# 영상 정보의 LDPC 부호화 및 복호기의 FPGA구현

김진수* · 제갈동* · 변건식*

*동아대학교

# LDPC Coding for image data and FPGA Implementation of LDPC Decoder

Jin Su Kim*· Jaegal Dong*· Kun Sik Byon*

*Dong-a University

E-mail : mimo_ofdm@daum.net

## 요 약

잡음이 존재하는 환경에서 채널로 정보를 전송하기 위해서는 정보를 부호화하는 기술이 필요하다. 오류 검출과 정정에 사용되는 여러 가지 부호화 기술 중 Shannon의 한계에 가장 근접한 부호화 기술이 LDPC 부호이다. LDPC 부호와 sum-product 알고리듬의 조합에 의해 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 알고리듬을 사용하는 LDPC 복호기를 FPGA로 구현한다.

## ABSTRACT

To transmit information over a channel in the presence of noise, there needs some technique to code the information. One of the coding techniques used for error detection and correction close to the Shannon limit is Low Density Parity Code. 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, EEC, System Generator, FPGA

## Ⅰ. 서 론

1949년 Shannon은 그의 논문[1]에서 오류 정정 부호화의 성능에 대한 이론적인 한계를 제시하였다. 그 이후 수많은 오류 정정 기술이 제안되었지만, 어떤것도 Berrou, Glavieux, Thitimajshima[2]가 발견한 터보 부호의 성능을 능가하지 못했다.

1962년에 Gallager가 처음 제안한 거의 이상적인 성능(Shannon의 한계)에 가까운 부호를 MacKay와 Neal[4,5]이 1996년에 새롭게 재발견하였다. 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 소한(행렬에서 1의 수가 적음) 패리티 검사 행열 $\boldsymbol{H}=[\boldsymbol{A}\ \ \boldsymbol{B}]$로 시작된다. $\boldsymbol{H}$의 부행열 $\boldsymbol{A}$는 비특이인 $(n-k)\times(n-k)$의 정방 행열이다. 따라서 역 행열 $\boldsymbol{A^{-1}}$이 존재하고, 부행열 $\boldsymbol{B}$의 차원은 $(n-k)\times k$이다.

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

LDPC 부호는 소한 패리티 검사 행열 $\boldsymbol{H}$를 발생하는데 이때 행과 열 당 1의 수가 변하는 소한 패리티 검사 행열 $\boldsymbol{H}$를 가지면 불규칙 LDPC 부

호라하고, 일정한 1의 수를 가지면 규칙 LDCP 부호라한다. 일반적으로 불규칙 LDPC 부호의 BER 성능이 규칙 LDPC 부호의 성능보다 우수하기 때문에 시뮬레이션에서 불규칙 LDPC 부호를 구성하였다. 2진 메시지 $m=[m_1,m_2,m_3,\cdots,m_k]$에 대응하는 부호어 $\boldsymbol{c}$는 $\boldsymbol{c}=\boldsymbol{G}^T\boldsymbol{m}$ 행렬식을 통해 부호화되고, 채널을 통해 전송된다.

## III. LDPC 부호의 복호화

(1) 복호 알고리듬

채널을 통과한 부호어는 전송중 잡음의 영향을 받아 수신 벡터 $\boldsymbol{r}=\boldsymbol{c}+\boldsymbol{n}$으로 변환되며, 이는 신드롬 벡터 $\boldsymbol{S}=\boldsymbol{Hr}=\boldsymbol{H}(\boldsymbol{G}^T\boldsymbol{m}+\boldsymbol{n})=\boldsymbol{Hn}$ 의 계산에 기초한 블록 부호의 전통적인 복호기의 입력 정보가 된다. 복호 알고리듬의 핵심은 조건 $\boldsymbol{Hd}=\boldsymbol{0}$를 만족하는 벡터 $\boldsymbol{d}$의 값을 추정하는 것이다.

(2) sum-product 알고리듬

LDPC의 복호 알고리듬은 전체적으로 메시지 패싱 알고리듬이라 하고, 본 논문에서는 sum-product 알고리듬을 사용하였다. 이 알고리듬은 각 메시지 심볼의 사후 확률을 수신 신호의 함수로 구하는 작업으로 시작된다. 이 알고리듬은 Tanner 그래프[3]라 하는 2분 그래프를 사용하여 편리하게 설명된다. Tanner 그래프는 대응하는 패리티 검사 행열 $\boldsymbol{H}$에서 설명된 패리티 식으로 정의된다.

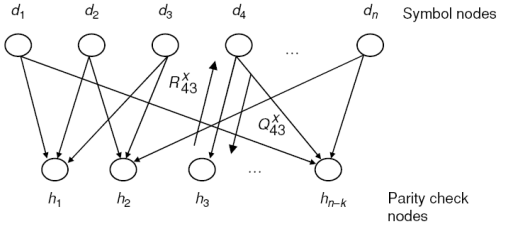


그림 1. Tanner 그래프
Fig. 1 Tanner graph

sum-product 알고리듬은 수신 심볼의 사후 추정으로, $Q_{ij}^x$를 구하므로 초기화 과정이 필요하다. 이 때 $f_j^x$는 $j$번째 심볼이 $x$일 확률이다. 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 그의 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 $\boldsymbol{d}$를 계산함을 의미한다. 패리티 검사 노드 $h_i$에 대해, 심볼 노드 $d_j$로 보내질 정보는 $x$의 각 값에 대해 계산되며, 다음과 같이 주어진다.

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

여기서 $N(i)$는 패리티 검사 노드 $h_i$에 연결된 모든 심볼 노드의 인덱스 집합을 나타내고, $N(i)\backslash j$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.

$$p(d_j=x/\{h_i\}_{i\in M(j)\backslash i}) = \frac{P(d_j=x)\,P(\{h_i\}_{i\in M(j)\backslash i}/d_j=x)}{P(\{h_i\}_{i\in M(j)\backslash i})} \quad (3)$$

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

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

여기서 $M(j)$는 심볼 노드 $d_j$에 연결된 모든 패리티 검사 노드의 인덱스 집합이며, $M(j)\backslash i$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 $\alpha_{ij}$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 $\hat{d}$가 신드롬 조건

$H\hat{d}=0$ 을 만족한다면, 추정 복호된 벡터 $\hat{d}$는 확실한 부호 벡터 $c=\hat{d}$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 그림과 같은 단계로 진행하였다.

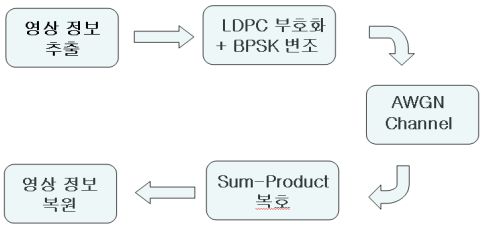


그림2. 영상 정보 전송 시뮬레이션
Fig. 2 Image data transmission simulation

먼저 영상 정보를 추출하고 LDPC 부호화를 위해서 크기가 $10\times20$(부호율 $R_c=1/2$)인 패리티 검사 행열 $H$를 생성한다. 이 패리티 검사 행열 $H$를 바탕으로 추출한 영상 정보를 부호화하였다. 그림3은 추출한 영상 정보의 원래 화상 정보와, 부호화된 영상 정보를 나타낸다.

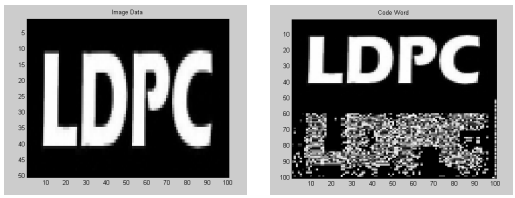

그림 3. 영상 정보와 부호화된 영상 정보
Fig. 3 Image data and Coded image data

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

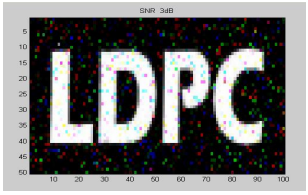

그림4. AWGN 채널 통과 후 영상 정보
Fig. 4 Image data after passes through an AWGN channel

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

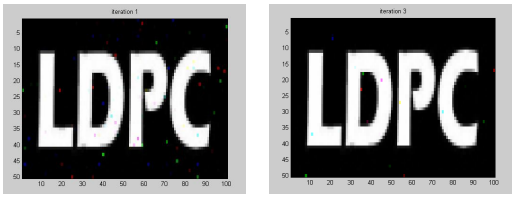

그림5. 복원된 영상 정보
(반복횟수 1회, 반복횟수3회)
Fig. 5 Decoded image data

## Ⅴ. BER 성능 결과

Sum-product 알고리듬을 사용해 복원한 영상 정보의 BER 성능 결과는 두 개로 나눠서 평가하였다. 첫 번째는 같은 SNR(dB)값일 때 반복 복호하는 횟수에 따른 BER 성능 평가이고, 두 번째는 다른 오류 정정 부호간의 BER 성능 비교 평가이다. 그림 6에서 가로축은 반복 횟수를 나타내고, SNR 값이 1,2,3,4dB일 때의 반복 횟수에 따른 BER 성능을 나타내었다. 높은 SNR값에서 가장 좋은 성능이 나왔고, 반복 횟수를 증가시키면 성능이 좋아지지만 5회이상시에는 BER성능이 향상되지 않았다.

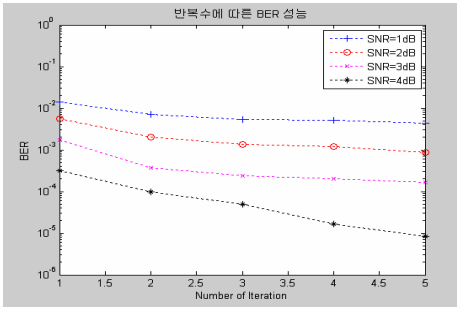


그림 6. BER 성능 비교
Fig. 6 Comparision of BER performance

그림 7은 AWGN 채널에서 다른 부호화 기법을 사용한 경우 각각의 BPSK BER 이론값과 LDPC Code를 사용해 시뮬레이션한 결과를 비교한 것이다.

① 부호화하지 않은 경우 (No coding)
② Block Code(N=7, k=3, Hamming distance=5)
③ Convolution Code (constraint length =7, code generator polynomials =171 and 133)
④ LDPC Code (Matlab simulation)

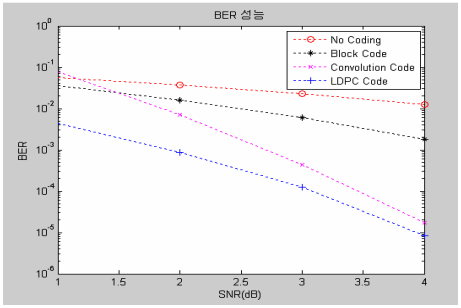


그림 7. 다른 ECC(Error Correcting Code)와 LDPC BER 성능 비교
Fig. 7 Comparision of BER performance between other ECCs and LDPC Code

## Ⅵ. System Generator를 이용한 하드웨어 모델 구현

LDPC Decoder 모델은 Xilinx사의 System Generator 9.1i를 사용해서 설계하였다. 먼저 Matlab을 이용하여 채널 사후 확률과 패리티 검사행렬 $\boldsymbol{H}$를 생성하고, 이를 Decoder의 입력으로 사용하였다.

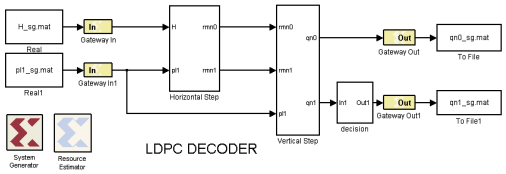


그림 8. System Generator 모델
Fig. 8 System Generator model

sum-product 복호 알고리듬은 크게 수평 연산부분과 수직 연산부분으로 나눠지는데 그림 8에서 첫 블록이 수평 연산부분, 두 번째 블록이 수직연산 부분을 나타낸다. System Generator를 이용하여 HDL 코드를 생성한 후 Synthesis, Implementation 과정을 Xilinx ISE 소프트웨어를 이용하여 FPGA로 하드웨어를 구현하였다

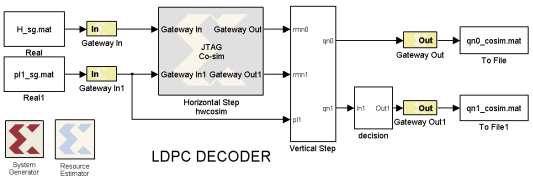


그림 9. Hardware Co-simulation 모델
Fig. 9 Hardware Co-simulation model

설계된 하드웨어 모델이 target device에서 동일하게 동작하는지 확인하기 위해 Hardware Co-simulation을 수행하였으며, target board에 사용된 Product family는 Spartan-3이며, 사용한 디바이스는 xc3s500e-4 fg320이다.

Timing Analyzer를 이용하여 timing error를 측정하고, 시스템 모델에서 사용한 resoure양을 추정한 결과가 아래에 있다.

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

 20509 items 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

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

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

## Ⅶ. 결 론

LDPC 부호를 영상 정보 전송에 적용하였다. sum-product 알고리듬을 사용해서 복호한 뒤 SNR(dB) 값에 따른 BER 성능 평가를 실시하였다. 그리고 다른 오류 정정 부호와의 BER 성능 비교를 통해 LDPC Code의 우수한 성능을 입증하였다. 복호기의 FPGA 구현을 위해 System Generator 모델을 설계하였고, Matlab 시뮬레이션과 동일한 결과를 얻었다. 차세대 이동 통신 부호화 기술의 핵심이 될 LDPC 부호의 Encoder 부분의 FPGA구현에 연구를 진행해 나가겠다.

## 참고문헌

[1] Shannon, C. E., “A mathematical theory of communication,” Bell Syst. Tech. J., vol. 27, pp. 379~423, 623~656, July and October 1948.
[2] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon Limit Error - correcting Coding and Decoding: Turbo-Codes(1),” in Proc. ICC’93, pp. 1064-1070, May 1993.
[3] Tanner, L. M., “A recursive approach to low complexity codes.” IEEE Trans. Inf. Theory, vol. 27, no. 5, pp. 533~547, 1981.
[4] LDPC toolkit for Matlab, available at http://arun-10.tripod.com/ldpc/generate.html
[5] Jorge Castiñeira Moreira, “Essentials of error-control coding.” pp.277~324