한국산학기술학회논문지
Vol. 11, No. 6 pp. 2202-2206, 2010

FSM을 이용한 수정된 유클리드 알고리즘 설계

강성진[1*]
[1]한국기술교육대학교 정보기술공학부

A Design of Modified Euclidean Algorithm using Finite State Machine

Sung-Jin Kang[1*]
[1]**School of Info. Tech. Engineering, Korea University of Tech. and Educ.**

요 약 본 논문에서는 FSM(finite-state machine)을 이용하여 차수 계산(degree computation)을 하지 않고 수정된 유클리드 알고리즘(modified Euclidean algorithm)을 구현할 수 있는 구조를 제안한다. 제안된 구조는 차수계산이 필요없기 때문에 RS(Reed-Solomon) 복호기의 하드웨어 복잡도를 줄일 수 있고, 고속의 복호기 설계가 가능하게 된다. 제안된 구조를 이용하는 RS(255,239) 복호기를 Verilog HDL로 구현하였고, 기존의 복호기에 비해 게이트 수를 약 13%정도 줄일 수 있다.

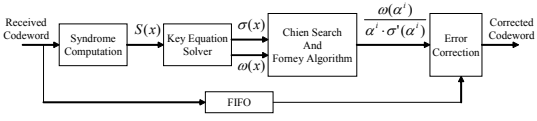
Abstract In this paper, an architecture for modified Euclidean(ME) algorithm is proposed, which is using finite-state machine(FSM) instead of degree computation. Since the proposed architecture does not have degree computation circuits, it is possible to reduce the hardware complexity of RS(Reed-Solomon) decoder, so that a very high-speed RS decoder can be implemented. RS(255,239) decoder with the proposed architecture is implemented using Verilog-HDL and requires about 13% fewer gate counts than conventional one.

Key Words : Reed-Solomon, Modified Euclidean, RS decoder, FSM

1. 서론

RS 부호는 연집 오류에 대하여 우수한 오류 정정 능력을 가지고 있어서, 광/자기 저장매체, 유무선 통신, 방송, 위성 통신 등 많은 통신시스템에서 널리 사용되고 있다. 또한, 최근에는 NAND 플래시 메모리 분야에서도 오류 정정을 하기위한 연구가 활발히 진행되고 있다.

일반적인 RS(n,k,t) 부호에서 n은 전체 부호어(codeword)의 길이(심볼 개수), k는 정보 심볼의 개수를 의미하며, $t = \lfloor (n-k)/2 \rfloor$는 RS 부호의 오류 정정 능력을 나타낸다[1,6]. RS부호에 대한 복호기는 그림 1과 같이 신드롬 연산(syndrome computation), 키 방정식 연산(Key Equation Solver, KES), Chien 탐색, Forney 알고리즘, 오류 정정 블록 및 FIFO(First Input First Output)로 구성된다[2-5]. 여기에서 KES 블록이 오류위치 다항식(error locator polynomial, $\sigma(x)$)과 오류값 다항식(error value polynomial, $\omega(x)$)을 찾기 위해 가장 많은 연산을 필요로 하며, 하드웨어 복잡도가 가장 높다.



[그림 1] RS 복호기의 블록도

RS 복호기에 관한 연구는 대부분 KES 알고리즘에 관한 것이며, 많은 복호 알고리즘과 복호기 구조가 연구되어 왔다[1-8]. 이 중에서 수정된 유클리드(Modified Euclidean, ME) 알고리즘은 하드웨어의 규칙성이 우수하여 쉽게 구현이 가능한 장점을 지니고 있다[4].

ME 알고리즘[2]은 차수 계산과 다항식 연산을 수행하는 processing element(PE) 블록을 $2t$개 사용하여 구현할 수 있

*교신저자 : 강성진(sjkang@kut.ac.kr)
접수일 10년 3월 29일 수정일 10년 04월 26일 게재확정일 10년 06월 18일

으며, 이러한 구조는 하드웨어 규칙성 및 경로 지연(critical path)이 작아서 고속으로 동작하는 RS 복호기를 구현할 수 있다[4,5]. [6]에서는 차수 계산이 필요치 않는 DCME(degree computationless ME)를 제안하였지만, 각 기본 셀(basic cell)내의 feedback되는 부분과 모든 셀에 입력되는 leading coefficient a_i, b_i가 feedback되므로 상대적으로 고속 구현이 어렵게 된다. [7]에서는 DCME 알고리즘의 지연시간과 basic cell을 개선하여 E-DCME 알고리즘을 제안하였다. [5]에서는 [4]의 구조를 개선하여 DCME 알고리즘 구조를 제안하였다. [8]에서는 [4]의 PE 구조를 개선하여 마지막 PE 블록의 출력신호에서 차수 비교 및 MUX(multiplexer)가 필요없는 구조를 제안하였다.

본 논문에서는 [8]에서 제안된 PE 구조의 차수 계산 회로를 FSM(finite-state machine)로 대치하여 하드웨어 복잡도를 줄일 수 있는 구조를 제안한다.

본 논문의 구성은 2장에서 제안된 PE 구조를 설명하고, 3장에서는 제안된 PE 구조를 이용한 RS(255,239,8) 복호기 설계에 대하여 설명한다. 4장에서는 성능평가 결과를 제시하고 5장에서 결론을 맺는다.

2. 제안된 PE 구조

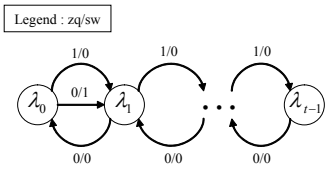
[8]에서는 맨 마지막 PE 블록의 출력 $R_{2t}(x)$와 $Q_{2t}(x)$의 차수를 비교하여 오류위치 다항식 $\sigma(x)$과 오류값 다항식 $\omega(x)$을 결정하게 된다. 이러한 이유는 PE 블록에 입력된 $R_{i-1}(x)$와 $Q_{i-1}(x)$의 차수를 비교하여 다항식 스위칭 여부를 결정한 후에 다항식 연산이 이루어지기 때문에 PE 블록 외부에서 출력 다항식의 차수의 변화를 알 수 없기 때문이다. [4]에서는 각 PE 블록의 출력에서 항상 $\deg(R_i(x)) \geq \deg(Q_i(x))$이 성립하도록, PE 블록의 출력 다항식에 대하여 다항식 스위치가 이루어지는 구조를 제안하였으며, 이를 통해 마지막 PE 블록의 출력으로에서 바로 $\sigma(x)$, $\omega(x)$를 얻을 수 있다.

[4,8]의 PE 구조에서 다항식 차수를 계산하는 블록은 스위치(sw)와 $stop$ 신호를 발생하기 위해서 필요하다. PE 블록에서 $R_{i-1}(x)$, $Q_{i-1}(x)$차수가 같고, $Q_{i-1}(x)$의 leading coefficient가 '0'이 아닌 경우에, 다항식 연산에서 $R_{i-1}(x)$의 최고차항 계수가 제거되어 차수가 1감소하였으므로, $\deg(R_i(x)) < \deg(Q_i(x))$가 되어 다항식 스위치가 일어나게 된다. $stop$ 신호는 PE 블록의 출력 다항식 $R_i(x)$, $Q_i(x)$의 차수가 오류정정 능력 t보다 작을 때 발생하여, 이후의 PE 블록이 동작하지 않도록 한다.

PE 블록에서 sw 신호를 발생하기 위해서는 $R_{i-1}(x)$의 차수와 $Q_{i-1}(x)$의 차수가 같은지를 판단할 수 있다면, 차수 계산을 하지 않아도 됨을 알 수 있다. 따라서, $|\deg(R_i(x)) - \deg(Q_i(x))|$를 관찰함으로써 차수 계산을 하지 않고 sw 신호를 발생시킬 수 있으며, 식 (1)과 같은 상태 변수를 정의 할 수 있다.

$$\Delta_i = \lambda_k = |\deg(R_i(x)) - \deg(Q_i(x))| \quad (1)$$

여기에서, $0 \leq k \leq t-1$이다. 즉, $R_i(x)$와 $Q_i(x)$의 차수 차이는 $t-1$을 초과할 수 없다. [8]의 PE는 $R_{i-1}(x)$의 차수 또는 $Q_{i-1}(x)$의 차수가 1씩 감소하는 구조이므로, 그림 2와 같은 상태도로 표현이 가능하다. 따라서, PE 블록은 그림 2와 같은 상태도를 갖는 FSM을 사용하여 차수 계산없이 sw 신호를 발생할 수 있다. 그림 2에서, zq는 $Q_{i-1}(x)$의 leading coefficient가 '0'일 때 1이고, 그렇치 않으면 0인 신호이다.



[그림 2] λ_k의 상태도

[8]의 PE는 $\deg(R_i(x)) \geq \deg(Q_i(x))$가 성립하므로, $Q_i(x)$의 차수가 t보다 작으면 $stop$ 신호를 발생한다. 식 (1)에 정의된 Δ_i로 부터 $R_i(x)$와 $Q_i(x)$의 차수의 차이를 알 수 있지만, $Q_i(x)$의 차수가 t보다 작은지를 알 수가 없다. 따라서, 각 PE에서 $Q_i(x)$의 변화를 관찰하고 있어야 한다. $Q_i(x)$의 차수가 감소하는 경우는 $Q_{i-1}(x)$의 leading coefficient가 '0'인 경우와 다항식 연산 후에 $\deg(R_i(x)) < \deg(Q_i(x))$가 되어 다항식 스위치가 일어나는 경우이다. 따라서 $Q_i(x)$의 차수가 감소하는 횟수를 카운트하는 상태변수를 식 (2)와 같이 정의할 수 있다. 만약, $\mu_i = 2$라면 $Q_i(x)$의 차수가 2번 감소함을 의미한다.

$$\mu_i = \begin{cases} \mu_{i-1}+1, & \text{if } (zq == 1) \text{ or } (sw == 1) \\ \mu_{i-1}, & otherwise \end{cases} \quad (2)$$

여기에서, $0 \leq \mu_i \leq t-1$이다. 왜냐하면, i번째 PE블록에서 $(zq == 1)$ or $(sw == 1)$이고 $\mu_{i-1} = t-1$이면,

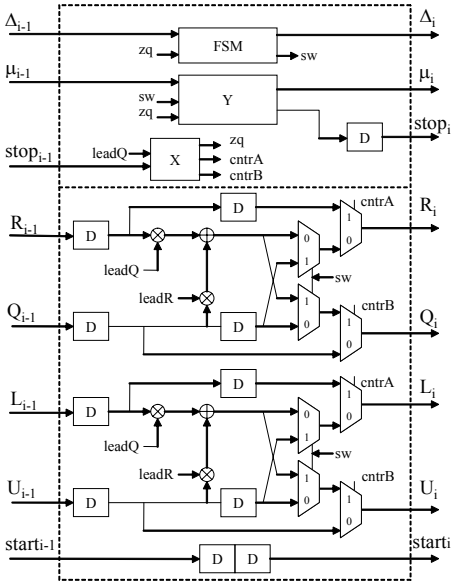
$\mu_i = t$가 되어야 하지만, 이 경우는 $Q_0(x)$의 차수가 $2t-1$에서 t만큼 줄어 $Q_i(x)$의 차수가 $t-1$이 되었음을 의미하기 때문에, $stop$ 신호가 발생하여 $(i+1)$번째 이후의 PE 블록은 동작할 필요가 없으므로, μ_i를 증가시킬 필요가 없기 때문이다. 따라서, $stop_{i-1}=1$이면, $\mu_i = \mu_{i-1}$이다. 이로부터 식 (3)과 같이 $stop_i$신호가 발생됨을 알 수 있다. $stop_i$ 신호는 $stop_{i-1}=0$일 때 식 (3)과 같이 계산되며, $stop_{i-1}=1$이면 $stop_i = stop_{i-1}$이다.

$$stop_i = \begin{cases} 1, \ \text{if}\{\mu_{i-1} == t-1\}\text{and} \\ \qquad \{(\text{zq}==1) \text{ or } (\text{sw}==1)\} \\ 0, \ \text{otherwise} \end{cases} \quad (3)$$

그림 3은 본 논문에서 제안하는 PE 블록의 구조이다. 그림 3에서 FSM은 그림 2의 상태도를 가지며, 'Y' 표시의 박스는 식 (2)와 식 (3)을 통해 μ_i와 $stop_i$신호를 발생하는 회로이다. 그림 3의 'X' 표시의 박스는 제어 신호 zq, $cntrA$, $cntrB$를 생성하는 조합회로이며, leadR, leadQ는 각각 $R_{i-1}(x)$, $Q_{i-1}(x)$의 leading coefficient를 나타낸다. 제어신호 zq는 $\text{leadQ}=0$일 때 '1'이 된다. 그리고, $cntrA$와 $cntrB$는 각각 식 (4), (5)와 같이 계산된다.

$$cntrA = stop_{i-1} \text{ or } zq \quad (4)$$

$$cntrB = stop_{i-1} \text{ or } (not\ zq) \quad (5)$$



[그림 3] 제안된 PE 블록 구조

3. RS(255,239,8) 복호기 설계

RS(255,239,8) 부호의 발생 다항식 $g(x)$는 식 (6)과 같다.

$$\begin{aligned} g(x) &= \prod_{i=1}^{16}(x-\alpha^i) \quad (6) \\ &= x^{16}+118x^{15}+52x^{14}+103x^{13} \\ &\quad +31x^{12}+104x^{11}+126x^{10}+187x^9 \\ &\quad +232x^8+17x^7+56x^6+183x^5 \\ &\quad +49x^4+100x^3+81x^2+44x+79 \end{aligned}$$

RS 부호기는 239byte의 정보 심볼을 입력받아서, 발생다항식 $g(x)$를 이용하여 RS 패리티 16byte를 구한 후에, 정보 심볼 239byte와 패리티 16byte를 합하여 총 255byte의 부호어를 발생시킨다.

RS(n,k,t)부호의 송신된 부호어(codeword) 다항식을 $c(x)$, 수신된 부호어 다항식을 $r(x)$, 에러 다항식을 $e(x)$라 하면, $r(x)$는 식 (7)과 같다.

$$\begin{aligned} r(x) &= c(x)+e(x) \quad (7) \\ &= r_{n-1}x^{n-1}+\cdots+r_1x+r_0 \end{aligned}$$

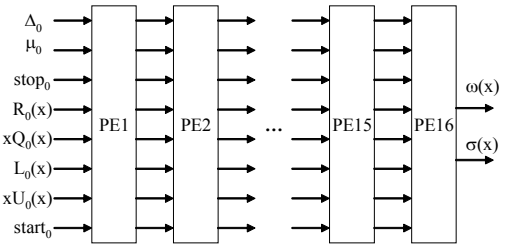
RS 복호기는 수신된 부호어로부터 식 (8)와 같이 신드롬(Syndrome) $S(x)$를 계산한다.

$$S(x) = \sum_{j=0}^{2t-1} S_j x^j, \ where \quad S_j = r(\alpha^j) \quad (8)$$

KES 블록은 신드롬 $S(x)$로부터 식 (9)의 키방정식 연산을 통해 오류위치 다항식 $\sigma(x)$와 오류값 다항식 $\omega(x)$을 계산한다[1-4].

$$S(x)\cdot\sigma(x) = \omega(x) \bmod x^{2t} \quad (9)$$

여기에서, $\sigma(x)$의 차수는 t이고, $\omega(x)$의 차수는 $t-1$이다. RS(255,239,8) 복호기를 위한 KES 블록은 2장에서 제안된 PE 블록을 $2t=16$개 연결하여 구현할 수 있다.



[그림 4] 제안된 PE블록을 이용한 KES 블록도

여기에서, Δ_0는 ME 알고리즘에서 $R_0(x)=x^{2t}$, $Q_0(x)=S(x)$이므로, $\Delta_0=1$이다. 그리고, $\mu_0=0$, $stop_0=0$이며, $start_0$는 [2]에서와 같이 발생된다. 즉, $R_0(x)$의 최고차항을 나타내는 시간동안에만 1이고, 나머지 시간에는 0이다. $L_0(x)=0$, $U_0(x)=1$이다. KES블록의 출력인 오류위치 다항식 $\sigma(x)$와 오류값 다항식 $\omega(x)$는 각각 식 (10), 식 (11)과 같다.

$$\sigma(x)=U_{16}(x) \tag{10}$$

$$\omega(x)=Q_{16}(x) \tag{11}$$

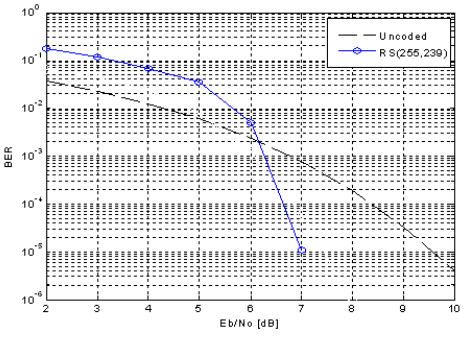
KES 블록에서 $\sigma(x)$와 $\omega(x)$가 계산되면, Chien 탐색과 Forney 알고리즘을 이용하여 식 (12)과 같이 오류 정정이 가능하다[3].

$$cc_{n-i}=\begin{cases} r_{n-i}+\left.\dfrac{\omega(x)}{x\sigma'(x)}\right|_{\alpha^i}, & \text{if } \sigma(\alpha^i)==0 \\ r_{n-i}, & otherwise \end{cases} \tag{12}$$

여기에서, $i=1,\cdots,n$이고, cc_i는 오류가 정정된 i번째 부호어 심볼이다. Chien 탐색과 Forney 알고리즘은 [4]에서와 같이 간단하게 구현될 수 있다.

4. 성능평가

제안된 ME알고리즘 구조의 다양한 오류패턴에 대한 유효성을 검증하기 위해 RS(255,239,8) 부호의 복호기를 C프로그램을 작성하여 시뮬레이션을 수행하였다. 그림 5는 AWGN(Additive White Gaussian Noise)채널에서 BPSK(Binary Phase Shift Keying)변조를 사용했을 때, RS(255,239)부호의 BER성능 곡선이다. RS(255,239)부호는 비트오류확률 10^{-5}에서 약 2.5dB의 부호이득을 가진다.



[그림 5] RS(255,239) 부호의 BER 성능

본 논문에서는 제안된 PE 구조를 이용하는 RS(255,239,8) 복호기를 Verilog HDL를 사용하여 구현하였으며, 삼성 65nm library로 합성하였다. 표 1은 본 논문에서 제안된 구조의 구현 결과를 비교한 것이며, 그림 1의 RS 복호기 중에서 KES 블록만을 비교하였고, 다른 블록은 [4,5]와 동일하다. [7]에서 제안된 DCME 구조는 latency와 gate count 측면에서 가장 우수하지만, 고속 복호에는 적합지 않음을 알 수 있다. 제안된 PE 구조와 유사한 구조를 갖는 [4,5]의 구현 결과와 비교하면, 유사한 동작 주파수를 가지면서 본 논문에서 제안된 구조가 [4]에 비해 약 13%정도 gate count가 줄어드는 것을 알 수 있고, latency도 [4,5]에 비해 현저하게 줄어드는 것을 알 수 있다.

[표 1] RS(255,239,8)복호기 구현 결과

Architecture	proposed	pDCME[5]	ME[4]	DCME[7]
Technology	65nm	0.13um	0.13um	0.18um
KES (gate count)	4,0060	46,200	55,500	18,000
Clock rate(MHz)	660	660	625	200
Latency (clock)	32	80	80	16

5. 결론

본 논문에서는 차수 계산을 하지 않고 FSM을 이용하여 ME 알고리즘을 구현할 수 있는 PE 구조를 제안하였다. 제안된 구조는 차수 계산 회로 대신 FSM을 이용하기 때문에, 고속 복호기 구현이 가능할 뿐 만 아니라 하드웨어 복잡도를 줄일 수 있다. 제안된 구조를 이용하는 KES 블록은 660MHz의 고속 clock에서 동작하며, [5]에 비해 약 13%정도 gate count가 줄어듬을 확인하였다.

참고문헌

[1] S. B. Wicker, Error Control Systems for Digital Communication and Storage, Englewood Cliffs, NJ, Prentice-Hall, 1995.

[2] H. Shao, T. Truong, L. Deutsch, J. Yuen, I. Reed, "A VLSI design of a Pipeline Reed-Solomon Decoder," IEEE Trans. on Computers, Vol.c-34, No.5, pp.393-403, May 1985.

[3] L. Song, M. Yu, M. Shaffer, "10- and 40-Gb/s

Forward Error Correction Devices for Optical Communications," IEEE Journal of Soild-State Circuits, Vol.37, No.11, pp.1565-1573, Nov. 2002.
[4] Hanho Lee, "High-Speed VLSI Architecture for Parallel Reed-Solomon Decoder," IEEE Trans. on VLSI Systems, Vol.11, No.2, pp.288-294, April 2003.
[5] S. Lee, H. Lee, J. Shin, J. Ko, "A High-Speed Pipelined Degree-Computationless Modified Euclidean Algorithm Architecture for Reed-Solomon Decoders," ISCAS, pp. 901-904, May, 2007.
[6] J. H. Baek and M. H. SunWoo, "New degree computationless modified Euclid's algorithm and architecture for Reed-Solomon decoder", IEEE Trans. Very Large Integr. (VLSI) Syst., vol. 14, no. 8, pp 915-920, Aug. 2006.
[7] J. H. Baek and M. H. SunWoo, "Enhanced degree computationless modified Euclid's algorithm for Reed-Solomon decoders," Electronics Letters, vol. 43, no. 3, pp. 175-176, Feb., 2007.
[8] 강성진, "RS(23,17) 리드-솔로몬 복호기 설계," 한국해양정보통신학회논문지, Vol.12, No.12, pp.2286-2292, Dec., 2008.

강 성 진(Sung-Jin Kang) **[정회원]**

- 1994년 8월 : 연세대학교 대학원 전자공학과 (공학석사)
- 1998년 8월 : 연세대학교 대학원 전자공학과 (공학박사)
- 2002년 9월 ~ 2007년 2월 : 전자부품연구원 책임연구원
- 2007년 3월 ~ 현재 : 한국기술교육대학교 정보기술공학부 조교수

<관심분야>
WPAN/WLAN, MODEM SoC