1988年度 電氣·電子工學 學術大會 論文集 88/7

R-S 복호기의 Systolic 설계에 관한 연구

°박 영만 김 창규 이 만영

한양 대학교

A study on the systolic architecture of R-S decoder

Young Man Park Chang Kyu Kim Man Young Rhee

Hanyang University

ABSTRACT

In this paper, the design of decoder for R-S code using discrete finite-field Fourier transform is presented. An important ingredient of this design is a modified Euclid algorithm for computing the error-locator polynomial. The computation of inverse elements is completely avoided in this modification of Euclid algorithm. This decoder is regular and simple, and naturally suitable for VLSI implementation.

1. 서 론

Reed-Solomon(RS) 부호는 오류 정정 능력이 우수하며 산발 오류와 연집 오류를 모두 정정할수 있는 바이트 오류 정정 부호이므로 각 종 디지탈 통신 시스템의 신뢰성 향상 대책으로써 광범위하게 사용되고 있다.

그러나 복호 과정이 복잡하고 오류 정정 능력이 커짐에 따라 복호기의 회로 규모가 크게 복잡하게 되고 불규칙하게 되어 VLSI화 하는데 많은 어려움이 따르게 된다.

본 논문에서는 이러한 문제점을 줄이기 위하여 유한체의 이산 Fourier 변환을 이용하여 오류 추정 다항식(Error evaluator polynomial)을 구하지 않고 오류를 정정하는 변환 복호법을 사용하였다. 또한, 오류 위치 다항식을 구하기 위하여 종전의 어떠한 알고리즘보다 이해하기 쉽고 규칙적인 Euclid 알고리즘을 이용하였고 쉽게 장치화할수 있도록 하기 위해서 제산이 필요없는 개선된 형태의 Euclid 알고리즘으로 발전시켜 이용하였다.

복호의 전 과정을 Systolic array cell 로 실현하여 부호의 오류 정정 능력이 커질때에는 각 array의 cell의 갯수를 늘리는 것에 의해서 임의의 복호기를 간단히 구성할수 있게 하였다. 따라서 유연한 시스템 구성이 가능하게 되었고 VLSI화 하는데에도 이용할수 있게 되었다.

2. R-S 부호의 변환 복호기 [2]

(N, I)R-S 부호는 2^m개의 심볼로 이루어지는 유한체 $GF(2^m)$의 블럭 계열이며 전송로 상에서 발생한 t 개의 오류를 정정할수 있을때 이 부호는 심볼 단위의 부호장이 $N = 2^m-1$ 이고 정보심볼의 길이는 $I = N-2t$ 이고 검사 심볼의 길이는 $N-I = 2t$ 이며 최소 거리는 $d_{min} = 2t+1$ 의 매개 변수를 가진다.

개선된 형태의 Euclid 알고리즘을 이용한 변환 복호법은 다음 4 단계로 나눌수 있다.

첫 단계는 수신 벡터 $\bar{r}$ 로 부터 오증을 계산하는 것이다.

$$S_j = \sum_{n=0}^{N-1} r_n \alpha^{nj} \quad , \quad 1 \leq j \leq 2t \qquad (1)$$

여기서, 변환 오류 $E_j = S_j$ $(1 \leq j \leq 2t)$ 이다.

두번째 단계는 개선된 Euclid 알고리즘을 이용하여 오류 위치 다항식의 계수를 결정하는 것이다.

셋번째 단계는 오류 위치 다항식의 계수 σ_k 로 부터 변환 오류 E_j 의 나머지 부분을 구하는 것이다.

$$E_{2t+j} + \sum_{k=1}^{t} (-1)^k \sigma_k E_{2t+j-k} = 0 \quad , \quad j \geq 1 \qquad (2)$$

네번째 단계는 $GF(2^m)$상의 변환 오류 E_j 를 역변환하여 오류 e_n 을 구성하는 것이다.

$$e_n = \sum_{j=0}^{N-1} E_j \alpha^{-nj} \quad , \quad 0 \leq n \leq N-1 \qquad (3)$$

그리하여 수신치와 오류치를 더하여 오류가 정정된 부호어를 구하게 된다.

3. (31,25) R-S 부호의 변환 복호기 구성

3.1 오증 (Fourier 변환)

$GF(2^m)$상의 기약 다항식 $p(x)=x^5+x^4+x^2+x+1$ 을 선택하여 3중 오류 정정 (31,25) R-S 부호의 생성 다항식을 아래와 같이 구할수 있다.

$$g(x) = \prod_{i=1}^{6}(x-\alpha^i) = x^6+\alpha^{16}x^5+\alpha^{18}x^4+\alpha^{26}x^3+\alpha^{23}x^2 \\ \alpha^{28}x+\alpha^{21}$$

(31,25) R-S 부호에서 영부호 벡터 $c(x)=0$ 을 전송하여 수신 계열이 $r(x)=\alpha^8x^2+\alpha^2x^5+\alpha x^{10}$ 일때의 복호기를 구성하여 보자. 식(1)에 의하여 오증 S_j 는 다음과 같다.

$$S_j = E_j = (\cdots(((r_{30}\alpha^j+r_{29})\alpha^j+r_{28})\alpha^j+ \\ \cdots)\alpha^j+r_0) \quad , \quad 1 \le j \le 6$$

따라서 오증 S_j 를 계산하는 Systolic array cell 은 그림 1 과 같이 6개의 cell로 구성할수 있다.

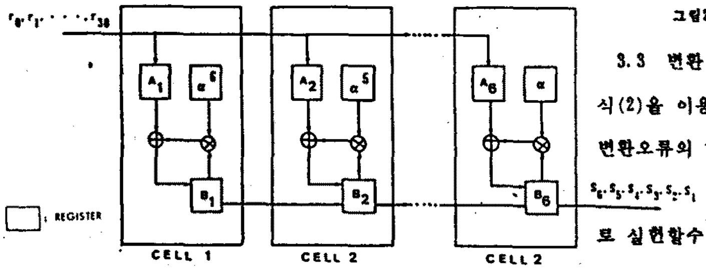


그림1. (31,25) R-S 부호의 오증 계산을 위한 Systolic array

3.2 오류 위치 다항식의 계수 결정

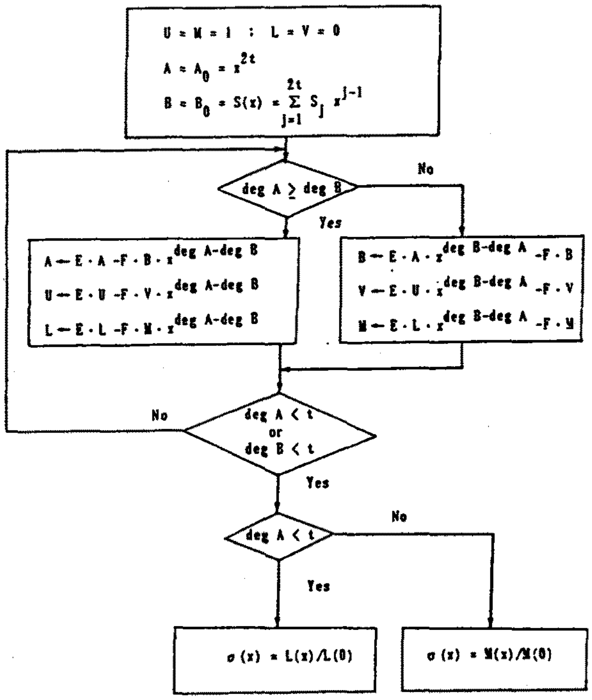
복호의 두번째 단계는 오류 위치 다항식 $\sigma(x)$를 구하는 것으로서 개선된 Euclid 알고리즘을 이용하여 오류 위치 다항식을 구할수 있다. 그림2 는 개선된 Euclid 알고리즘을 이용한 $\sigma(x)$ 계산을 나타낸 것이다.

그리고 이 알고리즘의 과정을 cell로 실현하면 그림3 과 같이 실현할 수 있다.

$L_6(x) = \alpha^{10}x^3+x^2+\alpha^{11}x+\alpha^{27}$ 로 부터 monic한 오류 위치 다항식을 구하기 위해서는 x^3 의 계수 α^{10} 으로 $L_6(x)$를 나눈값이 바로 오류 위치 다항식이 된다.

$$\sigma(x) = L_6(x)/\alpha^{10} = x^3+\alpha^{21}x^2+\alpha x+\alpha^{17}$$

따라서 $\sigma_1 = \alpha^{21}$, $\sigma_2 = \alpha$, $\sigma_3 = \alpha^{17}$ 이다.

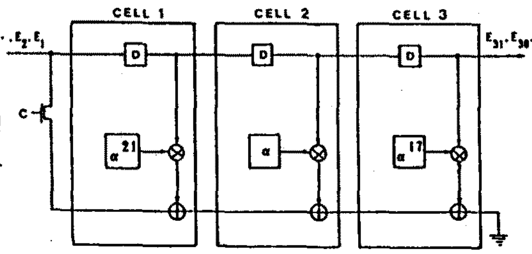


E,F:A,B의 최고차 계수

그림2. 개선된 Euclid 알고리즘을 이용한 $\sigma(x)$ 계산

3.3 변환 오류 구성

식(2)을 이용하면 오증과 오류 위치 다항식의 계수로 부터 변환오류의 나머지를 모두 구할수 있고 그림4 와 같이 cell 로 실현할수 있다.



C=0 : ON AND BEFORE E_6 ENTER CELL1.   C=1 : AFTER E_6 ENTER CELL1.

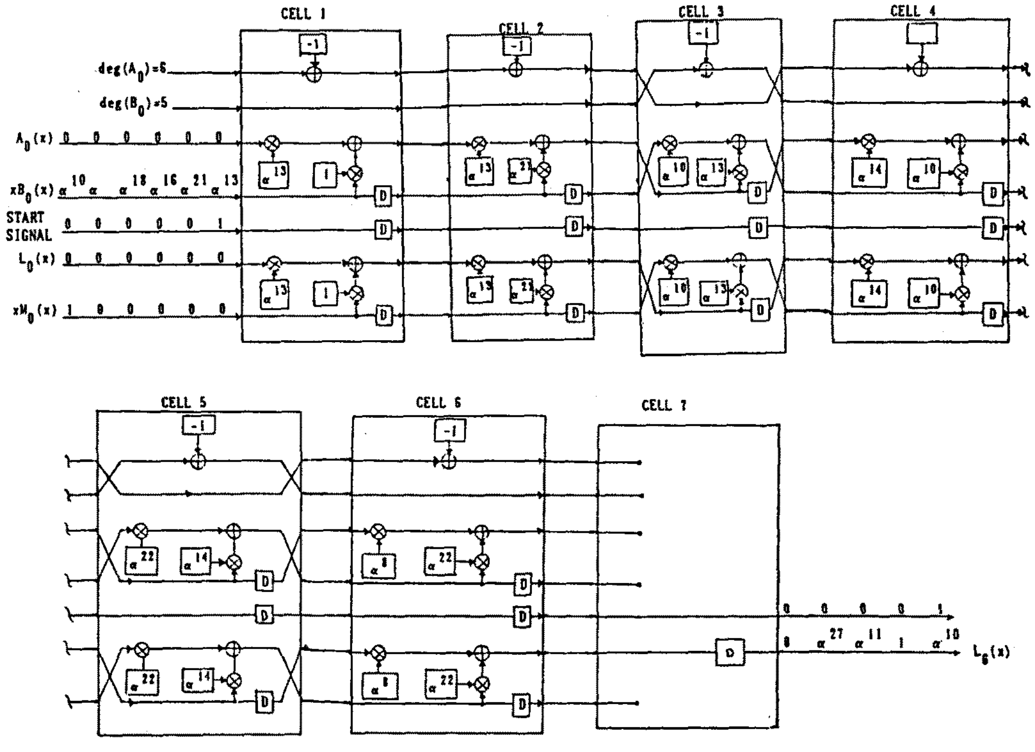
그림4 . 변환 오류의 계산을 위한 Systolic array

3.4 오류 정정 (Fourier 역변환)

식(3)을 이용하면 오류 e 는 변환오류 E 를 역변환하여 다음과 같이 구할수 있다.

$$e_n = E(\alpha^{-n}) \qquad 0 \le n \le 30$$

따라서 오증을 구할때와 같은 방법으로 표현하여 그림5 와 같이 31개의 cell로 실현할수 있다.



D : 4 BIT DELAY REGISTER

그림3. 오류 위치 다항식 계산을 위한 Systolic array

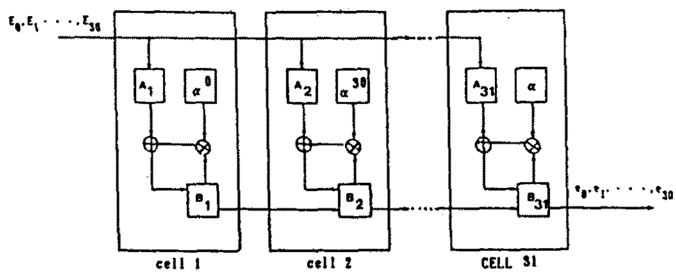


그림5. 오류 계산을 위한 Systolic array

4. 결 론

R-S.부호를 유한체의 이산 Fourier 변환(DFT)를 이용하여 오류를 정정하는 변환 복호법과 오류 위치 다항식의 결정에 있어 역원 계산이 필요없는 개선된 Euclid 알고리즘에 의한 방법을 제시하였다. 이 개선된 Euclid 알고리즘은 이해하기 쉽고 규칙적이다는 장점때문에 이를 VLSI화 할때에는 이 알고리즘이 가장 적합함을 알 수 있었다.

따라서 (31,25) R-S 부호의 변환 복호기를 Systolic array cell 로 실현하여 시스템 구성이 유연하게 되었다.

5. REFERENCE

1. 이 만영, 부호 이론, 희중당, 1984.
2. R.E. Blahut, Theory and Practice of Error Control Codes, Addison-Wesley Publishing co., 1983.
3. 김 상준, 김 창규, 이 만영, R-S 부호의 변환 복호기 설계에 관한 연구, 대한 전자 공학회 추계 종합 학술 대회 논문집, Vol 10, No 1, 1987.
4. R.J. McEliece, The Theory of Information and Coding, Addison-Wesley, 1977.