(47, 41) Reed-Solomon 복호기 설계

조 용 석*, 박 상 규**
*영동대학교 전자공학부, **한양대학교 전자전기공학부

Design of (47, 41) Reed-Solomon Decoder

Yong Suk Cho*, Sang Kyu Park**
*Faculty of Electronics Eng., Youngdong University
**Division of Electrical & Computer Eng., Hanyang University

요 약

본 논문에서는 광대역 CDMA용으로 제안되고 있는 유한체 $GF(2^8)$ 상의 3중 오류정정 (47, 41) Reed-Solomon 복호기를 설계하였다. 복호법으로는 오류정정 능력이 비교적 작은 경우 매우 효율적인 직접복호법을 이용하였다. 설계된 복호기는 복호지연이 매우 짧으며 기존의 복호기보다 훨씬 간단한 하드웨어로 구현할 수 있는 장점을 가지고 있다.

1. 서 론

Reed-Solomon 부호는 1960년에 I. S. Reed와 G. Solomon에 의해 제안된 부호로, 오류정정능력이 우수하고 랜덤오류(random error) 및 연집오류(burst error)를 동시에 정정할 수 있기 때문에 ATM(Asynchronous Transfer Mode), CDPD(Cellular Digital Packet Data) 등과 같은 디지털 통신시스템과 CD(Compact Disk), DVD(Digital Video Disk) 등과 같은 데이터 저장시스템에 널리 사용되고 있는 부호이다[1].

최근 제3세대 이동통신망으로 각광받고 있는 IMT-2000(International Mobile Telecommunication)의 무선접속 기술로 세계 각국에서 개발이 진행 중인 광대역 CDMA(Wideband CDMA)에서도 Reed-Solomon 부호의 사용을 권고하고 있다.

본 논문에서는 광대역 CDMA용으로 제안되고 있는 유한체(Galois field or finite field) $GF(2^8)$ 상의 3중 오류정정 (47, 41) Reed-Solomon 부호[2]의 복호기를 설계한다. 본 논문에서는 복호법으로 오류정정능력이 비교적 작은 경우 매우 효율적인 직접복호법을 이용하여 3중 오류정정 Reed-Solomon 복호기를 설계하고 기존의 PGZ(Peterson Gorenstein Zierler) 복호법으로 설계한 복호기[3]와 하드웨어 복잡도를 비교한다.

본 논문에서 설계한 복호기는 오증(syndrome)을 계산하는데 걸리는 부호길이 만큼의 지연만 소요되므로 복호지연(decoding delay)이 매우 짧으며 기존의 복호기에 비해 훨씬 간단한 하드웨어로 구현할 수 있다.

2. Reed-Solomon 부호의 직접복호법

Reed-Solomon 부호의 직접복호법은 오증으로부터 오류위치다항식(error locator polynomial)을 구한 다음 오류위치(error location number)와 이에 해당하는 오류값(error value)을 구하는 일반적인 복호법과는 달리 오증으로부터 직접 오류위치와 오류값을 구하여 오류를 정정하는 방법이다. 2진 BCH 부호에 대한 직접복호법은 Chien[4]이 처음 제안하였으며 Horiguchi와 Sato[5]는 이를 Reed-Solomon 부호로 확장하였다.

t개 이하의 모든 오류를 정정할 수 있는 t중 오류정정 Reed-Solomon 부호에서 $u(1 \le u \le t)$개의 오류가 $i_1, i_2, \cdots\cdots, i_u$ ($i_1 < i_2 \cdots\cdots < i_u$) 위치에서 발생하였다고 가정하고 오류위치와 오류값을 각각 X_k와 Y_k라 하면 오증 s_j는 다음과 같이 쓸 수 있다.

$$s_j = \sum_{i=1}^{u} Y_i X_i^j \quad , \quad j = 1, 2, \cdots 2t \qquad (1)$$

여기에서 오류위치다항식을 다음과 같이 오류위치의 역수를 근으로 갖는 다항식으로 정의하면

$$\sigma(x) = (1+X_1x)(1+X_2x)\cdots(1+X_ux) = \prod_{i=1}^{u}(1+X_ix) \quad (2)$$

오증 s_j와 오류위치다항식의 계수 σ_i간의 관계는 다음과 같은 행렬(matrix)로 표현할 수 있다.

$$\begin{bmatrix} s_1 & s_2 & \cdots\cdots & s_u \\ s_2 & s_3 & \cdots\cdots & s_{u+1} \\ s_3 & s_4 & \cdots\cdots & s_{u+2} \\ \vdots & \vdots & \vdots & \vdots \\ s_u & s_{u+1} & \cdots\cdots & s_{2u-1} \end{bmatrix} \cdot \begin{bmatrix} \sigma_u \\ \sigma_{u-1} \\ \sigma_{u-2} \\ \vdots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} s_{u+1} \\ s_{u+2} \\ s_{u+3} \\ \vdots \\ s_{2u} \end{bmatrix} \quad (3)$$

여기에서 오증 s_j를 요소로 하는 $u\times u$행렬을 $M_u(s)$라 하면 이것의 행렬식(determinant) $|M_u(s)|$는 다음과 같이 쓸 수 있다.

$$|M_u(s)| = \prod_{i=1}^{u} Y_iX_i \prod_{i>j\geq 1}^{u}(X_i+X_j)^2 \quad (4)$$

그러므로 행렬식 $|M_u(s)|$는 오류가 정확하게 u개 발생하였을 때는 0이 아니고 u개 보다 적게 발생하였을 경우에는 0이 된다[6].

오증에 관한 함수를 다음과 같이 정의하고

$$S_j(x) = s_jx^j \quad , \ j=1,2,\cdots\cdots,2t \quad (5)$$

$$A_j(x) = S_j(x) + S_{j+1}(x) \quad , \ j=1,2,\cdots\cdots,2t-1 \quad (6)$$

$$B_j(x) = S_j(x) + S_{j+2}(x) \quad , \ j=1,2,\cdots\cdots,2t-2 \quad (7)$$

여기에 식 (1)을 대입하면 다음과 같이 된다.

$$S_j(x) = \sum_{i=1}^{u} Y_iX_i^jx^j = \sum_{i=1}^{u} Y_iX_ix(X_ix)^{j-1} \quad (8)$$

$$A_j(x) = \sum_{i=1}^{u} Y_iX_ix(X_ix)^{j-1} + \sum_{i=1}^{u} Y_iX_ix(X_ix)^{j} = \sum_{i=1}^{u}[Y_iX_ix(1+X_ix)](X_ix)^{j-1} \quad (9)$$

$$B_j(x) = \sum_{i=1}^{u} Y_iX_ix(X_ix)^{j-1} + \sum_{i=1}^{u} Y_iX_ix(X_ix)^{j+1} = \sum_{i=1}^{u}[Y_iX_ix(1+X_ix)^2](X_ix)^{j-1} \quad (10)$$

$A_j(x)$를 요소로 하는 $u\times u$행렬 $M_u[A(x)]$의 행렬식을 식 (4)과 같이 전개하면 다음과 같이 된다.

$$\begin{aligned} &|M_u[A(x)]| \\ &= \prod_{i=1}^{u} Y_iX_ix(1+X_ix) \prod_{i>j\geq 1}^{u}(X_ix+X_jx)^2 \\ &= x^u \prod_{i=1}^{u} Y_iX_i \prod_{i=1}^{u}(1+X_ix)\, x^{u(u-1)} \prod_{i>j\geq 1}^{u}(X_i+X_j)^2 \\ &= \prod_{i=1}^{u} Y_iX_i \prod_{i>j\geq 1}^{u}(X_i+X_j)^2 x^{u^2} \prod_{i=1}^{u}(1+X_ix) \\ &= |M_u(s)|\cdot x^{u^2}\cdot\sigma(x) \end{aligned} \quad (11)$$

u개의 오류가 발생하였을 경우 행렬식 $|M_u(s)|$는 0이 아니므로 $|M_u[A(x)]|=0$의 근은 $\sigma(x)=0$를 만족하는 오류위치가 된다.

또 $S_j(x)$를 요소로 하는 $u\times u$행렬 $M_u[S(x)]$의 행렬식 $|M_u[S(x)]|$를 같은 방법으로 전개하면

$$|M_u[S(x)]| = \prod_{i=1}^{u} Y_iX_ix \prod_{i>j\geq 1}^{u}(X_ix+X_jx)^2 \quad (12)$$

가 되며 여기에 $i=1$, $j=1$, $x=X_1^{-1}$을 대입하면 다음과 같이 된다.

$$|M_u[S(X_1^{-1})]| = Y_1X_1X_1^{-1}\prod_{i=2}^{u} Y_iX_iX_1^{-1} \cdot (1+X_iX_1^{-1})^2 \prod_{i>j\geq 2}^{u}(X_iX_1^{-1}+X_jX_1^{-1})^2 \quad (13)$$

같은 방법으로 $B_j(x)$에 대한 행렬식 $|M_{u-1}[B(x)]|$는

$$|M_{u-1}[B(x)]| = \prod_{i=2}^{u} Y_iX_ix(1+X_ix)^2 \cdot \prod_{i>j\geq 2}^{u}(X_ix+X_jx)^2 \quad (14)$$

가 되며 여기에 $x=X_1^{-1}$을 대입하여 정리하면

$$|M_{u-1}[B(X_1^{-1})]| = \prod_{i=2}^{u} Y_iX_iX_1^{-1} \cdot (1+X_iX_1^{-1})^2 \prod_{i>j\geq 2}^{u}(X_iX_1^{-1}+X_jX_1^{-1})^2 \quad (15)$$

가 된다. 식 (13)을 식 (15)로 나누면

$$Y_1 = \frac{|M_u[S(X_1^{-1})]|}{|M_{u-1}[B(X_1^{-1})]|} \quad (16)$$

가 된다. 따라서 위 식을 일반화하면

$$Y_k = \frac{|M_u[S(X_k^{-1})]|}{|M_{u-1}[B(X_k^{-1})]|} \quad (17)$$

가 되므로 오류위치 $X_k^{-1}(k=1,2,\cdots\cdots)$에 대응하는 오류값 Y_k를 구할 수 있다.

이상과 같이 오류위치다항식과 오류값을 구하는 새로운 식을 유도하였다. 따라서 직접복호법은 먼저 행렬식 $|M_u(S)|$를 계산하여 실제 발생한 오류의 개수 u를 구한 다음, 방정식 $|M_u[A(x)]|=0$에서 x대신에 α^0, α^1, ……, α^{n-1}을 차례로 대입하여 오류위치를 구하고 식 (17)을 이용하여 그 위치에 해당하는 오류값 Y_k를 계산하여 오류를 정정하면 된다.

3. (47, 41) Reed-Solomon 복호기 설계

(47, 41) Reed-Solomon 부호는 유한체 $GF(2^8)$ 상의 3중 오류정정 부호인 (255, 249) Reed-Solomon 부호를 208 심벌만큼 단축시킨 부호이다. 따라서 오류가 1개, 2개, 3개 발생한 경우를 모두 고려하여야 한다. 먼저 오류위치다항식 $|M_1(A)|$, $|M_2(A)|$, $|M_3(A)|$는 다음과 같이 구할 수 있다.

$$|M_1(A)| = A_1 \tag{18}$$

$$|M_2(A)| = \begin{vmatrix} A_1 & A_2 \\ A_2 & A_3 \end{vmatrix} = A_2^2 + A_1 A_3 \tag{19}$$

$$|M_3(A)| = \begin{vmatrix} A_1 & A_2 & A_3 \\ A_2 & A_3 & A_4 \\ A_3 & A_4 & A_5 \end{vmatrix} = A_3^3 + A_1 A_4^2 + A_5 |M_2(A)| \tag{20}$$

같은 방법으로 $|M_1(S)|$, $|M_2(S)|$, $|M_3(S)|$, $|M_0(B)|$, $|M_1(B)|$, $|M_2(B)|$를 구하면 다음과 같이 된다.

$$|M_1(S)| = S_1 \tag{21}$$

$$|M_2(S)| = S_2^2 + S_1 S_3 \tag{22}$$

$$|M_3(S)| = S_3^3 + S_1 S_4^2 + S_5 |M_2(S)| \tag{23}$$

$$|M_0(B)| = 1 \tag{24}$$

$$|M_1(B)| = B_1 = S_1 + S_3 \tag{25}$$

$$|M_2(B)| = B_2^2 + B_1 B_3 \tag{26}$$

따라서 오류값 $Y^{(1)}$, $Y^{(2)}$, $Y^{(3)}$는

$$Y^{(1)} = \frac{|M_1(S)|}{|M_0(B)|} = S_1 \tag{27}$$

$$Y^{(2)} = \frac{|M_2(S)|}{|M_1(B)|} = \frac{S_2^2 + S_1 S_3}{B_1} \tag{28}$$

$$Y^{(3)} = \frac{|M_3(S)|}{|M_2(B)|} = \frac{|M_3(S)|}{B_2^2 + B_1 B_3} \tag{29}$$

가 되며 버퍼 레지스터의 출력과 더해지는 오류값 Y는 다음과 같이 정리할 수 있다.

$$Y = \begin{cases} Y^{(3)}, \text{ if } |M_3(S)| \neq 0 \text{ and } |M_3(A)| = 0 \\ Y^{(2)}, \text{ if } |M_3(S)| = 0 \text{ and } |M_2(S)| \neq 0 \\ \quad \text{and } |M_2(A)| = 0 \\ Y^{(1)}, \text{ if } |M_3(S)| = 0 \text{ and } |M_2(S)| = 0 \\ \quad \text{and } S_1 \neq 0 \text{ and } A_1 = 0 \end{cases} \tag{30}$$

이상의 결과를 이용하여 (47, 41) Reed-Solomon 복호기를 설계하면 그림 1과 같이 된다.

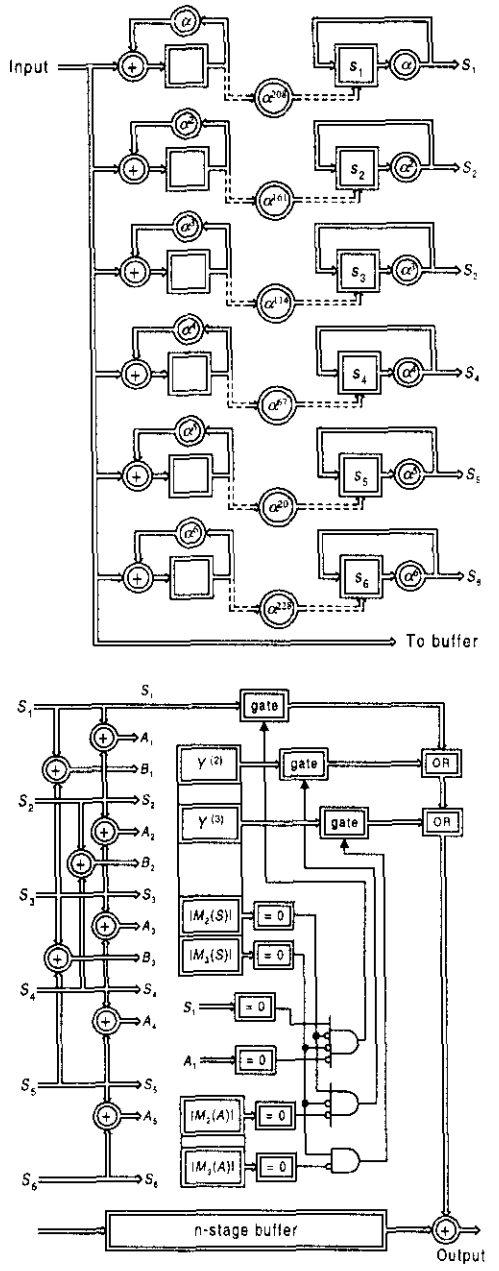

그림 1. (47, 41) Reed-Solomon 복호기

그림 1에서 2중 선은 8개의 선을 표시한 것이며 점선은 계산된 오중을 병렬 로드(load)하는 것을 나타내고 있다. ⊙는 $GF(2^8)$ 상의 덧셈기를, $Y^{(i)}$는 그림 2

와 같은 오류값 계산회로를, |M(A)|는 그림 3과 같은 오류위치 계산회로를 나타내고 있다. =0은 8개의 비트가 모두 0일 때 0을 출력하는 전영검출기(all zero detector)를 표시하고 있다. 또 OR는 비트 별로 OR하는 회로를, gate는 선택(select) 입력이 1일 때에만 입력을 출력으로 통과시키는 회로를 나타내고 있다. 그림 2와 그림 3에서 ×은 $GF(2^8)$ 상의 곱셈기를, $()^2$은 $GF(2^8)$ 상의 제곱기를, %은 $GF(2^8)$ 상의 나눗셈기를 표시한 것이다.

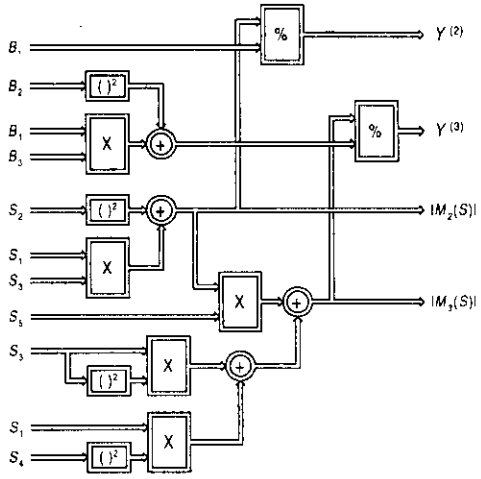

그림 2. 그림 1의 오류값 계산회로

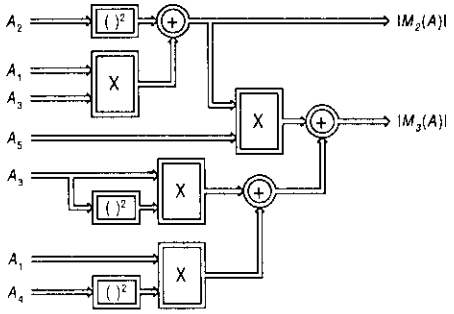

그림 3. 그림 1의 오류위치 계산회로

오류정정능력이 비교적 작을 때 효율적인 PGZ 알고리듬으로 설계한 3중 오류정정 Reed-Solomon 복호기[3]와 본 논문에서 설계한 복호기의 하드웨어 복잡도를 비교하면 표 1과 같이 된다. 오증 계산 및 치환회로는 기존의 복호기와 거의 같은 복잡도를 가지므로 비교 대상에서 제외하고 오류위치 및 오류값 계산에 소요되는 $GF(2^m)$ 상의 연산기 개수만을 비교하였다. 표 1에서 보듯이 본 논문에서 설계한 복호기가 기존의 복호기에 비해 하드웨어 복잡도 면에서 훨씬 우수함을 알 수 있다.

표 1. 3중 오류정정 Reed-Solomon 복호기의 소요 하드웨어 양 비교

$GF(2^m)$ 상의 연산기	문헌 [3]의 복호기	본 논문의 복호기
덧 셈 기	21 개	16 개
곱 셈 기	24 개	9 개
나눗셈기	1 개	2 개
제 곱 기	4 개	6 개

4. 결 론

본 논문에서는 오류정정능력이 비교적 작을 경우 효율적인 직접복호법을 이용하여, 광대역 CDMA용으로 제안되고 있는 유한체 $GF(2^8)$ 상의 3중 오류정정 (47, 41) Reed-Solomon 복호기를 설계하였다.

설계된 복호기는 복호지연이 매우 짧으며 기존의 복호기에 비해 훨씬 간단한 하드웨어로 구현할 수 있는 장점을 가지고 있다.

참 고 문 헌

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

[2] Multiband CDMA FPLMTS 무선접속규격, 한국전자통신연구원, 1997.

[3] A. M. Patel, "On-the-fly decoder for multiple byte errors," *IBM J. RES. DEVELOP.*, Vol. 30, No. 3, pp. 259~269, 1986.

[4] R. T. Chien, "Cyclic Decoding Procedure for the Bose Chaudhuri Hocquenghem Codes," *IEEE Trans. Inform. Theory*, IT-10, pp. 357~363, 1964.

[5] T. Horiguchi and Y. Sato, "A Decoding Method for Reed-Solomon Codes over $GF(2^m)$," *Trans. IEICE*, Vol. J66-A, pp. 97~98, 1983.

[6] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, 2nd Edition, M.I.T. Press, Cambridge, Mass., pp. 284~285, 1972.