論文 93-30A-3-2

광학식 디스크에 적합한 RS 부호의 새로운 복호 기법

(New Decoding Techniques of RS Codes for Optical Disks)

廉 興 烈*, 金 在 汶**, 李 晩 榮**

(Heung Youl Youm, Jae Moon Kim and Man Young Rhee)

要 約

본 논문에서는 오디오 정보의 저장을 위한 광학식 디스크 시스템용 오류정정부호로 표준화되어 있는 GF(2^8) 상에서의 2중 또는 3중 오류정정 RS 부호에 적용가능한 새로운 오류정정 알고리듬을 제안 및 제시한다. 먼저 수신 부호어에서 발생한 오류의 갯수를 정확히 판단할 수 있는 판별 알고리듬을 제시한다. RS 부호의 복호기의 복잡도를 증가시키는 회로 부분은 오증으로 부터 오류위치를 찾는 알고리듬을 구현하는 회로이므로 이 부분의 복잡도를 감소시키는 것이 전체 복호기의 복잡도를 감소시키게 된다. 유한체상의 2차 또는 3차의 오류위치다항식의 해를 구하기 위한 방법은 GF(2^m)상의 모든 원소를 대입하여 해를 구하는 Chien 기법, 모든 계수에 대응되는 해를 미리 ROM(read only memory)에 기억하여 주소부로 계수를 입력하여 해를 찾는 Polkinghorn 기법 등이 있다. 그러나 Chien의 방법은 한 프레임이 지연되고 난 후에야 오류위치를 구할 수 있고, Polkinghorn 방법은 일반적으로 회로 구성이 매우 복잡해지거나 외부에 별도의 ROM를 부가해야 한다는 문제점이 있다. 본 논문에서는 2차 또는 3차의 오류위치다항식을 변형하여 affine 다항식으로 만들고, Hilbert 정리를 이용하여 오류위치다항식의 해를 간단하고 신속하게 구하는 알고리듬을 도입함으로서 회로 구성이 간단하고 복호기의 복잡도를 현저하게 낮출수 있는 새로운 오류정정 알고리듬을 제시하고 이를 기존의 복호 방식과 성능 측면에서 비교.검토한다. 비교.검토 결과 본 논문에서 제시한 알고리듬을 이용한 RS 부호의 복호기의 복잡도는 기존의 복호 알고리듬을 이용한 복호기의 복잡도보다 현저히 줄어듬을 입증한다. 또한 3중 오류정정 RS 부호의 복호 알고리듬을 제시한다. 제시된 3중 오류정정 RS 부호의 복호 알고리듬은 DAT(digital audio tape) 용 오류정정 복호기 설계시 널리 활용될 수 있다.

Abstract

New decoding algorithm of double-error-correction Reed-Solomon codes over GF(2^8) for optical compact disks is proposed and decoding algorithm of RS codes with triple-error-correcting capability is presented in this paper. First of all, efficient algorithms for estimating the number of errors in the received code words are presented. The most complex circuits in the RS decoder are parts for soving the error-location numbers from error-location polynomial, so the complexity of those circuits has a great influence on overall decoder complexity. One of the most known algorithm for searching the error-location number is Chien's method, in which all the elements of GF(2^m) are substituted into the error-location polynomial and the error-location number can be found as the elements satisfying the error-location polynomial. But Chien's scheme needs another 1 frame delay in the decoder, which reduces decoding speed as well as require more stroage circuits for the received code symbols. The other is Polkinghorn method, in which the roots can be resolved directly by solving the error-location polynomial. But this method needs additional ROM (read-only memory) for storing tthe roots of the all possible coefficients of error-location polynomial or much more complex cicuit. Simple, efficient, and high speed method for solving the error-location number and decoding algorithm of double-error correction RS codes which reduce considerably the complexity of decoder are proposed by using Hilbert theorems in this paper. And the performance of the proposed decoding algorithm is compared with that of conventional decoding algorithms. As a result of comparison, the proposed decoding algorithm is superior to the conventional decoding algorithm with respect to decoding delay and decoder complexity. And decoding algorithm of RS codes with triple-error-correcting capability is presented, which is suitable for error-correction in digital audio tape, also.

*正會員, 順天鄕大學校 工科大學 電子工學科
(Dept.of Elec. Eng., Soonchunhang University)
**正會員, 漢陽大學校 工科大學 電子通信工學科
(Dept.of Elec. Comm. Eng., Hanyang Univ.)

(*이 논문은 1991 년도 교육부지원 한국학술진흥재단의 지방대학육성과제 학술연구조성비에 의해 연구되었음.)
接受日字:1992年 10月 15日

Ⅰ. 서론

최근들어 통신 및 데이타 저장 방식이 아날로그 방식에서 디지틀 방식으로 변환됨에 따라 막대한 양의 데이타, 오디오, 그리고 비디오 정보의 저장을 위한 광디스크 시스템이 널리 실용화되고 있는 추세이다. 이의 대표적인 시스템을 살펴보면, 오디오 신호를 광학식 디스크에 저장하기 위한 컴팩트 디스크 시스템(compact disc system), 오디오 정보를 자기 테이프에 저장하기 위한 DAT(digital audio tape) 시스템, 그리고 데이타를 광학식 디스크에 저장하는 CD-ROM (compact disk read only memory) 등을 들 수 있다. 광디스크상에 열지어 기록되어 있는 미세한 홈(pit) 을 이용하여 데이타를 저장하고 이를 레이저를 이용하여 읽어 내는 것을 바탕으로 설계되어 있는 광디스크 시스템은 불규칙한 잡음 및 변조(modulation) 잡음이 없고, 랜덤 액세스가 가능하며, 먼지와 흠에 따른 영향이 비교적 적으며, 정보가 장기간 안정적으로 기억되어 있고, 비디오 정보의 경우 재생시 화면상의 가상(ghoast) 현상이 없으며, 반영구적인 재생 및 기억이 가능하다는 주요 특징이 있다.[12-16] 따라서 이와 같은 장점을 바탕으로 데이타, 오디오, 비디오 정보의 광디스크를 이용한 저장 및 재생은 앞으로 널리 확대될 추세이다. 그러나 광디스크 표면에 발생한 여러 종류의 흠은 정보의 보전성(integrity)에 커다란 영향을 미치게 된다. 따라서 광저장 매체를 갖는 디지틀 저장 시스템 또는 재생기(player) 를 설계할 경우 반드시 고려해야 할 핵심 요소 기술은 오류정정기술이며, 이는 광저장 매체에서 발생하는 연속 또는 랜덤한 오류형태를 효율적으로 정정 및 제어하는 기술을 다루는 분야이다. RS 부호는 연집 오류뿐만 아니라 랜덤 오류 패턴의 정정이 가능하여 컴퓨터 기억장치 및 디지틀 통신시스템의 오류를 정정하기 위해 널리 응용되고 있는 오류정정부호이다.[1-2-3-4] 지금까지 알려진 RS 부호를 복호하기 위한 대표적인 복호 알고리듬은 Chien의 알고리듬을 이용하는 PGZ(Peterson-Gorenstein-Zieler) 복호 알고리듬, Berlekamp의 반복 알고리듬, Euclid 알고리듬, 변환 복호 알고리듬, 그리고 오증요소와 오류치와의 대수학적 관계를 이용한 직접 복호 알고리듬 등이 있다.[1-4-7-9-12-15] 본 논문에서는 오디오 정보의 저장을 위한 광학식 디스크 시스템용 오류정정부호로 표준화되어 있는 GF(2^8) 상에서의 2중 또는 3중 오류정정 RS에 적용가능한 새로운 오류정정 알고리듬을 제안 및 제시한다. 먼저 수신 부호어에서 발생한 오류의 갯수를 정확히 판단할 수 있는 판별 알고리듬을 제시한다. 3중 오류정정능력 이하의 RS 부호의 복호시 일반적으로 유한체상에서의 오증, 오류위치 다항식, 그리고 오류치간의 대수학적 관계를 이용하여 복호 알고리듬을 실현하고 있다. RS부호의 복호기 복잡도를 증가 시키는 회로 부분은 오증으로 부터 오류위치를 찾는 알고리듬를 구현하는 회로이므로 이 부분의 복잡도를 감소시키는 것이 전체 복호기의 복잡도를 감소시키게 된다. 오증으로 부터 오류위치는 2차 또는 3차의 오류위치다항식의 해를 풀어 구해진다. 본 논문에서는 RS 부호에 대한 기존의 복호 알고리듬을 분석하고 광학식 디스크에 적합한 2중 오류정정 RS 부호의 복호 알고리듬을 제안하였으며, 3중 오류정정 RS 부호의 복호 알고리듬을 제시한다. 오류위치다항식을 적당한 affine 다항식으로 변형한 후 이를 이용하여 해를 구하는 방법을 제시하여, 오류위치다항식의 해를 구하는 회로의 복잡도를 현저히 감소시킨다. 또한 2중 오류정정 RS 부호의 복호기 블럭도 및 복호 흐름도를 제안하고, 2중 오류정정 RS 부호의 복호기에 적용가능한 오류위치다항식으로 부터 오류위치를 구하기 위한 회로를 13개의 간단한 논리회로 들을 이용하여 실현한다. 제안된 복호 알고리듬의 성능에 대한 타당성을 보이기 위하여 지금까지 널리 알려진 복호 알고리듬과 그 성능을 비교한다. 비교 결과 본 연구에서 제안된 복호 알고리듬이 복호기에서 요구되는 지연과 복호기 복잡도 측면에서 제일 우수하다는 것을 입증한다. 그리고 3중 오류정정 RS 부호의 복호 알고리듬, 복호기 블럭도, 그리고 3차 방정식의 해를 구하는 알고리듬 등을 제시한다. 제시된 3중 오류정정 RS 부호의 복호 알고리듬은 DAT 용 오류정정 복호기 설계시 이용될 수 있을 것이다.

Ⅱ. 광학식 디스크에 적합한 오류정정

컴팩트 디스크 시스템에서 발생하는 오류를 정정하기 위한 2중 오류정정 (32,28), (28,24) 단축 RS 부호는 산발 오류뿐만 아니라 연집오류까지도 정정이 가능한 강력한 오류정정능력을 갖는 부호이다. RS 부호를 복호하기 위해서는 2원 BCH 부호의 복호시 요구하지 않던 오류치(error value)를 구하는 과정이 추가로 요구되므로 복호 과정이 매우 복잡하다.[2] 특히, 오류정정능력, 유한체의 크기 및 유한체 연산기의 형태 및 실현 알고리듬 등은 복호기의 복잡도(complexity)에 영향을 미치며, 복호 시간(decoding time) 역시 그에 비례하여 크게 달라진다. 그러므로 간단한 구조를 가지면서 신속하게 복호를 수행하는 복호 알고리듬은 복호기 뿐아니라 전체

시스템의 성능에 커다란 영향을 미치게 된다. RS 부호의 복호기 성능에 영향을 미치는 요소는 일반적으로 오류갯수 판별식 알고리듬, 오류위치 (error location) 및 오류치 (error value) 계산 알고리듬, 그리고 구현되는 유한체 원소간의 승.제산기 등에 대한 연산 알고리듬 등이다. 광디스크 시스템에 이용되는 단축 RS 부호는 원시다항식(primitive polynomial)이 $1 + x^2 + x^3 + x^4 + x^8$ 인 GF(2^8) 유한체를 이용하고 있다. 따라서 생성다항식 $g(x) = (x+1)(x+\alpha)(x+\alpha^2)(x+\alpha^3) = x^4 + \alpha^{75} \cdot x^3 + \alpha^{249} \cdot x^2 + \alpha^{78} \cdot x^1 + \alpha^6$이 됨을 알 수 있다.

1. 수학적 배경

유한체 GF(p^m) 상의 임의의 원소 k의 트레이스 (trace) 인 Tr(k)는 식 (1)과 같이 정의된다. [2]

$$Tr(k) = \sum_{i=0}^{m-1} k^{p^i} = k + k^{2^1} + \cdots + k^{2^{m-1}} \quad (1)$$

GF(p^m)상의 임의의 원소 k에 대한 트레이스 Tr(k)∈GF(p) 이다. [5] 일반적으로 트레이스는 다음과 같은 특성을 만족한다.

① $[Tr(k)^{p^i}] = Tr(k)$
② $Tr(k_1+k_2) = Tr(k_1) + Tr(k_2)$
③ $Tr(c \cdot k_1) = c \cdot Tr(k_1)$,
여기서, c는 GF(p)의 원소.
④ $Tr(1) = m \pmod p$ (2)

이후 p=2인 경우 Tr(k)를 $T_2(k)$로 표기한다. 그리고 p=2이고 m이 우수일 경우, k의 또 다른 트레이스 $T_4(k)$는 다음과 같이 정의한다.

$$T_4(k) = \sum_{i=0}^{(m-2)/2} k^{2^{2i}} = k + k^{2^2} + \cdots + k^{2^{m-2}} \quad (3)$$

GF(p^m) 상의 1차 방정식은 식 (4)와 같이 표현된다.

$$x + a = 0 \quad (4)$$

따라서 식 (4)의 해는 $x = a$ 이다. GF(p^m) 상의 2차 방정식은 식 (5)와 같이 표현될 수 있다.

$$ay^2 + by + c = 0 \quad (5)$$

y를 bx/a라 치환하면, 식 (5)는 식 (6)과 같이 변형된다.

$$x^2 + x + k = 0, \text{여기서, } k = a \cdot c/b^2 \quad (6)$$

식 (6)은 $T_2(k)=0$일 경우만 해를 갖는다 [5] 식 (6)의 한 해를 x_1이라 하면 $x_1^2 + x_1 + k = 0$ 이 된다. 식 (6)의 x_1 대신 x_1+1 를 대입하면 $(x_1+1)^2+(x_1+1)+k = x_1^2+x_1+k = 0$ 이 되어 다른 한 해는 $(1+x_1)$ 임을 알수 있다. 정리 1, 2는 본 논문에서 제시한 복호 알고리듬의 바탕이 되는 중요한 정리이다.

[정리 1] m이 우수이고 식 (4)가 GF(2^m)상의 해를 갖는다면, $T_4(k)$∈GF(2)이다. [6]

(증명 생략)

[정리 2] 식 (4)가 GF(2^m)상의 한 해 x_1를 갖고 $T_4(k) = 1$, $m \equiv 0 \pmod 4$ 이면, 해 x_1 은 식 (7)을 이용하여 구할 수 있다. [6]

$$T_4(k) = \sum_{i=0}^{(m-2)/2} k^{2^{2i}} = k + k^{2^2} + \cdots + k^{2^{m-2}} \quad (7)$$

여기서,

$$s = \sum_{j=1}^{m/4-1} \sum_{i=1}^{m/4-1} k^{2^{2i-1+m/2}+2^{2j-2}} \quad (8)$$

(증명) 식 (8)과 같이 주어진 s를 이용하여 $s+s^4$ 을 먼저 계산한다.

$$s + s^4 = \sum_{j=0}^{m/4-2} \sum_{i=j}^{m/4-2} k^{2^{2i+1+m/2}+2^{2j}} + \sum_{j=1}^{m/4-1} \sum_{i=j}^{m/4-1} k^{2^{2i+1+m/2}+2^{2j}}$$
$$= \sum_{i=0}^{m/4-2} k^{2^{2i+1+m/2+1}} + \sum_{i=1}^{m/4-1} k^{2^{m-1}+2^{2i}}$$

r를 식 (9)와 같이 정의한다.

$$r = s + s^2 + k^{2^{m-1}} + \sum_{i=0}^{m/4-1} k^{2^{2i+m/2}+2^{m-1}} \quad (9)$$

그러면 $r + r^2$은 다음과 같다.

$$r + r^2$$
$$= s + s^4 + k + k^{2^{m-1}} + \sum_{i=0}^{m/4-1} k^{2^{2i+m/2}+2^{m-1}} + \sum_{i=0}^{m/4-1} k^{2^{2i+m/2+1}+1}$$
$$= k + k^{2^{m-1}} + k^{2^{m-1}+1} + k^{2^{m-1}} \left(\sum_{i=1}^{m/4-1} k^{2^{2i}} + \sum_{i=0}^{m/4-1} k^{2^{2i+m/2}} \right)$$
$$= k + k^{2^{m-1}} + k^{2^{m-1}} \cdot \sum_{i=1}^{(m-2)/2} k^{2^{2i}}$$
$$= k + k^{2^{m-1}} + k^{2^{m-1}} \cdot T_4(k)$$

가정에 의해 $T_4(k)=1$ 이므로 다음 관계가 만족된다.

$$r + r^2 = k + k^{2^{m-1}} + k^{2^{m-1}} = k$$

그러므로 2차 방정식의 한 해 x_1 은 m=0 (mod 4), $T_4(k)$ =1일 경우 식 (9) 와 같은 r이 된다.
(증명완료)

정리 2로 부터 m=8, $T_2(k)$=0, $T_4(k)$=1 일 경우, $GF(2^8)$ 상의 식 (4)와 같은 2차 방정식의 한 해 x_1 은 식 (10)과 같다.

$$x_1 = k^{33} + k^{66} + k^{128} + k^{144} + k^{192} \quad (10)$$

m=8, $T_2(k)$ = 0, $T_4(k)$ = 0 인 경우, 2차 방정식의 두 해 x_1, x_2를 다음과 같은 과정을 통해 결정될 수 있다. ① $T_2(y)$ = 1 이 되는 $GF(2^8)$내의 임의의 한 원소 y 을 선택한다. ② $k_1 = y + y^2$ 을 이용하여 k_1 를 구한다. ③ $c = k + k_1$ 이라 하면, $T_4(c) = T_4(k+k_1)=1$ 을 만족함으로서 식 (10)을 이용하여 방정식 $x^2+x+c = x^2+x+k_1+k = 0$ 의 한 해 x_1' ($c^{33} + c^{66} + c^{128} + c^{144} + c^{192}$) 을 우선 구한다. ④ x_1' 에 y를 더한 결과가 m=8, $T_2(k)$ = 0, $T_4(k)$ = 0 인 경우의 2차 방정식의 해이다. 따라서 m=8, $T_2(k)$ = 0, $T_4(k)$ = 0 인 경우, 2차 방정식의 두 해 x_1, x_2 는 식 (11)과 같이 표현될 수 있다.

$$x_1 = y + c^{33} + c^{66} + c^{128} + c^{144} + c^{192}$$
$$x_2 = x_1 + 1 \quad (11)$$

$GF(2^m)$ 상의 3차 방정식은 식 (12)와 같이 표현될 수 있다.

$$y^3 + ay^2 + by + c = 0 \quad (12)$$

y를 $a+x'$이라 치환하면, 식 (12)는 식 (13)과 같이 변형된다.

$$x'^3 + (a^2+b)x' + (ab+c) = 0 \quad (13)$$

만약 $a^2+b=0$ 이면 3차 방정식은 3 중해 $x=(ab+c)^{1/3}$ 을 갖는다. 만약 $a^2+b\neq 0$ 이면 $x' = (a^2+b)^{1/3} \cdot x$라 치환하면 식 (13)은 식 (14)와 같이 된다.

$$x^3+x+C_k=0, \text{ 여기서, } C_k=(ab+c)/(a^2+b)^{3/2} \quad (14)$$

3차 방정식은 일반적으로 식 (15)와 같은 2차와 1차 방정식으로 분류될 수 있다.

$$x^3 + x + C_k = (x+m)(x^2+mx+n) \quad (15)$$

따라서 m, n, 그리고 C_k의 관계는 식 (16)과 같다.

$$m^2 + n = 1,\ m \cdot n = C_k \quad (16)$$

만약 $x=m \cdot X$ 라 치환하면, 식 (15)의 우변에서의 2차 방정식은 다음과 같이 변형될 수 있다.

$$X^2 + X + k = 0, \text{ 여기서, } k=n/m^2 \quad (17)$$

식 (16), (17)로 부터 m,n, 그리고 C_k를 k로 표현하면 식 (18)과 같다.

$$m = 1/(1+k)^{1/2},\ n = k/(1+k),\ C_k = m \cdot n = k/(1+k)^{3/2} \quad (18)$$

$T_2(k)$=0 일 경우 2차 방정식의 해는 존재하므로, $T_2(k)$=0인 k 에 대한 C_k 값은 미리 계산하여 ROM (read only memory) 에 저장한다. 이를 바탕으로 3차 방정식의 해를 구하는 과정은 다음과 같이 요약될 수 있다. ① 식 (14)를 이용하여 C_k를 구하고, C_k 에 대응되는 k 값을 미리 계산된 표를 이용하여 선택한다. ② $T_2(k)$=0 인가를 확인하여, $T_2(k)$=0 이면 식 (18)을 이용하여 m,n을 구한다. ③ 식 (17)을 이용하여 2차 방정식의 두 해 X_1' , X_2' 을 구한다. ④ 식 (14) 의 3차 방정식의 3해 $x_1 = m \cdot X_1'$, $x_2 = m \cdot X_2'$, $x_3 = m$ 을 구할 수 있다. ⑤ 식 (13) 의 3차 방정식의 3해 $x_1' = (a^2+b)^{1/3} \cdot x_1$, $x_2' = (a^2+b)^{1/3} \cdot x_2$, $x_3' = (a^2+b)^{1/3} \cdot x_3$을 구할 수 있다. ⑥ 식 (12) 의 3차 방정식의 3해 $y_1 = a + (a^2+b)^{1/3} \cdot x_1$, $y_2 = a + (a^2+b)^{1/3} \cdot x_2$, $y_3 = a + (a^2+b)^{1/3} \cdot x_3$을 구할 수 있다.

2. 2중 오류정정 RS 부호의 새로운 복호 알고리듬

일반적으로 RS 부호의 복호과정은 다음과 같은 5단계로 구성된다.

1) 오증요소 (syndrome component) s_i, $0 \le i \le 2t-1$ 계산
2) 오류위치다항식 (error locator polynomial) $\sigma(x)$ 계산
3) 오류위치번호 (error location number) 계산

4) 오류치 (error value) 계산
5) 오류정정 (error correction) 수행

부호계열 $c(x)$를 전송하였을때 전송도중 오류 $e(x)$가 발생하였다면 수신계열 $r(x)$는 식 (19)와 같다.

$$r(x) = c(x) + e(x) \tag{19}$$

α 를 유한체 $GF(2^m)$상의 원시원(primitive element)라 하면 $\alpha^i(0\le i\le 2t-1)$은 생성다항식 $g(x)$의 해가 되며, α^i를 식 (19)에 대입하면 식 (20)을 구할수 있다.

$$\begin{aligned} &c(\alpha^i) = 0,\ 0\le i\le 2t-1 \\ &r(\alpha^i) = e(\alpha^i),\ 0\le i\le 2t-1 \end{aligned} \tag{20}$$

오증요소 (syndrome component) si $(0\le i\le 2t-1)$ 는 식 (21)과 같다.

$$\begin{aligned} s_i &= r(\alpha^i) = e((\alpha^i) \\ &= r_0 + r_1\alpha^i + r_2\alpha^{2i} + \cdots + r_{n-1}\alpha^{(n-1)i} \\ &= r_0 + \alpha^i(r_1 + \alpha^i(r_2 + \alpha^i(r_3 + \cdots + \alpha^i(r_{n-2} + r_{n-1}\alpha^i))\cdots) \end{aligned} \tag{21}$$

2 중오류정정 능력을 갖는 (255,251) RS 부호의 오증 생성기를 설계하기 위한 기본 이론을 도입한다. 오증 생성기는 근본적으로 최소다항식 수신계열 $r(x)$를 $(x+\alpha^i)$로 나누는 제산 회로 (division circuit)이다. $GF(2^8)$상의 임의의 원소 b $(= b_0+b_1\alpha+b_2\alpha^2+b_3\alpha^3+b_4\alpha^4+b_5\alpha^5+b_6\alpha^6+b_7\alpha^7)$ 에 각각 1, α, α^2, 및 α^3을 곱할 경우, 이는 식 (22)와 같이 표현된다.

$$\begin{aligned} 1\cdot b &= b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4 + b_5\alpha^5 + b_6\alpha^6 + b_7\alpha^7 \\ \alpha\cdot b &= b_7 + b_0\alpha + (b_1+b_7)\alpha^2 + (b_2+b_7)\alpha^3 + (b_3+b_7)\alpha^4 + b_4\alpha^5 + b_5\alpha^6 + b_6\alpha^7 \\ \alpha^2\cdot b &= b_6 + b_7\alpha + (b_0+b_6)\alpha^2 + (b_1+b_6+b_7)\alpha^3 + (b_2+b_6+b_7)\alpha^4 + (b_3+b_7)\alpha^5 + b_4\alpha^6 + b_5\alpha^7 \\ \alpha^3\cdot b &= b_5 + b_6\alpha + (b_5+b_7)\alpha^2 + (b_0+b_5+b_6)\alpha^3 + (b_1+b_5+b_6+b_7)\alpha^4 + (b_2+b_6+b_7)\alpha^5 + (b_3+b_7)\alpha^6 + b_4\alpha^7 \end{aligned} \tag{22}$$

식 (21), (22)를 바탕으로 설계된 오증 요소 생성 회로는 그림 1과 같다.

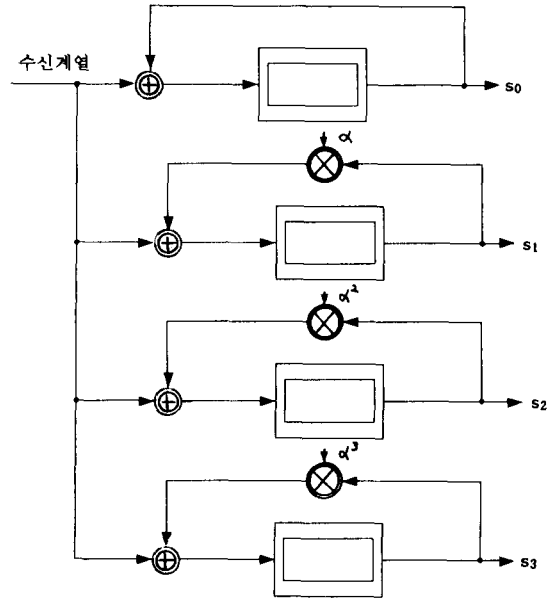

그림 1. 2중 오류정정 RS 부호의 오증 요소 생성 회로

Fig. 1. Circuit for syndrome generator of double-error-correction RS codes.

전송도중 발생한 오류계열은 식 (23)과 같다.

$$e(x) = e_0 + e_1x + e_2x^2 + \cdots + e_{n-1}x^{n-1} \tag{23}$$

실제로 v $(0\le v\le t)$ 개의 오류가 발생했다면, 식 (23)은 식 (24)와 같이 변형될 수 있다.

$$e(x) = e_{i1}x^{j1} + e_{i2}x^{j2} + \cdots + e_{iv}x^{jv} \tag{24}$$

따라서 오증요소 s_i는 수신계열에 생성다항식의 해 α^i $(0\le i\le 2t-1)$을 대입하여 구해지므로 식 (25)와 같다.

$$\begin{aligned} s_0 &= e_{i1} + e_{i2} + \cdots + e_{iv} \\ s_1 &= e_{i1}\cdot\alpha^{j1} + e_{i2}\cdot\alpha^{j2} + \cdots + e_{iv}\cdot\alpha^{jv} \\ &\cdots \\ s_{2t-1} &= e_{i1}\cdot\alpha^{(2t-1)j1} + e_{i2}\cdot\alpha^{(2t-1)j2} + \cdots + e_{iv}\cdot\alpha^{(2t-1)jv} \end{aligned} \tag{25}$$

오류치 $e_{ik}(1\le k\le v)$를 $Y_k(1\le k\le v)$라 치환하고, 오류위치번호 α^{jk} $(1\le k\le v)$ 를 $X_k(1\le k\le v)$라 치환하면 오증요소는 식 (26)과 같다.

$$S_0 = \sum_{k=1}^{v} Y_k = Y_1 + Y_2 + \cdots + Y_v$$
$$S_1 = \sum_{k=1}^{v} Y_k X_k = Y_1 \cdot X_1 + Y_2 \cdot X_2 + \cdots + Y_v \cdot X_v$$
$$\cdots$$
$$S_{2t-1} = \sum_{k=1}^{v} Y_k X_k^{2t-1} = Y_1 \cdot X_1^{2t-1} + Y_2 \cdot X_2^{2t-1} + \cdots + Y_v \cdot X_v^{2t-1} \quad (26)$$

식 (26)은 오증 요소와 오류치 Y_k, 오류위치 X_k 와의 관계를 나타내고 있다. 식 (26)을 이용하여 오류위치와 오증요소로 부터 오류치를 구할 수 있다. 오류정정능력이 2인 RS 부호의 수신 부호어에 발생한 오류 갯수 판별 알고리듬은 다음과 같다.

만약 수신부호어에 단일 오류가 발생했다면, 즉, 오류다항식이 $e(x) = ex^i$ $(0 \le i \le n-1,\ e_i \in GF(2^m))$ 인 경우, 오증 요소는 식 (27)과 같다.

$$S_0 = e_i$$
$$S_1 = e_i \cdot \alpha^i \quad (27)$$
$$S_2 = e_i \cdot \alpha^{2i}$$
$$S_3 = e_i \cdot \alpha^{3i}$$

여기서, ei : 오류치
α^i : 오류위치

만약 수신부호어에 2중 오류가 발생했다면, 즉, 오류다항식이 $e(x) = ex^i + ejx^j$, $(0 \le i < j \le n-1,\ e_i, e_j \in GF(2^m))$ 인 경우, 오증 요소는 식 (28)과 같다.

$$S_0 = ei + e_j$$
$$S_1 = ei \cdot \alpha^i + e_j \cdot \alpha^j \quad (28)$$
$$S_2 = ei \cdot \alpha^{2i} + e_j \cdot \alpha^{2j}$$
$$S_3 = ei \cdot \alpha^{3i} + e_j \cdot \alpha^{3j}$$

여기서, e_i, e_j : 오류치
α^i, α^j : 오류위치

따라서 2중 오류정정 RS의 부호의 복호는 오증요소로 부터 오류치 (e_i, e_j), 오류위치 (α^i, α^j)를 구하는 것이 된다. 식 (28)을 변형하면 식 (29)를 구할수 있다.

$$(S_0\alpha^j + S_1)(S_2\alpha^j + S_3) = (S_1\alpha^j + S_2)^2 \quad (29)$$

식 (29)는 식 (30)과 같이 변형될수 있다.

$$(S_1^2 + S_0 \cdot S_2)\alpha^{2j} + (S_0 \cdot S_3 + S_1 \cdot S_2)\alpha^j + (S_2^2 + S_1 \cdot S_3) = 0 \quad (30)$$

식 (30)의 각 계수를 식 (31)과 같이 표현하자.

$$D_1 = S_1^2 + S_0 \cdot S_2$$
$$D_2 = S_0 \cdot S_3 + S_1 \cdot S_2$$
$$D_3 = S_2^2 + S_1 \cdot S_3 \quad (31)$$

식 (31)을 이용하여 식 (30)을 표현하면 $D_1 \cdot \alpha^{2j} + D_2 \cdot \alpha^j + D_3 = 0$ 이 되어 $GF(2^m)$ 상의 2차 방정식이 된다. 식 (31)에서 α^j 대신 x를 치환하면 식 (32) 와 같이 변경된다.

$$D_1 \cdot x^2 + D_2 \cdot x + D_3 = 0 \quad (32)$$

2차의 오류위치다항식은 식 (33)과 같이 변형될 수 있다.

$$\sigma(x) = x^2 + \sigma_1 x + \sigma_2 \quad (33)$$
여기서, $\sigma_1 = D_2/D_1$, $\sigma_2 = D_3/D_1$

식 (33)과 같은 2차 오류위치다항식에서 $x = \sigma_1 x'$ 로 치환하면 식 (34)와 같은 변형된 affine 다항식 형태의 오류위치다항식을 구할수 있다.

$$\sigma(x') = x'^2 + x' + k \quad (34)$$
여기서, $k = \sigma_2/\sigma_1^2$

상기의 계수들과 오증요소들을 이용하면 이중 오류정정 RS 부호의 오류 갯수 판별 알고리듬을 생성할 수 있다.

① $S_0 = S_1 = S_2 = S_3 = 0$ 인 경우 :
수신 부호어에 심벌 오류가 발생하지 않은 것으로 판단.

② $S_0 \neq 0$, $S_3 \neq 0$, $D_1 = 0$, $D_2 = 0$, $D_3 = 0$ 인 경우:
수신 부호어에 단일 심벌오류가 발생한 것으로 판단.

③ $D_1 \neq 0$, $D_2 \neq 0$, $D_3 \neq 0$, $T_2(k) = 0$ 인 경우 :
수신 부호어에 2중 심벌 오류가 발생한 것으로 판단.

④ 상기의 ①, ②, ③ 이외의 경우 :
수신 부호어에 3중 심벌 이상의 오류가 발생한 것으로 판단.

따라서 위의 방법으로 수신부호어에 발생한 오류의 갯수를 판별하면, 이를 근거로 오류위치 및 오류치를 결정해야 한다. 단일 오류 및 이중 오류가 발생한 경우의 오류위치 및 오류치는 각각 다음과 같이 구할 수 있다.

단일 심벌 오류가 발생한 경우, $s_0 = e_i$, $s_1 = e_i \cdot \alpha^i$ 이므로, 단일 오류에 대한 오류치와 오류위치는 각각 식 (35)와 같다.

$$X_1 = s_1/s_0 \text{ : 오류위치}$$
$$Y_1 = s_0 \text{ : 오류치} \tag{35}$$

2중 심벌 오류가 발생의 경우, 오류위치 X_1, X_2를 해로 갖는 오류위치 다항식을 식 (36)과 같이 정의한다.

$$\sigma(x) = (x+X_1)(x+X_2) = x^2 + \sigma_1 x + \sigma_2 \tag{36}$$

유한체상의 2차 방정식의 해를 구하는 방법은 GF(2^m)상의 모든 원소를 대입하여 해를 구하는 Chien 기법과 모든 계수에 대응되는 해를 미리 표 (ROM)에 기억하여 계수에 대한 해를 찾는 Pol*k*inghorn 기법 등이 있다. 그러나 Chien의 방법은 복호기에서 수신 부호어를 한 프레임을 지연한 후에 오류위치를 알수 있고, Pol*k*inghorn 방법은 회로 구성이 매우 복잡해지거나 외부에 별도의 회로를 부가해야 한다는 문제점이 있다. 따라서 본 논문에서는 2차 방정식을 이용하여 해를 구하는 기존의 복호 방법과 2차 오류위치 다항식을 변형하여 affine 다항식으로 변형한후 이를 이용하여 해를 구하는 기법을 도입하여 회로 구성이 간단하여 복호기의 복잡도를 현저하게 낮출수 있는 새로운 오류정정 알고리듬을 제시한다. 식 (34)와 같은 2차 오류 위치 다항식의 해가 오류위치가 된다. GF(2^8)에서의 원소 k에 대한 $T_2(k)$와 $T_4(k)$는 각각 식 (37)과 같다.

$$T_2(k) = \sum_{i=0}^{7} k^{2^i}$$
$$= k + k^2 + k^4 + k^8 + k^{16} + k^{32} + k^{64} + k^{128}$$
$$T_4(k) = \sum_{i=0}^{(m-2)/2} k^{2^{2i}}$$
$$= \sum_{i=0}^{3} k^{2^{2i}} = k + k^4 + k^{16} + k^{64} \tag{37}$$

식 (34)는 $T_2(k) = 0$일때 해를 갖는다. 한편 k는 GF(2^8)의 한 원소이므로 식 (38)과 같이 표시된다.

$$k = k_0 + k_1 \cdot \alpha + k_2 \cdot \alpha^2 + k_3 \cdot \alpha^3 + k_4 \cdot \alpha^4 + k_5 \cdot \alpha^5 + k_6 \cdot \alpha^6 + k_7 \cdot \alpha^7 \tag{38}$$
여기서, $k_i \in GF(2)$ (i=0, 1, … , 7)

식 (38)의 양변에 트레이스를 취하면 식 (39)와 같다.

$$T_2(k) = k_0 \cdot T_2(1) + k_1 \cdot T_2(\alpha) + k_2 \cdot T_2(\alpha^2) + k_3 \cdot T_2(\alpha^3) + k_4 \cdot T_2(\alpha^4) + k_5 \cdot T_2(\alpha^5) + k_6 \cdot T_2(\alpha^6) + k_7 \cdot T_2(\alpha^7) \tag{39}$$

한편, GF(2^8) 에서 $T_2(1) = T_2(\alpha) = T_2(\alpha^2) = T_2(\alpha^3) = T_2(\alpha^4) = T_2(\alpha^6) = T_2(\alpha^7) = 0$ 이며 $T_2(\alpha^5) = 1$ 이므로, 특정 원소 k에대한 트레이스 값은 식 (40)과 같다.

$$T_2(k) = k_5 \tag{40}$$

따라서 원소 k의 α^5 의 계수 k_5가 0 일 경우만, $T_2(k)=0$ 이 되므로 식 (34)의 해가 존재한다.

만약 식 (34)의 k에 대하여 $T_2(k) = 0$ 이고 $T_4(k) = 1$ 이면, 정리 2에 의하여 식 (34)의 오류위치다항식 $\sigma(x')$의 두해 x_1, x_2 는 각각 식 (41)과 같다.

$$x_1 = k^{33} + k^{66} + k^{128} + k^{144} + k^{192}$$
$$x_2 = x_1 + 1 \tag{41}$$

그러나 식 (34)의 k에 대하여 $T_2(k) = 0$ 이고, $T_4(k) = 0$ 이면, 두 해 x_1, x_2은 식 (42)와 같다.

$$x_1 = y + c^{33} + c^{66} + c^{128} + c^{144} + c^{192}$$
$$x_2 = x_1 + 1 \tag{42}$$

여기서, y : $T_2(y) = 1$ 이 되는 GF(2^8)내의 임의의 원소 $k_1 = y + y^2$,
$c = k + k_1$,
$T_4(c) = T_4(k+k_1) = 1$

식 (34)의 두 해가 x_1, x_2다면, 이에 대응되는 오류위치 X_1, X_2는 식 (43)과 같다.

$$X_1 = \sigma_1 x_1,\ X_2 = \sigma_1 x_2 \tag{43}$$

$T_2(k) = 0$ 인 경우, 상기의 오류위치에 대응하는 오류치 Y_1, Y_2는 식 (44) 과 같다.

$$Y_1 = (s_0 \cdot X_2 + s_1)/(X_1 + X_2)$$
$$Y_2 = (s_0 \cdot X_1 + s_1)/(X_1 + X_2) \tag{44}$$

그리고 $T_2(k) \neq 0$ 이면 $\sigma(x)$의 해는 존재하지 않는다.

상기와 같은 복호 방식에서의 복호 흐름도는 그림 2와 같다.

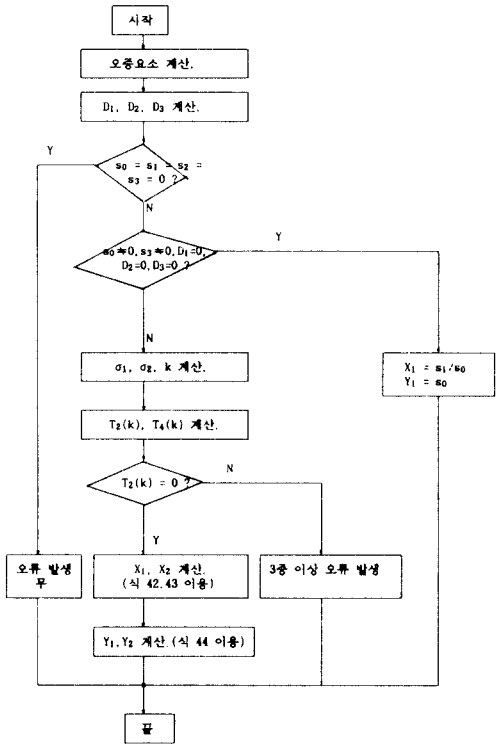

그림 2. 기존의 RS 부호의 복호 흐름도
Fig. 2. Flow diagram for conventional RS decoder.

상기의 오류정정 알고리듬을 바탕으로 복호기를 설계하면 그림 3과 같다.

그림 3에서 알 수 있듯이 기존의 알고리듬을 이용하여 복호기를 LSI 회로로 설계한 경우, 2차 방정식의 해를 구하기 위하여 외부에 별도의 ROM 을 이용하거나 복잡한 논리회로들로 구성되어야 한다. 이는 복호기의 복잡도를 현저히 증가시키는 원인이 된다. 따라서 간단한 논리회로 들을 이용하여 2차 방정식의 해를 구할 수 있어서 복호기의 복잡도를 현저하게 낮출수 있는 새로운 방법을 제시한다. 이 방법은 정리3, 4와 같은 Hilbert의 정리를 기초를 두고 구성된다.[17]

[정리 3] $GF(p^m)$상의 한 원소 $k = x - x^p$ 를 만족하는 $GF(p^m)$상의 한 원소 x를 갖을 경우, k의 트레이스인 $Tr(k) = 0$ 이다.

(증명) $k = x - x^p$ 의 양변에 트레이스를 취하면 $Tr(k) = Tr(x) - Tr(x^p)$ 가 된다. 트레이스 특성에 의해 $Tr(x) = Tr(x^p)$ 를 만족하므로 $Tr(k) = 0$ 이 된다. (증명완료)

[정리 4] k, y가 $GF(p^m)$상의 임의의 원소일 경우, 또 다른 원소 x를 식 (45)와 같이 정의하자.

$$x = k \cdot y^p + (k + k^p) \cdot y^{p^2} + \cdots + (k + k^p + \cdots + k^{p^{m-2}}) \cdot y^{p^{m-1}} \quad (45)$$

그러면 $x - x^p$ 는 식 (46)과 같다.

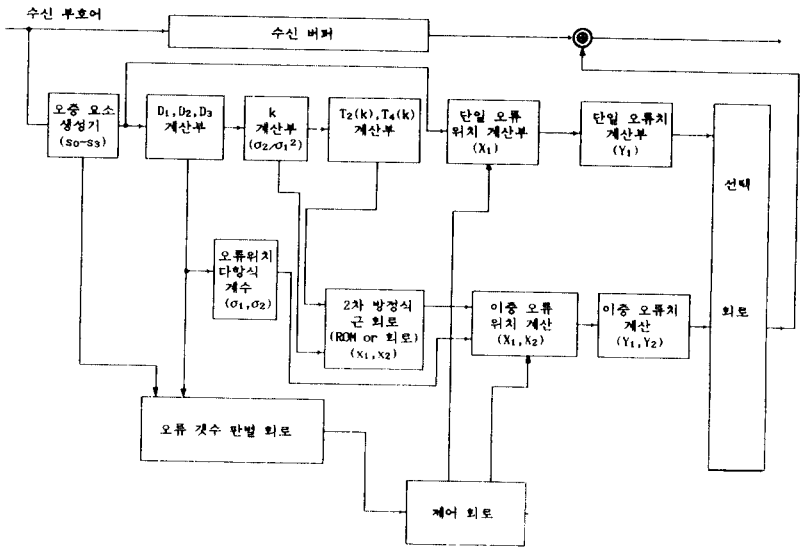

그림 3. 기존의 RS 부호의 복호기 구성도
Fig. 3. Structure of conventional RS decoder.

$$x-x^p = k \cdot [\mathrm{Tr}(y) - y] - y\,[\mathrm{Tr}(k) - k] \quad (46)$$

(증명) 식 (45)를 p승하면 다음과 같다.

$$x^p = k^p \cdot y^{p^2} + (k^p + k^{p^2}) \cdot y^{p^3} + \cdots + (k^p + k^{p^2} + \cdots + k^{p^{m-1}}) \cdot y^{p^m} \quad (47)$$

식 (45)에서 식 (47)을 빼면 식 (48)이 된다.

$$x - x^p = k \cdot (y^p + y^{p^2} + \cdots + y^{p^{m-1}}) - (k^p + k^{p^2} + \cdots + k^{p^{m-1}}) \cdot y^{p^m} \quad (48)$$

트레이스의 특성에 의하여 식 (49) 가 성립한다.

$$y^p + y^{p^2} + \cdots + y^{p^{m-1}} = \mathrm{Tr}(y) - y$$
$$k^p + k^{p^2} + \cdots + k^{p^{m-1}} = \mathrm{Tr}(k) - k \quad (49)$$

따라서 식 (48)은 식 (50)과 같이 변형될 수 있다.

$$x - x^p = k \cdot (\mathrm{Tr}(y) - y) - y \cdot (\mathrm{Tr}(k) - k) \quad (50)$$

(증명완료)

정리 4로 부터 $GF(p^m)$의 특정 원소(fixed element) y를 $\mathrm{Tr}(y) = 1$ 을 만족하도록 선택하고 $\mathrm{Tr}(k) = 0$ 이면, 식 (50)에 의해 $GF(p^m)$ 상의 임의의 원소 k는 2차 방정식 $k = x - x^p$ 를 만족하므로, 이 때의 x가 $GF(p^m)$ 상의 임의의 원소 k에 대한 2차 방정식의 해가 된다.

일반적으로 컴팩트 디스크에서 이용되고 있는 RS 부호는 $GF(2^8)$ 상의 (255,251) RS 부호를 단축한 (32,28) RS 부호와 (28,24) RS 부호이다. 따라서 $p = 2$이고 $m = 8$가 되며, 이를 정리 3과 정리 4에 적용하면 오류위치다항식를 쉽게 풀수 있는 다음과 같은 알고리듬을 유도할 수 있다. 2차 방정식에서 $T_2(k) = 0$ 이면 2차 방정식의 해가 존재하므로 다음과 같은 단계를 통하여 오류위치다항식의 해를 구할 수 있다.

(단계 1) $T_2(y) = 1$인 $GF(2^8)$상의 임의의 원소 $y = \alpha^5$ 를 선택한다. 즉, $T_2(\alpha^5) = 1$

(단계 2) x를 식 (45)를 이용하여 식 (51)과 같이 표현한다.

$$\begin{aligned} x = {} & k \cdot y^2 + (k+k^2) \cdot y^4 + (k+k^2+k^4) \cdot y^8 \\ & + (k^2+k^4+k^8) \cdot y^{16} + (k+k^2+k^4+k^8+k^{16}) \cdot y^{32} \\ & + (k+k^2+k^4+k^8+k^{16}+k^{32}) \cdot y^{64} \cdot \\ & + (k+k^2+k^4+k^8+k^{16}+k^{32}+k^{64}) \cdot y^{128} \\ = {} & (y^2+y^4+y^8+y^{16}+y^{32}+y^{64}+y^{128}) \cdot k \\ & + (y^4+y^8+y^{16}+y^{32}+y^{64}+y^{128}) \cdot k^2 \\ & + (y^8+y^{16}+y^{32}+y^{64}+y^{128}) \cdot k^4 + (y^{16}+y^{32}+y^{64}+y^{128}) \cdot k^8 \\ & + (y^{32}+y^{64}+y^{128}) \cdot k^{16} + (y^{64}+y^{128}) \cdot k^{32} + y^{128} \cdot k^{64} \end{aligned} \quad (51)$$

(단계 3) 식 (51)의 y를 α^5 로 치환하면 식 (52)와 같다.

① k 의 계수 $= y^2+y^4+y^8+y^{16}+y^{32}+y^{64}+y^{128}$
$= \alpha^{10}+\alpha^{20}+\alpha^{40}+\alpha^{80}+\alpha^{160}+\alpha^{65}$
$= 1+\alpha^5 = \alpha^{138}$

② k^2 의 계수 $= y^4+y^8+y^{16}+y^{32}+y^{64}+y^{128}$
$= 1+\alpha^2+\alpha^4+\alpha^6 = \alpha^{150}$

③ k^{2^2} 의 계수 $= y^8+y^{16}+y^{32}+y^{64}+y^{128}$
$= 1+\alpha^5+\alpha^6+\alpha^7 = \alpha^{89}$

④ k^{2^3} 의 계수 $= y^{16}+y^{32}+y^{64}+y^{128}$
$= 1+\alpha+\alpha^3+\alpha^7 = \alpha^{237}$

⑤ k^{2^4} 의 계수 $= y^{32}+y^{64}+y^{128}$
$= \alpha+\alpha^2+\alpha^4+\alpha^5+\alpha^6 = \alpha^{121}$

⑥ k^{2^5} 의 계수 $= y^{64}+y^{128} = \alpha^4+\alpha^7 = \alpha^{227}$

⑦ k^{2^6} 의 계수 $= y^{128} = \alpha+\alpha^2+\alpha^3+\alpha^5 = \alpha^{130}$

$$\begin{aligned} x = {} & (1+\alpha^5) \cdot k + (1+\alpha^2+\alpha^4+\alpha^6) \cdot k^2 + (1+\alpha^5+\alpha^6+\alpha^7) \cdot k^4 + (1+\alpha+\alpha^3+\alpha^7) \cdot k^8 \\ & + (\alpha+\alpha^2+\alpha^4+\alpha^5+\alpha^6) \cdot k^{16} + (\alpha^4+\alpha^7) \cdot k^{32} \\ & + (\alpha+\alpha^2+\alpha^3+\alpha^5) \cdot k^{64} \end{aligned} \quad (52)$$

식 (52)의 k 대신 식 (38)의 우변을 대입하면 식 (52)는 식 (53)과 같이 변형된다.

$x = k_0 \cdot$ (식 (52)의 k 대신 "1" 대입) $+ k_1 \cdot$ (식 (52)의 k 대신 "α" 대입) $+ k_2 \cdot$ (식 (52)의 k 대신 "α^2" 대입) $+ k_3 \cdot$ (식 (52)의 k 대신 "α^3" 대입) $+ k_4 \cdot$ (식 (52)의 k 대신 "α^4" 대입) $+ k_5 \cdot$ (식 (52)의 k 대신 "α^5" 대입) $+ k_6 \cdot$ (식 (52)의 k 대신 "α^6" 대입) $+ k_7 \cdot$ (식 (52)의 k 대신 "α^7" 대입) (53)

(단계 4) 식 (52)의 k 대신 표준기저의 각 원소 1, α, α^2, α^3, α^4, α^5, α^6, α^7를 차례로 대입하면 k 의 각 계수 k_i (i=0, … ,7) 와 x의 각 차수의 계수와의 관계식을 다음과 같이 구할 수 있다.

①식 (52)의 k 대신 "1" 를 대입하면, k의 상수항의 계수 k_0가 x의 각 차수에 미치는 영향을 나타낸다.

$(\alpha + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^7) \cdot k_0$

②식 (52)의 k 대신 "α" 를 대입하면, k의 계수 k_1이 x의 각 차수에 미치는 영향을 나타낸다.

$(\alpha + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^7) \cdot k_1$

③식 (52)의 k 대신 "α^2" 를 대입하면, k의 계수 k_2가 x의 각 차수에 미치는 영향을 나타낸다.

$(\alpha + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^7) \cdot k_2$

④식 (52)의 k 대신 "α^3" 를 대입하면, k의 계수 k_3이 x의 각 차수에 미치는 영향을 나타낸다.

$(1 + \alpha^2 + \alpha^3 + \alpha^5) \cdot k_3$

⑤식 (52)의 k 대신 "α^4" 를 대입하면, k의 계수 k_4가 x의 각 차수에 미치는 영향을 나타낸다.

$(\alpha + \alpha^2 + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^7) \cdot k_4$

⑥식 (52)의 k 대신 "α^5" 를 대입하면, k의 계수 k_5가 x의 각 차수에 미치는 영향을 나타낸다.

$(1) \cdot k_5$

⑦식 (52)의 k 대신 "α^6" 를 대입하면, k의 계수 k_6이 x의 각 차수에 미치는 영향을 나타낸다.

$(1 + \alpha^2 + \alpha^7) \cdot k_6$

⑧식 (52)의 k 대신 "α^7" 를 대입하면, k의 상수항의 계수 k_7이 x의 각 차수에 미치는 영향을 나타낸다.

$(\alpha^4 + \alpha^6) \cdot k_7$

그러므로 원소 x와 k의 각 계수와의 관계는 식 (54)와 같다.

$$\begin{aligned} x &= x_{10} + x_{11}\alpha^6 + x_{12}\alpha^5 + x_{13}\alpha^6 + x_{14}\alpha^6 + x_{15}\alpha^6 + x_{16}\alpha^6 + x_{17}\alpha^6 \\ &= (\alpha + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^7) \cdot k_0 \\ &+ (\alpha^3 + \alpha^5 + \alpha^6 + \alpha^7) \cdot k_1 \\ &+ (\alpha + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^7) \cdot k_2 \\ &+ (1 + \alpha^2 + \alpha^3 + \alpha^5) \cdot k_3 + (\alpha + \alpha^2 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7) \cdot k_4 + (1) \cdot k_5 + (1 + \alpha^2 + \alpha^5) \cdot k_6 + (\alpha^4 + \alpha^6) \cdot k_7 \end{aligned} \quad (54)$$

(단계 5) k 의 계수들 k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7과 오류위치 다항식의 한 해 x와의 관계는 다음과 같은 행열로 표현될 수 있다. 따라서 식 (55)와 같은 행열을 이용하여 오류위치다항식 $\sigma(x')$의 하나의 해 x 은 구할 수 있다.

$$X = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7) \cdot \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad (55)$$

따라서 x의 각 성분 요소는 식 (56)과 같이 k의 성분 요소들로 표현될 수 있다.

$$\begin{aligned} x_0 &= k_3 + k_5 + k_6 \\ x_1 &= k_0 + k_2 + k_4 \\ x_2 &= k_0 + k_3 + k_4 + k_6 \\ x_3 &= k_1 + k_2 + k_3 + k_4 \\ x_4 &= k_0 + k_7 \\ x_5 &= k_1 + k_2 + k_3 + k_4 + k_6 \\ x_6 &= k_0 + k_1 + k_2 + k_4 + k_7 \\ x_7 &= k_0 + k_1 + k_2 + k_4 \end{aligned} \quad (56)$$

식 (55)에서 구한 x가 오류위치다항식의 한 해 x_1이며, 또 다른 한 해는 $x_2 = x_1 + 1$ 이므로 x_2는 x_1를 이용하여 쉽게 구할 수 있다. 식 (56)를 바탕으로 구현된 임의의 원소 k에 대한 오류다항식 $\sigma(x')$의 두해를 구하는 회로는 그림 4와 같다.

두 해 x_1, x_2가 결정되면 실제의 오류위치 X_1, X_2는 식 (43)과 같이, 그리고 이에 대응되는 오류치 Y_1, Y_2는 식 (44)를 이용하여 구할 수 있다. 한편, $T_2(k) \neq$이면 $\sigma(x)$의 해는 존재하지 않으므로, 이 경우는 3중 이상의 오류가 발생한 것으로 복호기는 판단한다. 상기와 같이 제시된 복호 알고리듬을 이용하여 이중 오류 정정 RS 부호의 복호 흐름도를 작성하면 그림 5와 같다.

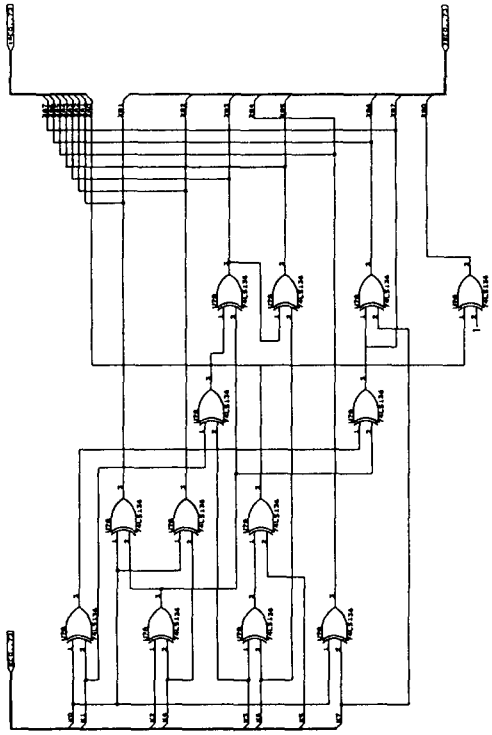

그림 4. 계수 k로 부터 오류위치다항식의 두 근을 구하는 회로

Fig. 4. Circuit for solving the roots from k.

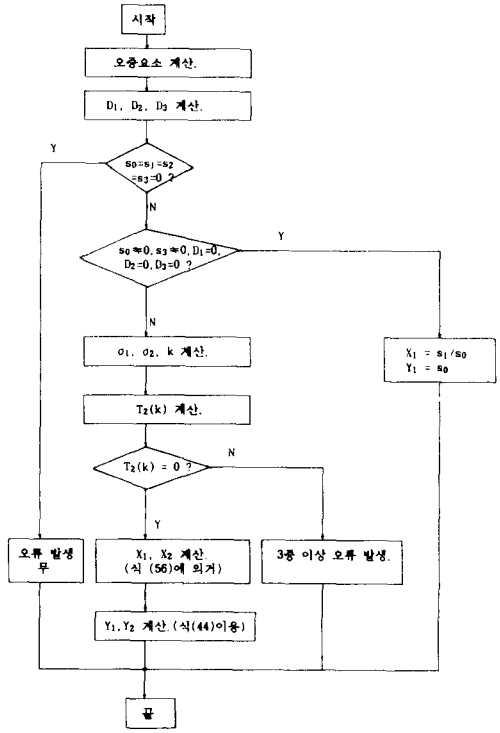

그림 5. 제시된 복호 알고리듬을 이용한 2중 오류정정 RS 부호의 복호 흐름도

Fig. 5. Flow diagram for double-error-correction RS decoder.

그림 5와 같은 복호 흐름도와 상기의 복호 알고리듬을 이용하여 설계된 2중 오류정정 RS 부호의 복호기는 그림 6과 같다.

본 논문에서 제안한 복호 알고리듬의 타당성은 다음 두 예제를 통해 입증한다.

(예제 1) 부호계열 $c(x) = 0$ 을 전송하였을 경우, 수신계열이 $r(x) = \alpha^2x^3$ 이다면 오류계열은 $e(x) = \alpha^2x^3$이다. 오증요소는 다음과 같다.

$$s = (s_0, s_1, s_2, s_3) = (\alpha^2, \alpha^5, \alpha^8, \alpha^{11})$$

한편, $s_0 \neq 0$, $s_3 \neq 0$, $D_1 = s_1^2 + s_0 \cdot s_2 = \alpha^{10} + \alpha^2 \cdot \alpha^8 = 0$, $D_2 = s_1 \cdot s_3 + s_1 \cdot s_2 = \alpha^2 \cdot \alpha^{11} + \alpha^5 \cdot \alpha^8 = 0$ 이므로, 복호기는 단일 심벌오류가 발생한 것으로 판단한다. 따라서 식 (35)에 의해 오류위치와 오류치는 계산하면 각각 다음과 같다.

$$X_1 = s_1/s_0 = \alpha^5/\alpha^2 = \alpha^3$$
$$Y_1 = s_0 = \alpha^2$$

그러므로 오류계열 $e(x) = \alpha^2x^3$ 이다.

$$r(x) + e(x) = \alpha^2x^3 + \alpha^2x^3 = 0 = c(x)$$

(예제 2) 부호계열 $c(x) = 0$ 을 전송하여 수신계열 $r(x) = \alpha x + \alpha^3x^5$ 이다면, 오류계열은 $e(x) = \alpha x + \alpha^3x^5$ 이다. 오증요소는 다음과 같다.

$$s = (s_0, s_1, s_2, s_3) = (\alpha^{51}, \alpha^{193}, \alpha^{24}, \alpha^{228})$$

오류위치다항식 $\sigma(x) = x_2 + \sigma_1 x + \sigma_2$에서의 계수 σ_1, σ_2는 각각 다음과 같이 구할 수 있다.

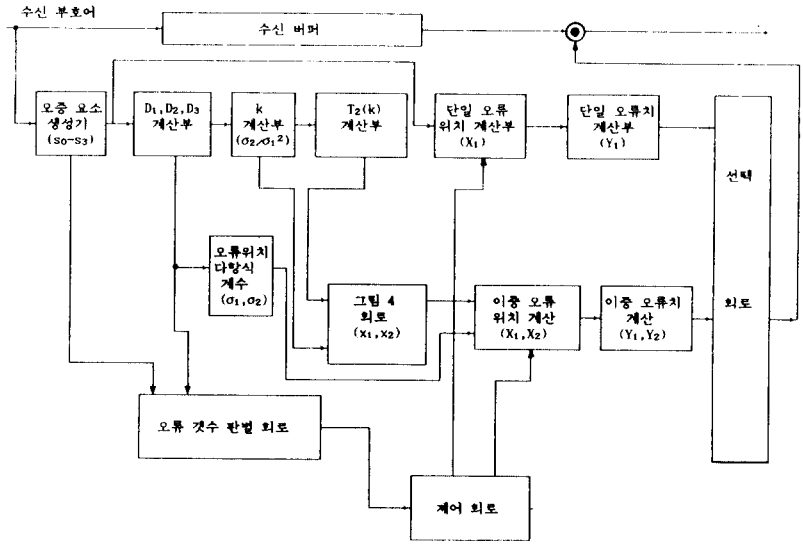

그림 6. 재시된 이중 오류 정정 RS 부호의 복호기 구성도
Fig. 6. Decoder Structure for double-error-correction RS codes.

$$\begin{bmatrix}\sigma_2\\ \sigma_1\end{bmatrix}=\begin{bmatrix}S_0 & S_1\\ S_1 & S_2\end{bmatrix}^{-1}\begin{bmatrix}S_2\\ S_3\end{bmatrix}$$
$$=\frac{1}{S_0S_2+S_1^2}\begin{bmatrix}S_2 & S_1\\ S_1 & S_0\end{bmatrix}\begin{bmatrix}S_2\\ S_3\end{bmatrix}$$
$$=\begin{bmatrix}\alpha^6\\ \alpha^{101}\end{bmatrix}$$

따라서 $\sigma(x) = x^2 + \sigma^{101}x + \sigma^6$이 된다. 그러므로 식 (34)에 의하여 $k = \sigma_2/\sigma_1^2$ 이다.

$k = \sigma^6/\sigma^{202} = \sigma^{59}$

$k = \alpha^{59}$ = (0 1 0 0 1 0 1 1) 이다. 따라서 $k_5 = 0$ 이므로 $T_2(k) = T_2(\alpha^{59}) = 0$ 이다. $s_0 \neq 0$, $s_3 \neq 0$, $D_1 \neq 0$, $D_2 \neq 0$, $D_3 \neq 0$ 이므로 복호기는 2중 심벌 오류가 발생한 것으로 판단한다. 식 (55)로 부터 오류위치다항식의 한 해 x은 다음과 같다.

$$x_1 = (0\,1\,0\,0\,1\,0\,1\,1)\begin{bmatrix}0&1&1&0&1&0&1&1\\0&0&0&1&0&1&1&1\\0&1&0&1&0&1&1&1\\1&0&1&1&0&1&0&0\\0&1&1&1&0&1&1&1\\1&0&0&0&0&0&0&0\\1&0&1&0&0&1&0&0\\0&0&0&0&1&0&1&0\end{bmatrix}$$
$$=(1\,1\,0\,0\,1\,1\,1\,0)$$
$$=\alpha^{159}$$

또 오류위치 다항식의 다른 한해 x_2는 다음과 같다.

$$x_2 = 1 + \alpha^{159} = \alpha^{155}$$

따라서 식 (43)로 부터 오류위치에 대응한 오류위치는 다음과 같다.

$$X_1 = \sigma_1 \cdot x_1 = \alpha^{101} \cdot \alpha^{159} = \alpha^5$$
$$X_2 = \sigma_1 \cdot x_2 = \alpha^{101} \cdot \alpha^{155} = \alpha$$

그리고 오류치는 식 (44)를 이용하여 다음과 같이 구할 수 있다.

$$Y_1 = \alpha^3$$

$$Y_2 = \alpha$$

오류계열 $e(x) = \alpha \cdot x + \alpha^3 \cdot x^5$을 구할 수 있다.

3 삼중 오류정정 RS 부호의 복호 알고리듬

1) 3차 방정식의 해

본 절에서는 2.1절에서와 다른 방법으로 GF(2^n) 상의 3차 방정식의 해를 구하는 방법을 기술한다. 일반적으로 GF(2^n) 상의 3차 방정식은 식 (57)과 같이 표현될 수 있다.

$$y^3 + \sigma_1 y^2 + \sigma_2 \cdot y + \sigma_3 = 0 \quad (57)$$

y를 $\sigma_1 + x'$ 이라 치환하면, 식 (57)은 식 (58)과 같이 변형된다.

$$x'^3 + (\sigma_1^2 + \sigma_2)x' + (\sigma_1\sigma_2 + \sigma_3) = 0 \quad (58)$$

만약 $\sigma_1^2 + \sigma_2 = 0$ 이다면 3차 방정식은 3중 해 $x = (\sigma_1\sigma_2 + \sigma_3)^{1/3}$을 갖는다. 만약 $\sigma_1^2 + \sigma_2 \neq 0$ 이다면 $x' = t + (\sigma_1^2 + \sigma_2)/t$ 라 치환하면 식 (58)은 식 (59)와 같이 된다.

$$t^3 + (\sigma_1\sigma_2 + \sigma_3) + (\sigma_1^2 + \sigma_2)^3/t^3 = 0 \quad (59)$$
$$t^6 + (\sigma_1\sigma_2 + \sigma_3)t^3 + (\sigma_1^2 + \sigma_2)^3 = 0$$

식 (59)에서 $u = t^3$으로 치환하면 식 (60)과 같다.

$$u^2 + (\sigma_1\sigma_2 + \sigma_3)u + (\sigma_1^2 + \sigma_2)^3 = 0 \quad (60)$$

식 (60)에서 $v = u/(\sigma_1\sigma_2 + \sigma_3)$으로 치환하면 식 (61)과 같다.

$$v^2 + v + (\sigma_1^2 + \sigma_2)^3/(\sigma_1\sigma_2 + \sigma_3)^2 = 0$$
$$v^2 + v + C_k = 0,$$

여기서,

$$C_k = (\sigma_1^2 + \sigma_2)^3/(\sigma_1\sigma_2 + \sigma_3)^2 \quad (61)$$

식 (61)과 같은 3차 방정식은 일반적으로 식 (56)을 이용하여 하나의 해를 쉽게 계산할 수 있다. 따라서 다음과 같은 절차로 식 (57)과 같은 3차 방정식의 해를 구할 수 있다. 만약 식 (61)의 한 해를 V_1이다고 가정하자. ① 식 (60)의 한 해 $U_1 = V_1 \cdot (\sigma_1\sigma_2 + \sigma_3)$ 이다. ② 식 (59)의 한 해 $T_1 = V_1 \cdot (\sigma_1\sigma_2 + \sigma_3)^{1/3}$ 이다. ③ GF(2^n) 상의 3차 오류위치다항식의 해는 3개이므로 나머지 해들 $T_2 = T_1 \cdot \alpha k$, $T_3 = T_1 \cdot \alpha^2 k$ 이다. 여기서, $k = (2^n - 1)/3 = 85$ ④ 식 (58)의 세 해들 X'_1 $T_1 + (\sigma_1^2 + \sigma_2)/T_1$, $X'_2 = T_2 + (\sigma_1^2 + \sigma_2)/T_2$, $X'_3 = T_3 + (\sigma_1^2 + \sigma_2)/T_3$ 이다. ⑤ 식 (57)의 세 해들 $X_1 = T_1 + (\sigma_1^2 + \sigma\sigma)/T\sigma + \sigma_1$, $X_2 = T_2 + (\sigma_1^2 + \sigma_2)/T_2 + \sigma_1$, $X_3 = T_3 + (\sigma_1^2 + \sigma_2)/T_3 + \sigma_1$ 이다.

2) 3중 오류정정 복호 알고리듬

3중 오류정정 RS 부호를 복호하기 위하여 오증요소와 오류치 및 오류위치는 식 (62)와 같다.

$$\begin{aligned} s_0 &= Y_1 + Y_2 + Y_3 \\ s_1 &= Y_1 \cdot X_1 + Y_2 \cdot X_2 + Y_3 \cdot X_3 \\ s_2 &= Y_1 \cdot X_1^2 + Y_2 \cdot X_2^2 + Y_3 \cdot X_3^2 \\ s_3 &= Y_1 \cdot X_1^3 + Y_2 \cdot X_2^3 + Y_3 \cdot X_3^3 \\ s_4 &= Y_1 \cdot X_1^4 + Y_2 \cdot X_2^4 + Y_3 \cdot X_3^4 \\ s_5 &= Y_1 \cdot X_1^5 + Y_2 \cdot X_2^5 + Y_3 \cdot X_3^5 \end{aligned} \quad (62)$$

오류정정능력이 3인 RS 부호의 수신 부호어에 발생한 오류 갯수 판별 알고리듬을 제시한다. 만약 수신부호어에 단일 오류가 발생했다면 오증 요소는 식 (63)과 같다.

$$\begin{aligned} s_0 &= Y_1 \\ s_1 &= Y_1 \cdot X_1 \\ s_2 &= Y_1 \cdot X_1^2 \\ s_3 &= Y_1 \cdot X_1^3 \\ s_4 &= Y_1 \cdot X_1^4 \\ s_5 &= Y_1 \cdot X_1^5 \end{aligned} \quad (63)$$

따라서 식 (61)로 부터 단일 오류 발생시 판별식을 식 (64)와 같이 구할 수 있다.

$$T_3 = s_0s_2s_4 + s_0s_3^2 + s_1^2s_4 + s_2^3 = 0,\ T_2 = s_0s_2 + s_1^2 = 0,\ s_0 \neq 0 \quad (64)$$

만약 수신부호어에 2중 오류가 발생했다면 오증 요소는 식 (65)와 같다.

$$\begin{aligned} s_0 &= Y_1 + Y_2 \\ s_1 &= Y_1 \cdot X_1 + Y_2 \cdot X_2 \\ s_2 &= Y_1 \cdot X_1^2 + Y_2 \cdot X_2^2 \\ s_3 &= Y_1 \cdot X_1^3 + Y_2 \cdot X_2^3 \\ s_4 &= Y_1 \cdot X_1^4 + Y_2 \cdot X_2^4 \\ s_5 &= Y_1 \cdot X_1^5 + Y_2 \cdot X_2^5 \end{aligned} \quad (65)$$

따라서 식 (63)으로 부터 이중 오류 발생시 판별식을 식 (66)과 같이 구할 수 있다.

$$T_3 = s_0s_2s_4 + s_0s_3^2 + s_1^2s_4 + s_2^3 = 0,\ T_2 = s_0s_2 + s_1^2 \neq 0 \quad (66)$$

만약 수신부호어에 3중 오류가 발생했다면 오증 요

소는 식 (67)과 같다.

$$
\begin{aligned}
s_0 &= Y_1 + Y_2 + Y_3 \\
s_1 &= Y_1 \cdot X_1 + Y_2 \cdot X_2 + Y_3 \cdot X_3 \\
s_2 &= Y_1 \cdot X_1^2 + Y_2 \cdot X_2^2 + Y_3 \cdot X_3^2 \\
s_3 &= Y_1 \cdot X_1^3 + Y_2 \cdot X_2^3 + Y_3 \cdot X_3^3 \\
s_4 &= Y_1 \cdot X_1^4 + Y_2 \cdot X_2^4 + Y_3 \cdot X_3^4 \\
s_5 &= Y_1 \cdot X_1^5 + Y_2 \cdot X_2^5 + Y_3 \cdot X_3^5
\end{aligned} \tag{67}
$$

따라서 식 (67)로 부터 3중 오류 발생시 판별식을 식 (68)과 같이 구할 수 있다.

$$
T_3 = s_0 s_2 s_4 + s_0 s_3^2 + s_1^2 s_4 + s_2^3 \neq 0,\ T_2(C_k) = 0 \tag{68}
$$

단일 오류 발생했을 경우, 오류위치와 오류치는 식 (35)를 이용하여 구할 수 있다. 이중 오류가 발생했을 경우, 오류위치는 식 (56)을 이용하고 오류치는 식 (44)을 이용하여 구할 수 있다. 삼중 오류가 발생했을 경우, 오류위치다항식의 계수와 오류치와의 관계는 다음과 같이 구한다. 식 (67)의 첫 3개의 식을 이용하여 오류위치 Y_1, Y_2, Y_3을 구하면 식 (69)와 같다.

$$
\begin{aligned}
Y &= \frac{\begin{vmatrix} s_0 & 1 & 1 \\ s_1 & X_2 & X_3 \\ s_2 & X_2^2 & X_3^2 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & 1 \\ X_1 & X_2 & X_3 \\ X_1^2 & X_2^2 & X_3^2 \end{vmatrix}} \\
&= (s_0 X_2 X_3 + s_1(X_2 + X_3) + s_2)/(X_1 + X_2)(X_3 + X_1)
\end{aligned}
$$

$$
\begin{aligned}
Y_2 &= (s_0 X_3 X_1 + s_1(X_3+X_1) + s_2) \ / \ (X_1+X_2)(X_2+X_3) \\
&= (s_0 X_3 + s_1 + Y_1(X_3+X_1)) \ / \ (X_2+X_3) \\
Y_3 &= (s_0 X_1 X_2 + s_1(X_1+X_2) + s_2) \ / \ (X_3+X_1)(X_2+X_3) \\
&= s_0 + Y_1 + Y_2
\end{aligned} \tag{69}
$$

식 (67)의 두번째 식부터 3개의 식을 이용하여 오류위치 Y_1을 구하면 식 (70)과 같다.

$$
Y_1 = (s_1 X_2 X_3 + s_2(X_2+X_3) + s_3) \ / \ X_1(X_1+X_2)(X_3+X_1) \tag{70}
$$

식 (69)의 첫째식과 식 (70)을 이용하면 식 (71)과 같은 관계를 구할 수 있다.

$$
\begin{aligned}
&(s_0 X_2 X_3 + s_1(X_2+X_3) + s_2) \ / \ (X_1+X_2)(X_3+X_1) \\
&= (s_1 X_2 X_3 + s_2(X_2+X_3) + s_3)/X_1(X_1+X_2)(X_3+X_1)
\end{aligned} \tag{71}
$$

식 (71)로 부터 식 (72)를 구할 수 있다.

$$
\begin{aligned}
&s_2(X_1+X_2+X_3) + s_1(X_1X_2+X_2X_3+X_3X_1) + s_0X_1X_2X3 \\
&+ s_3 = 0
\end{aligned} \tag{72}
$$

같은 방법으로 식 (73)을 구할 수 있다.

$$
\begin{aligned}
&s_3(X_1+X_2+X_3) + s_2(X_1X_2+X_2X_3+X_3X_1) + s_1X_1X_2X_3 \\
&+ s_4 = 0 \\
&s_4(X_1+X_2+X_3) + s_3(X_1X_2+X_2X_3+X_3X_1) + s_2X_1X_2X_3 \\
&+ s_5 = 0
\end{aligned} \tag{73}
$$

만약 삼중오류발생시 오류위치다항식이 식 (74)와 같다.

$$
\sigma(x) = (x+X_1)(x+X_2)(x+X_3) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 \tag{74}
$$

따라서 오류위치다항식의 계수와 오류위치와의 관계는 식 (75)와 같다.

$$
\begin{aligned}
\sigma_1 &= X_1+X_2+X_3 \\
\sigma_2 &= X_1X_2+X_2X_3+X_3X_1 \\
\sigma_3 &= X_1X_2X_3
\end{aligned} \tag{75}
$$

식 (72)와 식 (73)을 이용하여 오류위치다항식의 계수를 오증요소들로 표현하면 식 (76)와 같다.

$$
\begin{aligned}
\sigma_1 &= \frac{\begin{vmatrix} s_3 & s_1 & s_0 \\ s_4 & s_2 & s_1 \\ s_5 & s_3 & s_2 \end{vmatrix}}{\begin{vmatrix} s_2 & s_1 & s_0 \\ s_3 & s_2 & s_1 \\ s_4 & s_3 & s_2 \end{vmatrix}} \\
&= (s_0 s_2 s_5 + s_0 s_3 s_4 + s_1^2 s_5 + s_1 s_2 s_4 + s_1 s_3^2 + s_2^2 s_3) \\
&\quad / \ T_3 \\
\sigma_2 &= (s_1 s_3 s_5 + s_0^2 s_4 + s_1 s_2 s_5 + s_1 s_3 s_4 + s_2^2 s_4 + s_2 s_3^3) \\
&\quad / \ T_3 \\
\sigma_2 &= (s_1 s_3 s_5 + s_1 s_4^2 + s_2^2 s_5 + s_3^4) \ / \ T_3
\end{aligned} \tag{76}
$$

오류가 3개 발생했을 경우, 오류위치다항식은 3차

방정식 $\sigma(x) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3$ 이므로 이와 같은 3차 방정식의 해는 식 (57)의 해를 구하는 방법과 동일하게 구할 수 있다. 따라서 3중오류가 발생했을 경우, 식 (76)을 이용하여 오류위치다항식의 계수를 구하

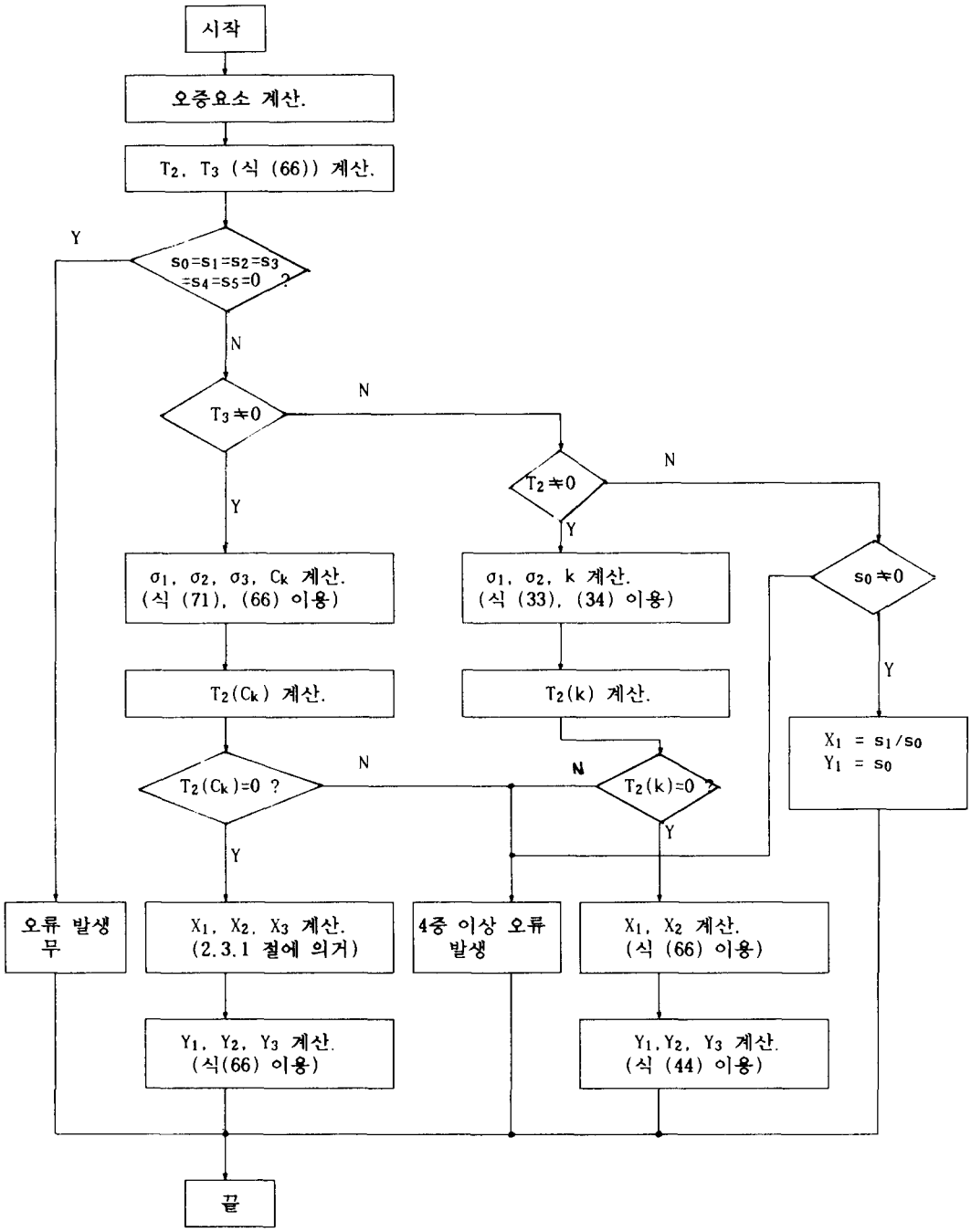

그림 7. 제시된 복호알고리듬을 이용한 3중 오류정정 RS 부호의 복호 흐름도
Fig. 7. Flow diagram for triple error-correction RS decoder.

고, 식 (74)와 같은 3차 방정식은 1)절에서 기술된 알고리듬을 이용하여 오류위치다항식의 3개의 해, 즉 오류위치 X_1, X_2, X_3을 구한후, 식 (69)을 이용하여 세개의 오류치 Y_1, Y_2, Y_3 을 구함으로서 복호를 완료한다. 상기와 같이 제시된 복호 알고리듬을 이용하여 3중 오류 정정 RS 부호의 복호 흐름도를 작성하면 그림 7과 같다.

4. 복호 알고리듬의 성능 비교

본 논문에서 제시된 복호 알고리듬의 성능을 분석하기 위하여 지금까지 널리 알려진 복호 알고리듬과의 성능을 비교한다. 기존의 복호 알고리듬과 제안된 복호 알고리듬을 이용하여 (32,28) 2중 오류정정 RS 부호의 복호기에 대하여 비교하였으며, 비교 항목은 오류위치다항식으로 부터 오류위치를 찾는 회로에 요구되는 회로의 복잡도, 복호기에서 요구되는 지연의 크기, 지연시 요구되는 소요 레지스터의 갯수 등의 측면에서 비교한다. 비교.결과는 표 1과 같다. 비교 대상 복호 알고리듬은 오류정정능력이 3 이하인 RS 부호의 복호기는 PGZ 복호 알고리듬과 같은 직접 복호알고리듬을 이용하는 것이 변환 복호 알고리듬이나 Berlekamp 복호 알고리듬을 이용한 복호기보다 복호기 복잡도보다 복잡도가 낮다는 사실에 기초하여 선정되었다. [2-4]

표 1. 기존의 복호 알고리듬과의 성능 비교

Table 1. Performance analysis of proposed decoding algorithm.

알고리듬 / 비교항목	Chien의 기법을 이용한 PGZ 복호기	Polkinghorn 방법을 이용한 복호기	본 논문에서의 복호기
복호기에서 요구되는 지연	2 프레임	1 프레임	1 프레임
오류위치를 찾는데 요구되는 복잡도	· 치환레지스터 : 14 · EX-OR 게이트 : 17	· ROM(8*8) : 1 or · 승산기 : 3 계산기 : 3 제곱기 : 1	EX-OR : 13
지연시 요구되는 버퍼량 (치환레지스터)	448개	224개	224개

일반적으로 복호기에서 지연은 오증요소를 계산하기 위하여 1 프레임의 지연이 반드시 요구되며 적용 알고리듬에 따라 오류위치를 계산하기 위하여 또 다른 1 프레임의 지연이 요구될 수 있다. 복호기의 복잡도 측면에서는 Chien 기법을 이용한 PGZ 복호 알고리듬 [4,7,9] 이 제일 우수하나, 복호기에서 2 프레임 이상의 지연이 요구되므로 실시간 처리가 요구되는 경우 곤란한 문제점이 있다. Polkinghorn 기법을 이용한 복호기의 경우 복호기에서 요구되는 지연이 1 프레임이나, 외부에 별도의 ROM 이 요구되거나 복잡한 GF(2^8) 상의 승산기, 제산기, 제곱기 등의 연산회로가 요구된다. 본 논문에서 제시된 알고리듬을 이용한 복호기의 경우, 복호기에서 요구되는 지연도 1 프레임이고 오류위치를 찾는데 요구되는 게이트가 13개의 EX-OR 게이트이므로 복호기에서 요구되는 지연 측면이나 복호기 복잡도 측면에서 제일 우수하다.

Ⅲ. 결론

오류정정능력이 3이하인 RS부호의 복호기의 복잡도에 가장 커다란 영향을 미치는 요인은 유한체상의 2차 혹은 3차 방정식의 해를 구하는 회로의 복잡도이다. 지금까지 널리 알려져 있는 유한체상의 2 또는 3차 방정식의 해를 구하는 알고리듬은 Chien 기법과 Polkinghorn 기법 등이 있다. 본 논문에서는 오류위치다항식을 적당한 2차 또는 3차의 affine 다항식으로 변형한후 이를 이용하여 해를 구하는 방법을 도입하여 복호기의 복잡도를 현저히 감소시키는 기법을 제시하였다. 그리고 복호기의 블럭도를 제시하고, 오류위치다항식으로 부터 오류위치를 구하기 위한 회로를 2중 오류정정 RS 부호의 경우 13 의 간단한 논리회로 들을 이용하여 실현하였다. 그리고 3중 오류정정 RS 부호의 복호 알고리듬과 3차의 오류위치 다항식의 해를 구하는 알고리듬을 제시하였다. 본 논문에서 제시된 복호 알고리듬의 성능의 타당성을 보이기 위하여 지금까지 널리 알려진 복호 알고리듬과의 성능을 비교하였다. 비교.결과 복호기의 복잡도 측면에서는 Chien 기법을 이용한 PGZ 복호 알고리듬이 제일 우수하나, 복호기에서 2 프레임 이상의 지연이 요구되므로 실시간 처리가 요구되는 경우 곤란한 문제점이 있고, Polkinghorn 기법을 이용한 복호기의 경우 복호기에서 요구되는 지연이 1 프레임이나, 외부에 별도의 ROM 이 요구되거나 복잡한 GF(2^8) 상의 승산기, 제산기, 제곱기 등의 연산회로가 요구됨을 알 수 있었다. 그리고 본 논문에서 제시된 복호 알고리듬을 이용한 RS 부호의 복호기의 경우, 복호기에서 요구되는 지연도 1 프레임이고 오류위치를 찾는데 요구되는 게이트가 13개의 EX-OR 게이트이므로 복호기에서 요구되는 지연 측면이나 복호기 복잡도 측면에서 제일 우수하다. 따라서 본 논문에서 제시한 방법을 이용하여 설계한 RS 부호의 복호기의 복잡도는 기존의 알고리듬을 이용한 복호기의 복잡도보다 현저히 줄어듬을 알수 있었다. 그리고 3중 오류정정

RS 부호의 복호 알고리듬, 복호 흐름도, 그리고 3차 방정식의 해를 구하는 알고리듬 등을 제시하였다. 여기서 제시된 3중 오류정정 RS 부호의 복호 알고리듬은 DAT용 오류정정 복호기 설계시 이용될 수 있을 것이다. 본 논문의 결과인 2중 또는 3중 오류정정능력을 갖는 RS 오류정정 부호의 오류정정 알고리듬은 CD player, DAT, CD-ROM 등의 광학식 데이타 저장시스템 분야의 오류정정 알고리듬으로 활용될 수 있을 것이다.

參 考 文 獻

[1] Rhee, M. Y., *Error Correcting Coding Theory*, McGraw-Hill, New York, 1989.

[2] Rhee, M. Y., *BCH Codes and Reed-Solomon Codes*, MinumSha, Seoul, Korea, 1990.

[3] Berlekamp, E. R., *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[4] Lin, S. and Costello,D.J., *Error Control Coding : Fundamentals and Applications*, Prentice-Hall, Englwood cliffs, N.J, 1983.

[5] E.R. Berlekamp, B.Rumsey, and G. Solomon, "On the Solution of Algebraic Equa tions over Finite Fields," Information and Control, 10, pp.553-564, 1967.

[6] C.L. Chen, "Formulas of Solution of Quadratic Equations over GF(2^m)," *IEEE Trans.* on Information Theory, vol. IT-28, no.5, pp.792-794, Sept. 1982.

[7] Chien, R. T., "Cyclic Decoding Procedure for the BCH Codes", *IEEE Trans.* on Information Theory, IT-10, pp.357-363, 1964.

[8] Berlekamp, E. R., On Decoding Binary Bose-Chaudhuri-Hocquenghem Codes," *IEEE Trans.* on Inform. Theory, IT-11, pp.580-585, 1965.

[9] Forney, G. D., "On Decoding BCH Codes," *IEEE Trans.* on Inf. Theory, IT-11, p p.577-580, 1965.

[10] F. Polkinhorn, "Decoding of Double Error Correcting Bose-Chaudri Code," *IEEE Trans.* on Inform. Theory, IT-12, pp.480-481, Oct. 1966.

[11] Deng, R. H., and Costello, D. J. JR., "Decoding of DBEC-TBED Reed-Solomon C odes," *IEEE Trans.* on Computers, vol. C-36, no.11, pp.1359-1363, Nov. 1987.

[12] Hoeve, H., J.Timmermans, and L. B. Vries, "Error Correction and Concealment in the Compact Disc System," Philips tech. Rev. 40, no.6, pp.166-172, 1982.

[13] Horiguchi, T. and Sato, Y., "A Decoding Method for Reed-Solomon Codes 3over GF(2^m)," *Trans.* IECE (Jpn.), vol.66(A), no.1, pp.97-98, 1983.

[14] Massey, J. L., "Shift-Register Synthesis and BCH Decoding," *IEEE rans.* on I nf. theory, IT-15, pp.122-127, 1969.

[15] Okano, H. and H. Imai: "A Construction Method of High-Speed Decoding using ROM's for Bose-Chaudhuri-Hocquenghem and Reed-Solomon Codes", *IEEE Trans.* C omput, C-36, pp.1165-1171, 1987.

[16] Vries, L. B. and K. Odaka: "CIRC - the Error Correcting Code for Compact Di sc", The AES Premier Conference-The New World of Digital Audio, New York, p p.3-6, June 1982.

[17] 이만영, 염흥열, 김재문외 2인, "CD용 오류정정 RS부호기 및 복호기 설계에 관한 연구," 한양대학교 산업과학연구소, 삼성전자(주), 위탁연구과제 최종 연구보고 서, 1991.2.

[18] 이만영, 염흥열, 김재문외 5인,"고속 디지틀 전송장치에 적합한 프레이밍 기법 및 ATM 전송 방식에 관한 연구," 한양대학교 산업과학연구소, 한국전자통신연구 소, 위탁연구과제 최종연구보고서, 1988.12.

[19] 이만영, 염흥열, 김재문외 4인, "오류정정 방법 및 장치," 1991.1. (한국, 영국 특허출원중)

著者紹介

廉 興 烈 (正會員)

1981年 漢陽大學校 電子工學科 卒業 (工學士). 1983年 漢陽大學校 大學院 電子工學科 卒業 (工學碩士). 1990年 漢陽大學校 大學院 電子工學科 卒業 (工學博士). 1982年 12月 ~ 1990年 9月 韓國電子通信研究所 先任研究員. 1990年 3月 ~ 현재 順天鄕大學校 工科大學 電子工學科 助教授 主 關心 分野는 暗號理論, 符號理論, 移動通信 分野 등임.

•

金 在 汶 (正會員) 第 28 卷 A編 第 6號 參照
현재 국립 서울 산업대학교 전자공학과 강사.

李 晩 榮 (正會員) 第 26 卷 第 2號 參照
현재 한양대학교 전자통신공학과 명예 교수.