Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

# Design of (255, 239) Reed Solomon Encoder for CCSDS Satellite Communication Standards

**Yong-Suk Cho***

*Division of IT & Securities, U1 University*

## ABSTRACT

Compared with other linear block codes Reed Solomon code has strong error correcting capability with the same coding efficiency's code and can correct not only random errors but also burst errors. Hence it is widely used in deep-space communication systems, digital subscriber loops, wireless systems, data storage systems, digital television transmission systems as well as in memory. (255,239) Reed Solomon code has been selected by the Consultative Committee for Space Data Systems (CCSDS) as a correction coding tool for the forward and backward signals in the communication link of Advance Orbiting Systems (AOS). In this paper, an architecture of (255, 239) Reed Solomon encoder for CCSDS Satellite communication standard is presented. The conventional architecture of Reed Solomon encoder utilizes bit-parallel multiplication to realize Reed Solomon encoding, which needs a great quantity of logic resources. However, it is not well-suited to simplicity of hardware implementation. In order to simplify hardware implementation, a bit-serial multiplication algorithm for the encoding of Reed Solomon codes using polynomial basis over Galois field is presented in this paper. The proposed RS encoder operates in bit-serial form and in polynomial basis of $GF(2^m)$. The resultant bit-serial Reed Solomon encoder requires substantially less complexity in hardware than the conventional bit-parallel Reed Solomon encoder.



**KEYWORDS:** Reed-Solomon encoders, Galois fields, Polynomial Basis, Bit-serial multiplications, Satellite communications

**ARTICLE INFO:** Received 21 September 2017, Revised 12 October 2017, Accepted 13 October 2017.

*Corresponding author is with the Department of IT & Securities, U1 University, 52-70 Yeonamsan-ro Eumbong-myeon Asan-si Chungcheongnam-do KOREA.
*E-mail address*: yscho@u1.ac.kr

## 1. 서 론

데이터의 전송 도중에 발생하는 오류를 정정하기 위한 오류정정부호 중에서 Reed Solomon 부호는 랜덤오류뿐만 아니라 연집오류에도 우수한 오류정정 능력을 가지고 있기 때문에 많은 통신 시스템과 디지털 저장장치에 폭넓게 사용되고 있다[1], [2].

특히 위성통신 시스템에서는 지상과 먼 거리에 위치하고 날씨 변화에 따른 감쇄와 각종 전자기 자극에 노출되기 때문에 데이터 전송의 오류가 발생할 확률이 높다. 따라서 이를 극복하기 위한 한 가지 방법으로 사용되는 것이 랜덤오류와 연집오류에 강한 특성을 가진 Reed Solomon 부호를 사용하는 것이다. Reed Solomon 부호는 보이저 탐사선에 본격적으로 사용된 이래로, 성능을 향상시키면서 우주통신과 위성통신에 꾸준히 사용되어 왔다. 위성통신 표준화 기구인 CCSDS (Consultative Committee for Space Data Systems)에서는 오류정정부호로 Reed Solomon 부호의 사용을 권고하고 있다[3]. 따라서 최근 CCSDS 표준용 Reed Solomon 부호의 구현에 대한 연구들이 발표되고 있다[4-9].

본 논문에서는 CCSDS에서 규정하는 (255, 239) Reed Solomon 부호의 부호기를 설계한다. Reed Solomon 부호기는 유한체 $GF(2^m)$ 상에서 정보다항식(information polynomial)을 생성다항식(generator polynomial)으로 나누는 나눗셈 회로로 구현된다[10]. 따라서 일반적인 Reed Solomon 부호기는 $m$ 비트씩 병렬로 동작되기 때문에 $m$ 과 오류정정능력 $t$ 가 커지면 회로가 복잡해지게 된다[11].

이러한 복잡도를 줄이기 위하여 Berlekamp는 쌍대기저(dual basis)를 이용하여 Reed Solomon 부호기를 직렬화 시킨 비트직렬 Reed Solomon 부호기를 제안하였다[12]. 이 부호기는 직렬로 동작되기 때문에 기존의 병렬로 동작되는 부호기보다 하드웨어 적으로 매우 간단하게 된다. 그러나 Berlekamp의 부호기는 출력이 쌍대기저 표현으로 나타나기 때문에 이를 다항식기저(polynomial basis)로 변환하는 변환 회로가 필요하게 된다[13],[14].

본 논문에서는 덧셈기가 쉬프트 레지스터 외부에 위치하는 다항식 나눗셈 회로와 비트직렬 곱셈기를 이용하여 다항식 기저 상에서 직렬로 동작하는 비트직렬 Reed Solomon 부호기를 설계하고, 이를 CCSDS 시스템 용 (255, 239) Reed Solomon 부호에 적용하여 그 부호기를 설계한다. 설계된 부호기는 기존의 병렬로 동작하는 부호기에 비하여 훨씬 간단한 하드웨어로 구현할 수 있는 장점을 가지고 있다. 또한 설계된 부호기는 다항식 기저에서 동작하므로 Berlekamp가 제안한 쌍대기저 상에서 동작하는 직렬 부호기가 갖는 기저 변환의 단점도 해결하였다.

본 논문의 구성은, 먼저 2.에서 Reed Solomon 부호기의 직렬 부호기를 설계하고, 3.에서는 CCSDS 표준용 (255, 239) Reed Solomon 부호의 직렬 부호기를 설계한다. 그리고 4.에서 결론을 맺는다.

## 2. Reed-Solomon 부호의 직렬 부호기

Reed Solomon 부호를 포함한 순회부호(cyclic codes)의 일반적인 부호화 방법은 정보다항식을 생성다항식으로 나누어 그 나머지를 찾는 것이다. 쉬프트 레지스터(shift register)를 이용하여 다항식 나눗셈 회로를 구성하는 방법으로는 덧셈기를 쉬프트 레지스터 사이에 위치시키는 방법과 덧셈기를 쉬프트 레지스터 외부에 위치시키는 2가지 방법이 있다[15]. 후자의 방법으로 Reed Solomon 부호기를 구성하면 <그림 1>과 같이 된다.

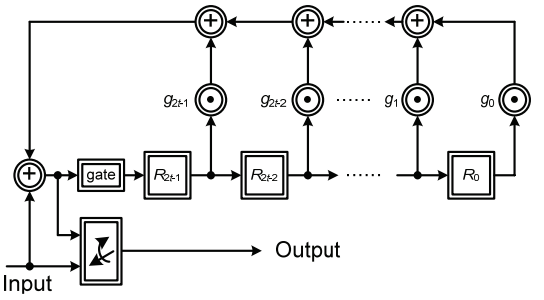


그림 1. Reed Solomon 부호기
Figure 1. Reed Solomon encoder

본 논문에서는 <그림 1>과 같은 Reed Solomon 부호기를 이용하여 직렬로 동작하는 Reed Solomon 부호기를 설계한다.

유한체 $GF(2^m)$ 상의 임의의 한 원소 $A$와 고정된 상수 $C$의 곱을 $Z$라 하면 $Z$는

$$Z = C \cdot A \\ = C \cdot (a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}) \quad (1)$$

가 된다. 여기에서 식 (1)을 다시 정리하면 다음과 같이 쓸 수 있다.

$$Z = (\cdots((Ca_{m-1})\alpha + Ca_{m-2})\alpha + \\ \cdots + Ca_1)\alpha + Ca_0 \quad (2)$$

식 (2)를 살펴보면, 두 원소의 곱 $Z$는 상수 $C$에 $A$의 계수들을 차례로 곱하고 여기에 $\alpha$를 계속 곱해 가면서 더하는 것이다. 따라서 식 (2)를 이용하면 <그림 2>와 같은 비트직렬 상수 곱셈기를 설계할 수 있다.

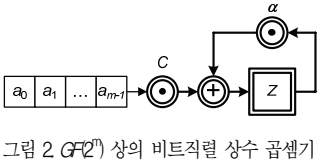


그림 2. $GF(2^m)$ 상의 비트직렬 상수 곱셈기
Figure 2. Bit-serial constant multiplier over $GF(2^m)$

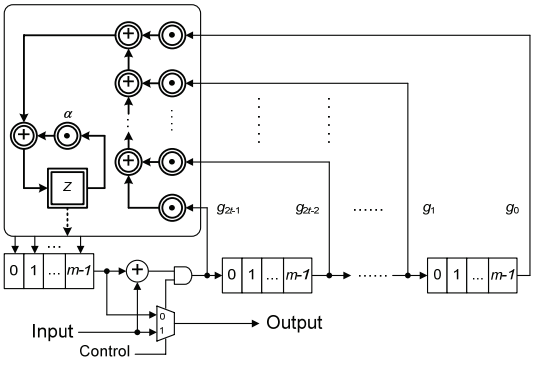


그림 3. 비트직렬 Reed Solomon 부호기
Figure 3. Bit-serial Reed Solomon encoder

<그림 1>과 같은 Reed Solomon 부호기에서 윗부분의 레지스터 출력들과 생성다항식의 계수들을 곱하여 더하는 회로를 <그림 2>와 같은 비트직렬 상수 곱셈기로 대체하면 <그림 3>과 같은 비트직렬 Reed Solomon 부호기를 설계할 수 있다.

## 3. (255, 239) Reed Solomon 부호기

CCSDS에서 규정하는 (255, 239) Reed Solomon 부호는 유한체 $GF(2^8)$ 상에서 오류정정능력 $t$가 8인 부호이다. 이 부호의 생성다항식은 다음과 같다.

$$g(x) = \prod_{j=128-t}^{127+t}(x + \alpha^{11j}) = \sum_{i=0}^{2E} g_i x^i \quad (3)$$

여기에서 유한체 $GF(2^8)$의 원시다항식(primitive polynomial)은 다음과 같다.

$$p(x) = x^8 + x^7 + x^2 + x + 1 \quad (4)$$

생성다항식의 계수 $g_i$는, 식 (4)를 이용하여 식 (3)을 전개하면 <표 1>과 같이 계산할 수 있다.

표 1. (255, 239) Reed Solomon 부호의 생성다항식 계수
Table 1. Coefficients of generator polynomial of (255, 239) Reed Solomon codes

| 계수 | $\alpha^7$ | $\alpha^6$ | $\alpha^5$ | $\alpha^4$ | $\alpha^3$ | $\alpha^2$ | $\alpha^1$ | $\alpha^0$ |
|---|---|---|---|---|---|---|---|---|
| $g_0 = g_{16} = \alpha^0$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| $g_1 = g_{15} = \alpha^{30}$ | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| $g_2 = g_{14} = \alpha^{230}$ | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| $g_3 = g_{13} = \alpha^{49}$ | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| $g_4 = g_{12} = \alpha^{235}$ | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| $g_5 = g_{11} = \alpha^{129}$ | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| $g_6 = g_{10} = \alpha^{81}$ | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| $g_7 = g_9 = \alpha^{76}$ | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| $g_8 = \alpha^{173}$ | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |

식 (3)을 이용하여 <그림 3>과 같은 비트직렬 Reed Solomon 부호기를 설계하면 <그림 4>와 같이 된다. <그림 4>에서 직렬 곱셈기는 다음과 같이 설계할 수 있다. 유한체 $GF(2^8)$의 임의의 한 원소 $U$에 원시원 $\alpha$를 곱하여 정리하면 다음과 같이 된다.

$$\begin{aligned} U \cdot \alpha &= (u_0 + u_1\alpha + u_2\alpha^2 + u_3\alpha^3 \\ &\quad + u_4\alpha^4 + u_5\alpha^5 + u_6\alpha^6 + u_7\alpha^7)\alpha \end{aligned} \tag{5}$$

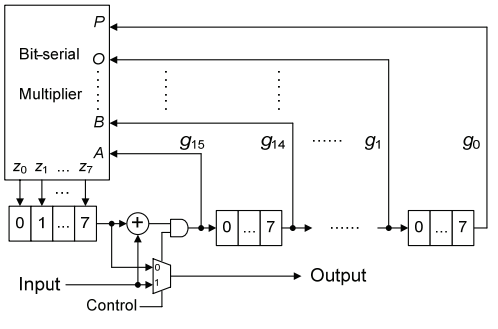


그림 4. (255, 239) Reed Solomon 부호기
Figure 4. (255, 239) Reed Solomon encoder

$$\begin{aligned} &= u_0\alpha + u_1\alpha^2 + u_2\alpha^3 + u_3\alpha^4 + u_4\alpha^5 \\ &\quad + u_5\alpha^6 + u_6\alpha^7 + u_7(\alpha^7 + \alpha^2 + \alpha + 1) \\ &= u_7 + (u_0 + u_7)\alpha + (u_1 + u_7)\alpha^2 + u_2\alpha^3 \\ &\quad + u_3\alpha^4 + u_4\alpha^5 + u_5\alpha^6 + (u_6 + u_7)\alpha^7 \end{aligned}$$

또한 출력 $Z$를 계산하면 다음과 같이 된다.

$$\begin{aligned} Z &= g_{15}A + g_{14}B + g_{13}C + g_{12}D \\ &\quad + g_{11}E + g_{10}F + g_9G + g_8H \\ &\quad + g_7I + g_6J + g_5K + g_4L \\ &\quad + g_3M + g_2N + g_1O + g_0P \end{aligned} \tag{6}$$

$$\begin{aligned} &= (A + O)\alpha^{30} + (B + N)\alpha^{230} \\ &\quad + (C + M)\alpha^{49} + (D + L)\alpha^{235} \\ &\quad + (E + K)\alpha^{129} + (F + J)\alpha^{81} \\ &\quad + (G + I)\alpha^{76} + H\alpha^{173} + P \end{aligned}$$

식(6)을 <표 1>을 이용하여 다시 정리하면 다음과 같이 된다.

$$\begin{aligned} Z &= ((A + O) + (D + L) + (F + J))\alpha^7 \\ &\quad + ((B + N) + (E + K) \\ &\qquad + (G + I) + H)\alpha^6 \\ &\quad + ((A + O) + (B + N) + (E + K) \\ &\qquad + (G + I))\alpha^5 \\ &\quad + ((C + M) + (D + L) + (F + J))\alpha^4 \\ &\quad + ((B + N) + (C + M) + (D + L) \\ &\qquad + (E + K) + (F + J) + H)\alpha^3 \\ &\quad + ((A + O) + (D + L) + (G + I))\alpha^2 \\ &\quad + ((C + M) + (D + L) + H)\alpha \\ &\quad + ((A + O) + (B + N) + (C + M) \\ &\qquad + (D + L) + (G + I) + P) \end{aligned} \tag{7}$$

따라서 <그림 4>에서의 직렬 곱셈기는 식 (7)을 이용하면 <그림 5>와 같이 구성할 수 있다.

<그림 5>의 비트직렬 곱셈기에 소요되는 2입력 XOR 게이트는 34개이다. 그러므로 <그림 3>의 비트직렬 Reed Solomon 부호기에 소요되는 2입력 XOR 게이트는 총 35개가 된다.

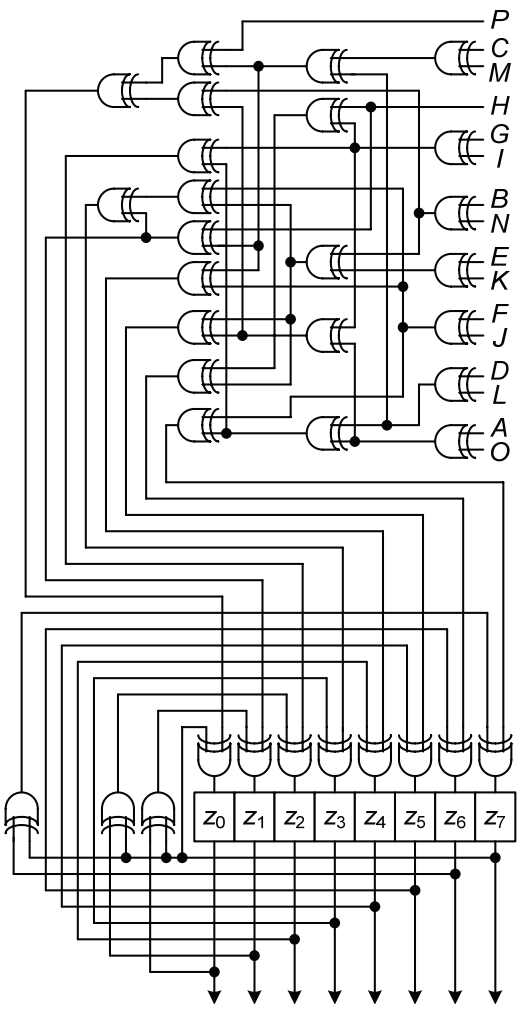


그림 5. 그림 4의 비트직렬 곱셈기

Figure 5. Bit-serial multiplier of Figure 4

<그림 1>과 같은 기존의 병렬로 동작하는 부호기는 $GF(2^8)$ 상의 덧셈기가 16개가 사용되므로 2입력 XOR 게이트로는 16×8=128개가 사용되며, 상수 곱셈기에 약 220개의 2입력 XOR 게이트가 사용되어 총 348개의 2입력 XOR 게이트가 필요하게 된다.

본 논문에서 설계한 부호기는 총 35개의 2입력 XOR 게이트만이 사용되었으므로 기존의 병렬 부호기에 비해 매우 간단한 하드웨어로 구현할 수 있음을 알 수 있다.

## 4. 결 론

본 논문에서는 CCSDS 시스템 용 (255, 239) Reed Solomon 부호기를 설계하였다. 저복잡도의 부호기를 설계하기 위하여, 덧셈기를 쉬프트 레지스터 외부에 위치시키는 다항식 나눗셈 회로와 비트직렬 곱셈기를 사용하여 기존의 병렬로 동작되는 Reed Solomon 부호기를 직렬화 시킨 비트직렬 부호기를 설계하였다. 설계된 비트직렬 부호기는 병렬로 동작하는 기존의 부호기에 비해 하드웨어적으로 매우 간단하며 복잡한 회로연결을 피할 수 있는 장점을 가지고 있다.

또한 설계된 부호기는 다항식 기저에서 동작하므로 쌍대기저 상에서 동작하는 비트직렬 부호기가 갖는 기저변환의 단점을 해결하였으며, 덧셈기를 쉬프트 레지스터 외부에 위치시키는 다항식 나눗셈 회로를 사용함으로써 회로의 구조를 규칙적으로 만들었기 때문에 VLSI 화에도 매우 적합할 것으로 생각된다.

## References

[1] M. Y. Rhee, *Error-correcting coding theory*, Mcgraw-Hill, 1989.

[2] S. Lin, and D. Costello, *Error control coding: Fundamentals and applications*, Pearson Prentice-Hall, 2nd ed. 2004.

[3] CCSDS, *CCSDS 131.0-B-2, CCSDS recommended standard for TM synchronization and channel coding*, The Consultative Committee for Space Data Systems, Technical Report, Aug. 2011.

[4] Dimple Garg, C. P. Sharma, P. Chaurasia, and A. R. Chowdhury, *High throughput FPGA implementation of Reed-Solomon encoder for space data systems,* 2013 Nirma University International Conference on Engineering (NUiCONE) pp. 1-5, 2013.

[5] Y. Zhang, J. Wang, and H. Zhao, *Implementation of RS encoder for CCSDS*, 2014 12th International Conference on Signal Processing (ICSP), pp. 98-101, 2014.

[6] Z. Lin, C. Liu, and L. Liu, *An efficient RS encoder for CCSDS*, 2013 IEEE 4th International Conference on Software Engineering and Service Science pp. 791-794, 2013.

[7] B-R. Wang, L. Liu, L-J. Fu, X-F. Yang, X-Z. Yao, and H-Z. Zhang, *Improvement and implementation of BM algorithm for increasing decoding speed of satellite receivers*, 2013 10th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), pp. 38-41, 2013.

[8] A. Deepa, and C. N. Marimuthu, *Study of Reed Solomon encoders and its Architectures,"* International Journal of Applied Engineering Research, Vol. 9, No. 20, pp. 6855-6862, 2014.

[9] X. Wu, X. Shen, and Z. Zeng, *An improved RS encoding algorithm*, 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 1648-1652, 2012.

[10] W. W. Peterson, and E. J. Weldon, *Error-correcting codes*, MIT Press, Cambridge, Mass., 1972.

[11] S. B. Wicker, and V. K. Bhargava, *Reed-Solomon codes and their applications*, IEEE Press, 1994.

[12] E. R. Berlekamp, *Bit-serial Reed-Solomon encoders*, IEEE Transactions on Information Theory, Vol. 28, pp. 869-874, Nov. 1982.

[13] T. K. Truong, L. J. Deutsch, I. S. Reed, I. S. Hsu, K. Wang, and C. S. Yeh, *The VLSI implementation of a Reed-Solomon encoder using berlekamp's bit-serial multiplier algorithm*, IEEE Transactions on Computers, Vol. 33, No. 10, pp. 06-911, Oct. 1984.

[14] T. S. Hsu, T. K. Truong, and L. J. Deutsch, *A comparison of VLSI architecture of finite field multipliers using dual, normal, or standard bases*, IEEE Transactions on Computers, Vol. 37, No. 6, pp. 735-739, Jun. 1988.

[15] Todd K. Moon, *Error correction coding: mathematical methods and algorithms*, John Wiley & Sons, 2005.

## CCSDS 위성통신 표준용 (255, 239) Reed Solomon 부호기 설계

**조용석**

*유원대학교 정보통신보안학과*

**요 약**

Reed Solomon 부호는 동일한 부호화 효율을 가진 다른 선형 블록부호와 비교할 때, 강력한 오류 정정 능력을 가지고 있으며 산발 오류뿐만 아니라 연집 오류도 정정할 수 있다. 따라서 Reed Solomon 부호는 메모리뿐만 아니라 우주 통신시스템, 디지털 가입자 루프, 무선통신 시스템, 데이터 저장 시스템, 디지털 텔레비전 전송 시스템 등에서도 널리 사용되고 있다. CCSDS (Consultative Committee for Space Data Systems)에서는 AOS (Advance Orbiting Systems)의 통신 링크에서 순방향 및 역방향 신호에 대한 오류 정정 도구로 (255, 239) Reed Solomon 부호를 채택하고

있다. 본 논문에서는 CCSDS 위성 통신 표준용 (255, 239) Reed Solomon 부호의 부호기를 설계한다. 기존의 Reed Solomon 부호기는 비트 병렬 곱셈기를 이용하여 부호기를 구현하기 때문에 소요되는 논리 소자의 양이 많아지게 된다. 그러므로 기존의 부호기는 간단한 하드웨어로 구현하기에는 적당하지 않다. 본 논문에서는 더 적은 하드웨어로 Reed Solomon 부호기를 구현하기 위하여, 유한체 $GF(2^m)$의 다항식 기저에서 비트 직렬 곱셈 알고리즘을 사용한다. 즉 설계된 부호기는 유한체 $GF(2^m)$의 다항식 기저에서 동작하며 비트 직렬 형식으로 동작한다. 설계된 부호기는 기존의 비트 병렬 Reed Solomon 부호기에 비해서 훨씬 간단한 하드웨어로 구현할 수 있다.

**Yong-Suk Cho** received the B.S., M.S., and Ph.D. degree in the Department of Electronic Communication Engineering from Hanyang University in 1986, 1988 and 1998, respectively. From 1989 to 1996, he was a researcher at Korea Telecom. He has been a professor in the Department of IT & Securities at U1 University since 1996. His current research interests include finite field arithmetic, cryptography, and error-control coding.

*E-mail address*: yscho@u1.ac.kr