

---

# 수정된 유클리드 알고리즘을 이용한 RS 부호화기/복호화기 설계

박종태\*

## Design of RS Encoder/Decoder using Modified Euclid algorithm

Jong-Tae Park\*

### 요 약

디지털 통신망을 통한 정보 송수신시 전송로 상에서의 잡음으로 인해 데이터 블록에 발생하는 오류는 전체 통신 시스템의 성능 및 전송효율에 지대한 영향을 미친다.

설계된 RS 코드 복호기는 오류 위치 다항식과 오류평가 다항식을 구하기 위해 수정된 유클리드 알고리즘을 적용하였다.

본 논문에서 적용된 설계 구조와 알고리즘 계산 방식은 복호기 설계시 1개의 셀을 사용하여 면적을 최소화하고, 연산을 ROM과 병렬 구조로 구성하였기 때문에 높은 동작주파수에서 고속 동작을 실현 할 수 있을 것이라 기대된다.

본 논문에서 설계된 회로는 ModelSim과 Active-HDL 그리고 Synopsys Tool상에서 설계되었으며, Xilinx Virtex2 XC2V3000에 PNR시 slice 점유율은 28% 시스템 클럭 스피드는 45Mhz의 결과를 얻었다.

### ABSTRACT

The error control of digital transmission system is a very important subject because of the noise effects, which is very sensitive to transmission performance of the digital communication system

It employs a modified Euclid's algorithm to compute the error-location polynomial and error-magnitude polynomial of input data.

The circuit size is reduced by selecting the Modified Euclid's Algorithm with one Euclid Cell of mutual operation. And the operation speed of Decoder is improved by using ROM and parallel structure. The proposed Encoder and Decoder are simulated with ModelSim and Active-HDL and synthesized with Synopsys. We can see that this chip is implemented on Xilinx Virtex2 XC2V3000. A share of slice is 28%. Clock speed of this paper is 45Mhz.

### 키워드

Reed-Solomon, 유클리드 알고리즘, PNR, VLSI

### 1. 서 론

정보사회의 발달과 더불어 통신의 중요성은 급격히 증가하고 있다. 특히 통신에 디지털 시스템의

도입은 이용자의 다양한 요구를 수용할 수 있도록 하였다. 정보 송수신시 전송로 상에서의 잡음으로 인해 데이터 블록에 발생하는 오류는 전체 통신 시스템의 성능 및 전송효율에 지대한 영향을 미친다.

오류정정부호를 통신 시스템에 도입하여 전송시스템의 성능을 향상 시키고자 하는 부호이론에 대한 연구는 1948년 Shannon [1]에 의해 처음으로 제안된 이후 오류 검출 및 정정능력이 우수한 효율적인 오류 검출 및 정정 부호의 발견, 보다 효율적이고 간단한 부호 및 복호 알고리즘의 개발 등에 대하여 지난 40 여 년 동안 집중적으로 수행되어 왔다.[2]

오류 제어를 목적으로 데이터 통신 시스템에서 사용하는 기법으로는 ARQ(automatic repeat request)와 FEC(forward error correction)가 있다.

ARQ는 수신 측에서 오류를 검출하게 되면 정보의 재전송을 송신 측에 요구함으로써 오류 없는 정보를 수신하고자 하는 방식으로 오류의 검출과 재전송을 수행하여 정보의 신뢰도를 높이는 방식이다. FEC는 오류정정부호(error-correction code)를 사용하여 데이터, 음성, 영상신호 등 정보의 전송, 저장, 처리과정에서 발생한 오류를 수신 측에서 직접 정정함으로써 비트오율(bit error rate)이 아주 낮은 고신뢰도의 통신이 가능하게 하는 방식이다.[3]

디지털 통신채널에서 발생하는 오류형태는 크게 산발 오류형태와 연접 오류형태로 나누어진다. 오류정정부호는 크게 블록부호 (block code) 와 길쌈부호 (convolutional code) 로 나눌 수 있다. 블록부호의 일종인 Reed - Soloman 부호 (이하 RS 라 약칭) 는 산발오류 뿐만 아니라 연접오류를 모두 정정할 수 있는 오류 정정부호로서, 특히 오류특성이 연접오류형태인 무선통신, 위성통신, 데이터통신시스템, 자기 디스크 등을 이용한 데이터 저장시스템, 그리고 컴퓨터의 데이터 저장시스템 등에 널리 적용되고 있다.[2,4]

오류정정부호의 디지털 통신망에의 적용은 효율적인 부호 및 복호 알고리즘의 개발, 디지털 전자공학과 VLSI(very large scale integration) 반도체 기술의 비약적 발전 및 이에 따른 가격 하락, 대역폭이 무한대인 광섬유통신의 도입 등의 요인으로 확대되고 있다.

본 논문에서는 신드롬 값으로부터 오류의 위치를 찾는 과정으로서 Modified Euclid 알고리즘을 사용하여 오류위치다항식  $\lambda(x)$ 와 오류 평가 다항식  $\omega(x)$ 를 생성한다.

## II. RS code 이론적 배경

### 1. RS encoder

RS code의 표기는  $(n, k)$  형태로 표현한다.  $n$ 은

parity를 포함한 총 심벌 개수이고,  $k$ 는 parity(16 심벌)를 뺀 실제 data의 심벌 수이다. 이 형태를 에러 정정 능력  $t$ 를 이용하여 표현하면 다음 식처럼 표현 할 수 있다.

$$(n, k) = (2^m - 1, 2^m - 1 - 2t)$$

설계된 RS code가 RS(255, 239)이고, 에러 정정 능력이 8이므로, 다음 식처럼 표현 할 수 있다.

$$RS(255,239) = (2^8 - 1, 2^8 - 1 - 16)$$

설계된 RS code는 RS(255, 239)의 shortened RS code이다. 4가지 형태를 만족하는데 그 형태는 다음과 같다. RS(204, 188), RS(69, 53), RS(39, 23), RS(32, 16)이다. 위의 4가지 형태뿐만 아니라  $(n-m, n-m-16)$ 의 어느 형태도 만족한다. ( $n > m+16$ )

RS coder(encoder/decoder)를 설계하는데 있어 encoder 설계는 RS(255, 239) encoder를 설계하고, 필요한 shortened RS code는 별도로 설계를 할 필요는 없다. 이 유는  $k$ 수(정보 심벌 수)를 조정함으로써 encoder를 자유자재로 조정할 수 있기 때문이다. 그러므로 추가적인 인터페이스는 필요하지 않다.[5][6]

그림 2.1은 rs encoder의 구조이다.

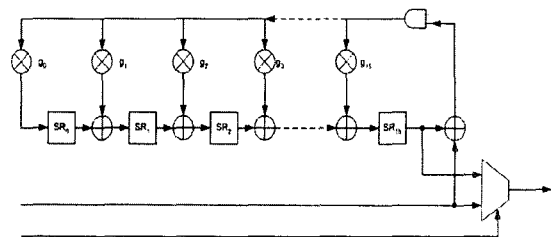


그림 1. RS encoder의 구조  
Fig 1. Architecture of RS encoder

그림 1에서도 알 수 있듯이 GF 곱셈기 16개, XOR 16개, 8bit 레지스터 16개, 기타 MUX 등이 필요하다.

### 2. RS decoder

RS decoder의 일반적인 구조는 그림 2처럼 크게 5부분으로 구성된다.

"Syndrome calculation"은 에러가 포함된 입력 데이터를 계산하여 오증(syndrome)을 생성하는 부분이다. 이 결과 값은 오류위치와 오류 값(크기)을

포함하고 있기 때문에 매우 중요하다. 만약 에러가 없는 데이터가 입력된다면 오증의 결과는 모두 '0'이 될 것이다. "Modified Euclid" 부분은 Euclid 알고리즘을 사용하며, 입력된 오증을 이용 에러 위치 다항식(Error position polynomial)과 에러 크기 다항식(Error size polynomial)을 계산하는 부분이다. "Error polynomial"은 오류 위치와 오류 크기를 결정하여 최종적으로 정확한 에러 위치와 에러 값을 그 다음 블록으로 출력한다. "Correct" 부분은 "Error polynomial"과 "Delay" 블록에서 입력된 데이터를 XOR 하여 에러가 정정된 데이터를 출력한다. "Delay" 블록은 "Error polynomial"부분에서 최종적으로 값을 출력할 때 그와 동시에 제일 처음 입력된 데이터를 저장하여 출력해야한다. 이 블록은 FIFO로 구성되며, 메모리 크기는 "Error polynomial"에서 출력 값이 나올 때까지의 지연시간까지의 데이터를 저장할 수 있는 메모리 크기를 요구한다.[5][6]

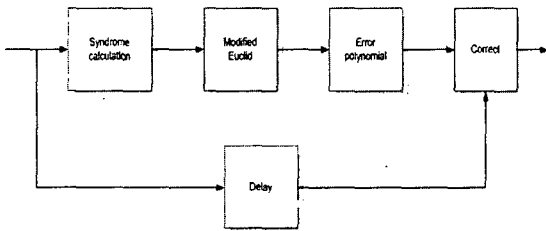


그림 2. RS 디코더의 구조  
Fig 2. Architecture of RS decoder

### III. 제안된 RS code 설계 및 구현

RS 코드의 디코딩 중 오류 위치 및 오류 평가 다항식을 구하는 방법에 대해서는 여러 가지가 있다. Berlekamp-Messy 알고리즘, Peterson-Gorenstien-Zierler 알고리즘, 유한체 Fourier 변환을 이용한 알고리즘, Euclid 알고리즘, Modified Euclid 알고리즘 등이 그것이다. 본 논문에서는 신드롬 값(신드롬 다항식)으로부터 오류의 위치를 찾는 Modified Euclid 알고리즘을 사용하여 오류 위치 다항식  $\lambda(x)$ 와 오류 평가 다항식  $\omega(x)$ 를 생성한다. 수정 유클리드(Modified Euclid)알고리즘을 설명하면 다음과 같다.

두 다항식  $R_0(x) = x^{2t}$ ,  $Q_0(x) = S(x)$ 에 대해 각 다항식의 최고차항의 계수(leading coefficient)가  $a_0, b_0$ 라 할때  $R_0(x)$ 와  $Q_0(x)$ 에

각각 상대방의 최고차항의 계수를 곱하여  $R_i(x)$ 와  $Q_i(x)$ 의 차수를 줄여나가는 방법이다. 표 1은 수정 유클리드 알고리즘을 위한 의 C modeling이다. 표 1의 C로 구현된 Modified Euclid 알고리즘의 진행은 그림 4의 순서 도를 따른다. 그림에서도 알 수 있듯이 구현된 rs decoder는 rs\_mode에 따라 입력 데이터 량이 차이가 있다. 특히 RS(32,16) mode에서는 데이터 심볼수 32개이다. 그러므로, 최대 clock수가 32개가 도달하기 전에 이 유클리드 알고리즘을 끝내고 필요한 데이터를 출력해야 한다.(clock 사용은 반드시 32개 이하이어야 한다.)

표 1. 수정 유클리드 알고리즘  
Table 1. Modified Euclid algorithm

```

void Modified_Euclid(void)
{
    int i;
    init_Euclid();
    do{
        ln=HR()-HQ();
        if(ln>=0)
            { l_oper();}
        else if(ln<0)
            { r_oper }
    }while(HR() >= HL());
    for(i=0; i<=16; i++)
    {
        OM[i]=R[i];
        LA[i]=L[i];}
}
    
```

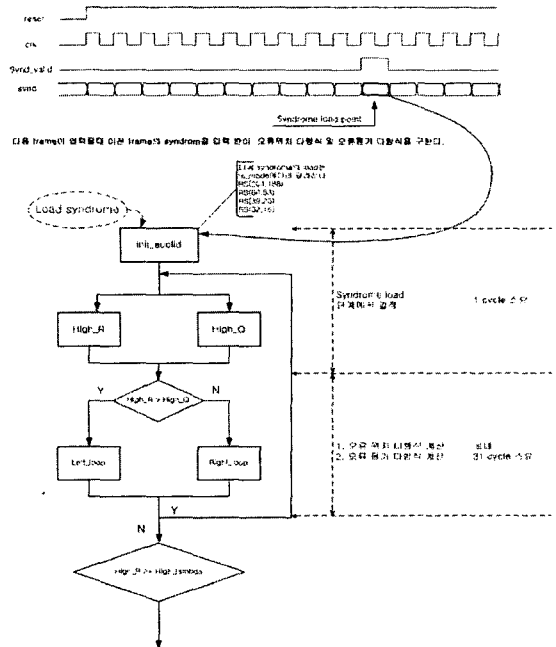


그림 3. 수정 유클리드 알고리즘의 순서도  
Fig 3. Flow-chart of modified euclid algorithm



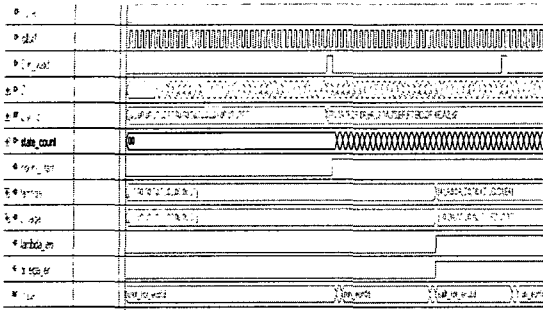


그림 8. euclid\_core block의 시뮬레이션 파형  
Fig 8. Simulation waveform of euclid\_core block

그림 9는 rs\_decoder의 Top 블록을 합성한 그림이다. 왼쪽부터 차례로 rs\_syndrome, rs\_euclid, rs\_chain\_forney, rs\_correct가 위치해 있으며, 아래 하단에는 delay FIFO인 rs\_wait가 위치해 있다.

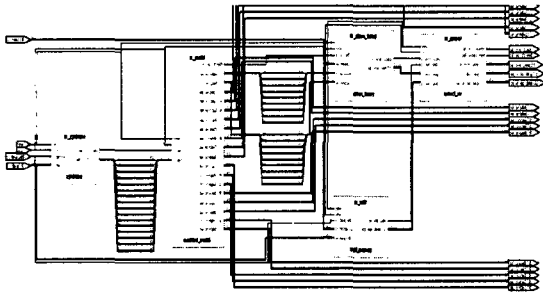


그림 9. rs\_decoder의 합성된 Top 블록  
Fig. 9. Synthesized Top Block of rs\_decoder

구현된 RS encode/decoder의 구현 시 사용한 툴은 알고리즘 디자인을 위해 VC++6.0을 사용하였고, HDL simulation을 위해서는 Mentor사의 Modelsim, Aldec사의 Active-HDL, gate level netlist파일을 얻기 위한 툴은, FPGA 합성 툴인 synplicity사의 synplify를 사용하였다. 그리고, FPGA구현을 위해서는 Xilinx ISE를 사용하였다.

Xilinx Virtex2 XC2V3000에 PNR시 slice 점유율은 28% 시스템 클럭 스피드는 45Mhz의 결과를 얻었다. 전체 블록의 critical path는 Euclid 블록이다.

본 논문에서 제안한 구조와 기존의 논문들과의 면적을 비교한 결과가 표2에 나와 있다. 게이트수는 Reference에 비해 월등히 감소하였고, Reference[3][4] 보다는 약간은 커졌지만 Reference[6]의 클럭스피드는 16Mhz으로, 제안된 본 논문의 클럭스피드보다 월등히 작았다.

표 2. AREA 비교표  
Table 2. AREA comparative table

Hardware block	Reference [3]	Reference [4]	Reference [6]	proposed
Syndrome Calculation	2375	2375	2375	2375
Modified Euclid's Algorithm	20450 (2 block)	18405 (1 block)	11043 (1 block)	12123 (1 block)
Total gate	29250	27205	17208	18021

### V. 결 론

디지털 통신망을 통한 정보 송수신시 전송로 상에서의 잡음으로 인해 데이터 블록에 발생하는 오류는 전체 통신 시스템의 성능 및 전송효율에 지대한 영향을 미친다.

오류정정 부호기 및 복호기는 부호기에서 생성된 부호어가 생성 다항식으로 나누면 '0'이 되는 원리를 이용하여 오류의 위치와 크기를 찾아내고, 그것을 이용하여 오류를 정정하는 방법을 사용한다. 본 논문에서는 8개까지의 심벌 오류 정정이 가능한 RS 복호기를 설계하였다. 복호기는 크게 5개의 블록으로 나누어지는데, 그중 본 논문에서는 오류 위치 다항식과 오류평가 다항식을 구하기 위해 수정된 유클리드 알고리즘을 적용하였다.

본 논문에서 적용된 설계 구조와 알고리즘 계산 방식은 복호기 설계 시 1개의 셀을 사용하여 면적을 최소화하고, 연산을 ROM과 병렬 구조로 구성하였기 때문에 높은 동작주파수에서 고속 동작을 실현 할 수 있을 것이라 기대된다.

### 참고문헌

- [1] Shannon, C.E., "Mathematical Theory of Communication," Bell Syst. Tech. J., vol.27, pp.379-423, 1948.
- [2] Rhee, M.Y., Error Correcting Coding Theory, McGraw-Hill, New York, 1989.
- [3] H. M. Shao, et al., "A VLSI design of a pipeline Reed-Solomon decoder", IEEE

Trans. comput, vol. C-34, no.5, pp.393-402,  
May 1985

- [4] Young-Jin Lim, Moon-ho Lee, "A Minimized Modified Euclid Architecture", VTC 2000-Spring Tokyo IEEE 51st, Vol. 1 2000
- [5] 이문호, 갈루이스필드리드솔로몬비터비터보부호기의설계, 영일(도), 2000
- [6] 조형래, 개선된 순환 유클리드 구조의 Reed Solomon 복호기의 설계, 건국대학교 석사학위논문

### 저자소개

#### 박종태(Jong-Tae Park)



1996년 2월 조선대학교 전자공학과 졸업

1998년 2월 조선대학교 전자공학과 석사졸업

2003년 3월 조선대학교 전자공학과 박사졸업

2003년 3월~2004년 현재 춘해대학 교수

※관심분야 : 멀티미디어 통신, 보안, VLSI