論文 89-26-2-2

# 2중 오류정정 Reed-Solomon 부호의 부호기 및 복호기 장치화에 관한 연구

# (On the Implementation of CODEC for the Double-Error Correction Reed-Solomon Codes)

李 晩 榮,* 金 彰 圭**

(Man Young Rhee and Chang Kyu Kim)

**要 約**

Reed-Solomon(RS) 부호의 복호에서 오류위치다항식을 구하기 위한 알고리듬 중 Peterson에 의해 제안되고 Gorenstein과 Zierler가 개선한 알고리듬은 오류정정능력 t가 비교적 작을 경우 Berlekamp-Massey의 반복 알고리듬, Euclid 알고리듬을 이용한 복호, 변환영역에서의 복호보다 오류위치다항식의 계산이 간단하고 장치화에 이점이 있다. 본 논문에서는 Peterson-Gorenstein-Zieler의 알고리듬및 RS 부호의 부호화와 복호과정을 체계적으로 연구, 분석하고 실제로 통신 시스템에 응용할 수 있도록 유한체 GF($2^5$)의 심볼로 이루어지는 2중 오류정정(31, 27) RS 부호의 부호기와 복호기를 설계하여 TTL IC로 장치화 하였다.

**Abstract**

The Berlekamp-Massey algorithm, the method of using the Euclid algorithm, and Fourier transforms over a finite field can be used for the decoding of Reed-Solomon codes (called RS codes). RS codes can also be decoded by the algorithm that was developed by Peterson and refined by the Gorenstein and Zierler. However, the decoding of RS codes using the Peterson-Gorenstein-Zieler algorithm offers sometimes computational or implementation advantages. The decoding procedure of the double-error correcting (31,27) Rs code over the symbol field GF ($2^5$) will be analyzed in this paper. The complete analysis, gate array design, and implementation for encoder/decoder pair of (31.27) RS code are performed with a strong theoretical justification.

*正會員, 漢陽大學校 電子通信工學科
(Dept. of Elec. Comm. Eng., Hanyang Univ.)
**正會員, 東義大學校 電子通信工學科
(Dept. of Elec. Comm. Eng., Dongeui Univ.)
接受日字 : 1988年 9月 3日
(※ 본 연구는 87년 한국전자통신연구소의 지원에 의하여 수행된 연구입니다.)

## I. 서 론

정보의 송수신 과정에서 전송로상의 여러가지 잡음으로 인해 발생하는 오류의 정정을 목적으로 디지탈 통신 시스템에서는 FEC(forward error correction) 기법을 사용하고 있다. 이 기법은 데이타, 음성, 영상신호 등 송수신이 가능한 거의 모든 디지탈

통신 시스템에 적용할 수 있으며 오류 정정부호(error-correction code)를 이용하여 비트오율이 아주 낮은 고신뢰도의 통신 시스템의 장치화가 가능하다.

비 2원 BCH부호의 한 범주에 속하는 RS 부호는 유한체 GF($2^m$) 상에서 부호화와 복호화가 이루어 지므로 산발오류(random error)뿐 아니라 연집오류(burst error)도 정정할 수 있기 때문에 군통신, 위성 및 우주통신, 전화망을 이용한 데이타 통신 시스템, 그리고 컴퓨터의 데이타 저장 시스템 등 많은 디지탈 통신망에서 오류정정을 목적으로 이용되고 있으며 그 대표적인 응용에는 미 연방 전략정보망(JTIDS)의 (31, 15)RS 부호, 미 공군위성통신망(AFSTATCOM)의 (7, 2)RS 부호, Compact Disk나 DAT에 이용되는 CIRS (cross interleaved reed-solomon codes), IBM 데이타 저장시스템에 이용되는 (61, 50) 단축 RS부호가 있다.

RS부호의 부호화는 정보다항식을 생성다항식으로 나누는 나눗셈회로에 의해 수행된다.[1] 복호에서는 오증과 오류위치다항식의 관계로 표시되는 Newton 항등식의 해를 구하는 것이 가장 큰 관건이다. 오증으로부터 오류위치다항식을 구하는 과정은 Peterson[2]에 의해 처음 고안되었고 Berlekamp[3], Massey[4]의 치환 레지스터를 이용한 복호, Welch와 Scholtz[5]의 Euclid 알고리듬을 이용한 복호, 변환영역을 이용한 Blahut[6]의 연구 등이 있다. 이 복호법들은 강력한 오류정정능력을 가지고 있으나 반복계산을 수행해야 하므로 복호기를 장치화한다는 아주 복잡한 단점이 있다. 그러나, Peterson의 연구를 개선한 Gorenstein-Zieler 알고리듬[7]은 t차원 정방행렬을 계산하면 되므로 오류정정능력 t가 비교적 작을 경우 계산이 간단하고 장치화에 이점이 있다.

본 논문에서는 RS부호의 구조를 체계적으로 고찰하고 오류정정능력 t가 비교적 작을 경우 Berlekamp-Massey의 반복 알고리듬보다 간단하고 장치화에 이점이 있는 Peterson-Gorenstein-Zierler 알고리듬 및 부호화와 복호과정을 연구, 분석하며 GF($2^5$) 상의 원소로 구성되는 2중 오류정정 (31, 27) RS 부호의 부호기와 복호기를 설계하고 이를 실제적으로 통신 시스템에 적용할 수 있도록 TTL IC로 장치화 하였다.

## Ⅱ. Reed-Solomon 부호의 부호화

Reed-Solomon(RS) 부호는 $2^m$개의 심볼로 이루어지는 유한체 GF($2^m$)의 블록계열이다. 이 블록계열을 다항식으로 표현한 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$를 부호다항식이라 하며 각 계수는 GF($2^m$)의 한 원소로서 m 비트로 표시된다. RS 부호가 전송로상에서 발생한 t개의 오류를 정정할 수 있을때 (n, k) RS 부호는 $k=2^m-1-2t$ 개의 정보심볼과 $n-k=2t$개의 검사심볼로 이루어지고 있으므로 심볼단위의 부호길이는 $n=2^m-1$이다.

정보다항식을 $d(x)=d_0+d_1x+\cdots+d_{k-1}x^{k-1}$라 하고 검사다항식을 $b(x)=b_0+b_1x+\cdots+b_{n-k-1}x^{n-k-1}$라 하면 부호화된 RS부호의 다항식은

$$c(x)=b(x)+x^{n-k}d(x)=\sum_{i=0}^{n-1}c_ix^i \qquad (1)$$

로 표시된다.

$c(x)$는 생성다항식 $g(x)$에 의해 만들어지며 $g(x)$의 곱이어야 한다. 그러므로 $x^{n-k}d(x)$를 $g(x)$로 나눈 나머지를 $b(x)$로 삼으면

$$x^{n-k}d(x)=q(x)g(x)+b(x) \qquad (2)$$

가 되어 $g(x)$의 곱으로 표현되는 부호다항식 $c(x)$를 얻을 수 있다. 이렇게 구한 $c(x)$의 계수로 부터 n차원 벡타 ($c_0, c_1, \cdots, c_{n-1}$)를 얻게되고 이를 부호어(code word)라 부른다. 즉 RS부호의 부호화는 GF($2^m$)의 심볼로 표시되는 정보를 생성다항식으로 나누는 나눗셈회로에 의해 수행된다.

GF(2)상의 m차 원시다항식 (primitive polynomial) $p(x)=p_0+p_1x+p_2x^2+\cdots+p_mx^m$의 근이 $\alpha$일때 유한체 GF($2^m$)의 원소 $\{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}$들은 m차 다항식으로 표현되며 m차원 벡타로도 표현된다. 예를들어 $p(x)=1+x^2+x^5$인 GF($2^5$)의 원소 $\alpha^5$는 $\alpha^4+\alpha^3+1$ 또는 (11001)로 표현된다.

[정의1] GF(q)가 체(field)를 형성하고 GF($q^m$)가 GF(q)의 확대체일때 GF($q^m$)의 한 원소 $\beta$에 대해 $m(\beta)=0$가 되는 GF(q)상에서 가장 낮은 차수의 기약다항식 $m(x)$를 GF(q)상에서의 $\beta$의 최소다항식(minimal polynomial)이라 한다.

[정의2] GF(q)상에서 같은 최소다항식을 갖는 GF($q^m$)의 두 원소를 공액(conjugate)이라 한다.

$\alpha$를 GF($2^m$)의 원시원(primitive element)이라 하고 $m_i(x)$를 GF(2)상의 $\alpha^i$의 최소다항식이라 하면 $m_i(x)$는 $\alpha^i$의 모든 공액을 근으로 가지며 t개의 오류를 정정할 수 있는 부호장 $n=2^m-1$인 BCH부호의 생성다항식은

$$g(x)=\mathrm{LCM}\ \{m_1(x), m_2(x), \cdots, m_{2t}(x)\} \qquad (3)$$

로 구해진다. 하지만 RS부호의 경우는 GF($2^m$)상에서 해석되므로 GF($2^m$)상의 최소다항식의 곱인

$$g(x)=(\alpha+x)\ (\alpha^2+x)\cdots(\alpha^{2t}+x)$$

$$=\sum_{i=0}^{2t}g_ix^i \qquad (4)$$

가 된다. 여기서 계수 $g_i$는 GF(2^m)의 원소이다.

[예제1] 원시다항식을 $p(x)=1+x^2+x^5$로 하면 (31, 27)RS 부호의 생성다항식은 식(4)로 부터 $g(x)=\alpha^{10}+\alpha^{29}x+\alpha^{19}x^2+\alpha^{24}x^3+x^4$이 된다. 정보다항식이 $d(x)=\alpha^4x^{26}+\alpha^4x^{25}$일때검사다항식을 계산하면 $b(x)=\alpha^5x^3+\alpha^4x^2+\alpha^{14}x+\alpha^7$이므로 부호다항식은 $c(x)=\alpha^4x^{26}+\alpha^4x^{25}+\alpha^5x^3+\alpha^4x^2+\alpha^{14}x+\alpha^7$이다.

(31, 27) RS부호의 부호기는 그림 1과 같은 나눗셈 회로로 설계되며 장치화한 부호기에 위 예제를 적용하여 그림 2와 같이 실험결과 검사심볼 b=(00101, 10000, 11101, 10100)와 정보심볼 d=(10000, 10000, 00000, ···, 00000)로 이루어지는 출력을 얻었다.

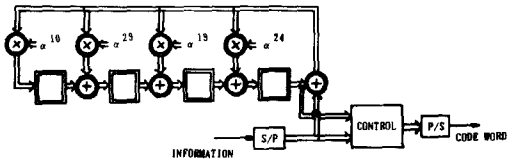



그림 1. (31, 27) Reed-Solomon 부호의 부호화 회로
Fig. 1. Encoding circuit for (31, 27) Reed-Solomon code.

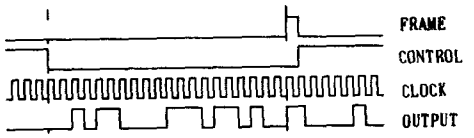



그림 2. $d(x)=\alpha^4x^{26}+\alpha^4x^{25}$ 일때 부호기의 출력
Fig. 2. Output of the encoder for $d(x)=\alpha^4x^{26}+\alpha^4x^{25}$.

## Ⅲ. 오증과 오류위치다항식

전송오류를 $e(x)$라 하면 수신계열에 오류가 발생한 경우 수신다항식 $r(x)$는

$$r(x)=c(x)+e(x) \tag{5}$$

로 될 것이다. 부호다항식은 생성다항식의 곱이므로 $c(x)$의 근 $\alpha$, $\alpha^2$, ···, $\alpha^{2t}$를 식(5)에 대입하면

$$r(\alpha^k)=e(\alpha^k),\quad 1\leqq k\leqq 2t \tag{6}$$

의 관계가 성립하며 이는 오증(syndrome)각 요소가 된다. 그런데, $r(x)$를 $\alpha^k$의 최소다항식 $m_k(x)$, $1\leqq k\leqq 2t$, 로 나눈 나머지를 $\gamma_k(x)$라 하면

$$r(x)=q_k(x)m_k(x)+\gamma_k(x) \tag{7}$$

인데 $m_k(\alpha^k)=0$이므로 오증요소 $s_k$는

$$s_k=r(\alpha^k)=\gamma_k(\alpha^k),\quad 1\leqq k\leqq 2t \tag{8}$$

와 같이 된다. 즉, 오증은 최소다항식으로 수신다항식을 나눈 나머지에 GF(2^m)의 원소를 대입하여 구하므로 그림 3과 같은 나눗셈회로에서 오증이 얻어진다.

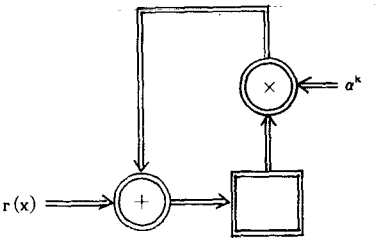



그림 3. Reed-Solomon 부호의 오증계산회로
Fig. 3. Syndrome computation circuit for Reed-Solomon code.

[예제2] 모든 요소가 '0'인 부호어를 송신하여 두 개의 오류가 발생한 $r(x)=\alpha^8x^2+\alpha^{25}x^{22}$을 수신하였을 경우 오증의 각 요소는 $s_1=\alpha^6$(01010), $s_2=\alpha^9$(11010), $s_3=\alpha^7$(10100), $s_4=\alpha^{26}$(10111)로 구해진다.

원시다항식이 $p(x)=1+x^2+x^5$인 GF(2^5)의 원소들의 곱을 다항식으로 표현하여 그림 3에 적용하면 (31, 27) RS부호의 오증회로를 설계할 수 있다. 장치화한 회로의 입력을 예제2의 경우로 했을때 오증요소들이 그림 4와 같이 얻어졌다.

RS부호의 경우 오류다항식 $e(x)$는 오류가 발생한 위치에서 GF(2^m)의 원소로 표시되는 오류치를 가진다. 실제로 $\nu$, $0\leqq\nu\leqq t$, 개의 오류가 발생하였다면 오류치를 $Y_i$, 오류위치번호를 $Z_i$라 하면 오증요소의 값은

$$s_k=\sum_{i=1}^{\nu}Y_iZ_i^k \tag{9}$$

로 된다. 이 식으로부터 $Y_i$와 $Z_i$의 값을 알아내는 것이 RS부호의 복호이다. $\nu$개의 오류가 발생한 경우 오류위치다항식은

$$\sigma(x)=\prod_{i=1}^{\nu}(1+Z_ix)=\sum_{i=0}^{\nu}\sigma_ix^i=1+\sigma_1x+\sigma_2x^2+\cdots+\sigma_\nu x^\nu \tag{10}$$

가 된다. $\sigma(x)$의 근 $Z_l^{-1}$, $1\leqq l\leqq\nu$, 을 식(10)에 대

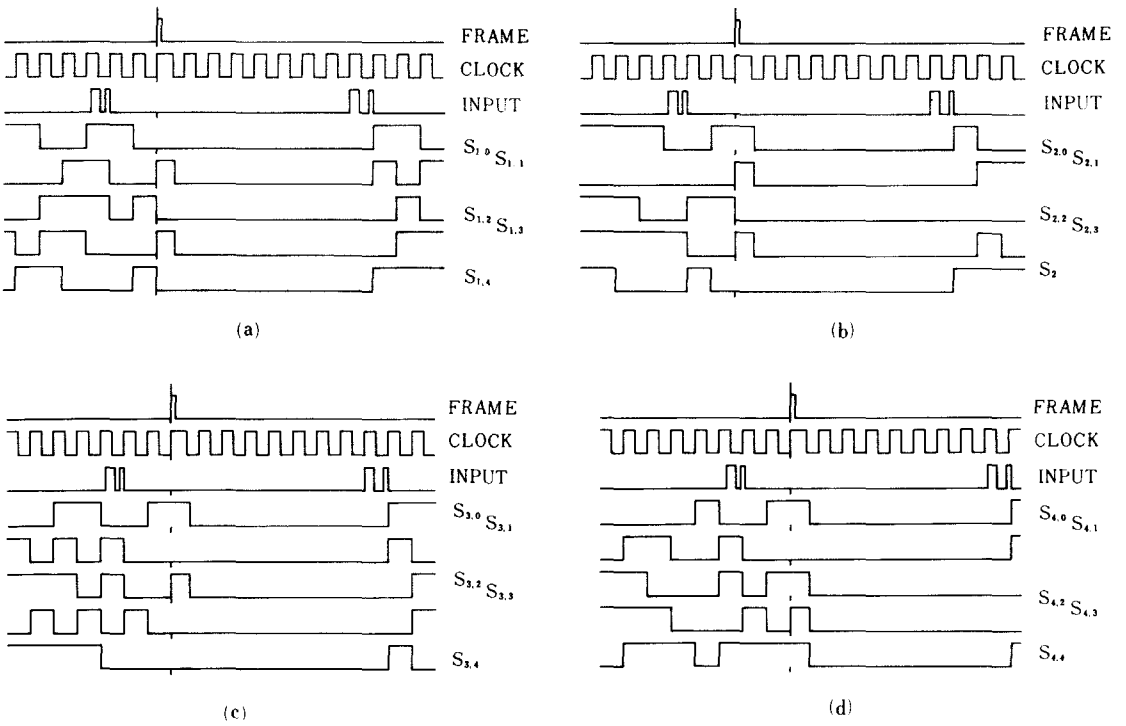



그림 4. $r(x)=\alpha^8x^2+\alpha^{25}x^{22}$ 일때 오증요소 (a) $s_1$, (b) $s_2$, (c) $s_3$, (d) $s_4$의 파형

Fig. 4. The waveform of syndrome components (a) $s_1$, (b) $s_2$, (c) $s_3$, and (d) $s_4$ for $r(x)=\alpha^8x^2+\alpha^{25}x^{22}$.

입하고 $Y_iZ_i^{j+\nu}$를 곱하면 $\sigma(Z_i^{-1})=0$이므로

$$Y_iZ_i^{j+\nu}\sum_{i=0}^{\nu}\sigma_iZ_i^{-i}=0$$

$$Y_i\sum_{i=0}^{\nu}\sigma_iZ_i^{j+\nu-i}=0 \qquad (11)$$

가 된다. $\sigma(x)$의 모든 근에 대해 적용하고 합하면

$$\sum_{i=1}^{\nu}Y_i\sum_{i=0}^{\nu}\sigma_iZ_i^{j+\nu-i}=0$$

$$\sum_{i=1}^{\nu}Y_iZ_i^{j+\nu}+\sigma_1\sum_{i=1}^{\nu}Y_iZ_i^{j+\nu-1}+\sigma_2\sum_{i=1}^{\nu}Y_iZ_i^{j+\nu-2}+\cdots$$
$$+\sigma_\nu\sum_{i=1}^{\nu}Y_iZ_i^{j}=0 \qquad (12)$$

로 표시된다. 따라서 식(9), (12)로부터 다음과 같은 결과를 얻는다.

$$s_{j+\nu}+\sigma_1s_{j+\nu-1}+\sigma_2s_{j+\nu-2}+\cdots+\sigma_\nu s_j=0 \qquad (13)$$

j를 1에서 $\nu$까지 변화시키면 $\nu$개의 연립방정식 즉, Newton의 항등식이 얻어진다. 수신다항식으로부터 구해진 오증을 이 식에 대입하여 오류위치다항식의 계수를 구할 수만 있다면 다항식의 근의 역수를 구할 수 있고 이것이 곧 오류위치번호가 된다.

## Ⅳ. Person-Gorenstein-Zierler 알고리듬

식(10)과 같이 표현된 Newton의 항등식을 행렬로 표시하면

$$\begin{bmatrix} s_1 & s_2 & s_3 & \cdots & s_{\nu-1} & s_\nu \\ s_2 & s_3 & s_4 & \cdots & s_\nu & s_{\nu+1} \\ s_3 & s_4 & s_5 & \cdots & s_{\nu+1} & s_{\nu+2} \\ & & \vdots & & & \\ s_\nu & s_{\nu+1} & s_{\nu+2} & \cdots & s_{2\nu-2} & s_{2\nu-1} \end{bmatrix} \cdot \begin{bmatrix} \sigma_\nu \\ \sigma_{\nu-1} \\ \sigma_{\nu-2} \\ \vdots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} s_{\nu+1} \\ s_{\nu+2} \\ s_{\nu+3} \\ \vdots \\ s_{2\nu} \end{bmatrix} \qquad (14)$$

가 얻어진다.

$$\overline{M}=\begin{bmatrix} s_1 & s_2 & \cdots & s_\nu \\ s_2 & s_3 & \cdots & s_{\nu+1} \\ s_3 & s_4 & \cdots & s_{\nu+2} \\ & & \vdots & \\ s_\nu & s_{\nu+1} & \cdots & s_{2\nu-1} \end{bmatrix} \qquad (15)$$

라 놓을때 $\det[\bar{M}]\neq 0$ 이면

$$\begin{bmatrix}\sigma_\nu\\ \sigma_{\nu-1}\\ \sigma_{\nu-2}\\ \vdots\\ \sigma_1\end{bmatrix}=\bar{M}^{-1}\cdot\begin{bmatrix}s_{\nu+1}\\ s_{\nu+2}\\ s_{\nu+3}\\ \vdots\\ s_{2\nu}\end{bmatrix} \tag{16}$$

로 쓸 수 있고 이 관계식에서 $\sigma_1$, $\sigma_2$, $\sigma_3$, …, $\sigma_\nu$ 를 결정할 수 있다. 그러나, $\nu$는 실제 오류의 수로서 오류정정능력 t이하의 값이므로 오류위치다항식의 계수를 구하기 위해서는 $\nu$의 값이 결정되어야 한다.

식(15)에서 $\nu=t$이면 $\det[\bar{M}]\neq 0$이고 $\nu<t$이면 $\det[\bar{M}]=0$가 된다. $\det[\bar{M}]=0$이면 $\nu=t-1$로 하여 행렬 $\bar{M}$을 재구성하고 다시 $\det[\bar{M}]$을 계산한다. 이와같은 방법으로 $\nu$의 값을 t에서 시작하여 하나씩 줄여가면서 $\det[\bar{M}]$을 계산할 때 최초로 $\det[\bar{M}]\neq 0$인 값 $\nu$가 실제로 발생한 오류의 수이다. $\nu$가 결정되면 식(15), (16)을 이용하여 $\sigma(x)$의 계수를 구하게 된다.

이상에 기술한 내용을 t=2인 경우에 적용하자. 식(15)에서 $\nu=t=2$이면 행렬 $\bar{M}$은

$$\bar{M}=\begin{bmatrix}s_1 & s_2\\ s_2 & s_3\end{bmatrix} \tag{17}$$

가 되며 $\det[\bar{M}]=s_1s_3+s_2^2$의 값에 따라 실제 오류의 수가 결정된다. $\det[\bar{M}]\neq 0$이면 2개의 오류가 발생한 것으로 판단하게 되고 오류위치다항식의 계수는 식(16)으로부터 다음과 같이 구해진다.

$$\begin{aligned}\sigma_2&=(s_3s_3+s_2s_4)/(s_1s_3+s_2^2)\\ \sigma_1&=(s_2s_3+s_1s_4)/(s_1s_3+s_2^2)\end{aligned} \tag{18}$$

또, $\det[\bar{M}]\neq 0$이면 $\bar{M}=[s_1]$이 되어 $\sigma_1=s_3/s_1$ 로서 단일오류가 발생한 경우이다. 만일 $s_1=0$이면 오류가 발생하지 않은 경우가 된다.

[예제3] 예제2의 결과로 얻어진 오증으로 $\sigma(x)$의 계수를 계산하면 $\sigma_1=\alpha^{10}(10001)$, $\sigma_2=\alpha^{24}(11110)$가 되어 오류위치번호는 $Z_1=\alpha^2(00100)$, $Z_2=\alpha^{22}(10101)$이다. 장치화된 복호기에서는 그림 5와 같이 계산된 값과 같은 $\sigma(x)$의 계수를 얻을 수 있었다.

## V. 오류치와 오류정정

$\nu$개의 오류가 발생한 수신계열에 대한 오증은 식(9)로 표현된다. 오증다항식의 차수는 $\nu$이지만 편의상 차수가 무한대인 것으로 생각하면 식(9)는

$$s(x)=\sum_{j=1}^{\nu}Y_j\sum_{i=0}^{\infty}(Z_j^i)x^i \tag{19}$$

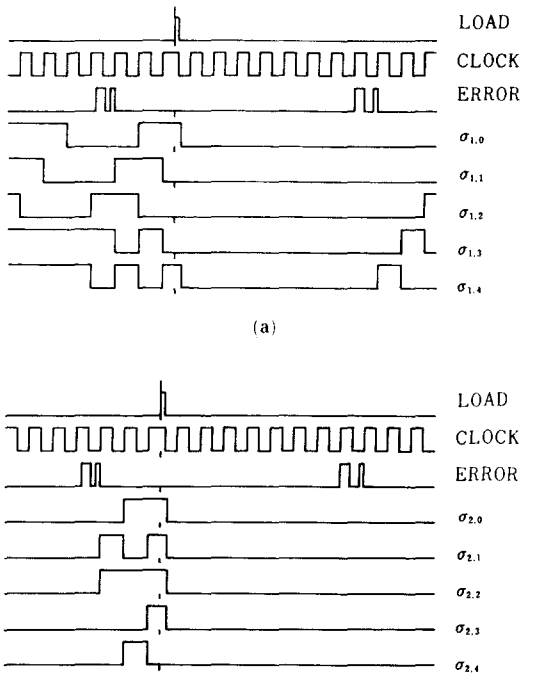



**그림 5.** (a) $\sigma_1$, (b) $\alpha_2$의 파형
**Fig. 5.** The waveform of (a) $\sigma_1$, (b) $\alpha_2$.

로 쓸 수 있으며

$$\sum_{i=0}^{\infty}(Z_j^i)x^i=1+Z_jx+(Z_j)^2x^2+\cdots=1/(1+Z_jx) \tag{20}$$

이므로 식(20)은

$$s(x)=\sum_{j=1}^{\nu}Y_j/(1+Z_jx) \tag{21}$$

와 같이 표현할 수 있다.

각 오류위치에 대응하는 오류치를 구하기 위해서 다음과 같은 다항식을 이용한다.

$$\Omega(x)=\sigma(x)s(x) \tag{22}$$

로 놓으면 식(10)과 (21)로부터 $\Omega(x)$를

$$\Omega(x)=\sum_{j=1}^{\nu}Y_j\prod_{\substack{k=1\\k\neq j}}^{\nu}(1+Z_kx) \tag{23}$$

로 쓸 수 있다. 이 식을 오류추정다항식이라 하며 $Z_i$위치에서의 오류치는 식(23)으로부터 아래와 같이 구해진다.[3,7]

$$Y_j=\Omega(Z_j^{-1})/\prod_{\substack{k=1\\k\neq j}}^{\nu}(1+Z_kZ_j^{-1}) \tag{24}$$

(31, 27) RS부호에 적용하기 위해 2중 오류일때의 오류치를 계산하면

$$Y_1=(s_1Z_2+s_2)/(Z_1Z_2+Z_1^2) \quad (25)$$

$$Y_2=(s_1Z_1+s_2)/(Z_1Z_2+Z_2^2)$$

이고 단일 오류일때는

$$Y_1=s_1/Z_1 \quad (26)$$

이다.

오류위치와 오류치가 구해지면 복호기에서는 오류정정을 행하게 된다. 수식적으로는 오류위치다항식의 근을 구하고 근의 역수를 취함으로서 오류위치를 구한다. 이렇게 오류위치다항식에서 오류위치를 구하는 것으로 Chien의 탐지회로[8]가 알려져 있다. 이 회로는 오류위치다항식의 계수가 초기값으로 기억된 t개의 레지스터를 치환시켜 각각 $\alpha$, $\alpha^2$, …, $\alpha^t$를 곱하는 승산기로 동작시킴으로서 $\sum_{i=0}^{t}\sigma_i(\alpha^k)^i$, $0\leqq k\leqq n-1$, 의 값이 '0'일때 $x^{n-1-k}$위치에 오류가 발생하였음을 탐지하는 방법으로 매우 능률적이다. 본 논문에서도 복호기를 장치화하는데 이 방법이 사용되었다.

〔예제4〕 예제2와 예제3의 결과로 얻어진 오증과 오류위치번호로부터 오류치를 구하면 $Y_1=\alpha^8$(01101), $Y_2=\alpha^{25}$(11001)가 된다. 그림 6은 장치화된 복호기에서 수신계열을 $r(x)=\alpha^8x^2+\alpha^{25}x^{22}$로 했을때 얻어진 결과이다.

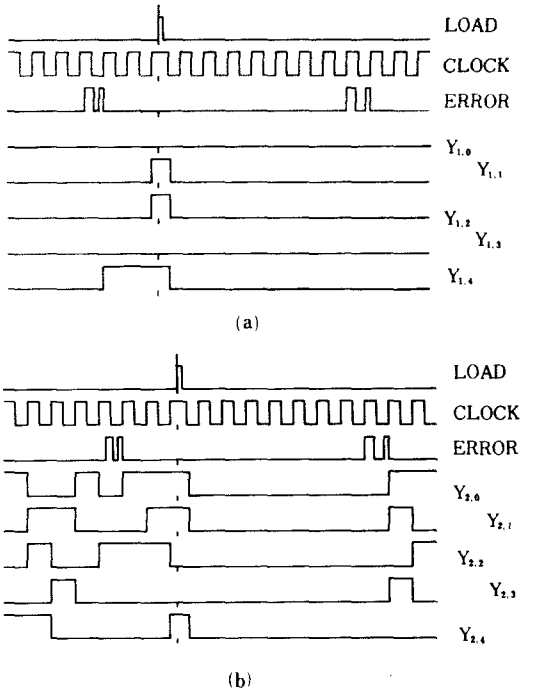



**그림 6.** 오류치 (a) $Y_1$ (b) $Y_2$의 파형
**Fig. 6.** The waveform of error values (a) $Y_1$, (b) $Y_2$.

## Ⅵ. 설계 및 장치화

(31, 27) RS부호의 생성다항식은 예제1에서 구한 바와 같이 $g(x)=\alpha^{10}+\alpha^{29}x+\alpha^{19}x^2+\alpha^{24}x^3+x^4$이다. 그러므로 부호기는 정보다항식을 이 생성다항식으로 나누는 나눗셈회로인 그림 1과 같이 된다. 부호기는 5비트가 1심볼로서 병렬로 처리된다. 하지만 전송은 비트별로 이루어지므로 나눗셈회로에 입력되기전에 직·병렬변환기를 통하게 된다. 하나의 정보심볼(5비트)이 회로에 입력되면서 동시에 채널로 빠져나간다. 이렇게 27개의 정보심볼(135비트)이 입력되면 생성다항식으로 정보다항식을 나눈 나머지인 검사다항식이 형성되어 병, 직렬변환기를 거쳐 비트별로 송출되도록 부호기를 장치화하였다.

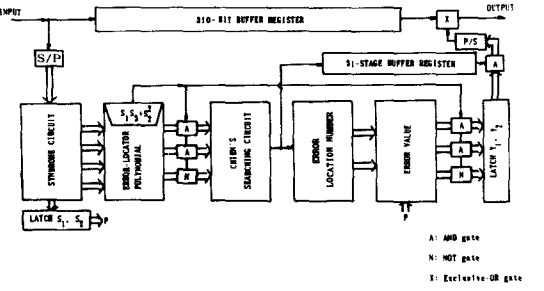



**그림 7.** (31, 27) Reed-Solomon 부호의 복호기 블럭도
**Fig. 7.** Block diagram of the decoder for (31, 27) Reed-Solomon code.

복호기의 설계는 그림 7과 같다. 그림 7에서 오증회로는 그림 3과 같은 나눗셈회로 4개로 구성된다. 오증회로에서 구해진 값중에서 $s_1$, $s_2$는 오류치를 계산하기 위해서 필요한 것이므로 이 값은 기억시켜 두어야 한다. 오류위치다항식의 계산은 2중 오류와 단일오류일 경우를 분리하여 계산하여야 하며 $s_1s_3+s_2^2$의 값에 의해 제어된다. 오증으로부터 오류위치다항식의 계수가 계산되는데 이 계산을 위하여 9개의 승산기와 2개의 역원계산기가 사용되었으며 승산기와 역원계산기는 ROM으로 처리하였다. $s_1s_3+s_2^2$의 값이 '1'이면 2개의 오류가 발생하였다고 판단하여 오류위치다항식의 계수가 AND 게이트를 통하여 Chien 탐지회로의 초기값이 된다. (그림 5 참조). 또 값이

'0' 이면 단일오류일때의 계수가 NOT 게이트를 통하여 탐지회로에 입력된다. 오류위치는 Chien의 탐지회로에서 얻어진다. 오류위치는 오류치의 계산에 필요하며 오류를 정정할때 사용하기 위해 31단 버퍼레지스터에 탐지회로의 출력을 기억시켰다. 오류치의 계산에도 2중오류와 단일오류를 위한 2개의 회로가 필요하고 $s_1s_3+s_2^2$의 값에 따라 오류위치다항식의 계산때와 같은 방법으로 제어되었으며 9개의 승산기와 3개의 역원계산기가 사용되었다. 이 오류치는 오류의 정정시 사용되기 위해 기억되어야한다(그림 6 참조). 복호에 소요되는 지연은 오증생성시 n단과 오류치 계산과정에서의 n단으로 총 2n단의 지연이 생기므로 310비트 버퍼를 통과한후 오류정정이 이루어지게 하였다. 또 복호는 심볼(5비트)별로 이루어지므로 오증회로의 입력에 앞서 직, 병렬변환기가 필요하고 역으로 오류정정에 앞서 병, 직렬변환기를 통하여 오류치가 출력되도록 하였다.

이상과 같이 설계, 제작된 (31, 27) RS부호의 복호기는 실험결과 2개 이하의 심볼(5비트)에 발생하는 어떠한 형태의 오류도 정정할 수 있었으며 1Mbps까지 안정되게 동작하였다. 장치화된 부호기와 복호기에는 모두 100여개의 TTL IC가 사용되었으며 실험결과를 위하여 DLG 7050 Logic Analyzer가 사용되었다.

## Ⅶ. 결 론

디지탈 통신 시스템에서 통신의 신뢰도를 높이기 위해 널리 사용되고 있는 RS부호의 부호화와 복호과정을 고찰하였으며, 오류위치다항식의 계산을 위한 여러 알고리듬중 오류정정능력이 비교적 작을 경우에 효율적인 Peterson-Gorenstein-Zieler 알고리듬을 분석하고 2중 오류정정 (31, 27) RS부호의 부호기와 복호기를 설계하여 TTL IC로 장치화하였다. 이를 바탕으로 모든 종류의 2중 오류정정 RS부호의 부호기와 복호기를 장치화할 수 있을 것이며, 디지탈 통신시스템 및 CD 또는 DAT에 적용가능하리라 사료된다. 한편, 일반적으로 통신시스템에 적용되는 오류정정부호는 시스템에 적합하도록 단축 또는 확장시켜 실용화하고 있으므로 제작에 앞서 특정시스템에 적합한 부호를 찾는 것이 선결과제이다.

## 參 考 文 獻


[1] 이만영, 부호이론, 희중당, 1984.

[2] Peterson, W.W., "Encoding and error correction procedure for bose-chaudhuri codes," *IRE Trans. Inf. Theory*, IT-6, 459-470, 1960.

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

[4] Massey, J.L., "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, IT-15, 122-127, 1969.

[5] Welch, L.R., and R.A. Scholtz, "Continued fractions and berlekamp's algorithm," *IEEE Trans. Inf. Theory*, IT-25, 19-27, 1979.

[6] Blahut, R.E "Transform techniques for error-control code," *IBM J. Res.* Dev., 23 299-315, 1979.

[7] Gorenstein, D.C., and N. Zieler, A Class of Error-Correcting Codes in p*m Symbols, J. Soc. Indust. Appl. Math.* 9, 207-214, 1961.

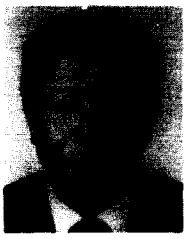
[8] Forney, G.D., Jr., "On decoding BCH codes," *IEEE Trans. Inf. Theory*, IT-11, 549-557, 1965.

[9] Chien, R.T., "Cyclic decoding procedures for bose-chaudhuri-hocquenghem codes," *IEEE Trans. Inf. Theory*, IT-10, 357-363, 1964.

[10] Peterson, W.W., and E.J. Weldon, Jr., *Erro-Correcting Codes*, 2nd ed., MIT Press Cambridge, MA, 1972.

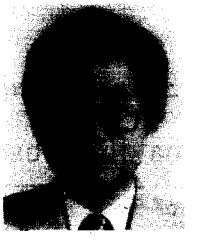
[11] Lin, S., D.J. Costello, *Error Control Coding*, Prentice-Hall, Inc., N.J., 1984. *

## 著 者 紹 介



**李 晩 榮(正會員)**

1924年 11月 30日生. 서울대학교 전기과 공학사학위 취득. 미국 Univ. of Colorado 공학박사학위취득(1958). 미국 Virginia 공대교수, 국방과학연구소 부소장, 한국전자통신(주)사장, 삼성반도체통신 사장, 현재 한양대학교 교수. 주관심분야는 Coding이론, 암호이론 등임.



**金 彰 圭(正會員)**

1958年 7月 21日生. 1981年 3月 한양대학교 전자통신공학과 공학사학위 취득. 1984年 8月 한양대학교 대학원 전자통신공학과 공학석사학위 취득. 1985年 3月～현재 한양대학교 대학원 박사과정. 1988年 3月～현재 동의대학교 전자통신공학과 전임강사. 주관심분야는 Coding 이론, 암호이론 등임.