

영상 정보의 LDPC 부호화 및 복호기의 FPGA구현

장은영*

LDPC Coding for image data and FPGA Implementation of LDPC Decoder

Eun-Young Jang*

요 약

잡음이 존재하는 채널환경에서의 정보전송을 위해서는 정보의 부호화 기술이 필요하다. 오류 검출과 정정에 사용되는 여러 가지 부호화 기술 중 Shannon의 한계에 가장 근접한 부호화 기술이 저밀도 패리티 체크(Low density Parity Check :LDPC) 부호이다. LDPC 부호와 sum-product 알고리즘의 조합에 의하여 얻어지는 복호 특성은 터보 부호, RA(Repeat Accumulate) 부호의 성능에 필적하며, 부호장이 매우 긴 경우에는 이들 성능을 추월한다. 본 논문에서는 영상 정보의 LDPC 부호화와 복호화 기술 원리에 관해 설명하고, Sum-product 알고리즘을 사용하는 LDPC 복호기를 FPGA로 구현한다.

ABSTRACT

In order to transmit information in a channel environment in which noise exists, a coding technique of information is required. One of the coding techniques used for error detection and correction close to the Shannon limit is Low Density Parity Code(LDPC). LDPC and decoding characteristic features by Sum-product algorithm are matched for the performance to Turbo Code, RA(Repeat Accumulate) code, in case of very long code length of LDPC surpass their performance. This paper explains LDPC coding scheme of image data and decoding scheme, implements LDPC decoder in FPGA.

키워드

LDPC, Sum-product, ECC, FPGA
저밀도 패리티 체크 부호, Sum-product, ECC, FPGA

1. 서 론

1948년 Shannon은 채널을 통해 전송할 수 있는 최대 정보량을 채널용량이라고 하였다. 그리고 오류 정정 부호화의 성능에 대한 이론적인 한계를 제시하였다[1]. 그 이후 수많은 오류 정정 기술이 제안되었지만, 어떠한 기술도 1993년 Berrou, Glavieux와 Thitimajshima가 발견한 터보 부호보다 향상된 오류 정정 능력에 미치지 못했다[2].

그리고 1962년에 Gallager가 처음 제안한 LDPC는 거의 이상적인 성능(Shannon의 한계)에 가까운 부호였지만 계산이 너무 크고 복잡하며 구현이 어려워 사용되지 않다가 MacKay와 Neal이 1996년에 새롭게 해석하여 이 부호들이 긴 길이를 가지는 경우 실현할 수 있는 복잡도의 복호 알고리즘으로 점대점 채널의 채널 용량에 근접하고 오류 정정 능력에서 좋은 성능을 가짐을 확인하였다[3-4]. LDPC부호는 고속 데이터 전송이 가능한 오류정정부호이며 부호 길이가

* 교신저자 : 신라대학교 전자공학과
• 접수일 : 2017. 04. 27
• 수정완료일 : 2017. 07. 13
• 게재확정일 : 2017. 08. 01

• Received : Apr 27, 2017, Revised : July 13, 2017, Accepted : Aug 01, 2017
• Corresponding Author : Eun-Young Jang
Dept. of Electronic Engineering, SILLA University,
Email : eunyoung@silla.ac.kr

커짐에 따라 오류 정정 능력은 좋아지고 계산 복잡도는 그대로 유지되는 반복 복호 기법을 사용한다. 이러한 LDPC 부호의 BER 성능은 터보 부호 성능과 유사하며, 만약 $GF(q)$ ($q = 4, 8, 16$)에서 동작하는 원래의 기술을 수정하면 터보 부호의 성능보다 우수하다.

II. LDPC 부호의 부호화

LDPC 부호의 설계 방법은 행렬에서 1의 수가 적은 소한 패리티 검사 행렬 $H = [A \ B]$ 로 시작된다. H 의 부 행렬 A 는 비특이(nonsingular)인 $(n-k) \times (n-k)$ 의 정방 행렬이다. 따라서 역 행렬 A^{-1} 이 존재하고, 부행렬 B 의 차원은 $(n-k) \times k$ 이다.

가우시언 소거법으로 행렬 $H = [A \ B]$ 를 $H' = [I_{n-k} \ A^{-1} B] = [I_k \ P^T]$ 형태로 수정할 수 있다. 일단 등가 패리티 검사 행렬 H' 가 구해지면, 생성 행렬 G 는 $G = [P \ I_k]$ 로 구성한다. 이와 같이 생성 행렬과 패리티 검사 행렬이 정의되면 LDPC 부호화가 진행된다.

LDPC 부호는 소한 패리티 검사 행렬 H 를 발생하는데 이때 행과 열 당 1의 수가 변하는 소한 패리티 검사 행렬 H 를 가지면 불규칙 LDPC 부호라하고, 일정한 1의 수를 가지면 규칙 LDPC 부호라한다. 일반적으로 불규칙 LDPC 부호의 BER 성능이 규칙 LDPC 부호의 성능보다 우수하기 때문에 시뮬레이션에서 불규칙 LDPC 부호를 구성하였다.

2진 메시지 $m = [m_1, m_2, m_3, \dots, m_k]$ 에 대응하는 부호어 c 는 $c = G^T m$ 행렬식을 통해 부호화되고, 채널을 통해 전송된다.

III. LDPC 부호의 복호화

3.1 복호 알고리즘

채널을 통과한 부호어는 전송 중 잡음의 영향을 받아 수신 벡터 $r = c + n$ 으로 변환되며, 이는 신드롬 벡터 $S = Hr = H(G^T m + n) = Hn$ 의 계산에 기초한 블록 부호의 전통적인 복호기의 입력 정보가 된다.

복호 알고리즘의 핵심은 조건 $Hd = 0$ 를 만족하는 벡터 d 의 값을 추정하는 것이다.

3.2 sum-product 알고리즘

LDPC의 복호 알고리즘은 전체적으로 메시지패싱 알고리즘이라 하며 sum-product 알고리즘을 사용하였다. 이 알고리즘은 각 메시지 심볼의 사후 확률을 수신 신호의 함수로 구하는 작업으로부터 시작되며 Tanner 그래프라 하는 등가의 이분(bipartite graph) 그래프를 사용하여 편리하게 설명된다[3]. Tanner 그래프는 대응하는 패리티 검사 행렬 H 에서 설명된 패리티 식으로 정의된다.

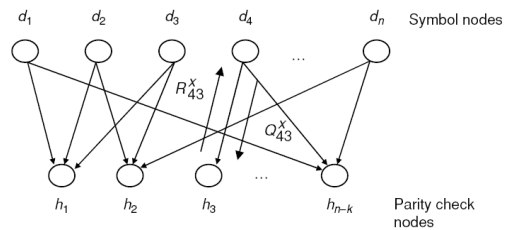


그림 1. Tanner 그래프
Fig. 1 Tanner graph

sum-product 알고리즘은 수신 심볼의 사후 추정으로 패리티검사노드로 보내는 정보인 Q 를 구하기 위한 초기화 과정이 필요하다. 이 정보는 이용한 채널 모델에 종속되고 AWGN 채널의 경우 확률값은 가우시언 확률 밀도 함수를 사용하여 구한다.

초기화한 후, 심볼과 패리티 검사 노드 사이에 정보 교환이 시작된다. 각 패리티 검사 노드 h_i 에서 그 의 심볼 노드 d_j 로 보내는 정보 R_{ij}^x 는, 정보를 가지고 있는 심볼 노드가 상태 x 에 있을 때 패리티 검사 노드 h_i 가 만족될 확률이다. 패리티 검사 식이 만족될 확률은 다음과 같다.

$$P(h_i/d_j = x) = \sum_{d: d_j = x} P(h_i/d)P(d/d_j = x) \quad (1)$$

이 확률은 전송된 심볼 노드가 상태 x 에 있을 때, 패리티 검사 식을 만족하기 위해서 가능한 모든 복호된 벡터 d 를 계산함의 의미한다.

패리티 검사 노드 h_i 에 대해, 심볼 노드 d_j 로 보내 질 정보는 x 의 각 값에 대해 계산되며, 다음과 같이 주어진다.

$$R_{ij}^x = \sum_{d: d_j=x} p(h_i/d) \prod_{k \in N(i) \setminus j} Q_{ik}^{d_k} \quad (2)$$

여기서 $N(i)$ 는 패리티 검사 노드 h_i 에 연결된 모든 심볼 노드의 인덱스 집합을 나타내고, $N(i) \setminus j$ 는 심볼 노드 d_j 를 제외한 집합을 나타낸다. 심볼 노드 d_j 는 그의 패리티 검사 노드 h_i 로 추정값 Q_{ij}^x 을 보낸다. 이 추정값은 심볼 노드에 연결된 다른 패리티 검사 노드가 제공하는 정보에 따라 노드가 상태 x 에 있다는 추정치이다. Bayes 정리를 적용하면 다음과 같다.

$$\begin{aligned} p(d_j = x / \{h_i\}_{i \in M(j) \setminus i}) \\ = \frac{P(d_j = x) P(\{h_i\}_{i \in M(j) \setminus i} / d_j = x)}{P(\{h_i\}_{i \in M(j) \setminus i})} \end{aligned} \quad (3)$$

심볼 노드 d_j 가 그의 패리티 검사 노드로 보내는 정보는 다음과 같다.

$$Q_{ij}^x = \alpha_{ij} f_j^x \prod_{k \in M(j) \setminus i} R_{kj}^x \quad (4)$$

여기서 $M(j)$ 는 심볼 노드 d_j 에 연결된 모든 패리티 검사 노드의 인덱스 집합이며, $M(j) \setminus i$ 는 패리티 검사 노드 h_i 를 제외한 같은 집합을 나타낸다. 계수 f_j^x 는 d_j 가 상태 x 에 있는 사전 확률이다. 정규화 상수 α_{ij} 는 정규화 조건 $\sum_x Q_{ij}^x = 1$ 을 만족하도록 설정한다.

이와 같이 계수 Q_{ij}^x 의 계산은 인덱스 j 의 각 값에 대한 추정을 수행하기 위해 사용될 수 있는 계수 R_{ij}^x 의 값을 결정하도록 한다. 이는 수신 벡터의 각 심볼에 대한 추정이며, 2진 경우에는 변수 x 의 두 가지 가능한 값에 대한 추정으로 표현된다. 이 추정은 다음과 같다.

$$\hat{d}_j = \arg_x \max f_j^x \prod_{k \in M(j)} R_{kj}^x \quad (5)$$

식(5)는 j 위치에서의 심볼에 대한 추정을 나타낸다. 만약 추정 복호된 벡터 $\hat{\mathbf{d}}$ 가 신드롬 조건 $\mathbf{H}\hat{\mathbf{d}} = \mathbf{0}$ 을 만족한다면, 추정 복호된 벡터 $\hat{\mathbf{d}}$ 는 확실한 부호 벡터 $\mathbf{c} = \hat{\mathbf{d}}$ 로 간주된다. 그렇지 않고 만약 복호기가 위의 신드롬 조건을 만족하는 적절한 부호 벡터를 찾지 못하고 미리 정해진 반복수에 도달한다면, 각 심볼은 부호 벡터의 모든 심볼이 실제로 송신되지 않더라도 최적으로 추정되며 정확히 복호된다.

IV. 영상 정보의 LDPC 부호화와 복호화

영상 정보의 전송 시뮬레이션은 다음 그림2와 같은 단계로 진행하였다.

먼저 영상 정보를 추출하고 LDPC 부호화를 위해서 크기가 10×20 (부호율 $R_c = 1/2$)인 패리티 검사 행렬 \mathbf{H} 를 생성한다. 이 패리티 검사 행렬 \mathbf{H} 를 바탕으로 추출한 영상 정보를 부호화하였다.

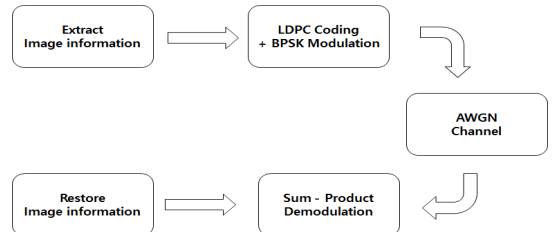


그림 2. 영상 정보 전송 시뮬레이션
Fig. 2 Image data transmission simulation

그림3은 추출한 영상 정보의 원래 화상 정보와 부호화된 영상 정보를 나타낸다[5].

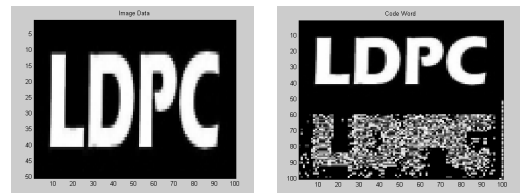


그림 3. 영상 정보와 부호화된 영상 정보
Fig. 3 Image data and Coded image data

부호화된 영상 정보를 BPSK 변조한 뒤 AWGN 채널(SNR 3dB)을 통과하면 원래의 영상정보는 그림 4와 같이 왜곡된다.

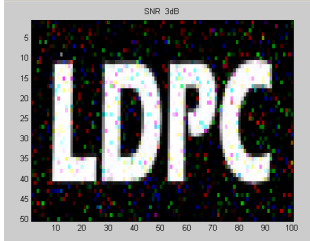
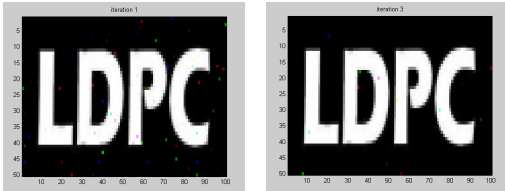


그림 4. AWGN 채널 통과 후 영상 정보
Fig. 4 Image data after passes through an AWGN channel

잡음에 왜곡된 영상 데이터를 sum-product 알고리즘을 사용해 복원한 모습을 그림 5에 나타내었다.



(a) Repeat times 1 (b) Repeat times 3
그림 5. 복원된 영상 정보
Fig. 5 Decoded image data

V. BER 성능 결과

sum-product 알고리즘을 사용한 복원 영상의 BER 성능평가 결과를 두 가지로 나누어 비교 평가했다.

첫 번째, SNR값이 같을 때 복호화의 반복 회수에 따른 BER의 성능평가이고, 두 번째, 다른 오류 정정 부호와 BER의 성능을 비교 평가하였다[6].

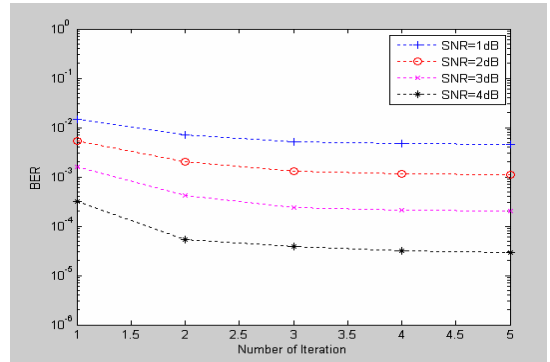


그림 6. BER 성능 비교
Fig. 6 Comparison of BER performance

그림 6은 SNR값이 1에서 4dB까지 증가할 때 복호화의 반복 횟수에 따른 BER 성능이다. SNR값이 클수록 성능이 좋아지고 반복횟수가 증가 할수록 성능이 좋아지는 것을 확인할 수 있다. 그러나 복호의 횟수가 5회를 넘어가면 BER의 성능은 거의 향상되지 않는 것을 확인하였다.

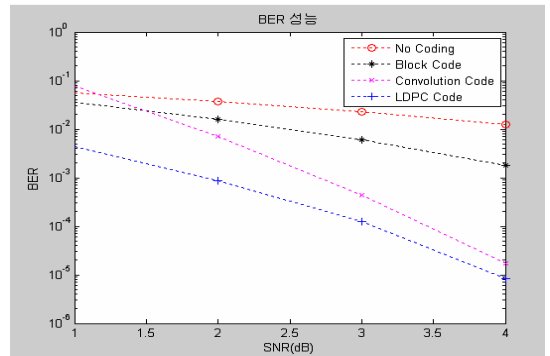


그림 7. 다른 ECC(Error Correcting Code)와 LDPC BER 성능 비교
Fig. 7 Comparison of BER performance between other ECCs and LDPC Code

그림 7은 AWGN 환경에서 다른 오류 정정 부호기법을 사용하여 BPSK의 BER이론값과 LDPC 부호를 사용한 시뮬레이션 결과이다.

부호화를 하지 않았을 경우 성능이 가장 나쁘고 컨벌루션 코드는 SNR이 증가할수록 성능이 많이 좋아지는 것을 확인할 수 있지만 성능이 가장 좋은 것은 LDPC 코드인 것을 확인할 수 있다.

VI. System Generator를 이용한 FPGA 구현

LDPC Decoder 모델의 구현은 Xilinx사의 System Generator를 사용해 설계하였다. Matlab을 이용하여 채널 사후 확률과 패리티 검사행렬 H 를 생성하고, 이를 Decoder의 입력으로 사용하였다[7].

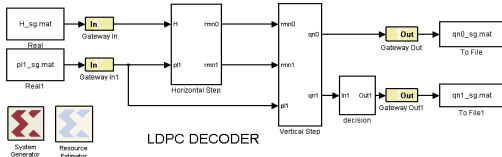


그림 8. System Generator 모델
Fig. 8 System Generator model

sum-product 복호 알고리즘은 크게 수평 연산부분과 수직 연산부분으로 나뉘는데 그림 8에서 첫 블록이 수평 연산부분, 두 번째 블록이 수직연산 부분을 나타낸다.

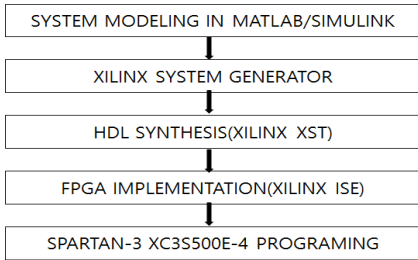


그림 9. FPGA구현의 순서도
Fig. 9 Flowchart for FPGA implementation

System Generator를 이용해 HDL 코드 생성 후 Xilinx사의 ISE를 이용해 Synthesis, Implementation 과정을 거쳐 FPGA로 하드웨어를 구현하였다[8].

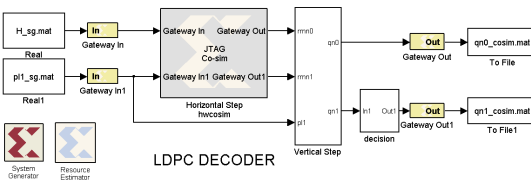


그림 10. Hardware Co-simulation 모델
Fig. 10 Hardware Co-simulation model

설계된 하드웨어 모델의 검증과 target device의 동일한 동작 확인을 위해 Hardware Co-simulation을 수행하였다[9].

```

=====
Timing constraint: TS_clk_3398266e = PERIOD TIMEGRP "clk_3398266e" 20 ns HIGH 50%;

28509 itens analyzed, 0 timing errors detected. (0 setup errors, 0 hold errors)
Minimum period is 9.683ns.
=====
    
```

그림 10. 타이밍 해석 결과
Fig. 10 Result of Timing analysis

Timing Analyzer를 이용하여 timing error를 측정하고, 시스템 모델에서 사용한 resource량을 추정한 결과는 그림 10과 같다.

표 1. Resource량 추정 결과
Table 1. Result of Resource estimation

	resource
Slices	1741
FFs	2598
LUTs	2790
Bonded IOBs	71
Mult 18x18s	5

FPGA의 Mapping 과정을 사용하면 사용자가 작성한 모든 로직이 기본 유닛과 일대일 Mapping이 되어 사용한 로직의 양을 알 수 있다. 표 1은 Resource량의 추정 결과이다.

VII. 결론

본 논문에서는 LDPC 부호를 영상 정보 전송에 적용하였다. sum-product 알고리즘을 사용해서 복호한 뒤 SNR(dB) 값에 따른 BER 성능 평가를 실시하였다. 또한 다른 오류 정정 부호들과 BER의 성능 비교를 통하여 LDPC Code의 우수한 성능을 입증하였다. 그리고 복호기의 FPGA 구현을 위해 System Generator 모델을 설계하였고, Matlab 시뮬레이션과 동일한 결과를

얻었다. 부호화 기술의 핵심이 될 LDPC 부호의 Encoder 부분의 FPGA구현에 연구를 진행해 나가겠다.

저자 소개

References

- [1] E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.* July Oct, 1948, vol. 27, no.3, pp. 379-423.
- [2] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-correcting Coding and Decoding: Turbo-Codes(1)," In *Proc. International Conference on Communications 93*, Geneva, Switzerland, May 1993, pp. 1064-1070.
- [3] L. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, 1981, pp. 533-547.
- [4] D. MacKay and R. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, no. 18, Aug. 1996, pp.1645-1646.
- [5] W, Zhang and H, Suh" International Conference on Communications," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 1, Feb. 2017, pp. 61-68.
- [6] J. C. Moreira, *Essentials of error-control coding*. Chippenhaam, England John Wiley & Sons, 2006.
- [7] S. Hong and E. Jang, "FPGA implementation of digital transceiver using chaotic signal," *J. of Korean Inst. Inform. Technol.*, vol. 8, no. 8, Aug. 2010, pp. 9-15.
- [8] E. Jang "Design of digital communication systems using DCSK chaotic modulation," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 5, May 2015, pp. 565-570.
- [9] E. Jang "Design of FM-QCSK Chaotic Communication System for high-speed communication," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 10, Oct. 2015, pp. 1183-1188.



장은영(Eun-Young Jang)

1998년 동아대학교 전자공학과 졸업 (공학사)

2000년 동아대학교 대학원 전자공학과 졸업(공학석사)

2008년 동아대학교 대학원 전자공학과 졸업(공학박사)

2014년 ~현재 신라대학교 공과대학 전자공학과 조교수

※ 관심분야 : 무선통신시스템, 5G이동통신 시스템