[4-2] CD에서 발생하는 산발오류와 연집오류를 정정하기 위한 효율적인 오류갯수판별알고리즘

°진영철 *염흥열 이만영
한양대학교 전자통신공학과
*순천향대학교 전자공학과

An Efficient Algorithm on Estimating the Number of Errors for Correcting Both the Random and Burst Errors on CD

°JIN, YOUNG CHUL *YOUM, HEUNG YOL RHEE, MAN YOUNG
Dept. of Electronic Commun. Engineering, Hanyang Univ.
*Dept. of Electronics, Sunchonhyang Univ.

Abstract

The Cross Interleaved Reed-Solomon Coding(CIRC)Scheme is widely used for the error control of compact disk system. The Reed-Solomon code are known as powerful nonbinary codes which are capable of correcting the random symbol errors as well as the burst symbol errors in the received codeword. In this paper, new algorithm for estimating the number of errors is proposed for the CIRC of the compact disk system for more efficient error control. In this algorithm, the number of symbol errors can efficiently be estimated based on the coefficients of the error-location polynomial and the trace of $k(=\sigma_2/\sigma_1^2)$, for correcting the symbol errors in decoder. The above-mentioned algorithm can give the more correct estimation capability of the number of errors compared to the conventional algorithm.

1.서론

CIRC를 이용한 CD의 부호기와 복호기의 기본구조는 그림 1-a와 그림1-b와같이 이루어진다.

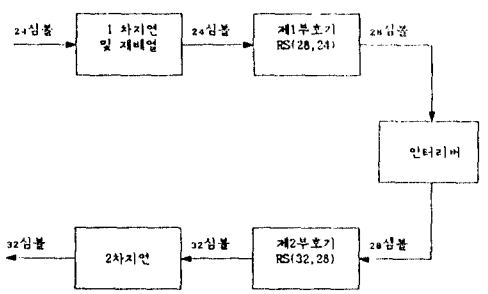


그림 1-a CIRC 부호기

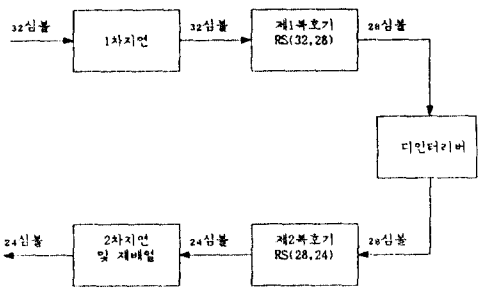


그림 1-b CIRC 복호기

CIRC복호기의 블록도를 보면 RS부호에의한 복호가 이루어지는 제1복호기와 제2복호기에의해 오류정정이 두번 이루어진다. 여기서 오류정정능력(t)이 2심볼인 정정이 이루어질 때 전송채널상에서 산발오류 또는 연집오류가 발생하면 제1복호기에서는 기수번째 채널에대해 1심볼의 지연이 되어서 데이타계열이 수신되므로 공통의오류정정블록의 오류총수는 채널상의 오류갯수의 절반으로 줄어들어 0,1,2개의 오류에 대해서는 정정하지만 2심볼을 초과하면 정정하지 못한다. 따라서 제1복호기에서 정정하지 못한 심볼들이 재배열되고 지연이 되어서 산발적으로 제2복호기에 수신될 때 정확한 정정을 위해서는 제1복호기내에서 정정능력을 초과하는 오류에대해 미정정오류심볼임을 플래그비트로써 표시할 필요가 있다. 이 같이 표시하기 위해서는 정정능력을 초과하는 오류발생을 탐지하는 정확한 오류갯수판별이 이루어져야한다. 제2복호기에서는 역시 디인터리브의 동작에의해서 각 채널에 각각 다른 지연이 이루어지므로 공통의 에러정정블록에 포함되는 오류가 줄어들지라도 연속되는 오류발생에의해서 정정능력을 초과할 경우에는 플래그비트를 부가해서 CIRC복호기에서 출력되는 데이타계열에서 워어드간의 오류워어드를 평균치로 대치함으로써 근사치정정을 하는 보간법(interpolation)에의해 정정을 할 필요가 있다. 이를 위해서도 오류갯수판별을 한 다음 제2복호기에서 수신된 공통의 에러정정블록내의 플래그비트의 총수에 따라 그 오류갯수판

별의 신뢰도를 가능하고 평균치보간을 위한 플래그비트의 부가여부를 판단해야 된다. 이와같이 오류갯수판별식은 제1복호기와 제2복호기에서 필요로한다.

2.본론

첫째, PGZ복호알고리즘에의한 오류갯수판별법을 보임으로써 이 판별법을 CD에 이용하기 위해서는 정정능력이상의 오류가 발생했을 때 판별할 수 있는 조건이 필요함을 제시한다. 둘째, PGZ복호알고리즘을 이용해서 두개의 오류가 발생했을 때의 이차방정식을 유도하고 이 계수들을 이용해서 오류가 없을 때,오류가 하나일 때,오류가 두개이상일 때를 판별하는 수식을 제시한다. 세째, 오류가 두개일 때와 세개일 때를 구별하기 위한 첫째 단계로써 이차방정식의계수의 0의 여부에의한 판별을 제시한다. 네째, 오류가 두개일 때의 조건중의 한가지는 트레이스의 값($T_2(k)$)이 0이어야됨을 보인다. 다섯째, 마지막 단계로서 T_2가 0일 때의 두개의 오류와 세개이상의오류판별하기위한 방법을 제시한다. 여섯째, 본 연구의 오류개수판별법을 흐름도로 제시한다.

2.1. PGZ복호알고리즘을 이용한 오류갯수판별

오류정정능력 t개에서 u개의 오류가 $x^{n1},x^{n2},\ldots,x^{nu}$위치에서 오류가 발생하면 오류위치다항식 e(x)는

$$e(x)=e_{n1}x^{n1}+e_{n2}x^{n2}+\ldots+e_{nu}x^{nu}$$

(e_{nj}:오류치, 1≤j≤u) ...(1-a)

이고 오증요소 S_i는 다음과 같이 표현할 수 있다.

$$S_i=e(\alpha^i)=e_{n1}\alpha^{i\,n1}+e_{n2}\alpha^{i\,n2}+\ldots+e_{nu}\alpha^{i\,nu}$$
$$=Y_1X_1{}^i+Y_2X_2{}^i+\ldots+Y_uX_u{}^i$$
$$(Y_j=e_{nj},\ X_j=\alpha^{nj},\ 0\le i\le 2t-1) \quad ...(1-b)$$

그리고 모든 오증요소를 구하면 다음과 같다.

$$S_0=Y_1+Y_2+\ldots+Y_u=\sum_{j=1}^{u}Y_jX_j{}^0$$

$$S_1=Y_1X_1+Y_2X_2+\ldots+Y_uX_u=\sum_{j=1}^{u}Y_jX_j{}^1$$
$$\vdots \qquad\qquad \vdots$$
$$S_{2t-1}=Y_1X_1{}^{2u-1}+Y_2X_2{}^{2u-1}+\ldots+Y_uX_u{}^{2u-1}=\sum_{j=1}^{u}Y_jX_j{}^{2u-1} \quad (1-c)$$

(1-c)식은 2t개의 비선형방정식이다. 오류위치를 구하기 위하여 오류위치,$X_1,X_2,\ldots,X_u$로 구성된 오류위치방정식은

$$\sigma(x)=(x+X_1)(x+X_2)\ldots(x+X_u)$$
$$=x^u+\sigma_1x^{u-1}+\sigma_2x^{u-2}+\ldots+\sigma_{u-1}x+\sigma_u \quad ...(1-d)$$

이 되고 (1-d)양변에 $Y_jX_j{}^i$를 곱하면

$$\sigma(x)Y_jX_j{}^i=(x^u+\sigma_1x^{u-1}+\ldots+\sigma_u)Y_jX_j{}^i$$

이고 x에 X_j를 대입하면

$$0=(X_j{}^u+\sigma_1X_j{}^{u-1}+\sigma_2X_j{}^{u-2}+\sigma_{u-1}X_j+\sigma_u)Y_jX_j{}^i$$
$$=Y_jX_j{}^{i+u}+\sigma_1Y_jX_j{}^{i+u-1}+\sigma_2Y_jX_j{}^{i+u-2}+\ldots+\sigma_{u-1}Y_jX_j{}^{i+1}+\sigma_uY_jX_j{}^i$$

이고 다음이 성립한다.

$$\sum_{j=1}^{u}Y_jX_j{}^{i+u}+\sigma_1\sum_{j=1}^{u}Y_jX_j{}^{i+u-1}+\sigma_2\sum_{j=1}^{u}Y_jX_j{}^{i+u-2}+\ldots$$
$$\ldots+\sigma_{u-1}\sum_{j=1}^{u}Y_jX_j{}^{i+1}+\sigma_u\sum_{j=1}^{u}Y_jX_j{}^{i}=0$$

$$S_{i+u}+\sigma_1S_{i+u-1}+\sigma_2S_{i+u-2}+\ldots+\sigma_{u-1}S_{i+1}+\sigma_uS_i=0 \quad ...(1-e)$$

(1-e)를 i의 각각에 대해서 전개를 하면

$$\sigma_uS_0+\sigma_{u-1}S_1+\ldots+\sigma_1S_{u-1}=S_u$$
$$\sigma_uS_1+\sigma_{u-1}S_2+\ldots+\sigma_1S_u=S_{u+1}$$
$$\sigma_uS_{u-1}+\sigma_{u-1}S_u+\ldots+\sigma_1S_{2u-2}=S_{2u-1} \quad ...(1-f)$$

이 된다. 그리고 (1-f)식은 다음과 같이 행렬로 표현할 수 있다.

$$\begin{bmatrix} S_0 & S_1 & \ldots & S_{u-1} \\ S_1 & S_2 & & S_u \\ & & & \\ S_{u-2} & S_{u-1} & & S_{2u-3} \\ S_{u-1} & S_u & & S_{2u-2} \end{bmatrix} \cdot \begin{bmatrix} \sigma_u \\ \sigma_{u-1} \\ \vdots \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_u \\ S_{u+1} \\ \vdots \\ S_{2u-2} \\ S_{2u-1} \end{bmatrix} \quad ...(1-g)$$

여기서

$$M_u(s)=\begin{bmatrix} S_0 & S_1 & \ldots & S_{u-1} \\ S_1 & S_2 & \ldots & S_u \\ & & & \\ S_{u-2} & S_{u-1} & & S_{2u-3} \\ S_{u-1} & S_u & \ldots & S_{2u-2} \end{bmatrix}$$

로 정의하면

$$M_u(s)=\begin{bmatrix} \Sigma Y_j & \Sigma Y_jX_j & \Sigma Y_jX_j{}^{u-1} \\ \Sigma Y_jX_j & \Sigma Y_jX_j{}^2 & \Sigma Y_jX_j{}^u \\ \vdots & & \\ \Sigma Y_jX_j{}^{u-2} & \Sigma Y_jX_j{}^{u-1} & \Sigma Y_jX_j{}^{2u-3} \\ \Sigma Y_jX_j{}^{u-1} & \Sigma Y_jX_j{}^u & \Sigma Y_jX_j{}^{2u-2} \end{bmatrix}$$

$$=\begin{bmatrix} Y_1+Y_2+\ldots+Y_u & Y_1X_1+Y_2X_2+\ldots+Y_uX_u \\ Y_1X_1+Y_2X_2+\ldots+Y_uX_u & Y_1X_1{}^2+Y_2X_2{}^2+\ldots+Y_uX_u{}^2 \\ \vdots & \\ Y_1X_1{}^{u-2}+Y_2X_2{}^{u-2}+\ldots+Y_uX_u{}^{u-2} & Y_1X_1{}^{u-1}+Y_2X_2{}^{u-1}+\ldots+Y_uX_u{}^{u-1} \\ Y_1X_1{}^{u-1}+Y_2X_2{}^{u-1}+\ldots+Y_uX_u{}^{u-1} & Y_1X_1{}^u+Y_2X_2{}^u+\ldots+Y_uX_u{}^u \end{bmatrix}$$

$$\begin{matrix} \ldots & Y_1X_1{}^{u-1}+Y_2X_2{}^{u-1}+\ldots+Y_uX_u{}^{u-1} \\ \ldots & Y_1X_1{}^u+Y_2X_2{}^u+\ldots+Y_uX_u{}^u \\ & \\ \ldots & Y_1X_1{}^{2u-3}+Y_2X_2{}^{2u-3}+\ldots+Y_uX_u{}^{2u-3} \\ \ldots & Y_1X_1{}^{2u-2}+Y_2X_2{}^{2u-2}+\ldots+Y_uX_u{}^{2u-2} \end{matrix}\Bigg]$$

$$=\begin{bmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_u \\ \vdots & & & \\ X_1{}^{u-2} & X_2{}^{u-2} & \ldots & X_u{}^{u-2} \\ X_1{}^{u-1} & X_2{}^{u-1} & \ldots & X_u{}^{u-1} \end{bmatrix} \cdot \begin{bmatrix} Y_1 & 0 & \ldots & 0 \\ 0 & Y_2 & \ldots & 0 \\ & & \vdots & \\ 0 & 0 & \ldots & Y_{u-1} \\ 0 & 0 & \ldots & Y_u \end{bmatrix}$$

$$\cdot \begin{bmatrix} 1 & X_1 & X_1{}^2 & \ldots & X_1{}^{u-1} \\ 1 & X_2 & X_2{}^2 & \ldots & X_2{}^{u-1} \\ & & \vdots & & \\ 1 & X_{u-1} & X_{u-1}{}^2 & \ldots & X_{u-1}{}^{u-1} \\ 1 & X_u & X_u{}^2 & \ldots & X_u{}^{u-1} \end{bmatrix}$$

$$=A\cdot B\cdot A^T$$

가 되는데 여기서

$$A=\begin{bmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_u \\ \vdots & & & \\ X_1{}^{u-2} & X_2{}^{u-2} & \ldots & X_u{}^{u-2} \\ X_1{}^{u-1} & X_2{}^{u-1} & \ldots & X_u{}^{u-1} \end{bmatrix}, B=\begin{bmatrix} Y_1 & 0 & \ldots & 0 \\ 0 & Y_2 & \ldots & 0 \\ & & \vdots & \\ 0 & 0 & \ldots & Y_{u-1} \\ 0 & 0 & \ldots & Y_u \end{bmatrix}$$

이다. 따라서 $M_u(s)=A\cdot B\cdot A^T$ 이므로각각의 행렬식(determinant)도 등식이 성립하므로

$$|M_u(s)|=|A\cdot B\cdot A^T|=|A|\cdot|B|\cdot|A^T|$$

가 되는데 실제 발생한 오류갯수가 u보다 작다면 $|B|=0$이므로 $|M_u(s)|=0$가 된다. 그러므로실제 발생한 오류갯수가 u라면 $|B|\neq0$이고 $|A|\neq0,|A^T|\neq0$이므로 $|M_u(s)|\neq0$가 된다.

<예제1>

어떤 정보어가 RS(32,28)부호로 부호화 되어 c(x)가 되었다. c(x)가 송신이 되어 r(x)를 받았다면 다음과 같이 판별된다.

$c(x)=0\cdot x^{31}+0\cdot x^{30}+\ldots+0\cdot x+0=0$

(i) $r(x)=\alpha^{100}x^{15}$일 때

$S_0=\alpha^{100}, S_1=\alpha^{115}, S_2=\alpha^{130}, S_3=\alpha^{145}$

$|M_0(s)|=0$

∴ 하나의 오류발생

(ii) $r(x)=\alpha^{111}x^{24}+\alpha^{26}x^{13}$일 때

$S_0=\alpha^{196}, S_1=\alpha^{75}, S_2=\alpha^{110}, S_3=\alpha^{220}$

$|M_0(s)|=\alpha^{143}\neq 0$

∴ 두개의 오류발생

(iii) $r(x)=\alpha^{108}x^{23}+\alpha^{24}x^{12}+\alpha^{25}x^{11}$일 때

$S_0=\alpha^{131}, S_1=\alpha^{130}, S_2=\alpha^{240}, S_3=\alpha^{138}$

$|M_0(s)|=\alpha^{251}\neq 0$

∴ 두개의 오류발생(잘못 판별)

(iii)경우같이 발생한 오류가 u보다 크면, 즉 오류정정능력을 넘으면 판별할 수 없음을 알 수 있다. 따라서 오류정정능력을 넘는 오류갯수가 나타났을 때를 포함하는 판별조건이 필요함을 알 수 있다.

2.2. t=2에서의 오류위치다항식의 계수를 이용한 조건

(1-d)식에서 $x^2+\sigma_1 x+\sigma_2=0$이고 계수 σ_1과σ_2는 다음과 같이 구해진다. (1-g)식에서

$$\begin{bmatrix}\sigma_2\\ \sigma_1\end{bmatrix}=\begin{bmatrix}S_0 & S_1\\ S_1 & S_2\end{bmatrix}^{-1}\begin{bmatrix}S_2\\ S_3\end{bmatrix}$$

$$=\frac{1}{S_0S_2+S_1^2}\begin{bmatrix}S_2 & S_1\\ S_1 & S_0\end{bmatrix}\begin{bmatrix}S_2\\ S_3\end{bmatrix}$$

$$=\frac{1}{S_0S_2+S_1^2}\begin{bmatrix}S_1S_3+S_2^2\\ S_1S_2+S_0S_3\end{bmatrix}$$

$$\sigma_1=\frac{S_1S_2+S_0S_3}{S_0S_2+S_1^2},\quad \sigma_2=\frac{S_1S_3+S_2^2}{S_0S_2+S_1^2}\qquad\cdots(1\text{-g-1})$$

와 같이 나타낼 수 있고 σ_1과 σ_2를 2차방정식인 오류위치다항식에 대입하면

$$x^2+\frac{S_1S_2+S_0S_3}{S_0S_2+S_1^2}x+\frac{S_1S_3+S_2^2}{S_0S_2+S_1^2}=0$$

이고 양변에 $(S_0S_2+S_1^2)$를 곱하면

$$(S_0S_2+S_1^2)x^2+(S_1S_2+S_0S_3)x+(S_1S_3+S_2^2)=0\quad\cdots(1\text{-h})$$

이고 여기서 $C=(S_0S_2+S_1^2)$, $D=(S_1S_2+S_0S_3)$, $E=(S_1S_3+S_2^2)$라고 놓는다.

〈가〉 오류가 없는 경우

오류가 없는 경우에는 식(1-a)의 $e(x)$가 0이므로 식(1-b)의 S_i 즉 S_0,S_1,S_2,S_3는 모두 0이 된다. 따라서 계수를 이용한 일반적 판별식은 C=0,D=0,E=0 그리고 $S_0=0, S_3=0$가 된다.

〈나〉 오류가 하나인 경우

오류가 오류위치 x^i에서 오류치 e_i가 발생했다면 $e(x)=e_ix^i$ 이므로

$S_0=e(\alpha^0)=e_i,\ S_1=e(\alpha)=e_i\alpha^i,\ S_2=e_i(\alpha^2)=e_i\alpha^{2i}$

$S_3=e(\alpha^3)=e_i\alpha^{3i}$

이 된다. 이것을 변형시키면

$$\frac{S_1}{S_0}=\frac{S_2}{S_1}=\frac{S_3}{S_2}=\alpha^i$$

$$\frac{S_1}{S_0}=\frac{S_2}{S_1},\quad \frac{S_1}{S_0}=\frac{S_3}{S_2},\quad \frac{S_2}{S_1}=\frac{S_3}{S_2}$$

$S_0S_2=S_1^2,\ S_1S_2=S_0S_3,\ S_1S_3=S_2^2$

가 되므로 C=0,D=0,E=0 이고 $S_0\neq 0, S_3\neq 0$이면 오류가 하나일 경우에 독립적으로 작용한다.

〈예제2〉

$r(x)=\alpha^{127}x^{16}$일 때

$S_0=\alpha^{127}, S_1=\alpha^{111}, S_2=\alpha^{159}, S_3=\alpha^{175}$

C=0,D=0,E=0

∴ 하나의 오류발생

〈나〉오류가 두개이상일 경우

〈가〉와 〈나〉를 만족하지 않는다면 오류가 두개이상이 발생한 것으로 판정하고 오류가 두개일 경우는 오류위치다항식이 두개의 서로다른 해를 갖기 위해서 C≠0,D≠0,E≠0을 만족하거나 세개이상일 경우에는 위 조건을 만족하는 경우도 있고 그렇지 않은 경우도 있다.

〈예제2〉

$r(x)=\alpha^{110}x^{20}+\alpha^{23}x^{11}+\alpha^{24}x^{11}+\alpha^{23}x^{15}$일 때

$S_0=\alpha^{11}, S_1=\alpha^{135}, S_2=\alpha^{89}, S_3=\alpha^{213}$

$C=\alpha^{187}, D=0, E=\alpha^{8}$

〈가〉,〈나〉를 만족못함, C≠0,D≠0,E≠0를 만족하지 않으므로 세개이상의 오류가 발생한것임

〈예제4〉

$r(x)=\alpha^{108}x^{20}+\alpha^{23}x^{11}+\alpha^{24}x^{11}+\alpha^{25}x^{15}$일 때

$S_0=\alpha^{181}, S_1=\alpha^{168}, S_2=\alpha^{186}, S_3=\alpha^{76}$

$C=\alpha^{137}, D=\alpha^{209}, E=\alpha^{129}$

(ii) 두개이상의 오류가 발생(〈가〉,〈나〉를 만족못함)

(iii) C≠0,D≠0,E≠0를 만족함

일단 C≠0,D≠0,E≠0 을 만족하지 않는 경우를 세개이상으로 판별하고 만족하는 경우는 다음에 새로 도입하는 트레이스의 여러방정식해의 범위에 의한 순차적인 방법에의해 판별한다.

2.3. 트레이스를 이용한 판별

오류위치다항식 $\sigma(x)$의 근x_1,x_2가 $GF(2^m)$상에 있다고 가정하고 이 근을 갖기 위한 필요충분조건을 찾기 위해서 트레이스$T_2(k), T_1(k)$를 이용한다. k를 $GF(2^m)$상의 원소라 하면 다음을 정의한다.

$$Tr(k)=T_2(k)=\sum_{i=0}^{m-1}k^{2^i}\qquad(m:\text{우수,기수})$$

$$T_1(k)=\sum_{i=0}^{(m-2)/2}k^{2^{2i}}\qquad(m:\text{우수})$$

그리고 오류위치다항식 $\sigma(x)$를 변형하면$\sigma(x)=x^2+\sigma_1x+\sigma_2=0$에서 $y=x/\sigma_1, k=\sigma_2/\sigma_1^2$라 놓고 각 변수에 대입하면 다음과 같은 새로운 이차방정식을 얻을 수 있다.

$\sigma(y)=y^2+y+k=0$

오류해는에따라 k값이 좌우되는 새로운 이차방정식에서 해를 갖기 위한 필요충분조건은 $T_2(k)=0$임을 보이기위해 다음과 같은 절차에의해 일반적인 다항식으로부터 증명한다.

〈정리1〉

f(x)가 $GF(2^m)$상에서 r개의 기약다항식의 곱인 n차의 다항식이고 $f^{(i)}(x)$는 $GF(2^m)$상에서 기약다항식이며 (n-r)는 2로 나누어 질 때 즉,

$f(x)=f_n\prod_{i=1}^{n}(x+X_i)=\prod_{i=1}^{r}f^{(i)}(x)$, $n=r(\text{mod}2)$이면

$Tr[\rho(f)]=0$이다.

단, $\rho(f)=\sum_{1\le i<j\le n}\frac{X_iX_j}{(X_i+X_j)^2}$

(f_n:상수, X_i:근, n:차수)

<증명> GF(2)상에서 다음과 같이 증명된다.

$Tr[\rho(f)]$

$=Tr[\rho(\prod_{i=1}^{t}f^{(i)}(x))]=Tr[\rho(f^{(1)}(x)\cdot f^{(2)}(x)\cdots f^{(t)}(x))]$

$=Tr[\rho(f^{(1)}(x))]+Tr[\rho(f^{(2)}(x))]+\cdots+Tr[\rho(f^{(t)}(x))]$ ···<보조정리3>

$=\sum_{i=1}^{t}Tr[\rho(f^{(i)}(x))]$

$=\sum_{i=1}^{r}[degf^{(i)}(x)-1]$ ... <보조정리2>

$=degf(x)-r$ <degf(x)는 f(x)의 차수>

$=n-r$

$=2\cdot w$ <w:0,1,2,···>

$=0$ <mod2> Q.E.D.

<보조정리1>

$Tr[\rho(f)]=\sum_{1\le i<j\le n}\left[\frac{1}{1+X_j/X_i}+\frac{1}{1+(X_j/X_i)^m}\right]$,단 $m=2^m$

<보조정리2>

[r=1일 때 $Tr[\rho(f)]=degf(x)-1$ 이다.]

<보조정리3>

[f(x)와 g(x)가 GF(2^m)상에서 다항식들이 서로소이면

$Tr[\rho(fg)]=Tr[\rho(f)]+Tr[\rho(g)]$ 이다.]

따라서 <정리1>에 의해

$\sigma(y)=y^2+y+k=1\prod_{i=1}^{2}(y+y_i)$, $<y_1+y_2=1, y_1y_2=k>$

$\rho(\sigma(y))=\sum_{1\le i<j\le 2}\frac{y_iy_j}{(y_i+y_j)^2}=\frac{y_1y_2}{(y_1+y_2)^2}=k$

이 되고 n-r=2-2=0이므로 근 y_1, y_2를 갖기 위해서는 $Tr(\rho(\sigma(y)))=Tr(k)=T_2(k)=0$이어야 된다. 그러므로 오류가 두개이상이 발생한 경우에 $Tr(k)\neq 0$이면 세개이상의 오류가 발생한 것으로 판별하면된다. 그런데 오류가 세개이상인 경우에서도 이차방정식의 근을 갖는 경우가 있다. 즉 Tr(k)=0인 경우도 있으므로 이런 경우를 판별하기위한 방법을 제시한다.

<예제5>

$r(x)=\alpha^{109}x^{15}+\alpha^{24}x^{19}+\alpha^{2}x^{2}$일 때

$S_0=\alpha^{234}, S_1=\alpha^{176}, S_2=\alpha^{225}, S_3=\alpha^{44}$

$C=\alpha^{168}, D=\alpha^{217}, E=\alpha^{209}$

(i) 두개이상의 오류가 발생(C.2.2.의 가),나)를 만족못함)

(ii) $C\neq 0, D\neq 0, E\neq 0$를 만족함

(iii) $k=\alpha^{198}, T_2(k)=0$를 만족함

<예제6>

$r(x)=\alpha^{110}x^{20}+\alpha^{13}x^{1}+\alpha^{25}x^{11}+\alpha^{6}x^{15}+\alpha^{10}x^{19}$일 때

$S_0=\alpha^{170}, S_1=\alpha^{56}, S_2=\alpha^{125}, S_3=\alpha^{9}$

$C=\alpha^{235}, D=\alpha^{220}, E=\alpha^{59}$

(i) 두개이상의 오류가 발생(C.2.2.의 가),나)를 만족못함)

(ii) $C\neq 0, D\neq 0, E\neq 0$를 만족함

(iii) $k=\alpha^{91}, T_2(k)=\alpha^{0}=1$를 만족함

2.4.오류위치를 이용한 판별법

CD의 CIRC의 오류정정기법은 오류정정능력이 2심볼(t=2)인 RS(255,251)부호를 단축시켜 RS(32,28),RS(28,24)부호를 이용하는 것이므로 오류가 하나,두개가 발생한 경우에 있어서는 그 오류위치가 반드시 단축된 범위내에 존재하여야된다. 즉 제1복호기[RS(32,28)]에서는 $\alpha^0\sim\alpha^{31}$내에, 제2복호기[RS(28,24)]에서는 $\alpha^0\sim\alpha^{27}$내에 그 오류위치가 존재해야 하므로 단축된 범위내에 존재하지 않는다면 정정능력이상의 오류가 발생한 것으로 판별하면 된다. 따라서 $Tr(k)=0$인 경우에 오류가 두개인 경우와 두개를 초과 했을 때를 구별하기 위해서 이차방정식의 해를 구해야하는 데 해를 구하는 방법에는 GF(2^m)상의 원소들을 하나 씩 대입해서 해를 구하는 Chien탐지법이 있으나 $T_2(k), T_4(k)$의 값에 따라 k의 먹들의 합으로 구하는 방법을 제시한다.

$\sigma(y)$의 한근을 y_1이라하면 $y_1^2+y_1+k=0$이고 또다른 한근은 $1+y_1$이다.왜냐하면

$(1+y_1)^2+(1+y_1)+k=1^2+y_1^2+y_1+1+k=y_1^2+y_1+k=0$이기 때문이다. 따라서 근 y_1만 구하면 다른 한근은 쉽게 구할 수 있다. 여기서 y_1을 k만의 함수로 표현하기위해 다음에 정리와 보조정리를 도입한다.

<정리2>

$y^2+y+k=0$가 GF(2^m)상에서 해를 갖고[$T_2(k)=0$] $m\equiv 0 \pmod 4$이고 $T_1(k)=1$이면 한근y_1은 다음과 같이 표현된다.

$y_1=s+s^2+k^{2^{m-1}}(1+\sum_{i=0}^{(m/4)-1}k^{2^{2i+m/2}})$

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

<증명>

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

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

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

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

여기서 <정리2>의 우변을 Q라한다.

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

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

$=k+k^{2^{m-1}}+(k^{2^{m-1}}\sum_{i=1}^{(m-2)/2}k^{2^{2i}})+k^{2^{m-1}}k$

$=k+k^{2^{m-1}}+k^{2^{m-1}}T_4(k)$

$=k$

따라서 $y_1=Q$이다. Q.E.D.

<보조정리4>

[$y^2+y+k=0$이 GF(2^m)상에서 해를 가지면 m이 우수일 때 $T_4(k)$는 0 또는 1이다.]

〈보조정리5〉

[m이 우수일 때 GF(2^m)상의 y_1이 $y^2+y+k=0$의 한근이고 $T_2(y_1)=1$이면 $T_4(k)=1$이다.]

따라서 GF(2^8)상에서 $T_2(k)=0$이고 $T_4(k)=1$일 때 $y^2+y+k=0$의 해y_1,y_2를 구하기위해 〈정리2〉를 적용하면 다음과 같다.

$y_1=k^{33}+k^{66}+k^{128}+k^{144}+k^{192}$

$y_2=1+y_1=1+k^{33}+k^{66}+k^{128}+k^{144}+k^{192}$

그러면 GF(2^m)상에서 $T_2(k)=0$이고 $T_4(k)=0$일 때 일반적인 $y^2+y+k=0$의 해를 구하는 방법을 제시한다.

$y^2+y=k=0$에 y대신에 $(w,z\in GF(2^m))$인 w+z를 대입하면

$(w+z)^2+(w+z)+k=z^2+z+(w^2+w+k)$

이 된다. 따라서 $z^2+z+(w^2+w+k)=0$가 해z_1,z_2를 가지면 $w+z_1$은 $y^2+y+k=0$의 한해이다. $z^2+z+(w^2+w+k)=0$가 해를 가지고 또 〈정리2〉에의해 한해z_1을 구할려면 $T_2(w^2+w+k)=0$이고 $T_4(w^2+w+k)=1$이어야한다. $T_2(w)=1$인 w만 존재한다면 위 두 조건을 만족한다. $k_1=w+w^2$이라 놓으면 해가 존재하므로 $T_2(k_1)=0$이다. 그러므로 〈보조정리5〉에의해 $T_4(k_1)=1$이다. 따라서 다음이 성립한다.

$T_2(w^2+w+k)=T_2(w^2+w)+T_2(k)$

$=T_2(k_1)+T_2(k)$

$=0+0=0$

$T_4(w^2+w+k)=T_4(w^2+w)+T_4(k)$

$=T_4(k_1)+T_4(k)$

$=1+0=1$

그러므로 〈정리2〉에의해 $z^2+z+(w^2+w+k)=0$를 풀어서 z_1을 구하고 $T_2(w)=1$을 만족하는 w를 구한다. 따라서 $y^2+y+k=0$을 만족하는 한근은 z_1+w가 된다.

GF(2^8)에대해서 $T_2(k)=0,T_4(k)=0$일 때 $y^2+y+k=0$의 해 y_1,y_2를 구해보면 다음과 같다.

$y_1=z_1+w=w+c^{33}+c^{66}+c^{128}+c^{144}+c^{192}$

$y_2=1+y_1=1+z_1+w=1+w+c^{33}+c^{66}+c^{128}+c^{144}+c^{192}$

(단, $T_2(w)=1, c=w^2+w+k$)

결과적으로 GF(2^8)상에서 $x^2+\sigma_1x+\sigma_2=0$의 해는 다음과 같다.

〈가〉 $T_2(k)=0,T_4(k)=1$일 때의 해

$x_1=\sigma_1y_1=\sigma_1(k^{33}+k^{66}+k^{128}+k^{144}+k^{192})$

$x_2=\sigma_1(1+y_1)=\sigma_1(1+k^{33}+k^{66}+k^{128}+k^{144}+k^{192})$

〈나〉 $T_2(k)=0,T_4(k)=0$일 때의 해

$x_1=\sigma_1(z_1+w)=\sigma_1(w+c^{33}+c^{66}+c^{128}+c^{144}+c^{192})$

$x_2=\sigma_1(1+z_1+w)=\sigma_1(1+w+c^{33}+c^{66}+c^{128}+c^{144}+c^{192})$

(단, $T_2(w)=1, c=w^2+w+k$)

이 공식을 이용하여 판별하는 예제는 다음과 같다.

〈예제7〉

$r(x)=\alpha^{110}x^{20}+\alpha^{23}x^{1}+\alpha^{24}x^{11}+\alpha^{25}x^{15}$일 때

$S_0=\alpha^{101},S_1=\alpha^{189},S_2=\alpha^{58},S_3=\alpha^{39}$

$C=\alpha^{93},D=\alpha^{198},E=\alpha^{123}$

(i) 두개이상의 오류가 발생(∵2.2.의 가),나)를 만족못함)

(ii) $C\neq0,D\neq0,E\neq0$를 만족함

(iii) $k=\alpha^{75},T_2(k)=0$를 만족함

(iv) $T_4(k)=\alpha^0=1,x_1=\alpha^{221},x_2=\alpha^{64}$이므로 세개이상의 오류가 발생한 것이다.($\alpha$의 지수가 31을 넘는다.)

〈예제8〉

$r(x)=\alpha^{108}x^{17}+\alpha^{13}x^{6}+\alpha^{24}x^{23}+\alpha^{6}x^{15}+\alpha^{9}x^{16}$일 때

$S_0=\alpha^{209},S_1=\alpha^{77},S_2=\alpha^{99},S_3=\alpha^{42}$

$C=\alpha^{100},D=\alpha^{120},E=\alpha^{38}$

(i) 두개이상의 오류가 발생(∵2.2.의 가),나)를 만족못함)

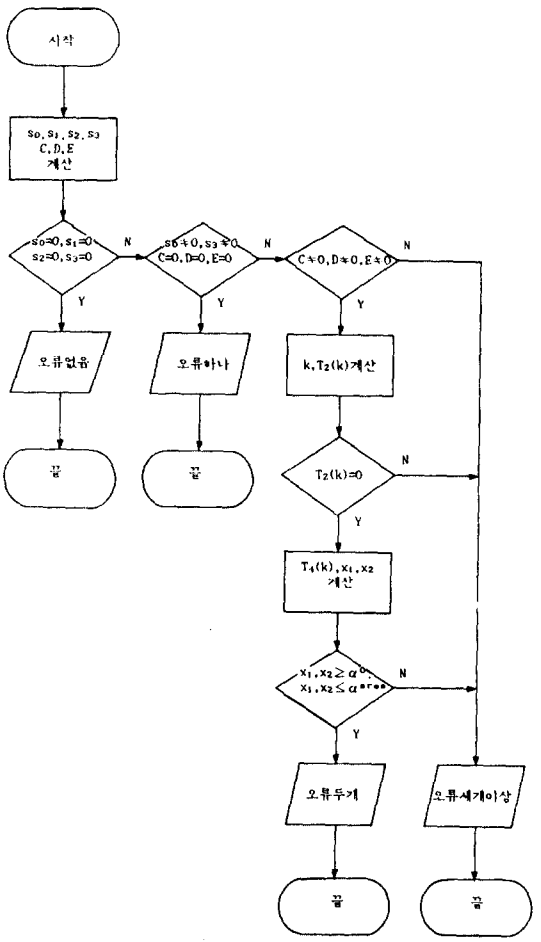
(ii) $C\neq0,D\neq0,E\neq0$를 만족함

(iii) $k=\alpha^{15},T_2(k)=0$를 만족함

(iv) $T_4(k)=0,x_1=\alpha^{209},x_2=\alpha^{27}$이므로 세개이상의 오류가 발생한 것이다.($\alpha$의 지수가 31을 넘는다.)

2.5.오류갯수판별 플로우차트

지금까지의 알고리즘 플로우차트로 나타내면 다음과 같다.



여기서 변수 error는 제1복호기에서는 31이고 제2복호기에서는 27이다.

3. 결론

본 연구는 CIRC의 오류정정을 위한 첫 단계인 오류갯수판별을 위해서 PGZ복호알고리즘의 오류갯수판별방법과 오류위치다항식을 변형한 이차방정식의 계수를 근거로 하여 정정능력이만의 오류수를 판별하고 정정능력이상의 오류수를 탐지하기위해 트레이스와 오류위치의 범위를 이용하므로써 기존의 방법에 비해 특히 정정능력이상의 오류가 수신 되었을 때 오류판별이 정확하며 독특한 특징을 가짐으로써 실제로 이 알고리즘은 CDP에 유용하게 쓰일 수 있다.

참고문헌

[1] Rhee, M.Y., *Error Correcting Coding Theory*, McGraw-Hill, New York, 1989.
[2] 이 만영, BCH부호와 Reed-Solomon부호, 민음사, 1990.
[3] 정 기혁, 콤팩트디스크, 가남사, 1988.
[4] Chen, C.L. "*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.
[5] Lin,S. and Costello,D.J., *Error Control Coding : Fundamentals and Applications*, Prentice-Hall, Englwood Cliffs, N.J, 1983.
[6] Berlekamp, E.R., *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.