3중 오류정정 BCH부호의 병렬복호기 구현에 관한연구

° 김 창 수 이 만 영

한양대학교 대학원 전자통신공학과

(An Implementation of parallel Decoder for TEC-BCH Codes)

Chang Soo Kim Man Young Rhee

Hanyang University

* ABSTRACT *

Some efficient methods for solving the equations over GF(2^m) are proposed in this paper. Using these algorithms, parallel decoder for a triple-error-correcting(31, 16) BCH code is implemented. By incorporating with ROM and PAL which are inserted in a decoder, the complex logic circuits can be substantially reduced and therefore a high speed decoder can be constructed.

1. 서 론

블럭부호중에서 BCH 부호는 1959년에 Hocquenghem과 1960년에 Bose와 Chaudhuri에 의해여 독자적으로 발표된 부호로써 블럭부호중 강력한 오류정정능력을 갖는 순회부호의 일종이다. Computer를 예로들면 현재 SEC/DEC 부호는 Computer의 주기억장치에 널리 사용 되어지고 있다. 본 논문에서는 Polkinghorn[4]의 복호방법과 Yamagish[5]복호기를 개선하여 3중 오류정정 (31,16)BCH 부호의 병렬 복호기를 만드는 새로운 방법을 제시하여 장치화 하였다. 이 복호기는 병렬로 처리되므로 Computer의 주/보조 기억장치에 사용되어질 수 있다. 특히 복호기에 ROM을 사용하여 복잡한 회로를 간소화하였고, 기존의 연산회로도 역시 간소화하였다. 앞으로 소자상의 지연을 더욱 줄이기 위하여 하나의 LSI칩으로 설계하여 장치화하면 더욱 고속의 복호기를 얻을 수 있을 것이다.

2. GF(2^m)상의 3차 방정식의 해를 구하는 방법

본 논문에서는 오류위치다항식에서 오류위치를 구하기 위하여 Polkinghorn의 방법을 기초로 하였다. 3차 방정식의 경우 Polkinghorn의 방법을 설명하면 다음과 같다.

$$x^3 + \sigma_{31}x^2 + \sigma_{32}x + \sigma_{33} = 0 \quad \cdots\cdots(1)$$

이므로 여기서 $x = y + \sigma_{31}$로 치환하면

$$y^3 + \lambda y + \delta = 0 \quad \cdots\cdots(2)$$

$$(\lambda = \sigma_{31}^2 + \sigma_{32}, \quad \delta = \sigma_{31}\sigma_{32} + \sigma_{33})$$

$y = \lambda^{1/2} \cdot z$ 로 치환하면

$$z^3 + z + c_k = 0 \quad , \quad (c_k = \delta/\lambda^{3/2}) \quad \cdots\cdots(3)$$

이다. 식(3)의 근들은 c_k 값에 의하여 결정된다. 그러면 식(1)의 방정식 근들은

$$x_i = \lambda^{1/2} \cdot z_i + \sigma_{31}, \quad (i=1, 2, 3) \quad \cdots\cdots(4)$$

이다.

3. GF(2^m)상의 각종 회로 구성

GF(2^m)상의 α를 원시원소(primitive element)라 하면 모든 non-zero원소는 GF(2^m)상의 지수표현(exponential expression)이라는 α의 멱(power)으로 표시된다. 한편 2^m개 원소는 차수가 m-1인 GF(2)상의 modulo-p(x)의 다항식으로 표현되어질 수 있고, 그 다항식의 계수들 만으로 표현하면 백터표현 이라고 한다. 예를 들어 GF(2^5)상의 원시다항식 $p(\alpha) = 1 + \alpha^2 + \alpha^5 = 0$ 일때

$$\alpha^{16} = 1 + \alpha + \alpha^3 + \alpha^4 = (1\ 1\ 0\ 1\ 1) = (0\ 0\ 0\ 0\ 1)$$

다항식표현 백터표현 지수표현

Galois Field에서는 곱셈과 나눗셈의 계산회로는 복잡하므로 계산수행을 효율적으로 처리하기 위하여 nonzero원소 α의 멱(power), 즉 지수표현으로 계산한다. 그러면 원소들간의 곱셈과 나눗셈은 원소 α의 멱을 덧셈과 뺄셈하는 형태로 간단히 처리된다.

단 zero원소와 α^0원소를 구별하기 위하여 α^U원소는 m비트로 표현되는 지수표현중 가장높은 값으로 바꿔어야한다.

3-1. 곱셈 회로

원소들 간에 곱셈을 수행하기 위한 곱셈회로는 modulo-2^m-1의 덧셈형태로 된다. 이 회로에 대한 blockdiagram과 symbol이 그림.1에 나타나 있다.

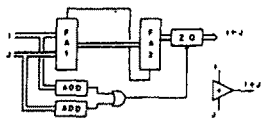

그림.1 곱셈 회로

그림.1에서 FA는 m-bits로된 전가산기이다. modulo 2^m-1을 수행하기 위하여 FA1의 합과 carry가 FA2에서 더해진다. AOD는 입력원소들이 zero원소 인지를 감지 하는 회로이며 ZO는 AOD에서 zero원소가 감지되었을때 출력을 zero원소로 보내는 회로이다.

3-2. 나눗셈 회로

원소들 간에 나눗셈을 수행하기 위한 나눗셈회로는 지수표현의 분자를 분모로 뺄셈하는 과정이다. 이 회로의 block diamgram과 symbol은 그림.2에 나타나 있다.

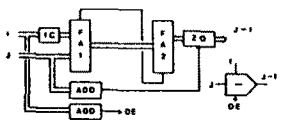

그림.2 나눗셈 회로

여기서 1C는 1의 보수를 취하는 회로이다. DE는 분모가 zero원소일때 불능이므로 이것을 감지하는 회로이다.

3-3. 덧셈 회로

원소들간에 덧셈을 수행하는 과정은 다음과 같다.

$$\alpha^i + \alpha^j = \alpha^i \cdot (1 + \alpha^{j-i}) \quad \cdots\cdots\cdots\cdots (5)$$

여기서 j-i=k 이라면, $1+\alpha^k=\alpha^{k^*}$로 놓을수 있다.

$$\alpha^i + \alpha^j = \alpha^i \cdot \alpha^{k^*} \quad \cdots\cdots\cdots\cdots (6)$$

로 되어서 덧셈이 곱셈형태로 바뀌게된다. 덧셈을 수행하는 회로는 그림.3과 같다

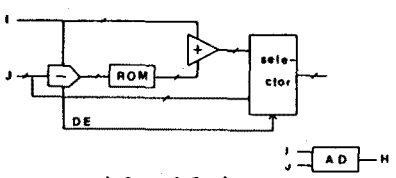

그림.3 덧셈 회로

4. 3중 오류정정 (31,16)BCH 부호의 병렬복호

4-1. 오증 계산

부호어$\bar{c}$를 전송했을때 오류형태$\bar{e}$로 인해 수신어$\bar{r}$는 다음과 같다.

$$\bar{r} = \bar{c} + \bar{e} \quad \cdots\cdots\cdots\cdots (7)$$

식(7)의 수신어$\bar{r}$로 부터 오증$\bar{S}$를 계산하는 것인데 본 논문에서는 3중 오류정정 BCH 부호이므로 오증$\bar{S}$은

$$\bar{S} = (s_1 , s_3 , s_5) = \bar{r} \cdot \bar{H}^T \quad \cdots\cdots\cdots\cdots (8)$$

이 된다. 식(8)로 부터 GF(2^5)상의 검사행렬$\bar{H}$은

$$\bar{H} = \begin{bmatrix} \alpha^0 \alpha^1 \alpha^2 \alpha^3 \alpha^4 \alpha^5 \alpha^6 \alpha^7 \alpha^8 \alpha^9 \alpha^{10} \alpha^{11} \alpha^{12} \alpha^{13} \\ \alpha^0 \alpha^3 \alpha^6 \alpha^9 \alpha^{12} \alpha^{15} \alpha^{18} \alpha^{21} \alpha^{24} \alpha^{27} \alpha^{30} \alpha^2 \alpha^5 \alpha^8 \\ \alpha^0 \alpha^5 \alpha^{10} \alpha^{15} \alpha^{20} \alpha^{25} \alpha^{30} \alpha^4 \alpha^9 \alpha^{14} \alpha^{19} \alpha^{24} \alpha^{29} \alpha^3 \end{bmatrix}$$

$$\begin{bmatrix} \alpha^{14} \alpha^{15} \alpha^{16} \alpha^{17} \alpha^{18} \alpha^{19} \alpha^{20} \alpha^{21} \alpha^{22} \alpha^{23} \alpha^{24} \alpha^{25} \\ \alpha^{11} \alpha^{14} \alpha^{17} \alpha^{20} \alpha^{23} \alpha^{26} \alpha^{29} \alpha^1 \alpha^4 \alpha^7 \alpha^{10} \alpha^{13} \\ \alpha^8 \alpha^{13} \alpha^{18} \alpha^{23} \alpha^{28} \alpha^2 \alpha^7 \alpha^{12} \alpha^{17} \alpha^{22} \alpha^{27} \alpha^1 \end{bmatrix}$$

$$\begin{bmatrix} \alpha^{26} \alpha^{27} \alpha^{28} \alpha^{29} \alpha^{30} \\ \alpha^{16} \alpha^{19} \alpha^{22} \alpha^{25} \alpha^{28} \\ \alpha^6 \alpha^{11} \alpha^{16} \alpha^{21} \alpha^{26} \end{bmatrix} \quad \cdots\cdots\cdots\cdots (9)$$

이다. 식(8)에서 오증$\bar{S}$는 수신어$\bar{r}$로 부터 구해진다. 오증$\bar{S}$에 대한 설계는 그림.4과 같다.

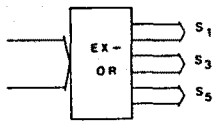

그림.4 3중 오류 정정 BCH 부호의 오증 회로

4-2. 오류 위치 다항식

오증$\bar{S}$로 부터 오류위치를 알아내기 위하여 오류위치다항식[1]-[3]을 구해야 된다. 오류위치다항식의 계수는

$$\begin{bmatrix} s_l & s_{l+1} & \cdots & s_{l+v-1} \\ s_{l+1} & s_{l+2} & \cdots & s_{l+v} \\ \cdot & \cdot & \cdots & \cdot \\ s_{l+v-1} & & \cdots & s_{l+2v-2} \end{bmatrix} \begin{bmatrix} \sigma_{l+v-1} \\ \sigma_{l+v-2} \\ \cdot \\ \sigma_l \end{bmatrix} = \begin{bmatrix} -s_{l+v} \\ -s_{l+v+1} \\ \\ -s_{l+2v-1} \end{bmatrix}$$

$$\cdots\cdots\cdots\cdots (10)$$

이다. 식(10)에서 l=1일때 3중 오류정정 BCH부호의 오류위치다항식의 계수는

$$\begin{bmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \\ s_3 & s_4 & s_5 \end{bmatrix} \begin{bmatrix} \sigma_{33} \\ \sigma_{32} \\ \sigma_{31} \end{bmatrix} = \begin{bmatrix} -s_4 \\ -s_5 \\ -s_6 \end{bmatrix}$$

$$\begin{bmatrix} \sigma_{33} \\ \sigma_{32} \\ \sigma_{31} \end{bmatrix} = \begin{bmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \\ s_3 & s_4 & s_5 \end{bmatrix}^{-1} \begin{bmatrix} -s_4 \\ -s_5 \\ -s_6 \end{bmatrix} \quad \cdots\cdots\cdots(11)$$

$\sigma_{31} = s_1$

$\sigma_{32} = (s_1^2 \cdot s_3 + s_5) / (s_1^3 + s_3)$

$\sigma_{33} = s_1^3 + s_3 + s_1(s_1^2 s_3 + s_5)/(s_1^3 + s_3)$

이다. 식(11)으로 부터 오류위치다항식을 표시하면

$$x^3 + \sigma_{31}x^2 + \sigma_{32}x + \sigma_{33} = 0 \quad \cdots\cdots\cdots(12)$$

이 된다. 2장의 해를 구하기위한 절차와 식(12)을 토대로 3차방정식의 해를 구한다.

4-3. 3중 오류정정 (31,16)BCH 부호의 병렬복호기

3중 오류정정 (31,16)BCH 부호의 병렬복호기를 설계하면 그림.5과 같다. 그림.5에서 ROM-E와 ROM-V사이에서는 지수형태로 수행되고 그 밖에서는 벡터형태로 계산이 수행된다. DE가 1일때는 switch D는 위로 올라가고 오류가 발생하지 않았을때와 1개 발생하였을때를 나타낸다. DE가 0일때는 switch D는 아래로 내려오며 2중오류나 3중오류가 발생함을 나타낸다.

그림.6는 $c(x)=0$을 전송하여 $r(x)=1+x+x^2$ 을 수신하였을때 오증과 오류위치를 나타내었다

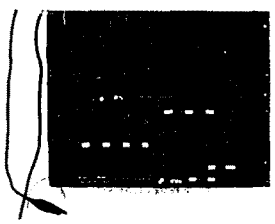

그림.6 $c(x)=0, r(x)=1+x+x^2$ 일때 오증과 오류위치

6. 결 론

본 논문에서는 새로운 복호알고리즘을 이용하여 3중 오류정정 BCH부호의 병렬 복호이론을 설명하고 (31,16)BCH부호의 병렬복호기를 설계하여 장치화하였다.

복호기에 ROM과 PAL을 사용하여 hardware양을 감소시켰으며 또 연산회로를 간소화 하였으며, 부호장이 변함에 따라 복호지연이 일정한 잇점이 있다.

이 복호기의 소자의 지연을 더욱 감소시켜서 고속의 system을 만들려면 LSI로 칩화하면 원하는 system을 얻을 수 있다.

참 고 문 헌

1. 이 만 영, 부호이론, 희중당, 서울, 1984.
2. S.Lin and D.J.Costello, Error Coding fundamentals and applications, Prentice-Hall, Englewood Cliffs, N.J, 1983.
3. R.E.Blahut, Theory and Pratice of Error Control Codes, Addison-wesley Publishing Co., Reading, MA, 1983.
4. F.Polkinghorn, "Decoding of double and triple error correcting Bose-Chaudhuri code, "IEEE Trans. Inform. Theory, vol. IT-12, pp. 480-481, Oct. 1966.
5. A.Yamagish and H.Imai, "A construction method for decoders of BCH codes using ROM's," Trans. IECE Japan, vol.J63-D, pp.1034-1041, Dec.1980.
6. M.Y.Hsiao, "A class of optimal minimum odd-weigyt-column SEC-DED codes, "IBM J.Res.Develop., July.1970.

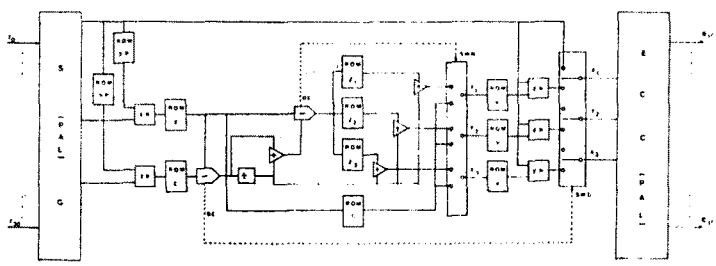

그림. 5 3중 오류정정 (31,16)BCH 부호의 병렬 복호기