

RS 부호를 위한 저면적 신드롬 연산기

김현규¹, 이영주², 유호영¹

¹충남대학교, ²포항공대

전화: (042)821-6585, E-mail: hyyoo@cnu.ac.kr

Area-Optimized Syndrome Calculation for ReedSolomon Decoder

Hyeonkyu Kim¹, Youngjoo Lee², Hoyoung Yoo¹,

¹Chungnam National University, ²Pohang University of Science and Technology

요약

본 논문에서는 ReedSolomon 복호기를 위한 효율적인 신드롬 연산기 구조를 제안한다. 공통 표현식 공유 기법은 반복적으로 표현되는 식을 하나의 하드웨어로 구현하고 이를 공유하여 사용함으로써 하드웨어 복잡도를 낮추는 방법이다. 신드롬과 관련된 모든 연산을 단일 행렬 곱으로 표현하고, 행렬 곱에서 사용되는 공통 표현식에 대한 하드웨어를 공유하여 하드웨어 복잡도를 향상 시킨다. 기존의 공통 표현식 공유 기법 대비 검색 범위를 최대한으로 확장시킴으로써 최소의 하드웨어 리소스를 이용하여 동일한 연산을 진행한다. 130 nm CMOS 공정을 이용하여 구현하여 실험을 진행하였으며, RS 부호를 위한 병렬 신드롬 연산기 구조에 대하여 제안하는 구조가 기존 하드웨어 대비 50% 정도의 복잡도를 가진다.

Abstract

In this paper an efficient structure to compute syndromes is proposed for Reed-Solomon decoders. The proposed method formulates all the computations relevant to syndromes as a matrix multiplication so as to enlarge the search area for common sub-expressions. The hardware resources are drastically reduced by sharing common sub-expressions and eliminating finite-field adders. Syndrome calculation blocks for various RS codes are synthesized with a 0.13μm CMOS technology, and experimental results show that the proposed method reduces the hardware complexity of parallel syndrome calculation by approximately 50% compared to the conventional structure.

Keywords: ReedSolomon 부호, 오류 정정 부호, 신드롬 계산, 최적화 알고리즘.

I. 서론

다양한 오류 정정 부호 중 ReedSolomon (RS) 부호는 집단 오류와 랜덤 오류 모두에 강점을 보이며, 다양한 통신 시스템과 저장 매체에 가장 널리 사용되는 산술 오류 정정 부호 중에 하나이다 [1]. 부호 길이 n , 메시지 길이 k , 오류 정정 능력 t 를 가지는 RS (n, k, t) 부호의 복호기 하드웨어는 일반적으로 4 단 구조로 구성이 되어 있다. 1) 신드롬 연산 블록 (SC: syndrome calculation), 2) 키-방정식 풀이 블록, (KES: key-equation solving), 3) 오류 위치 검색 블록 (EPS: Error-position), 4)

오류 크기 결정 블록 (EME: Error-magnitude evaluation). 특히 Chein 알고리즘과 Forney 알고리즘이 EPS 와 EME 블록을 위하여 널리 사용된다. 하드웨어 복잡도를 낮추기 위하여 Folding 알고리즘과 공통 표현식 공유 기법이 Chien 알고리즘과 Forney 알고리즘에 적용되어 왔다. 신드롬 연산 블록은 상대적으로 낮은 복잡도 때문에 복잡도가 낮은 것으로 간주되어 왔지만, 신드롬 블록을 제외하고 적용된 다양한 최적화 기법으로 인하여 전체의 1/4 에 해당하는 복잡도를 갖게 되었다. 본 논문에서는 RS 복호기의 신드롬 연산 블록에 대한 복잡도 최적화 기법에 대하여 기술한다.

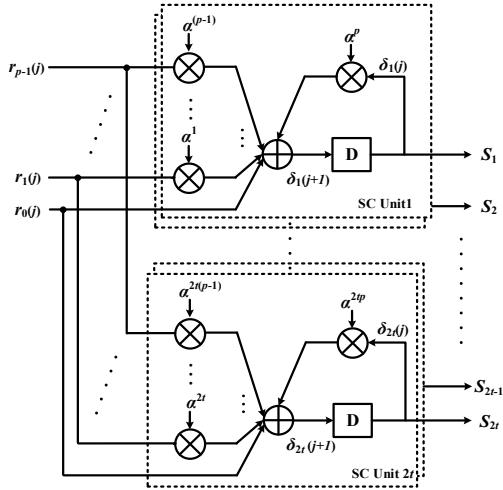


그림 1. 병렬화 계수 p 를 가지는 신드롬 연산기.

II. 본론

병렬화 계수 p 를 가지는 신드롬 연산기의 경우 그림 1과 같이 p 개의 입력을 갖는 신드롬 유닛이 $2t$ 개 존재한다. 신드롬 유닛은 p 개의 갈로아필드 (GF: Galois Field) 곱셈기와 1개의 갈로아필드 GF 덧셈기로 구성된다. 신드롬 블록의 하드웨어 복잡도를 낮추기 위하여 IMA [3]에서는 각각의 GF 곱셈기에서 하드웨어 공유를 진행하였다. 공통 표현식 공유 기법은 하드웨어 복잡도를 낮추기 위하여 적용되는 대표적인 기법 중 하나로, 반복적으로 표현되는 식을 하나의 하드웨어로 구현하고 이를 공유하는 방법이다. 하지만 기존 공통 표현식 공유 기법 IMA [3]는 GF 곱셈기에서만 하드웨어 공유를 진행함으로써, 하드웨어 공유에 제약이 존재한다.

제안하는 알고리즘에서는 기존의 공통 표현식 공유 기법을 기반으로 공유 가능한 식을 찾는 범위를 아래와 같이 두 단계로 확장시킴으로써 검색 가능한 모든 공통 표현식을 찾도록 한다.

- 1) 각각의 GF 곱셈기에 대하여 적용되던 공유 알고리즘을 p 개의 입력을 동시에 받아 처리하는 하나의 SC 유닛으로 공유 범위를 1차적으로 확대한다.
- 2) 1차적으로 확대된 공유 범위를 $2t$ 개의 SC 유닛으로 공유 범위를 확대시키고, 이를 통해 신드롬과 관련된

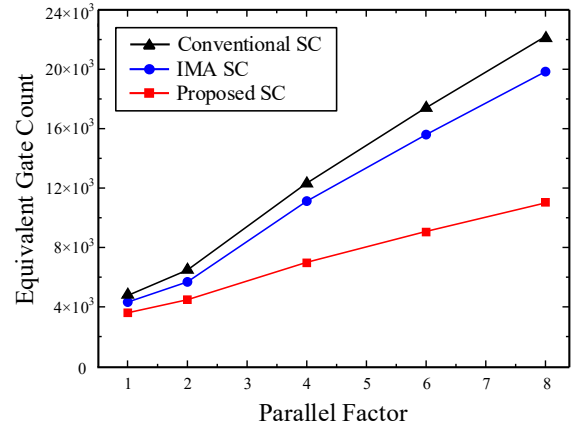


그림 2. 병렬화 계수에 따른 복잡도 비교.

전체 연산을 하나의 행렬 곱으로 표현하였고, 이는 최소한의 하드웨어 복잡도를 보장한다.

III. 실험결과 및 결론

그림 2에서는 다양한 병렬화 계수에 따른 RS (255, 239, 8) 복호기에 대한 합성 결과를 나타내고 있다. 130 nm 공정을 이용하여 200 MHz의 동작 주파수를 가지는 회로를 구현하였다. 제안하는 복호기는 공유 범위를 최대한 확대시킴으로써 공유를 최대화 할 수 있고, 이를 통해 기존 신드롬 연산기와 단순 공유 구조 대비 월등히 적은 하드웨어 복잡도를 가진다.

ACKNOWLEDGEMENTS

이 성과는 한국연구재단의 지원(2017R1C1B5015962)과 IDEC의 지원을 받아 수행된 연구임.

참고문헌

- [1] S. B. Wicker and V. K. Bhargava, *Reed-Solomon Codes and Their Application*. Picataway, NJ: IEEE Press, 1994.
- [2] S. Lin and D. J. Costello, *Error control coding: Fundamentals and Applications*, 2nd ed. Englewood Cliff, NJ: Prentice-Hall Inc., 2004.
- [3] M. Potkonjak, et. al, "Multiple Constant Multiplications: Efficient and Versatile Framework and Algorithms for Exploring Common Subexpression Elimination," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol.15, no.2, pp.151-165, Feb. 1996.