

다중 QoS 서비스와 시변 채널을 위한 적응형 RS 부호기의 설계

다중 QoS 서비스와 시변 채널을 위한 적응형 RS 부호기의 설계

공민한*, 송문규*, 김응배**, 정찬복**

* 원광대학교 전기전자 및 정보공학부, ** 한국전자통신연구원

전화 : 063-850-6341 / 핸드폰 : 016-614-6341

Design of Adaptive Reed-Solomon Encoder for Multi QoS Services or Time-Varying Channels

Min-Han Kong, Moon-Kyou Song, Eung Bae Kim, Chan Bok Jeong
Dept. of Electrical Electronic and Information Engineering, Wonkwang University
Radio & Broadcasting Technology Lab., ETRI
E-mail : mksong@wonkwang.ac.kr

Abstract

Reed-Solomon(RS) code is the most powerful burst error correcting code. In this paper, the architecture for the adaptive RS encoder adaptable for multi QoS requirements or time-varying channel environments has been designed. In the adaptive RS code, the message length k and the error correction capability t are allowed to be variable so that the block length n is also variable. We proposed the architecture of the adaptive RS encoder by designing the optimal structure of Galois fields multiplier with comparison of fixed multiplier and variable multiplier. The proposed architecture is implemented in VHDL and verified with the simulation tool.

I. 서론

최근 정보의 양과 종류가 다양해짐에 따라 멀티미디어 자료와 같은 실시간 데이터 전송에 대한 수요가 증가하고 있다. 이러한 현상은 무선에서도 나타나고 있으며, 기존의 이동 통신 서비스 역시 데이터 서비스형

태로의 서비스 변환이 이루어지고 있다. 그러나 무선의 경우 기존의 우선망에 비해 제한된 대역폭을 가지며, 채널에서 발생하는 에러에 의해 데이터의 손실률도 높아진다. 따라서, 무선 환경에서의 고속 데이터 전송에서는 이론에 가까운 대역폭의 효율적인 사용이 요구되며, 높은 데이터 손실에 대처할 수 있는 효과적이고 적응성을 갖는 에러정정 기법이 요구된다. 또한 기존의 고정형 에러정정 기법은 채널 환경에서 최악조건 특성을 기준으로 원하는 성능을 얻기 위한 원리로 설계되므로, 다중 접속에서의 다중 QoS(Quality of Service)를 위한 개별성을 보장받지 못하고 있다[1],[2].

다중 QoS의 보장을 위해 IMT-2000 시스템에서는 Turbo Code를 표준으로 채택하였으나, QoS의 증가에 따른 복호 지연이 필수적으로 수반된다. 이에 반해 채널 적응형 RS Code의 경우 Code Rate의 변화와 에러정정 능력(t)의 변화로 요구 QoS와 무관하게 일정한 복호속도를 보일 수 있으며, 다양한 통신 응용에 따른 coding 기법 변화에 대하여 하드웨어의 변화 없이 적용할 수 있다.

본 논문은 채널 적응형 RS 부호기에서 가장 많은 면적을 차지하는 갈로아 필드(Galois field) 곱셈기를 상수 곱셈기 및 변수 곱셈기 방식으로 각각 구현하고 비교를 통하여 복잡도 및 성능을 개선할 수 있는 구조를 제시한다. 또한 시변하는 채널의 특성에 따라서 예

러정정 능력($t=1\sim 10$)과 한 프레임을 구성하는 코드 워드의 길이를 가변으로 설정할 수 있는 채널 적응형 RS 부호기의 효율적인 구조를 제시하고, 이를 시뮬레이션을 통하여 검증한다.

II. 적응형 RS 부호기

2.1 갈로아 필드 곱셈기

$2t$ 개의 패리티 심볼 계산에 요구되는 갈로아 필드 곱셈기는 최근까지 연구되었으며, 특히 VLSI로 구현하기 쉬운 3가지 형태의 곱셈기가 제안되었으며, 각각 다음과 같은 특징을 가지고 있다[3].

- 1) Dual basis 곱셈기 : basis 변환부를 제외하면 요구 칩 면적이 가장 적으며, 필드의 차수가 증가할수록 타 방식보다 유리해진다.
- 2) Normal basis 곱셈기 : 역원, 제곱, 지수 연산을 수행할 때 매우 효과적이다. 필드의 차수가 증가할수록 칩 면적이 가장 증가한다.
- 3) Standard basis 곱셈기 : basis 변환이 불필요하여 임의의 입출력 시스템에 적용이 가능하고, 디자인 복잡도가 낮고, 단순하고, 규칙적이고, 모듈화가 유리하기 때문에 다양한 응용에 확장이 용이하다.

이상의 방식을 위한 systolic array 곱셈기가 제안되었으며, 각 systolic array 곱셈기는 기본 셀을 제시하고 이를 통해서 연산을 수행한다. 그러나 이러한 systolic array 곱셈기의 경우 한 셀에서 계산된 값들이 다른 셀로 전이를 통해 연산되므로, 계산 결과의 출력에 $3m$ 주기의 지연을 갖게 된다.

따라서 본 논문에서는 Standard basis 곱셈기 원리를 적용하여 갈로아 필드 내의 심볼을 취하여 직접 연산하는 방식으로 상수 곱셈기 및 변수 곱셈기를 구현하였다. 변수 곱셈기의 계산과정은 $A(x)$ 와 $B(x)$ 를 $GF(2^m)$ 의 원소라 하고 $P(x)$ 를 원시다항식이라 할 때 $C(x) = A(x)B(x) \bmod G(x)$ 는 다음과 같이 계산된다.

$$A(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_1x + a_0$$

$$B(x) = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \dots + b_1x + b_0$$

$$G(x) = x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_1x + a_0$$

$$\begin{aligned} C(x) &= A(x)B(x) \bmod P(x) \\ &= b_0A(x) + b_1[A(x)x \bmod G(x)] + \dots \\ &\quad + b_{m-1}[A(x)^{m-1} \bmod G(x)] \end{aligned}$$

표 1에 각 곱셈기의 소요 게이트 수 및 지연시간을 나타내었다.

표 1. 각 곱셈기의 비교

종류	게이트 수	지연시간
상수 곱셈기	88	8.2ns
변수 곱셈기	500	11.9ns

2.2 부호기의 설계

RS 부호들을 정의하기 위한 심볼들은 갈로아 필드 상에서 취해지게 되며, 갈로아 필드를 구성하기 위한 원시 다항식은 식 (1)과 같고, 부호화에 필요한 생성자 다항식은 식 (2)와 같다.

$$p(x) = x^8 + x^4 + x^3 + x^2 + 1 \quad (1)$$

$$g(x) = \prod_{i=0}^{2t-1} (x - \alpha^{i+b}) \quad (2)$$

길이가 k 인 메시지 다항식은 $k-1$ 차의 형태로 표현되며, 부호 다항식은 메시지 다항식과 생성자 다항식의 곱으로 쉽게 얻을 수 있으나, 조직 부호어를 얻기 위해 식 (3), (4)를 이용한다.

$$c(x) = x^{n-k}m(x) + d(x) \quad (3)$$

$$d(x) = x^{n-k}m(x) \bmod g(x) \quad (4)$$

상수 곱셈기를 사용할 경우 생성자 다항식의 계수(곱셈기의 승수 값)는 가변 t 값과 레지스터의 단 수에 따라서 총 110개가 사용되어야 하지만, 이 중에서 20개의 상수 곱셈기는 중복되므로 총 90개의 상수 곱셈기를 구현하면 된다. 이 중에서 중복 사용되는 상수 곱셈기의 구조는 그림 1에 보였다. 예러정정 능력 t 값의 결정에 의해 각 곱셈기 출력에 대한 enable 신호가 생성되고 이 enable 신호에 의해 곱셈 결과 값의 출력 여부가 결정된다.

다중 QoS 서비스와 시변 채널을 위한 적응형 RS 부호기의 설계

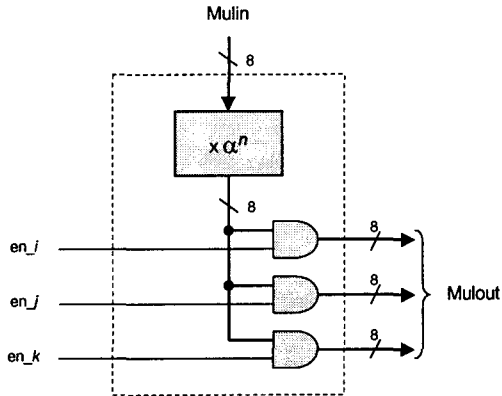


그림 1 중복 사용되는 상수 곱셈기의 구조

변수 곱셈기를 사용할 경우 곱셈기는 총 20개의 곱셈기가 사용된다. 각 변수 곱셈기의 구조는 그림 2에 나타나 있다. 각각의 승수 값은 상수 곱셈기와 마찬가지로 t 값에 의해 생성되는 enable 신호에 의해 결정된다.

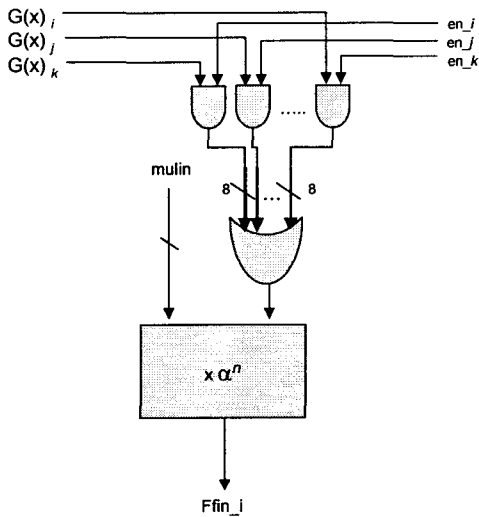


그림 2 변수 곱셈기의 구조

제안하는 채널 적응형 부호기의 전반적인 블록도는 그림 3과 같다. 에러정정 능력 t 의 가변에 따라 decoder에 의해 제어신호 enable이 생성되며, 한 프레임 구성하는 코드워드의 가변을 위해 최초의 메시지

심볼이 들어오면 inc가 high가 되고, 마지막 메시지 심볼이 들어오면 inc는 low가 된다. 이를 이용하여 메시지 또한 각각의지 블록을 가변으로 할 수 있다. 최초의 메시지 심볼은 그대로 출력됨과 동시에 곱셈기 뱅크를 통해 계산된 나머지 값들이 매 클럭마다 갱신되어 레지스터에 저장된다. 마지막 메시지가 입력된 후 곱셈기 뱅크의 입력은 0이 되고, 계산된 패리티 심볼이 매 클럭마다 출력된다. 한 프레임의 코드워드가 출력된 후에 각 레지스터 값은 0이 되므로 연속된 메시지의 입력에 따른 리셋을 요하지 않는다.

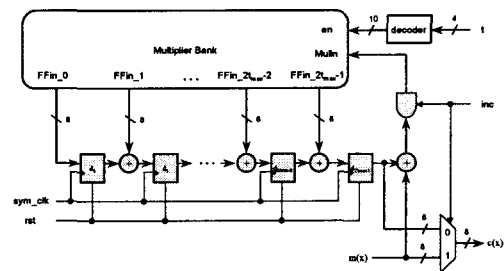


그림 3. RS 부호기의 구성도

표 2에 상수 곱셈기 및 변수 곱셈기를 사용하여 곱셈기 뱅크를 구현하고, 이에 따른 부호기 전체의 게이트 수와 속도를 비교하였다.

표 2. 부호기의 비교

곱셈기 뱅크	게이트 수	속도
상수 곱셈기	21300	51.3Msps
변수 곱셈기	13650	50Msps

표 2에 나타난 것처럼 변수 곱셈기를 이용하여 곱셈기 뱅크를 구현한 부호기가 적응형에 보다 적합하다는 것을 알 수 있다. 상수 곱셈기의 경우 곱셈기 하나의 게이트 수 및 속도는 빠르지만, 적응형 부호기에서 요구되는 곱셈기 수가 매우 많고, 각각의 곱셈기를 간소화할 수 없는 것이 원인으로 사료된다.

2.3 설계된 부호기의 검증

설계된 부호기의 동작은 기능적 동작 검증을 위해 C

언어로 구현되었으며, 임의의 메시지 신호에 대하여 에러정정 능력의 변화에 따른 패리티 심볼 값을 확인하였다. 본 연구에서는 구현을 위해 VHDL 시뮬레이터를 이용하여 시뮬레이션을 수행하여, C로 구현된 검증 프로그램 데이터와 비교하였다. 타이밍 시뮬레이션 결과 본 논문에서 설계된 적응형 RS 부호기는 최고 50Msps(symbol per second)의 입력 데이터를 부호화할 수 있으며, 시뮬레이션 결과는 그림 4와 같다.

III. 결론

본 논문에서는 고속의 데이터 통신에서 요구하는 효율적인 대역폭의 사용과 채널 환경에 적응성을 가지는 에러정정 기법 및 다중접속에서의 다중 QoS의 보장을 위해 채널 적응성을 가지는 RS 부호기를 설계하고 검증하였다. 또한 패리티 심볼 계산에 필요한 갈로아 필드 곱셈기 뱅크가 차지하는 면적이 크므로, 상수 곱셈기 및 변수 곱셈기로 구현하고 비교하여 효율적인 구조를 제시하였다.

본 논문은 앞으로 설계될 채널 적응형 RS 부호기 설계를 위한 기초 자료로 사용될 것이다.

참고문헌

- [1] M. A. Hasan, V. K. Bhargava, "Architecture for a low complexity rate-adaptive Reed-Solomon encoder", *IEEE Trans. Computers*, Vol. 44, No. 7, pp. 938~942, 1988.
- [2] S. J. Li, K.F. Pan, J. S. Yuan, A. J. Vigil, Al. Berg, "adaptive Reed-Solomon Coding for Wireless ATM communication", *Southeastcon 2000. Proceedings of the IEEE*, pp. 27~30, 2000.
- [3] Chin-Liang Wang, Jung-Lung Lin, "Systolic array implementation of multipliers for finite fields $GF(2^m)$ ", *IEEE Trans. Circuit and System*, Vol. 38, pp. 796~800. No.7, 1991.
- [4] P. A. Scott, S. E. Tavares, L. E. Peppard, "A fast VLSI multiplier for $GF(2^m)$ ", *IEEE Trans. Computers*, Vol. SAC-4, pp. 62~66, 1986.
- [5] C. S. Yeh, Irving S. Reed, T. K. Truong, "Systolic multipliers for finite fields $GF(2^m)$ ", *IEEE Trans. Computers*, Vol. C-33, No. 4, pp. 357~360, 1984.

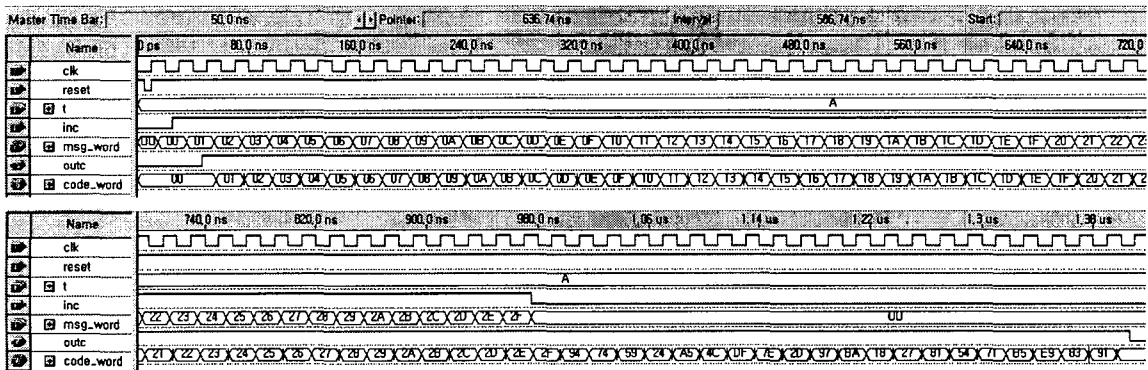


그림 4 구현된 적응형 RS 부호기의 시뮬레이션 과정