수정된 유클리드 알고리즘을 이용한 RS(255,239) 복호기의 설계

손영수* · 강성진*

*한국기술교육대학교 정보기술공학부

A Design of Modified Euclidean Algorithm for RS(255,239) Decoder

Young-Soo Son* · Sung-Jin Kang*

*Korea University of Technology and Education Infomation Technology Engineering

E-mail : sys8312@kut.ac.kr

요 약

본 논문에서는 수정된 유클리드 알고리즘을 이용하여 RS(255,239) 복호기를 설계하였다. 설계된 복호기는 수정된 유클리드 알고리즘에서 차수를 계산하는 대신, 다항식의 차수를 state machine으로 표현한다. 수정된 유클리드 알고리즘을 이용하여 복잡도를 감소시킬 수 있고, 고속의 리드-솔로몬 복호기를 구현할 수 있다. Xilinx FPGA인 XC4VLX60을 타겟으로 ISE9.1i에서 합성한 결과 동작주파수가 77.4MHz이며, gate count가 39,759로 나타났다.

ABSTRACT

In this paper, We design RS(255,239) decoder with modified Euclidean algorithm, which show polynomic coefficient state machine instead of calculating coefficients of modified Euclidean algorithm. This design can reduce complexity and implement High-speed Read Solomon decoder. Additionally, we have synthesized with Xilinx XC4VLX60. From synthesis, it can operate at clock frequency of 77.4MHz, and gate count is 20,710

키워드

리드-솔로몬 복호기, 수정된 유클리드 알고리즘, KES, error correction

Ⅰ. 서 론

RS(Reed-Solomon) 부호는 우수한 연집 오류 정정 능력으로 인해, 광 저장매체, 유선 및 위성 통신 등 다양한 분야에서 사용되고 있다. 일반적인 RS(n,k) 부호에서 t=(n-k)/2는 RS 부호의 오류 정정 능력을 나타낸다. RS(255,239) 부호는 8바이트 오류정정 능력을 갖는다. [1-3]

일반적인 RS 복호기는 그림 1과 같이 수신된 코드워드(code word)의 오류패턴을 표현하는 신드롬 연산(Syndrome Computation), 오류를 정정하기 위한 키 방정식 연산(KES, key Eqation Solver), Chein 탐색 및 Forney알고리즘, 오류 정정 블록 및 FIFO로 구성된다[3]. 이중에서 오류 위치 다항식(error locator polynomial)과 오류 크기 다항식(error value polynomial)을 찾기 위한 KES 블록이 가장 많은 연산을 필요로 하며, 하드웨어 복잡도가 가장 높다. RS 복호기에 관한 연구는 대부분 키 방정식 연산 알고리즘에 관한 것이며, 많은 복호 알고리즘과 복호기 구조가 연구되어 왔다. 이 중에서 ME(Modified Euclidean) 알고리즘이 하드웨어 규칙성이 우수하여 구현에 적합하다.

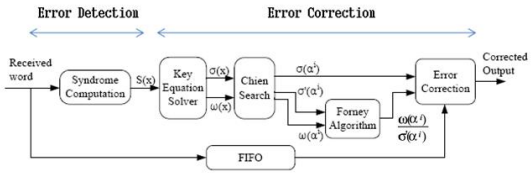

그림 1. 일반적인 RS 복호기의 블록도

이 논문에서는 [4]에서 제안된 파이프라인 ME 알고리즘을 이용하여 RS(255,239) 복호기를 설계하고 성능을 분석한다.

Ⅱ. 제안된 ME 알고리즘 블록 구조

2.1 RS(255,239) 부호

RS(255,239) 부호의 발생 다항식은 다음과 같다.

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

RS(255,239) 부호는 RS 부호기에 239byte가 입력 된 후, 식(2)와 같은 연산을 수행하여 RS 패리티 16byte를 구한다.

$$p(x)=\sum_{i=0}^{15}p_ix^i=x^{16}m(x)\bmod g(x) \quad (2)$$

여기에서 $m(x)$는 정보 다항식(Infomation Polynomial)이며, 아래 식 (3)과 같다.

$$m(x)=\sum_{i=0}^{239}m_ix^i \quad (3)$$

따라서, RS(255,239)부호기의 출력 코드워드(code word)는 식 (4)와 같이 정의된다.

$$c=(c_{255},c_{254},\cdots,c_0) \quad (4)$$
$$=(m_{238},m_{237},\cdots,m_0,p_{15},p_{14},\cdots,p_0)$$

여기서, c_i는 8bit이며, $GF(2^8)$의 원소이다.

2.2 제안된 ME 알고리즘

RS(255,239)의 송신된 부호어(codeword) 다항식을 $c(x)$, 수신된 부호어 다항식을 $r(x)$, 에러 다항식을 $e(x)$라 하면, $r(x)$는 식 (5)와 같다.

$$r(x)=c(x)+e(x) \quad (5)$$
$$=r_{254}x^{254}+r_{253}x^{253}+\cdots+r_1x+r_0$$

복호 알고리즘의 첫 단계는 정정 가능한 오류들을 정정할 수 있는 2t syndrome $S_i, (0\le i\le 2t-1)$를 계산하는 것이다. 신드롬 다항식 $S(x)$는 다음과 같이 정의될 수 있다.

$$S(x)=S_0+S_1x+\cdots+S_{2t-1}x^{2t-1}=\sum_{i=0}^{2t-1}S_ix^i$$

$$S_i=\sum_{j=0}^{n-1}r_i(\alpha^j)^i \quad (6)$$

여기서 α는 원시 다항식(primitive polynomial) $p(x)=x^8+x^4+x^3+x^2+1, t=8$,의 근(root)이고 $GF(2^8)$에서의 원시 원소(primitive element)이다. RS(255,239)코드에서 α^i는 가능한 오류위치를 의미한다.

R S복호기의 KES 블록은 식(7)의 키방정식 연산을 통해 오류위치 다항식 $\sigma(x)$와 오류값 다항식 $\omega(x)$을 계산한다. RS(255,239)부호에서 $\sigma(x)$의 차수는 2t = 16, $\omega(x)$의 차수는 2t-1 = 15가 된다.[2,3]

$$S(x)\cdot\sigma(x)=\omega(x)\bmod x^{2t} \quad (7)$$

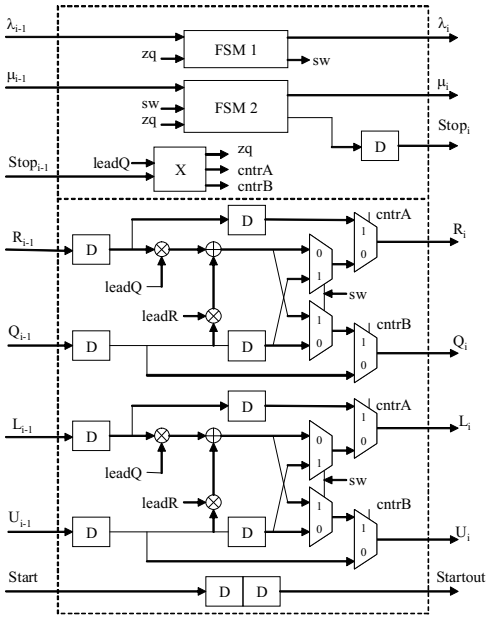

그림 2. 제안된 PE 블록 구조

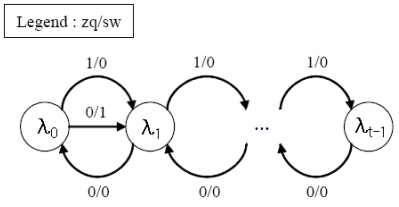

그림 3. λ_i의 상태도

그림 2는 [4]에서 제안된 PE 블록의 구조이다.

그림 2에서 X는 제어신호 zq, cntrA, cntB를 생성하는 조합회로이며, leadR, leadQ는 각각 $R_{i-1}(x)$, $Q_{i-1}(x)$의 leading coefficient를 나타낸다. 제어신호 zq는 leadQ = 0일 때 '1'이 된다. 그리고, cntrA와 cntrB는 각각 식(8)와 식(9)과 같이 계산된다. FSM1과 FSM2는 FSM(Finite State Machine)이며, FSM1은 그림 3과 같고, FSM2는 식 (10)과 같다. FSM1과 FSM2는 $Stop_{i-1} = 1$일 때는 동작하지 않고 이전 상태를 유지한다. $Stop_i$신호는 $Stop_{i-1}$일 때 식(11)과 같이 계산되며, $Stop_{i-1}$이면 $Stop_i = Stop_{i-1}$이다. λ_i와 μ_i의 초기치는 $\lambda_0 = 1, \mu_0 = 0$이다.[4]

$$cntrA = Stop_{i-1} \text{ or } zq \tag{8}$$

$$cntrB = Stop_{i-1} \text{ or } \sim zq \tag{9}$$

$$\mu_i = \begin{cases} \mu_{i-1}+1, \text{ if } (zq=1) \text{ or } (sw=1) \\ \mu_{i-1}, \quad otherwise \end{cases} \tag{10}$$

$$Stop_i = \begin{cases} 1, \text{if} \{\mu_{i-1} = t-1\} \\ \quad \text{and} \{(zq=1) \text{ or } (sw=1)\} \\ 0, otherwise \end{cases} \tag{11}$$

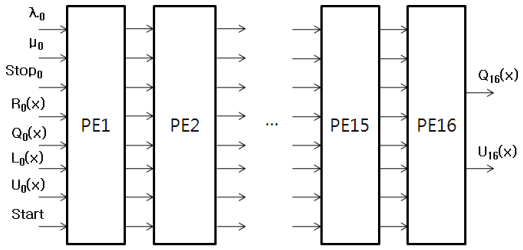

그림 4. 제안된 ME 알고리즘 블록도

그림 4는 그림 2의 PE블로 16개를 이용하여 RS(255,239) 복호기를 위한 블록도이다. PE16의 출력은 식 (12), (13)가 된다.[5]

$$\sigma(x) = U_{16}(x) \tag{12}$$

$$\omega(x) = Q_{16}(x) \tag{13}$$

KES 블록에서 $\sigma(x)$와 $\omega(x)$가 계산되면, Chien search와 Forney 알고리즘을 이용하여 식 (14)과 같이 오류 정정이 가능하다.[2]

$$CC_{n-i} = \begin{cases} r_{n-i} + \dfrac{\omega(x)}{x\sigma'(x)}\Big|_{\alpha^i}, \text{if} \sigma(\alpha^i) = 0 \\ r_{n-i}, \quad otherwise \end{cases} \tag{14}$$

여기에서, $i = 1, \cdots, n$이고, cc_i는 i번째 오류정정된 부호이다.

III. 성능평가

[4]에서 제안된 ME알고리즘 구조의 유효성을 검증하기 위해 RS(255,239) 부호의 복호기를 제안된 구조를 사용하여 C프로그램을 작성하여 시뮬레이션을 수행하였다. 그림 5는 AWGN채널에서 BPSK변조를 사용했을 때, RS(255,239)부호의 BER 성능 곡선이다. RS(255,239)부호는 비트오류확률 10^{-5}에서 약 2.5dB의 부호이득을 가진다.

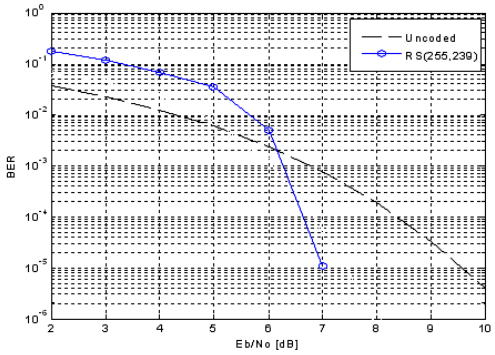

그림 5. RS(255,239) 부호의 BER 성능

그림 6은 구현된 복호기의 fuctional simulation 결과이고, ModelSim을 이용하여 시뮬레이션을 수행하였다. 이 결과로부터 알 수 있듯이, 구현된 복호기는 수신 심볼 255byte가 신드롬 계산 블록에 입력되고 나서, 41clock 뒤에 오류 정정된 정보 심볼이 출력되는 것을 볼 수 있다.

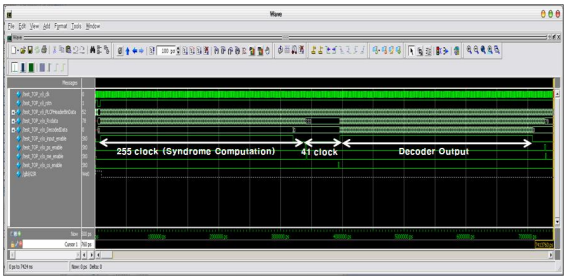

그림 6. ModelSim 시뮬레이션 결과

본 논문에서 설계한 RS(255,239) 복호기는 239byte FIFO를 가지며, KES 블록이 [3]에 비해 gate gount가 약 20% 줄어드는 효과를 가지는 것을 알 수 있다. Xilinx FPGA인 xc4vlx60-10ff668을 타겟으로 하여 ISE9.1i에서 합성한 경우 동작주파수가 약 77.4MHz이며, 그림 7에서 볼수 있듯이 total equivalent gate count는 37,759이다.

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Flip Flops	1,348	53,248	2%	
Number of 4 input LUTs	4,314	53,248	8%	
Logic Distribution				
Number of occupied Slices	2,684	26,624	10%	
Number of Slices containing only related logic	2,684	2,684	100%	
Number of Slices containing unrelated logic	0	2,684	0%	
Total Number of 4 input LUTs	4,322	53,248	8%	
Number used as logic	4,314			
Number used as a route-thru	8			
Number of bonded IOBs	147	448	32%	
Number of BUFG/BUFGCTRLs	1	32	3%	
Number used as BUFGs	1			
Number used as BUFGCTRLs	0			
Total equivalent gate count for design	37,759			
Additional JTAG gate count for IOBs	7,056			

그림 7. Xilix FPGA(XC4VLX60) 합성 결과

Ⅴ. 결 론

본 논문에서는 수정된 유클리드 알고리즘을 이용하여 RS(255,239)부호의 복호기를 설계하였다. 설계된 복호기는 [3]에서 제안된 ME 알고리즘의 processing element를 수정하여 Q(x)에서 항상 오류값 다항식이 출력되고, U(x)가 항상 오류 위치 다항식을 출력하도록 하여 최종 출력단에서 차수 비교를 하지 않는 구조이다.

본 논문에서 설계된 RS(255,239) 복호기는 239byte의 FIFO를 가지며, KES 블록이 [3]에 비해 gate count가 약 20% 줄어드는 효과를 가진다.

참고문헌

[1] 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

[2] 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

[3] 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

[4] 강성진, 김용성, 김선희, 김도훈, 조진웅 "고속 리드-솔로몬 복호기를 위한 수정된 유클리드 알고리즘 구조 개선," 2009한국통신학회 하계종합학술대회,Vol39,No.8, pp.777, June,2009

[5] 강성진, 김한종, "UWB 시스템을 위한 RS(23,17) 복호기 최적 설계," 한국통신학회논문지, Vol.33, No.8, pp.821-828, Aug. 2008