

BCH 부호를 위한 저전력 에너지 키-방정식 풀이 알고리즘

최소연¹, 이영주², 유호영¹

¹충남대학교, ²포항공대

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

Energy-efficient Key-equation Solving Algorithm for BCH Decoding

Soyeon Choi¹, Youngjoo Lee², Hoyoung Yoo¹,

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

요약

강력한 BCH 복호기에서 키-방정식 풀이 블록은 원하지 않는 핫 스팟을 발생시키며 가장 많은 에너지를 소모한다. 고성능 BCH 복호기 구현을 위하여 에너지 효율적인 키-방정식 풀이 알고리즘은 필수적이다. 본 논문에서는 신드롬 간의 관계를 이용하여 단일 오류를 검출하는 새로운 방법을 제안한다. 단일 오류를 우선적으로 판별하고, 조건을 만족할 시 복잡한 키 방정식을 풀지 않고 오류 위치 다항식을 단순 연산으로 대체하여 계산한다. BCH (16383, 15543, 60) 복호기의 경우 제안 된 방법은 기존의 알고리즘과 오류 없는 케이스에 대하여 각각 99%와 91%의 에너지를 절약한다.

Abstract

The key-equation solving block dominates the overall energy dissipation of strong BCH decoding and induces unwanted hot-spots. In achieving a high-performance BCH decoder, an energy-efficient algorithm should be developed for solving the key equation. This paper proposes a novel method to detect the case of single error by exploiting the relation among syndromes. If a single-error case is detected, the modified error-locator polynomial is obtained without solving the key-equation. For a (16383, 15543, 60) decoder implemented in a 130nm CMOS process, the proposed method saves 99% and 91% of energy compared to the conventional algorithm and the previous method that detects the error-free case, respectively.

Keywords: BCH 복호화, 키-방정식 풀이, 저전력 설계.

I. 서론

BCH 부호는 다양한 통신 시스템과 저장 매체에서 오류 정정을 목적으로 널리 사용되고 있다 [1]. 부호 길이 n , 메시지 길이 k , 오류 정정 능력 t 를 가지는 BCH (n, k, t) 부호의 복호기 하드웨어는 일반적으로 3 단 구조로 구성이 되며, 이 때 최대 t 개의 비트까지 정정이 가능하다 [2]. 수신 벡터 $R(x)$ 를 처리하기 위하여 BCH 복호기는 첫번째 블록인 신드롬 연산 (SC: Syndrome Calculation) 블록에서 $2t$ 개의 신드롬을

생성하고, 두번째 키-방정식 풀이 (KES: Key-equation solver) 블록에서는 주어진 신드롬 방정식 $S(x) = s_1 + s_2x + \dots + s_{2t}x^{2t-1}$ 를 이용하여 키-방정식을 유도한다. 끝으로 세번째 오류 위치 판별 (EPS: Error-Position Search) 블록에서 오류의 위치를 찾고 오류 정정을 진행한다 [2].

II. 본론

BCH 복호기의 효율적인 에너지 관리를 위하여 오류가 없는 경우를 검출하는 방법을 널리 이용하였다.

표 1. BCH (16383, 15543, 60) 합성 결과

구조	기존 구조	비 오류 검출 [3]	단일오류검출
에너지 소모량*	1.2×10^{-8} J	1.81×10^{-9} J	1.59×10^{-10} J
게이트 수	148 k	149k	149 k
평균 사이클 수*	60	10.06	1.72
평균 레이턴시*	300 ns	50.3 ns	8.6 ns

* 채널 비트 BER of 10^{-5} 을 가정함.

[3]. 주어진 수신 벡터 $R(x)$ 에 오류가 없다고 판별될 경우, KES 와 EPS 의 연산을 생략함으로써 불필요한 에너지 소모를 방지하였다. 이러한 비 오류 검출 방법은 $2t$ 개의 전체 신드롬들이 0 인지 아닌지를 확인함으로써 간단하게 판별이 가능하다. 본 논문에서는 검출 범위를 비 오류 경우에서 단일 오류까지 확대함으로써 전체 에너지 소모를 효율적으로 줄이는 방안을 제시한다.

신드롬 방정식 $S(x)$ 에서 i 번째 신드롬 s_i 는 (1)과 같이 n 비트 길이 수신 벡터 $R(x)$ 에 α^i 를 대입함으로써 계산 된다.

$$s_i = R(\alpha^i) = r_0 + r_1\alpha^i + \dots + r_{n-1}\alpha^{(n-1)i} \quad (1)$$

이 때, ω 번째 비트 위치에 단일 오류가 존재한다면, i 번째 신드롬 $s_i = R(\alpha^i) = \alpha^{\omega i}$ 을 갖게 된다. 이 때 식 (1)을 활용하면, 단일 오류의 경우 전체 $2t$ 개의 신드롬들은 (2)의 관계식을 만족함을 알 수 있다.

$$s_i = s_{i-1} \times s_1 \quad (2 \leq i \leq 2t) \quad (2)$$

다시 말해, s_1 이 0 이 아니며 전체 신드롬들이 식 (2)를 만족할 때, 단일 오류라고 판단할 수 있다.

비 오류 검출에서는 판별 즉시 복호화 과정을 중단할 수 있지만, 단일 오류 검출의 경우 EPS 블록에서 연산을 진행하여야 하기 때문에 오류 위치 방정식 $\Lambda(x)$ 을 반드시 생성해 주어야 한다. 제안하는 알고리즘에서는 식 (1)을 이용하여 오류 위치 다항식 $\Lambda(x) = \alpha^{\omega x} + 1 = s_1 \cdot x + 1$ 을 계산한다. 기존의 알고리즘들은 단일 오류를 처리하기 위하여 t 사이클의

클럭 수가 필요한 반면, 제안하는 알고리즘은 1 사이클의 클럭 수 만으로도 동일한 연산을 진행할 수 있다. 따라서 제안하는 방식에서는 BCH 복호기 중 가장 전력 소모가 큰 KES 블록에 대하여 오류 검출 범위를 확장시킴으로써 전체적인 전력 소모를 감소시킬 수 있다.

III. 실험결과 및 결론

BCH (16383, 15543, 60) 복호기에 대한 합성 결과를 표 1에 정리하였다. 제안하는 단일 오류 검출 복호기를 기존 구조 [2]과 비 오류 검출 복호기 [3]와 비교하였다. 오류가 없는 경우와 단일 오류의 경우를 판별함으로써 평균 사이클 수와 레이턴시를 줄임으로써, 실험결과 BER 10^{-5} 을 기준으로 제안하는 하드웨어 구조가 가장 적은 에너지 소모를 가진다.

ACKNOWLEDGEMENTS

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

참고문헌

- [1] *Forward Error Correction for Submarine Systems*. ITU Telecommunication Standardization Sector, ITU-T Recommendation G.975, 2000.
- [2] S. Lin and D. J. Costello, *Error control coding: Fundamentals and Applications*, 2nd ed. Englewood Cliff, NJ: Prentice-Hall Inc., 2004.
- [3] B. Park, J. Park, and Y. Lee, "Area-optimized fully-flexible BCH decoder for multiple GF dimensions," *IEEE Access*, in press.