DEC-TED (31, 20)BCH 부호의 병렬부호기및 복호기 실현에 관한연구

°염 흥 렬 김 희 도 김 창 수 이 만 영

한 양 대 학 교

(A Study on the parallel codec realization of DEC-TED (31, 20)BCH codes)

Heung Youl Youm Hie Do Kim Chang Soo Kim Man Young Rhee

Hanyang University

* ABSTRACT *

In this paper, a codec for DEC-TED (31, 20)BCH code is realized. Moreover, using ROM and efficient elementary circuits in a decoder, we propose a method of making high-speed decoder.

1. 서 론

BCH 부호는 Computer, 위성통신, Compact disk, 이동전화기와 제어장치등 많은 정보처리시스템에 널리 사용되어 지고 있다. Computer를 예를들면 현재 SEC/DED (single-error-correcting/double-error-detecting)부호는 Computer의 주기억장치에 널리 사용되어지고 있다. 그러나 더 우수하고 더 많은 오류정정 능력을 가지는 부호들이 [6]-[7] 연구되어지고 있다.

본 논문에서는 Polkinghorn[5]의 복호방법과 Yamagish[6] 복호기를 개선하여 DEC-TED(31, 20)BCH 부호의 병렬 codec을 만드는 direct solution방법을 제시하여 장치화 하였다.

이 codec은 병렬로 처리되므로 Computer의 주/보조기억장치에 사용되어질 수 있을 뿐 만아니라 고속을 요하는 디지탈 정보시스템에도 역시 사용되어질 수 있다.

2. DEC-TED (31, 20)BCH 부호의 병렬부호기

DEC-TED BCH 부호의 생성다항식g(x)는

$$g(x) = m_0(x) \cdot m_1(x) \cdot m_3(x) \quad \cdots\cdots\cdots\cdots (1)$$

로 표시된다. 여기서 $m_i(x)$는 $GF(2^5)$의 원소 α에 대한 최소다항식(minimal-polynominal)이다. 식(1)로부터 DEC-TED (31, 20)BCH 부호의 생성다항식 g(x)는

$$g(x)=(1+x)(1+x^2+x^5)(1+x^2+x^3+x^4+x^5) \quad \cdots\cdots (2)$$

와 같이 구해진다. 식(2)로 부터 조직형 생성행렬을 만들기 위하여 생성다항식g(x)로 x^{11+i} 를 나누면

$$x^{11+i} = a_i(x) \cdot g(x) + p_i(x), \quad 0 \le i \le 19$$

$$g_i(x)= p_i(x) + x^{11+i}, \quad 0 \le i \le 19 \quad \cdots\cdots (3)$$

가 된다. 식(3)으로부터 (20x31)행렬을 만들기 위하여 행으로 20개의 $\bar{g}_i$를 배열하면

$$\bar{G} = \begin{bmatrix} \bar{g}_0 \\ \bar{g}_1 \\ \bar{g}_2 \\ \bar{g}_3 \\ \bar{g}_4 \\ \bar{g}_5 \\ \bar{g}_6 \\ \bar{g}_7 \\ \bar{g}_8 \\ \bar{g}_9 \\ \bar{g}_{10} \\ \bar{g}_{11} \\ \bar{g}_{12} \\ \bar{g}_{13} \\ \bar{g}_{14} \\ \bar{g}_{15} \\ \bar{g}_{16} \\ \bar{g}_{17} \\ \bar{g}_{18} \\ \bar{g}_{19} \end{bmatrix} = \begin{bmatrix} 1101110110010000000000000000000 \\ 0110111011001000000000000000000 \\ 0011011101100100000000000000000 \\ 1100011000100010000000000000000 \\ 1011111010000001000000000000000 \\ 0101111101000000100000000000000 \\ 0010111110100000010000000000000 \\ 1100101001000000001000000000000 \\ 0110010100100000000100000000000 \\ 1110111100000000000010000000000 \\ 0111011110000000000001000000000 \\ 0011101111000000000000100000000 \\ 0001110111100000000000010000000 \\ 1101001101100000000000001000000 \\ 1011010000100000000000000100000 \\ 1000011110000000000000000010000 \\ 0100001111000000000000000001000 \\ 0010000111100000000000000000100 \\ 1100110101100000000000000000010 \\ 1011011001000000000000000000001 \end{bmatrix} \quad \cdots (4)$$

가 된다.

부호어$\bar{c}$는

$$\bar{c} = (c_0, c_1, c_2, c_3, \ldots, c_{30}) = (d_0, d_1, d_2, d_3, \ldots, d_{19}) \cdot \bar{G} \quad \ldots\ldots\ldots (5)$$

이다.

식(5)를 이용하여 DEC-TED (31, 20)BCH 부호의 병렬 부호기를 설계하면 그림.1와 같다.

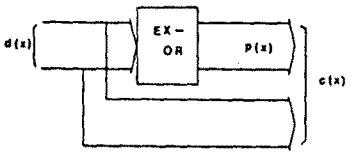

그림.1 DEC-TED (31, 20)BCH 부호의 병렬부호기 회로

3. $GF(2^m)$상의 회로 구성

$GF(2^m)$상의 α를 원시원소(primitive element)라 하면 모든 non-zero원소는 $GF(2^m)$상의 지수표현(exponential-expression)이라는 α멱(power)으로 표시된다.

한편 2^m개 원소는 차수가 m-1인 GF(2)상의 modulo-p(x)의 다항식으로 표현되어질 수 있고, 그 다항식의 계수를 만으로 표현하면 벡터표현 이라고 한다.

예를들어 $GF(2^5)$상의 원시다항식$p(\alpha)=1+\alpha^2+\alpha^5=0$ 일때

$\alpha^{29} = 1 + \alpha^3 = (1\,0\,0\,1\,0) = (1\,0\,1\,1\,1)$

다항식표현 벡터표현 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^0원소는 m-비트로 표현되는 지수표현중 가장높은 값으로 바뀌어야 한다. 그러나 지수표현으로 계산을 수행하면 곱셈과 나눗셈은 쉽게 처리되는데 비하여 덧셈은 복잡해진다. 그러므로 회로를 간단히 하여 위하여 가능한 벡터표현에서 덧셈이 수행하고 지수표현에서 곱셈과 나눗셈을 수행하도록 회로를 설계해야 한다.

3-1. 곱 셈 회 로

원소들 간에 곱셈을 수행하기 위한 곱셈회로는 modulo(2^m-1)의 덧셈 형태로 된다. 이 회로에 대한 block diagram과 symbol이 그림.2에 나타나 있다. 그림.2에서 FA는 m-bits로 된 전 가산기이다. modulo(2^m-1)을 수행하기 위하여 FA-1의 합과 carry가 FA2에서 더해진다. AOD는 입력원소들이 zero원소 인지를 감지하는 회로이며 ZO는 AOD에서 zero원소가 감지되었을때 출력을 zero원소로 보내는 회로이다.

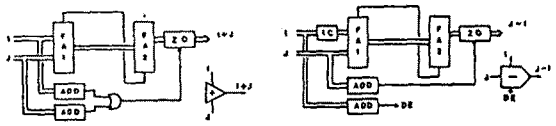

그림.2 곱셈회로 나눗셈회로

3-2. 나눗셈 회로

원소들 간에 나눗셈을 수행하기 위한 나눗셈회로는 지수표현의 분자를 분모로 뺄셈하는 과정이다. 이 회로의 block diagram과 symbol은 그림.2에 나타 나 있다. 여기서 IC는 보수를 취하는 회로이다. DE는 분모가 zero원소일때 불능이므로 이것을 감지하는 회로이다.

3-3. $x^2 + \sigma_{21}x + \sigma_{22} = 0$ 를 풀기 위한 회로

오류위치다항식에서 오류위치를 구하기 위하여 2차 방정식을 풀면 다음과 같다.

$$x^2 + \sigma_{21}x + \sigma_{22} = 0 \quad \ldots\ldots\ldots (6)$$

만약 $\sigma_{21}=0$ 이면 $x = \sigma_{22}^{1/2}$이다. 또 $\sigma_{21} \neq 0$ 이면 $x = \sigma_{21} \cdot y$ 로 치환한다. 그러면 식(6)은

$$y^2 + y + c_i = 0 \quad \ldots\ldots\ldots (7)$$

이 된다. 여기서 $c_i = \sigma_{22}/\sigma_{21}^2$이다. 식(7)의 근들은 단지 c_i의 값에 의하여 결정된다. 그러므로 모든 c_i의 값에 대응하는 근들을 모두 구하여 두면 c_i가 변함에 따라 쉽게 식(7)의 y의 근들인 y_1, y_2를 구할 수 있다. 따라서 식(6)에 대한 근들은 $x_1 = \sigma_{21} \cdot y_1$, $x_2 = \sigma_{21} \cdot y_2$ 가 된다. 식(6)에 대한 회로도는 그림.3에 있다.

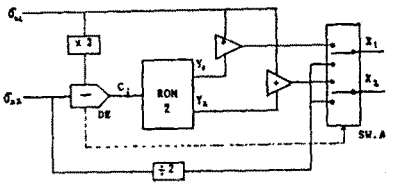

그림.3 $x^2 + \sigma_{21}x + \sigma_{22} = 0$

그림.3의 회로동작을 설명하면 σ_{21}=zero일때 DE는 1이되며 switch A는 아래로 내려오고, σ_{21}≠zero 일때 DE는 0이되어 switch A는위로 올라간다.

4. DEC-TED BCH 부호의 병렬복호기

4-1. 오 증 계 산

수신어$\bar{r}$로 부터 오증$\bar{s}$를 계산하는 것인데 본 논문에서는 DEC-TED BCH 부호이므로 오증$\bar{s}$는

$$\bar{s} = (s_0 , s_1 , s_3) = \bar{r} \cdot \bar{H} \quad \cdots\cdots\cdots (8)$$

이 된다.

이다. 식(8)로 부터 GF(2)상에서의 검사행렬$\bar{H}$은

$$\bar{H} = \left[\begin{array}{cccccccccccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
\hline
1&0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0\\
0&1&0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0\\
0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&0&0&0&1&1\\
0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1\\
0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0\\
\hline
1&0&0&0&0&1&1&0&0&1&0&0&1&1&1&1&1&0&1&1\\
0&0&1&1&1&1&1&0&1&1&1&0&0&0&1&0&1&0&1&1&0\\
0&0&0&0&1&1&0&0&1&0&0&1&1&1&1&1&0&1&1&1&0\\
0&1&1&1&1&1&0&1&1&1&0&0&0&1&0&1&0&1&1&0&1\\
0&0&0&1&0&1&0&1&1&0&1&0&0&0&0&1&1&0&0&1&0
\end{array}\right]$$

$$= \left[\begin{array}{ccccccccccc}
1&1&1&1&1&1&1&1&1&1&1\\
\hline
0&1&1&0&1&1&1&0&1&0\\
0&0&1&1&0&1&1&1&0&1\\
0&1&1&1&0&1&0&1&0&0\\
1&0&1&1&1&0&1&0&1&0\\
1&1&0&1&1&1&0&1&0&1\\
\hline
0&0&0&1&0&1&0&1&1&0\\
1&0&0&0&0&1&1&0&0&1\\
0&0&1&0&1&0&1&1&0&1\\
0&0&0&0&1&1&0&0&1&0\\
0&1&1&1&1&1&1&1&1&1
\end{array}\right] \quad \cdots\cdots (9)$$

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

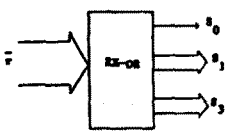

그림.4 DEC-TED BCH 부호의 오증회로$\bar{s}$

4-2. 오류위치 다항식

오증 $\bar{s}$ 로부터 오류위치를 알아내기 위하여 오류위치다항식[1]~[4]를 구해야 된다. 오류위치다항식의 계수는

$$\left[\begin{array}{cccc} s_l & s_{l+1} & \cdots & s_{l+v-1} \\ s_{l+1} & s_{l+2} & \cdots & s_{l+v} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ s_{l+v-1} & s_{l+v} & \cdots & s_{l+2v-2} \end{array}\right] \cdot \left[\begin{array}{c} \sigma_{l+v-1} \\ \sigma_{l+v-2} \\ \cdot \\ \cdot \\ \sigma_l \end{array}\right] = \left[\begin{array}{c} -s_{l+v} \\ -s_{l+v+1} \\ \cdot \\ \cdot \\ -s_{l+2v-1} \end{array}\right] \quad \cdots\cdots\cdots\cdots (10)$$

이다. 식(10)에서 3중 오류를 검출하기 위하여 l = 0로 놓고 determinent 를 구하면

$$\begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} = s_0 (s_1^6 + s_3^2)$$

$$TED = S_0 (S_1^6 + S_3^2) = S_0 (S_1^3 + S_3)^2 \quad \cdots (11)$$

이다. 만약 TED = 0 이면 오류가 2개 이하가 발생했음을 알수있고 TED = 1이면 3개의 오류가 발생했음을 나타낸다. 또 2중 오류를 정정하기 위하여 식(10)에서 l = 1일때 2중 오류정정 BCH 부호의 오류위치다항식의 계수는

$$\begin{bmatrix} s_1 & s_2 \\ s_2 & s_3 \end{bmatrix} \cdot \begin{bmatrix} \sigma_{22} \\ \sigma_{21} \end{bmatrix} = \begin{bmatrix} -s_3 \\ -s_4 \end{bmatrix}$$

$$\begin{bmatrix} \sigma_{22} \\ \sigma_{21} \end{bmatrix} = \begin{bmatrix} s_1 & s_2 \\ s_2 & s_3 \end{bmatrix}^{-1} \cdot \begin{bmatrix} -s_3 \\ -s_4 \end{bmatrix}$$

$$\sigma_{21} = s_1$$

$$\sigma_{22} = (s_1^3 + s_3) / s_1 \quad \cdots\cdots (12)$$

식(12)로 부터 오류위치다항식을 표시하면

$$x^2 + \sigma_{21} x + \sigma_{22} = 0$$

$$x^2 + s_1 x + (s_1^3 + s_3) / s_1 \quad \cdots\cdots (13)$$

식(6)을 이용하여 $s_1 = 0$ 이 일때 $x = s_1 \cdot y$ 로 치환한다. 그러면 식(13)는

$$y^2 + y + (s_1^3 + s_3) / s_1^3 = 0$$

$$y^2 + y + (1 + s_3 / s_1^3) = 0$$

$$y^2 + y + (1 + c_1') = 0 \quad \cdots\cdots (14)$$

이 된다.

4-3. DEC-TED (31, 20)BCH 부호의 병렬 복호기

DEC-TED (31, 20)BCH 복호기를 설계하면 그림.5와 같다.

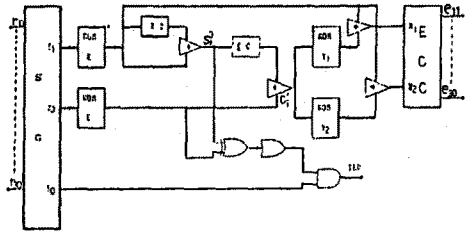

그림.5 DEC-TED (31, 20)BCH 부호의 병렬복호기

그림.5에서 ROM-E는 벡터형태에서 지수형태로 바꿔주는 과정이다. ROM-Y_1, ROM-Y_2는 식(14)에서 c_i 값이 변함에 따라 y_1 , y_2 의 해를 구하는과정이다.

부호및 복호기 장치도는 그림.6에 나타내었다.

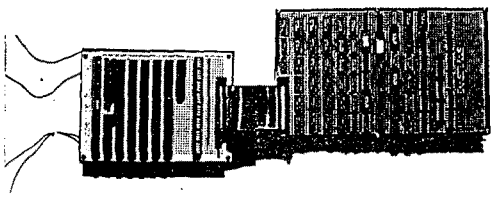

그림.6 부호기및 복호기 장치도

예] $GF(2^5)$상의 원시다항식이 $P(x) = 1 + x^2 + x^5$ 일때 각 비트가 모두 zero인 송신어를 보냈을때 수신단에서는 2개의 오류가 $1 + x$ 의 위치에서 발생한 수신어를 받았다면 오증은 $\bar{s} = \bar{r} \cdot \bar{H}$ 이므로, 수신벡터와 식(9)의 검사행렬 $\bar{H}$을 사용하여 오증$\bar{s}$를 구하면

$$\bar{s} = (s_0 , s_1 , s_3) = (0 , \alpha^{18} , \alpha^{29}) \quad ....(15)$$

이다. 식(15)로 부터 $c_1' = \alpha^6$ 이 되며 $y_1 = \alpha^{13}$, $y_2 = \alpha^{14}$ 이며 이 근으로 부터 $x_i (i=1, 2)$ 값은

$$x_1 = s_1 \cdot y_1 = \alpha^{18} \cdot \alpha^{13} = 1 \quad .....(16)$$

$$x_2 = s_1 \cdot y_2 = \alpha^{18} \cdot \alpha^{14} = x$$

가 된다. 한편 TED를 식(16)로 부터 구하여 보면

$$TED = s_0 (s_1^3 + s_3) = 0 \cdot (\alpha^{23} + \alpha^{29}) = 0 \quad ..(17)$$

이 되며 3중 오류가 발생하지 않음을 알수 있다.

오류가 $1 + x + x^2$ 의 위치에서 발생하였다면

$$\bar{s} = (s_0 , s_1 , s_3) = (1, \alpha^{11} , \alpha^{18})$$

$$TED = s_0 (s_1^3 + s_3) = \alpha^{11} \quad .....(18)$$

이 되며 TED ≠ 0 이다. 그러므로 3중 오류가 발생함을 검출할 수 있다. 앞의 예문으로 오류 발생 시켰을때 결과를 그림으로 나타내 었다.

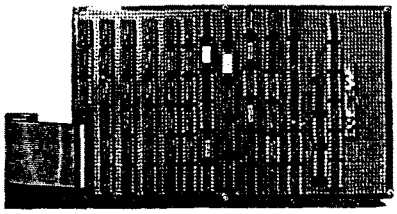

그림. 7 $c(x)=0$ 일때 오류$e(x)=1+x$ 발생

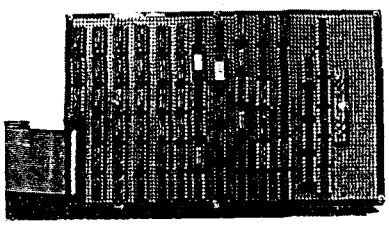

그림. 8 $c(x)=0$ 일때 오류$e(x)=1+x+x^2$ 발생

5. 결 론

본 논문에서는 direct solution복호 알고리즘을 이용하여 DEC-TED (31,20)BCH 부호의 병렬 encoder/decoder를 설계하여 장치화 하였다.

특히 2중 오류정정 (31,21)BCH code에서 검사 비트를 "1" 비트 더 첨가하여 (31,20)BCH code를 만들므로써 2중오류를 정정하고 3중오류을 검출 할 수 있게 하였다.

이 encoder/decoder는 무지연 병렬로 처리 하였으므로 고속의 병렬 digital system에 사용하면 ststem을 고품질화 할수 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. E.R.Berlekamp, Algebraic Coding Theory, McGraw-Hill Book Co., Inc. New York, 1968.
4. R.E.Blahut, Theory and Pratice of Error Control Codes, Addison-wesley Publishing Co., Reading,MA, 1983.
5. F. Polkinghorn, " Decoding of double and triple error correcting Bose-Chaudhuri code," IEEE Trans. Inform. Theory, vol. IT-12, pp.480-481, Oct. 1966.
6. 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.
7. M. Y. Hsiao,"A class of optimal minimum odd-weigyt-column SEC-DED codes," IBM J. Res. Develop., July. 1970.