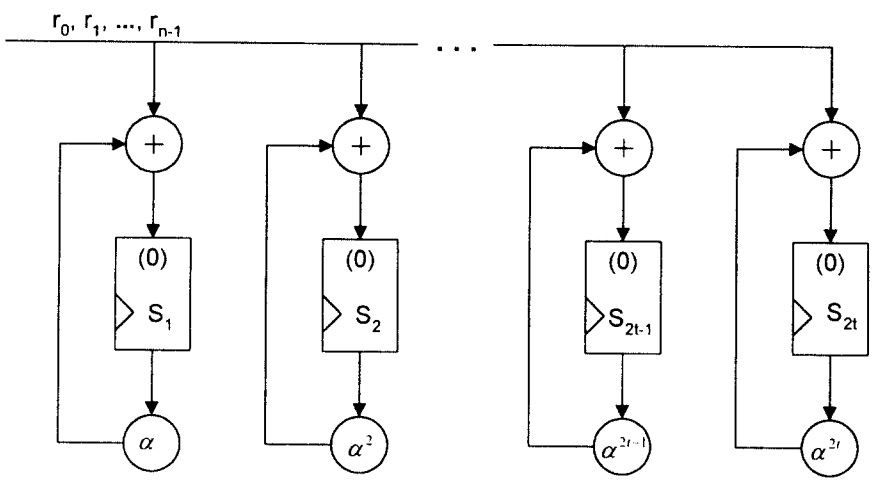
$$\Lambda(x) = (x + X_1)(x + X_2)\cdots(x + X_v) \quad (3.4)$$

또한, v개의 계수를 갖는 수식으로도 표현될 수 있다.

$$\begin{aligned} \Lambda(x) = x^v &+ \Lambda_{v-1}x^{v-1} + \Lambda_{v-2}x^{v-2} \\ &+ \cdots + \Lambda_1 x^v + \Lambda_0 \end{aligned} \quad (3.5)$$

그런데 이 두 수식은 동일한 수식을 단지 달리 표기한 것뿐이므로 일치해야 한다. 따라서 처음의 수식을 푼 후, 계수가 동일하다고 하면 다음과 같은 결과를 얻을 수 있으며, 오류위치 다항식이 구해지면 오

[그림 5] RS의 신드롬을 계산하는 시스톨릭 어레이



류의 크기를 계산할 수 있다.

$$\Lambda_{v-1} = X_1 + X_2 + \cdots + X_v \quad (3.6)$$
$$\Lambda_{v-2} = X_1X_2 + X_2X_3 + \cdots + X_{v-1}X_v$$
$$\cdots$$
$$\Lambda_0 = X_1X_2\cdots X_v$$

이러한 오류위치 다항식을 구하는 알고리즘중에 BM(Berlekamp-Massey) 알고리즘을 설명하면, 신드롬 S_j는 오류위치 다항식 $\Lambda(x)$의 계수들과 그 이전 신드롬들의 함수로서 결과식은 식 (3.7)처럼 표현될 수 있고, LFSR로 표현하면 [그림 6]과 같다[4].

$$\Lambda_v S_{j-v} + \Lambda_{v-1} S_{j-v+1} + \cdots + \Lambda_1 S_{j-1} = S_j \quad (3.7)$$

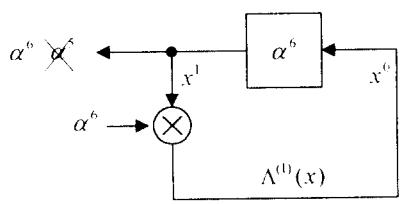
BM 알고리즘은 RS 부호의 복호문제를 처음 2t개의 출력이 신드롬 열 $S_1, S_2, \cdots, S_{2t}$가 되는 최소 길이의 LFSR을 찾는 문제로 설명된다.

$\Lambda^{(k)}(x) = \Lambda_k x^k + \Lambda_{k-1}x^{k-1} + \cdots + \Lambda_1 x + \Lambda_0$를 길이 k인 연결다항식이라 한다. BM 알고리즘은 첫 번째 출력이 S_1인 LFSR의 연결다항식 $\Lambda^{(1)}(x)$를 찾는 것에서 시작한다. 이 LFSR의 두 번째 출력과 S_2를 비교해서, 다를 경우, 그 사이의 차이(Discrepancy)를 연결다항식을 수정하기 위해서 사용한다. 그러나 만일 차이가 없다면, 그 구조 그대로의 세 번째 출력을 생성한 후 S_3와 비교한다. 이러한 과정을 LFSR의 연속적인 2t개의 출력과 $S_1, S_2, \cdots, S_{2t}$가 일치할 때까지 반복한다.

다음의 일련의 과정은 $GF(2^3)$ (mod (2^3-1) 연산 적용)상에서 2t=4인 RS부호를 예로 BM 알고리즘을 설명한 것으로, 4개의 신드롬 $S_1=\alpha^6$, $S_2=\alpha^3$, $S_3=\alpha^4$, $S_4=\alpha^3$을 출력하는 LFSR을 찾는 과정을 설명한 것이다.

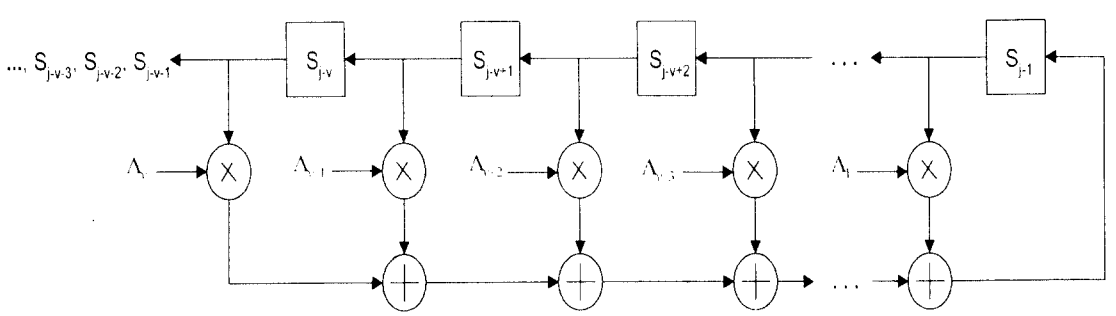
단계 1 : 첫 번째의 출력이 S_1이 되기 위한 조건은 연결다항식이 $\Lambda^{(1)}(x) = \alpha^6 x + 1$일 때이다. 이 때 두 번째 출력이 S_2와 다르므로 연결다항식을 수정한다.

[그림 7] $\Lambda^{(1)}(x) = \alpha^6 x + 1$일 때의 LFSR



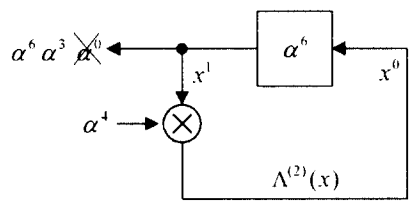
두 번째 출력 : $\alpha^6 \times \alpha^6 = \alpha^{12} = \alpha^{12 \bmod 7} = \alpha^5 \neq S_2$

[그림 6] 식(3.7)에 대한 LFSR 표현



단계 2: 두 번째의 출력이 S_2일 조건은 연결다항식이 $\Lambda^{(2)}(x) = \alpha^4 x + 1$일 때이다. 이 때 세 번째의 출력이 S_3와 다르므로 연결다항식을 수정한다.

[그림 8] $\Lambda^{(2)}(x) = \alpha^4 x + 1$일 때의 LFSR

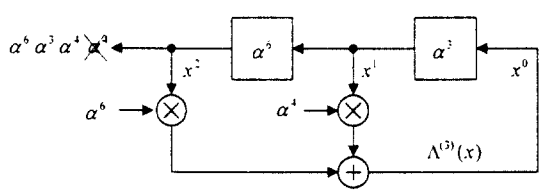


세 번째 출력 : $\alpha^3 \times \alpha^4 = \alpha^7 =$

$$\alpha^{7 \bmod 7} = \alpha^0 \neq S_3$$

단계 3: 세 번째의 출력이 S_3일 조건은 연결다항식이 $\Lambda^{(3)}(x) = \alpha^6 x^2 + \alpha^4 x + 1$일 때이다. 이 때 네 번째 출력이 S_4와 다르기 때문에 연결다항식을 수정한다.

[그림 9] $\Lambda^{(3)}(x) = \alpha^6 x^2 + \alpha^4 x + 1$일 때의 LFSR



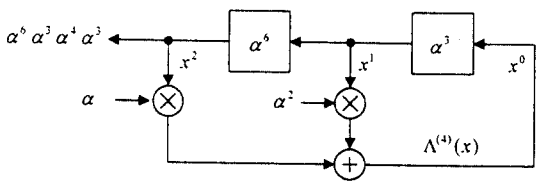
네 번째 출력 : $\alpha^3 \times \alpha^6 + \alpha^4 \times \alpha^4$

$= \alpha^{9 \bmod 7} + \alpha^{8 \bmod 7} = \alpha^2 + \alpha$

$= \alpha^4 \neq S_4$

단계 4: 네 번째 출력이 S_4일 조건은 연결다항식이 $\Lambda^{(4)}(x) = \alpha x^2 + \alpha^2 x + 1$일 때이다. 이 때 [그림 10]의 LFSR의 처음 연속된 4개 출력이 S_1, S_2, S_3, S_4와 같으므로 최종적인 연결다항식은 $\Lambda^{(4)}(x) = \alpha x^2 + \alpha^2 x + 1$이 된다.

[그림 10] $\Lambda^{(4)}(x) = \alpha x^2 + \alpha^2 x + 1$일 때의 LFSR



단계 4에서와 같이 최종적인 연결다항식이 구해지면, 이 것을 오류위치 다항식 $\Lambda(x)$로 하고 근을 구한다. 근이 구해지면 중근인지 여부를 확인하고 중근이 아니라면 오류위치 다항식은 옳게 구해진 것으로 판정된다. 이때 근이 구해지지 않거나, 중근으로 판정이 되면, 복호는 실패했다고 선언이 되고, 복호 성공의 판정이 끝나면 오류정정에 들어간다.

3.3 오류위치 결정

오류위치를 찾는 방법은 두 가지 방법이 있다.

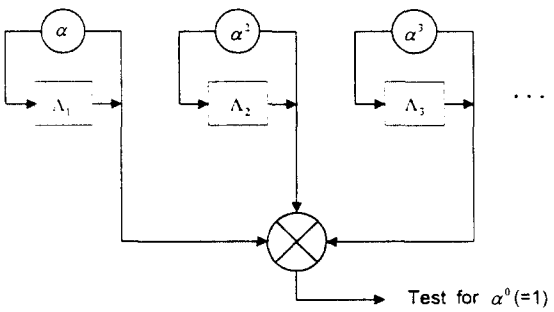
- Chien Search : 오류위치는 오류위치 다항식의 근이므로 오류위치 다항식 $\Lambda(x)$에 $x = \alpha^{p_i}$를 대입했을 때 0의 값을 가지게 된다.
- 인수 분해 : $\Lambda(x)$를 직접 인수분해 한다.

그러나 대부분의 복호기의 구현에 적용되는 것은 Chien Search 방법이므로 여기서는 Chien Search 방법에 대해서 설명하기로 한다. 오류위치 다항식의 근이 α^{p_1}, α^{p_2}, ..., α^{p_v}일 때

$$\Lambda(x)\Big|_{x=\alpha^e} = 0, \quad i = 1, 2, \ldots, v$$

이 된다. 따라서 오류위치 다항식에 α^i를 대입하여 계산했을 때 그 값이 0이면 α^i 위치에 오류가 발생하였고, 0이 아니면 그 위치에는 오류가 없음을 알 수 있다. Chien Search를 하드웨어로 구현한 것은 [그림 11]과 같다[4][7].

[그림 11] RS의 Chien Search 회로



3.4 오류크기 계산 및 오류 정정

오류위치 방정식으로부터의 오류의 위치와 다음의 Key Equation을 가지고 Forney 알고리즘[2][7]을 이용하여 오류의 크기를 계산할 수 있는데, Key Equation은 다음과 같이 정의된다.

$$\Lambda(x)[1+S(x)] \equiv \Omega(x) \bmod x^{2t+1} \qquad (3.8)$$

Forney 알고리즘의 일반식은 식 (3.9)와 같다[2][7].

$$e_{j_k} = \frac{-X_k \cdot \Omega(X_k^{-1})}{\Lambda'(X_k^{-1})} \qquad (3.9)$$

이를 구하기 위한 GF(q)상에 존재하는 계수를 갖는 다항식에 미분(derivative)을 적용하면

$$f(x) = f_0 + f_1 x + \cdots\cdots + f_n x^n + \cdots\cdots \qquad (3.10)$$

$$f'(x) = f_1 + 2f_2 x + \cdots\cdots + n f_n x^{n-1} + \cdots\cdots \qquad (3.11)$$

이 때 식 (3.11)을 보면 GF(q)상에서 XOR연산이 적용이 되므로 미분 후에 나타나는 짝수 계수를 가지는 항들은 전부 0이 된다는 재미있는 특징을 알 수 있다.

식 (3.8)과 식 (3.9)에 x를 X_k^{-1}로 치환하여 계산하면 오류의 크기를 구할 수 있고, 구해진 오류크기를 가지고 오류다항식을 생성한 다음에, 수신심볼 다항식에 더해주게 되면 오류를 정정하게 된다.

$$\begin{aligned} r(x) &= c(x) + e(x) \\ \hat{c}(x) &= r(x) + e(x) \\ &= \{c(x) + e(x)\} + e(x) = c(x) \end{aligned} \qquad (3.12)$$

r(x) : 수신심볼 다항식
c(x) : 부호심볼 다항식
e(x) : 오류 다항식
$\hat{c}(x)$: 수정된 부호심볼 다항식

($\because\ \hat{c}(x) = c(x),\ 2e(x) \rightarrow 0$)

3.5 RS부호의 BER(Bit Error Rate)

E_b/N_0에 대한 RS부호의 비트 오류 확율(BER)을 알아보기 위해 n=31, 32-ary MFSK (M-ary Frequency Shift Keying) 변조 시스템을 예로 비트 오류 확률(BER)을 구하기 위해 먼저 심볼 오류 확률(P_E)을 먼저 알아보면,

$$P_E = \frac{1}{M} \exp\left(-\frac{E_s}{N_0}\right) \sum_{j=2}^{M} \binom{M}{j} (-1)^j \exp\left(\frac{E_s}{jN_0}\right) \qquad (3.13)$$

$$E_s = E_b \log_2 M$$

식 (3.13)에 M-ary 직교신호 set에 대한 P_B와 P_E의 관계인 $\frac{P_B}{P_E} = \frac{2^{m-1}}{2^m - 1}$

를 대입하여 비트 오류 확률(BER) 구할 수 있다.

$$P_B = \sum_{j=t+1}^{2^m-1} \frac{j}{2^m-1} \binom{2^m-1}{j} P_E{}^j (1-P_E)^{2^m-1-j} \qquad (3.14)$$

여기에서 t는 오류 정정 능력이고, t=1, 2, 4, 8의 값을 가지며 m은 MFSK에서 $M=2^m$, 2^m-ary으로 나타내어지는 m비트 심볼을 의미한다.

식 (3.14)에서 t=1일 때의 P^B를 정리하면 식 (3.15)와 같이 된다[7].

(3.15)

$$P_B = \sum_{j=2}^{2^m-1} \frac{j}{2^m-1}\binom{2^m-1}{j} P_E^{\,j}(1-P_E)^{2^m-1-j}$$

$$= P_E - P_E(1-P_E)^{2^m-2}$$

■ 증명

$$j\binom{2^m-1}{j} = j\frac{(2^m-1)!}{j!(2^m-1-j)!} = \frac{(2^m-1)!}{(j-1)!(2^m-1-j)!}$$

$$= (2^m-1)\frac{(2^m-2)!}{(j-1)![(2^m-2)-(j-1)!]}$$

$$= (2^m-1)\binom{2^m-2}{j-1}$$

$$\therefore P_B = \sum_{j=2}^{2^m-1}\binom{2^m-2}{j-1} P_E^{\,j}(1-P_E)^{2^m-1-j}$$

$$= P_E\sum_{j=2}^{2^m-1}\binom{2^m-2}{j-1} P_E^{\,j-1}(1-P_E)^{(2^m-2)-(j-1)}$$

i = (j-1)로 치환하면,

$$P_B = P_E\sum_{i=1}^{2^m-2}\binom{2^m-2}{i} P_E^{\,i}(1-P_E)^{2^m-2-i}$$

$$= P_E\sum_{i=0}^{2^m-2}\left[\binom{2^m-2}{i} P_E^{\,i}(1-P_E)^{2^m-2-i} - \binom{2^m-2}{0} P_E^{\,0}(1-P_E)^{2^m-2-0}\right]$$

$$= P_E[1-(1-P_E)^{2^m-2}]$$

$$= P_E - P_E(1-P_E)^{2^m-2}$$ ■

한편, Hamming 부호의 비트오류확률(BER)은 다음 식으로 표현된다.

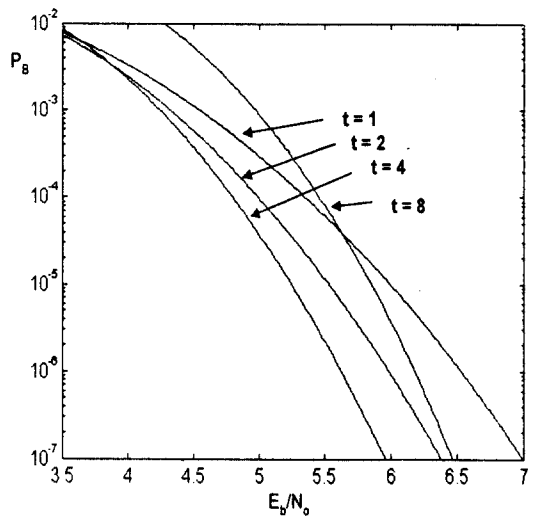
$$P_B \simeq \frac{1}{n}\sum_{j=2}^{n} j\binom{n}{j} p^j(1-p)^{n-j}$$

$$\cong p - p(1-p)^{n-1} \quad (3.16)$$

여기서, p는 2진 부호에서 채널 비트 오류 확률이다. 그런데, 식 (3.16)에서 $n = 2^m-1$이라고 보면 t=1인 경우의 RS의 P_B인 식 (3.15)와 Hamming의 P_B인 식 (3.16)은 꼭 같은 식이 되어 식 (3.15)이 타당함이 입증되었다. ■

[그림 12]는 P_B와 E_b/N_0의 성능비교를 나타내고 있는데, 낮은 dB에서는 t=4인 경우가 월등한 성능을 보여주고 있고, 높은 dB에서는 기울기에서 알 수 있듯이 t=8인 경우의 성능이 우수하다[7]. 그러나 실제 시스템에서 채택하고 있는 오류정정능력(t)을 보면 Digital TV(미국의 8VSB)와 HDTV(High Definition TV)에서 t=10인 경우를, 광대역 CDMA 시스템에서는 t=3인 경우를, ATM(Asynchronous Transfer Mode)의 AAL type 1에서 t=2인 경우를 사용하고 있다([표 2] 참조).

[그림 12] n = 31인 t오류 정정 RS부호를 이용한 32-ary MFSK 부호화시 P_B와 E_b/N_0의 성능비교



4. RS 부호의 응용분야 및 최근 기술동향

RS 부호는 BCH 부호와 같은 이진부호가 아닌 m-bit로 한 심볼을 구성하는 비이진 부호이다. 이러한 심볼 단위로 부호화와 복호화가 수행이 되기 때문에 랜덤 오류(random error) 뿐만 아니라 특히 연

집 오류(burst error) 에 강한 특성을 가지고 있어, ATM (Asynchronous Transfer Mode), CDPD(Cellular Digital Packet Data) 등과 같은 디지털 통신 시스템과 DAT, CD(Compact Disk), DVD(Digital Video Disk) 등과 같은 데이터 저장 시스템에 널리 사용되고 있고 우주통신에서도 사용되며, SDTV(Standard-Definition TV)나 HDTV (High-Definition TV), DTV(Digital Television) 시스템등의 채널 부호기에 사용이 되고 우주통신에서도 사용 된다. IMT-2000 시스템의 채널 부호에서도 RS부호를 사용하는 연접부호와 Turbo 부호가 사용되고 있다. [표 1]은 현재 DTV(Digital TV) 시스템과 IMT-2000 시스템에서 적용하고 있는 채널 부호에 대해 정리하였고, [표 2]에는 국내외 RS 칩의 최근기술개발 동향에 대해 정리했다.

5. 결 론

부호이론의 역사에 및 RS 부호가 탄생하기까지의 숨겨진 연구배경에 대해 살펴보았으며, 부호화에 대해 설명하였다. 또한 전반적인 복호과정중에 복호과정에서 가장 중요하리라 생각되는 오류위치 다항식을 구하기 위한 여러 알고리즘 중에서 Berlekamp-

[표 1] 디지털 방송 및 차세대 이동전화에서의 RS부호 적용현황

서비스 분류 / 채널	디지털 방송		차세대 이동전화
	8VSB(미국)	DVB-T COFDM(유럽)	IMT-2000
채널	■ 연접부호화 내부 부호 Trellis 2/3 + 외부 부호 RS(187,207) (∵연집오류에 강함)	■ 연접부호화 내부 부호 길쌈 1/2, 2/3, 3/4, 5/6, 7/8 + 외부 부호 RS(188, 204) (∵연집오류에 강함)	● 트래픽 채널 ■ 연접부호화 *유럽 · 일본:* 길쌈부호(K=9, R=1/2, 1/3) + RS *한국 ETRI:* 길쌈부호(K=9, R=1/2, 1/3, 1/4) + RS(41, 47)

[표 2] 국내외 RS 칩 기술개발 동향

	LG(한국)[9]	Sharp(일본)[10]	AHA(미국)	Proposed[8]
처리 속도	5MByte/sec (40Mbps)	16MByte/sec (128Mbps)	10Mbyte/sec (80Mbps)	23Mbyte/sec (184Mbps)
오류정정능력	-	1 ~ 4	1 ~ 10	2
이레이저정정능력	-	1~ 8	2 ~ 20	4

Massey 알고리즘에 대해 설명을 하였고, RS 부호의 BER을 유도하여 Hamming 부호와 비교 설명하였다. 현재 RS 부호가 사용되는 응용분야에 대해서 뿐만 아니라 최근의 기술동향으로 한국의 LG, 일본의 Sharp, 미국의 AHA(Advanced Hardware Architecture)사의 칩을 소개하였다.

※ 참고문헌

〔1〕 C. E. Shannon, "A Mathematical Theory of Comm." BSTJ Vol. 27, pp. 379-423 and pp. 623-656, 1948.

〔2〕 G. D. Forney, "On Decoding BCH Codes," IEEE Transactions on Information Theory, Vol. IT-11, pp. 549-557, Oct. 1965.

〔3〕 J. L. Massey, "Shift Register Synthesis and BCH Decoding," IEEE Transactions on Information Theory, Vol. IT-15, No. 1, pp. 122-127, Jan. 1969.

〔4〕 S. B. Wicker, Error Control Systems for Digital Communication and Storage, Prentice Hall, 1995.

〔5〕 S. B. Wicker, V. K. Bhargava, Reed-Solomon Codes and Their Applications, IEEE Press, 1994.

〔6〕 이문호, 실용 정보 이론-오류정정이론의 기초, 복두출판사, 1998.

〔7〕 이문호, C · Matlab 실용 디지털 통신, 도서출판 영일, 1998.

〔8 Moon Ho Lee, S. B. Choi, "A High Speed Reed-Solomon Decoder", IEEE Trans. on Consumer Elect. Vol. 41, no. 4, Nov. 1995.

〔9〕 Youngho Park, Sangjin Park, "Reed Solomon VLSI Codec for HDTV", Asic Center Goldstar Central Research Lab., 1994.

〔10〕 T. Iwaki, T. Tanaka, E. Yamada, T. Okuda, T. Sasada, "Architecture of a High Speed Reed-Solomon Decoder", IEEE Trans. Consumer Electronics, Jan. 14, 1994.

〔11〕 Ungerboeck, "Channel Coding with Multilevel/Phase Signals," IEEE Trans. Inform. Theory. Vol IT-28, no. 1, pp. 55-67, jan. 1980.

〔12〕 J. Hagenauer and P. Hoeher, "A Viterbi Algorithm with Soft-Decision Outputs and Its Applications", Proc. of Globe com '89, Dallas, Texas, pp. 47.11-47.17, Nov. 1989.

〔13〕 C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon Limit Error-correcting Coding and Decoding: Turbo-codes," ICC 1993, Geneva, Switzerland, pp. 1064-1070, May. 1993.

〔14〕 H. Imai, "부호이론", 일본전자정보통신학회, 1990.

〔15〕 Y. Sugiyama, Y. Kasahara, S. Hirasawa, T. Namekawa, "A Method for Solving Key Equation for Goppa Codes," Information and Control, Vol. 27, pp. 87-99, 1975.

이 문 호

- 일본 동경대 전자과 공학 박사(1990), 통신 기술사(1983)
- 미국 미네소타 주립대 전기과 포스트 닥터(1985), 남양 MBC 송신소장 (1970 - 1980)
- 독일 하노버 대학(1990 겨울), 아흔 공대(1992 여름, 1995 겨울), 뮌헨 공대 (1998 여름) 연구 교수
- 1980 ~ 현재 전북대학교 정보통신공학과 교수
- 1997년 ~ 현재 한국 공학 한림원 회원 및 정보통신 정책 심의 위원, 디지털 방송 추진위원