변형 유클리디안 알고리즘을 이용한 리드 - 솔로몬 디코더의 VLSI 구현

최 광 석, 김 수 원
고려대학교 전자공학과
서울시 성북구 안암동 5-1, #136-701

The VLSI implementation of RS Decoder using the Modified Euclidean Algorithm

GoangSeog Choi, SooWon Kim
School of Electrical Engineering, Korea Univ., Seoul, Korea
e-mail : gschoi@asic.korea.ac.kr

Abstract - This paper presents the VLSI implementation of RS(Reed-Solomon) Decoder using the Modified Euclidean Algorithm(hereafter MEA) for DVD(Digital Versatile Disc) and CD(Compact Disc). The decoder has a capability of correcting 8-error or 16-erasure for DVD and 2-error or 4-erasure for CD. The technique of polynomial evaluation is introduced to realize syndrome calculation and a polynomial expansion circuit is developed to calculate the Forney syndrome polynomial and the erasure locator polynomial. Due to the property of our system with buffer memory, the MEA architecture can have a recursive structure which the number of basic operating cells can be reduced to one. We also proposed five criteria to determine an uncorrectable codeword in using the MEA.

The overall architecture is a simple and regular and has a 4-stage pipelined structure.

1. 서 론

디지탈 시스템의 신뢰성은 재생 신호의 에러 확률과 에러 정정 능력에 달려있다. 그래서 높은 신뢰성을 가진 정보를 얻기 위하여 변조된 원신호에 에러 정정 코드를 부가하는 것이 저장 및 전송장치에 필요하다. 여러가지 에러 정정 코드중에서 리드-솔로몬(이후에는 RS) 코드는 버스트 에러 정정에 뛰어난 능력과 구현 하기가 쉽기 때문에 A/V 시스템에 많이 채택되고 있다. DVD/CD 시스템의 경우 변조된 원신호에 이중으로 에러 정정 코드를 부가한 이중 RS를 채택하고 있다. 이중 RS코드를 디코딩하는데 베르켐프-메시 알고리즘(Berlekamp Massay Algorithm, 이후 BMA)이나 MEA를 이용하는데 본 논문에서는 알고리즘을 이해하기 쉽고 구현도 쉬운 MEA를 이용한다.

MEA의 초기치를 1과 신드롬 다항식으로 놓는 대신에 이레져 위치다항식과 포니 신드롬 다항식으로 잡음으로써 에러 및 이레져를 동시에 정정할 수 있는 에러타 위치 다항식과 에러타 평가다항식을 얻는다.

2. MEA

CD 및 DVD의 (n,k) RS 코드에서, n은 부호어 길이, k는 정보길이, t는 정정할 수 있는 에러의 개수, d는 GF(2^8)상의 최소거리(Minimum Distance)를 나타낸다. 원시 다항식(Primitive Polynomial)은 $x^8 + x^4 + x^3 + x^2 + 1$이며 2^8개 원소를 가진 유한체(Galois Field) GF(2^8)상의 원소를 가지고 부호어를 만든다. 생성다항식(Generator Polynomial) g(x)는 다음과 같다.

$$g(x) = \prod_{i=0}^{d-2} (x - \alpha^i)$$

정정가능한 부호어를 가정한다. 즉, e개 에러와 E개 이레져를 가진 부호어가 2e+E ≤ d-1의 관계를 가정하고 수신부호어(Received Codeword)를 다항식 v(x)로 표현하면 식 (1)과 같다.

$$v(x) = v_{n-1}x^{n-1} + v_{n-2}x^{n-2} + \ldots + v_1x + v_0 \quad (1)$$

신드롬은 v(x)에 g(x)의 근을 대입해 식 (2)와같이 얻고, 여기서 얻은 신드롬을 계수로 하는 신드롬 다항식 S(x)는 식 (3)과 같다.

$$S_{k+1} = v(\alpha^k) = v_{n-1}(\alpha^k)^{n-1} + v_{n-2}(\alpha^k)^{n-2} + \ldots + v_1(\alpha^k) + v_0 \quad (2)$$

$$S(x) = S_{2t}x^{2t-1} + S_{2t-1}x^{2t-2} + \cdots + S_2x + S_1 \quad (3)$$

여기서, k = 0,1,...,2t-1, t는 정정가능한 에러수

길이 n의 이진형태의 이레져 위치정보가 연속적으로 들어온다고 가정하고 이레져 위치 다항식 Λ(x)는 식 (4)와

같다.

$$\Lambda(x) = \Pi\ (x - \alpha^{-i}) = e_{2t}x^{2t} + e_{2t-1}x^{2t-1} + \cdots + e_1x + 1 \quad (4)$$

여기서, α^{-i} 는 $\Lambda(x)$의 근이다.

신드롬 다항식 S(x)와 이레져 위치 다항식 $\Lambda(x)$에서 포니 신드롬 다항식 T(x)는 식 (5)와같이 정의된다.

$$T(x) = S(x)\Lambda(x) \bmod X^{d-1} = T_{2t}x^{2t-1} + T_{2t-1}x^{2t-2} + \cdots + T_2x + T_1 \quad (5)$$

$\Lambda(x)$과 T(x)를 초기치로 하여 MEA를 수행한다. 여기서, $\deg(\Lambda(x)) > \deg(T(x))$인 경우, 에러는 없고 이레져만 존재하므로 에러라 위치다항식 $\sigma(x) = \Lambda(x)$와 에러라 평가다항식 $\omega(x) = T(x)$가 되고, $\deg(\Lambda(x)) \le \deg(T(x))$인 경우 아래와 같은 초기치를 가지고 T(x)와 X^{d-1}에 대해 MEA를 행한다.

$$\mu_0(x)=\Lambda(x),\ R_0(x)=X^{d-1},\ \lambda_0(x)=0\quad Q_0(x)=T(x) \quad (6)$$

$$R_i(x) = [\tau_{i-1}b_{i-1}R_{i-1}(x) + \phi_{i-1}a_{i-1}Q_{i-1}(x)] - x^{[1]}[\tau_{i-1}a_{i-1}Q_{i-1}(x) + \phi_{i-1}b_{i-1}R_{i-1}(x)] \quad (7)$$

$$\lambda_i(x) = [\tau_{i-1}b_{i-1}\lambda_{i-1}(x) + \phi_{i-1}a_{i-1}\mu_{i-1}(x)] - x^{[1]}[\tau_{i-1}a_{i-1}\mu_{i-1}(x) + \phi_{i-1}b_{i-1}\mu_{i-1}(x)] \quad (8)$$

$$Q_i(x) = \tau_{i-1}Q_{i-1}(x) + \phi_{i-1}R_{i-1}(x) \quad (9)$$

$$\mu_i(x) = \tau_{i-1}\mu_{i-1}(x) + \phi_{i-1}\lambda_{i-1}(x) \quad (10)$$

여기서, a_{i-1}와 b_{i-1}는 $R_{i-1}(x)$와 $Q_{i-1}(x)$의 최고차항의 계수들,

$i = 1, \ldots, 2t-1, 2t$

$l = l_{i-1} = \deg(R_{i-1}(x)) - \deg(Q_{i-1}(x))$,

$\tau_{i-1} = 1,\ \phi_{i-1} = 0$ if $l_{i-1} \ge 0$,

$\tau_{i-1} = 0,\ \phi_{i-1} = 1$ if $l_{i-1} < 0$

$\deg(\lambda_i(x)) > \deg(R_i(x))$일 때, 반복은 중단되고 에러라 위치다항식 $\sigma(x) = \lambda_i(x)$와 에러라 평가다항식 $\omega(x) = R_i(x)$가 된다. $\sigma(x)$와 $\omega(x)$는 식 (11)과 식 (12)와 같이 다항식으로 표현된다. $\sigma(x)$를 정규화하여 $\sigma^{nm}(x)$를 얻고 α^{-i} (i = 0, ... ,n-1)에 대해 평가를 한다. 만약 $\sigma(\alpha^{-i}) = 0$ 이면 그 위치의 심벌은 오염된 심벌이다.

$$\sigma(x) = \sigma_{2t}X^{2t} + \sigma_{2t-1}X^{2t-1} + \cdots + \sigma_1x + \sigma_0 \quad (11)$$

$$\omega(x) = \omega_{2t-1}X^{2t-1} + \omega_{2t-2}X^{2t-2} + \cdots + \omega_1x + \omega_0 \quad (12)$$

$$\sigma(x)/\sigma_0 = \sigma_{2t}x^{2t}/\sigma_0 + \ldots + \sigma_1x/\sigma_0 + 1 \quad (13)$$

$$\sigma^{nm}(x) = \sigma^{nm}_{2t}x^{2t} + \cdots + \sigma^{nm}_1x + 1 \quad (14)$$

$$\sigma^{nm}(\alpha^{-i}) = \Sigma^{2t}_i\sigma^{nm}_i(\alpha^{-i})^i + 1 = \Sigma^{2t}_i\sigma^{nm}_i(\alpha^{-i})^j + 1 \quad (15)$$

여기서, j = 0,1,...,n-1이다.

상응하는 에러라 크기를 구하기 위하여 $\omega(x)$과 $\sigma'(x)$를 α^{-i} (i = 0,...,n-1)에 대해 평가 한다. $\sigma'(x)$의 평가는 $\sigma(x)$의 기수 차수항들(Odd Power Terms)의 유한체 합이다.

$$\omega(\alpha^{-i}) = \Sigma^{2t-1}_i\omega_i(\alpha^{-i})^i = \Sigma^{2t-1}_i\omega_i(\alpha^{-i})^j \quad (16)$$

$$Y_j = -\omega(\alpha^{-j}) / \sigma'(\alpha^{-j}) = \omega(\alpha^{-j}) / \sigma_0(\sigma^{nm}_{odd}\sigma(\alpha^{-j})) \quad (17)$$

에러라 위치와 크기가 구해지면 정정된 심벌 v^{corr}_j는 오염된 심벌에서 에러라크기를 빼면 된다.

$$v^{corr}_j = v_j - Y_j$$

3. VLSI 구현

그림.1은 본 논문에서 제안한 버퍼 메모리를 포함한 DVD/CD 겸용 RS 디코더의 전체 블럭도이다.

그림 2는 신드롬 생성 회로이다. 신드롬은 d-1개의 위치에서 길이 n의 다항식을 평가하는 것이다. 신드롬 계산 회로를 구현하기 위해 식(2)는 아래 식 (16)과 같이 반복적인 형태로 표시할 수 있다.

$$S_{k+1} = ((\ldots((v_{n-1}\alpha^k)+v_{n-2})\alpha^k+\ldots+v_1)\alpha^k + v_0 \quad (16)$$

여기서, k = 0,1,...,2t-2,2t-1

v_{n-1}는 첫번째 수신되는 심벌이고, 신드롬 S_{k+1}는 괄호 안에서부터 시작해서 v_i (i = 0,1,...,n-1)가 입력 되면서 점차로 계산된다. 최종적으로 v_0 가 입력되고 난 뒤, d-1개의 위치에서 모든 신드롬이 동시에 계산되어진다.

그림 3은 플래그 메모리에서 읽은 플래그 E_i를 α^k로 생성하는 블럭도이다. CD의 C1 및 DVD의 PI 부호어 정정결과 에러 플래그를 C2 및 PO 부호어 정정에 활용한다. 이 동작을 위해서 C1 및 PI의 에러 플래그를 플래그 메모리에 저장한다. C2 및 PO정정시, 저장된 이진형태의 이레져 플래그를 읽어서 활용하는데 이진형태의 읽는 값이 1이면 에러 위치 의미하는 α^k를 만든다.

α^k를 입력으로 한 이레져 위치 다항식과 포니 신드롬 다항식의 회로구현에는 이 다항식들의 확장이 필요한다. 그리하여, T(x)와 $\Lambda(x)$를 계산하기 위해 다항식 확장회로가 도입되었다. 식 (5)에서, T(x)는 S(x)와 $\Lambda(x)$의 곱이고, 이 의미는 S(x)와 여러개의 $(x - \alpha^{-i})$곱들이다. 이는 S(x)의 선형이동과 S(x)의 모든 계수와 α^{-i}와의 곱의 유한체 덧셈으로 이루어진다. 그림 4는 T(x)를 생성하는 다항식 확장회로를 나타낸다. d-1개의 위치에서 초기치를 신드롬 S_i로 놓고, α^k 시퀀스를 입력시키면 최종적인 포니 신드롬 계수를 얻는다. 그리고 $\Lambda(x)$ 생성 회로는 T(x)와 동일하나 초기치로 S(x) 대신에 1을 두고 다항식 확장을 하면 된다.

MEA를 구현하는 기본 연산 셀은 그림 5과 같다. 기본 셀은 길이 (2t+1)인 다항식을 2t번 반복한다. 고로, 한 셀이 MEA를 수행하면 2t*(2t+1)개의 계산시간을 가진다. 이런경우, DVD의 PO(208,192)부호어 정정시, 16*17=272개의 MEA계산시간을 가짐으로써 208개인 신드롬 계산시간보다 길어서 한 셀로 실시간 처리 하는데 문제가 있어 보인다. 그러나 실제 DVD 응용에서는 버퍼 메모리에서 부호어 정보를 읽어내는데 목조 데이터 저장시간 및 전송 데이터 읽는 시간 때문에 208개의 신드롬 계산시간 및 MEA 계산시간 보다 훨씬 길다. 다시 말하면, 목조된 데이

터의 저장, 정정된 데이터의 읽기 및 정정된 데이터의 디스크램블 및 EDC 체크로 인한 메모리 제어때문에 한 부호어를 읽는데 많은 시간이 소요되므로 신드롬 계산시간이 MEA계산시간 보다 훨씬 길어져서 실시간 처리에 아무런 문제가 되지않는다.

초기치 T(x)와 X^{d+1}에대해 MEA를 수행하기 전에 A (x)의 차수를 T(x)와 비교하여 A (x)가 높으면 알고리즘을 끝내고 낮으면 $\mu_0(x) = A(x)$, $R_0(x) = X^{d+1}$, $\Lambda_0(x) = 0$, $Q_0(x) = T(x)$로 초기치로 놓고 MEA 를 수행한다. 첫 연산후에 $\mu_1, R_1, \Lambda_1, Q_1$를얻고 다시 R_1 와 Λ_1의 차수를 비교한다. 이 때 R_1의 차수가 높거나 같으면 계속해서 MEA를 수행하고, 낮으면 알고리즘을 끝내고 원하는 에라타 위치 다항식과 에라타 평가 다항식을 얻는다.

MEA로 얻어진 σ (x)와 ω (x)는 식 (11)과 (12)로 표현되어진다. σ (x)는 식 (13)과같이 상수항으로 정규화시켜서 새로운 $\sigma^{new}(x)$를 얻고 α^{-j}(j = 0,...,n-1)에 대해 치엔서치(Chien Search)를 한다. 치엔 서치를 하는동안 $\sigma^{new}(\alpha^{-j})=0$인 경우 그곳이 에라타 위치가 된다. 상응하는 에라타 크기는 식 (17)과 같이 ω (α^{-j})와 σ $'(\alpha^{-j})$를 평가하면 된다. 그림 6은 치엔 서치 및 에라타 크기를 구하는데 필요한 σ '(x)를 얻는 블럭도이다. σ '(x)를 평가하는 것은 σ (x)의 기수 차수항을 평가하는 것과 같으므로 σ (x)를 기수차수와 우수차수항으로 나누어 평가한다. 버퍼 메모리에 저장된 오염 심벌을 읽어서 여기서 구해진 에라타에 유한체 덧셈을 행하면 정정된 심벌을 얻을 수 있는데 이를 다시 버퍼 메모리에 저장하면 모든 에러정정 동작은 끝난다.

앞에서 MEA를 적용하기위하여 수신부호어가 정정가능하다고 가정했다. 그러나 실제로 정정 불가능한 수신 부호어가 입력될 수도 있다. BMA에서는 불일치(Discrepency) 파라미터가 정정 불능 부호어를 결정하는데 중요한 역할을 한다. 그러나 MEA에서는 정정불능 부호어를 판단할 방법이 없다. 그래서 본 논문에서는 정정불능의 부호어를 판단하는 5가지 기준을 제시한다. 첫째, 에라타 위치 다항식의 차수가 (2t)보다 작거나 같아야 한다. 둘째, 에라타 위치 다항식의 차수는 에라타 평가 다항식의 차수보다 반드시 높아야 한다. 셋째, σ (x)의 모든 근들은 GF (2^s)상에 존재 해야 한다. 넷째, σ (x)의 근들은 개별적이어야 한다. 다섯째, σ (x)는 0에서 근을 가져서는 안된다. 이 5가지 조건들은 정정불능의 부호어를 판단하는 조건들로 활용하여 회로를 구현하였다.

4. 결 론

변형 유클리디안 알고리즘을 이용하여 DVD/CD에 들어가는 RS 디코더를 구현하였다. 반복적이고 정형적인 성질 때문에 MEA를 선택했고 에러와 이레져를 동시에 정정하기 위하여 α^0와 신드롬 다항식 대신에 이레져 위치 다항식과 모니 신드롬 다항식을 초기치로 사용하여 MEA를 수행했다. 신드롬 계산에 필요한 시간이 길기 때문에 MEA를 수행하는데 필요한 기본 연산 셀 하나로도 실시간 처리를 할 수 있었다. 정정불능의 부호어를 판단하는데 필요한 5가지 기준이 도입되었고 실현되었다.

이 ASIC의 게이트 규모는 40,000정도이고, 0.5 μ mm CMOS 공정을 통해 동작을 검증하였다.

참고 문헌

[1] Howard M. Shao and Irving S. Reed," On the VLSI Design of a Pipeline Reed-Solomon Decoder Using Systolic Arrays", IEEE Trans. on Computers, Vol.37, No. 10, Oct.1988

[2] Howard M. Shao," A VLSI Design of a Pipeline Reed-Solomon Decoder", IEEE Trans. on Computers, Vol.C-34, No.5, May. 1985

[3] Kuang Yung Liu," Architecture for VLSI Design of Reed Solomon Decoders", IEEE Trans. on Computers, Vol.C-33, No.2, Feb. 1984

[4] Richard P. Brent and H.T.Kung," Systolic VLSI Arrays for Polynomial GCD Computation", IEEE Trans. on Computers, Vol.C-33, No.8, Aug. 1984

[5] DVD Specifications for Read-Only Disc

[6] DVD Specifications for Recordable Disc

[7] DVD Specifications for Rewritable

[8] CD Specifications

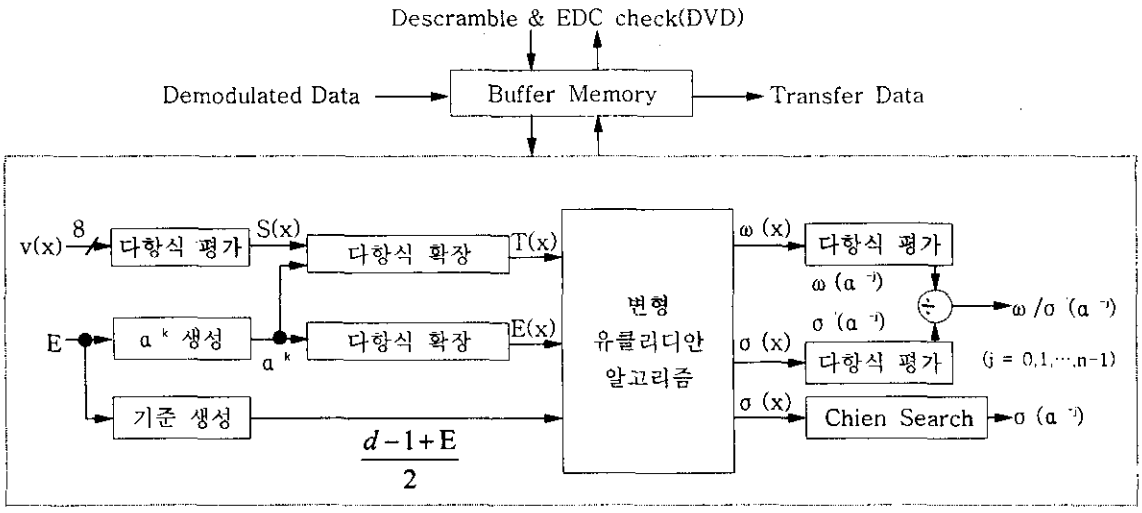

그림. 1 전체 블럭도

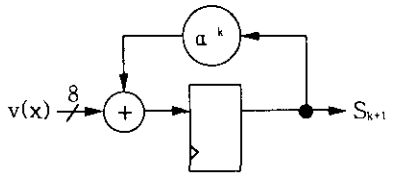

그림. 2 신드롬 생성

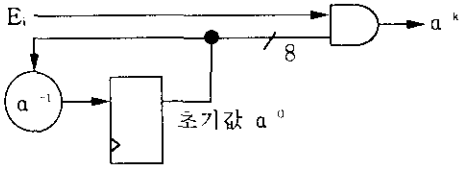

그림. 3 α^k 생성

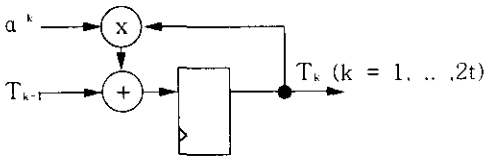

그림. 4 T(x) 생성하는 다항식 확장회로

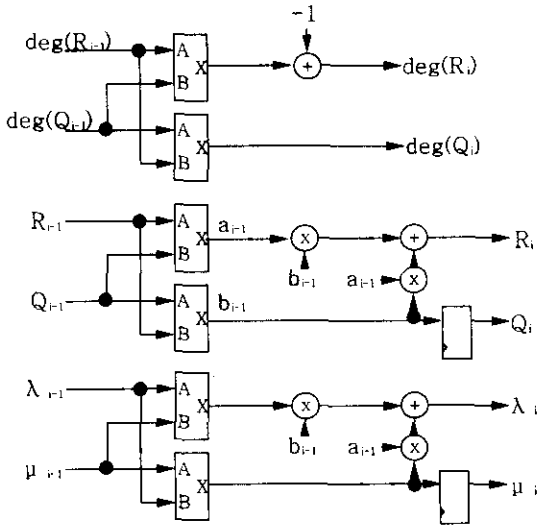

그림. 5 MEA를 수행하는 기본 연산 셀

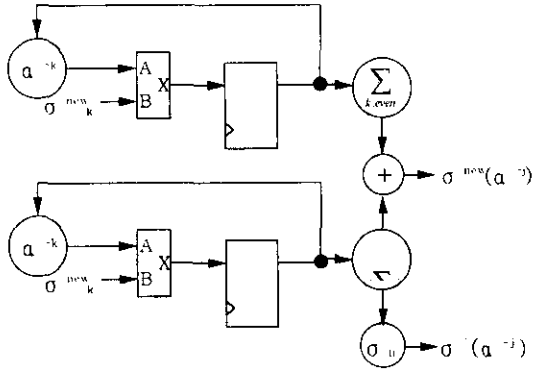

그림. 6 Chien Search