

근사화된 체크노드함수를 이용한 LDPC 부호의 반복 복호 기법

정회원 정 호 영*, 김 신 령**

An Iterative Decoding for LDPC Codes using Approximated Check Node Function

Ho-Young Cheong*, Sin-Ryeong Kim** *Regular Members*

요 약

LDPC 부호에 대한 반복 복호 알고리즘의 복잡 도를 개선하기 위해 min-sum 알고리즘과 같은 여러 가지 종류의 복호 알고리즘들이 제시되어 왔다. 이들은 체크 노드 메시지 함수를 단순화하여 복잡 도를 줄이는 것으로 복잡 도는 감소되었지만 SPA 알고리즘에 비해 성능 차이가 약 0.5[dB]의 값을 가지며 무시할 수 없는 성능 열화로 개선이 필요하다.

본 논문에서는 체크 노드 메시지 함수를 역함수 형태로 근사 화하여 복잡 도를 줄이는 복호 알고리즘을 제안 한다. 시뮬레이션 결과 제안된 알고리즘은 min-sum 알고리즘이 가지고 있는 복잡도 개선 효과를 유지하면서도 sum-product 알고리즘의 성능과 약 0.1[dB] 이내의 근접한 값을 보였다.

Key Words : Check Node Message, Sum-Product, Min-Sum, Normalized Min-Sum, Iterative Decoding

ABSTRACT

In order to reduce the decoding complexity of low density parity-check(LDPC) codes, some fast algorithms called suboptimal decoding, such as min-sum algorithm, normalized min-sum algorithm, were proposed. However, there would be approximation inaccuracy between the sum-product algorithm and the min-sum algorithm, which incurs some degradation in decoding performance.

In this paper, an efficient iterative decoding algorithm using approximated check-node function is proposed to improve the approximation inaccuracy. Simulation results show that the proposed algorithm achieves a performance very close to that of the SPA algorithm while preserving the low decoding complexity.

I. 서 론

LDPC 부호는 체크노드(check node) 집합과 심벌 노드(symbol node) 집합으로 나누어진 이분구조 그래프(bipartite graph)를 이용하여 복호 된다. 이 그래프 상의 심벌노드가 d_s 개의 체크노드 들과 연결 되어 있고 반대로 체크노드는 d_c 개의 심벌노드 들과

연결되어 있을 경우 우리는 (d_s, d_c) -균일(regular) LDPC 부호라고 하고 그렇지 않을 경우 불 균일(irregular) LDPC 부호라고 부른다.

LDPC 부호는 메시지-전달 알고리즘(message passing algorithm)을 이용해 반복적으로 복호할 수 있는데, LDPC 부호의 반복 복호 알고리즘은 크게 복호성능에 따라 최적(optimal) 복호, sub-optimal

* 남서울대학교 정보통신공학과(hycheong@nsu.ac.kr), ** 동서대학교 전자통신과(srkim@haksan.dsc.ac.kr)
논문번호 : 08078-1130, 접수일자 : 2008년 11월 30일

복호 및 quasi-optimal 복호 기법 등으로 나눌 수 있다^[1]. 다양한 분야에 LDPC 부호가 적용됨에 따라 효율적인 LDPC 복호 기법의 구현 방법이 연구되어 왔으며 최적 복호 기법의 장점인 우수한 복호 성능을 유지하면서도 복잡 도를 줄이는 방향으로 연구가 진행되어 왔다. 최적 복호기법은 SPA(sum-product algorithm) 혹은 BPA(belief propagation algorithm)라고 말하며 최적의 복호성능을 나타내지만 체크 노드의 메시지를 계산하는 계산 양이 너무 많아 하드웨어로 구현하기가 곤란한 단점이 있다. SPA와 근접한 복호 성능을 유지하면서도 복잡 도를 줄이기 위해 고안된 sub-optimal 복호기법 중 대표적인 것으로 MSA(min-sum algorithm)^[5]를 들 수 있는데 MSA는 복잡도가 크게 줄어든 반면 SPA와의 성능 저하가 무시할 수 없는 값을 나타낸다. 이러한 성능차이를 극복하기 위해 여러 가지 기법의 MSA 보완 알고리즘이 제시되었는데 NMSA(normalized min-sum algorithm)^[3], OMSA(offset min-sum algorithm)^[1] 등을 들 수 있다. 이들은 복잡한 연산 함수 형태를 갖는 체크 노드 메시지 함수를 단순화한 것으로 복잡 도는 크게 줄어들었지만 SPA 알고리즘의 성능과의 차이가 무시할 수 없을 정도이어서 이에 대한 개선이 요구되어 왔다.

본 논문에서는 체크 노드 메시지 함수를 역함수 형태로 근사 화하여 복잡 도를 개선한 복호 알고리즘을 제안한다. 제안한 복호 기법은 최적 복호 기법으로 알려진 SPA 방식과 거의 근접한 오율 성능을 보이며, 이를 보이기 위해 Monte-Carlo 시뮬레이션 기법을 이용하여 AWGN 채널에서 제안된 복호 알고리즘의 성능을 모의실험 하였다. SPA, MSA 및 NMSA 알고리즘에 대해서도 모의실험을 수행하여 그 결과를 비교 분석하였다. 시뮬레이션 결과 제안된 알고리즘은 min-sum 알고리즘이 가지고 있는 복잡도 개선 효과를 유지하면서도 SPA 방식에 비해 약 0.1[dB] 이하의 성능 차이를 보였다. 본 논문의 구성은 다음과 같다. 먼저 II 장에서는 SPA와 MSA 및 NMSA 복호 기법의 동작원리를 기술 하였으며, III 장에서 근사 화된 함수를 이용하여 체크노드 메시지를 계산하는 복호 알고리즘에 대해 기술하였다. IV 장에서는 (8000, 4000) 균일 LDPC 부호에 대해 각 복호 방식에 따른 오율 성능을 모의실험을 통해 비교 분석하였으며, V 장에서 결론을 내렸다.

II. LDPC 반복 복호의 동작 원리

LDPC 부호의 반복 복호는 체크 노드(check node) 집합과 심벌 노드(symbol node) 집합으로 나누어진 이분구조그래프(bipartite graph) 상에서 메시지를 반복적으로 갱신하여 상호 교환하는 과정에서 전송 심벌 값을 추정하는 기법이다. LDPC 부호의 반복 복호 기법은 최적 복호 알고리즘으로 알려져 있는 SPA(sum-product algorithm) 혹은 BP(belief propagation) 알고리즘과 SPA 복호 기법의 복잡 도를 크게 줄인 MSA(min-sum algorithm) 형태가 있다. MSA 알고리즘은 SPA 알고리즘에 비해 복잡 도를 크게 줄이는 데는 성공했지만 이로 인해 발생된 성능 열화는 무시하지 못할 정도의 값을 보인다. MSA의 복잡도 개선을 유지하면서도 성능 열화를 보완할 수 있는 MSA-type 알고리즘들이 제시되었는데 대표적인 것으로 정규 화된 MSA 알고리즘(NMSA : normalized min-sum algorithm)을 들 수 있다. 본 절에서는 이들의 동작원리를 살펴본다.

2.1 SPA 복호 기법의 동작원리

SPA 알고리즘은 먼저 채널의 통계적 특성을 고려하여 심벌 n 의 APP(a posterior probability) 값을 계산한 후 이를 심벌 노드 메시지 값 $q_{n \rightarrow m}(i)$ 으로 식 (1), (2) 와 같이 초기화한다.

$$q_{n \rightarrow m}(0) = P_{X|Y}(x_n = 0 | y_n) \quad (1)$$

$$q_{n \rightarrow m}(1) = P_{X|Y}(x_n = 1 | y_n) \quad (2)$$

위의 두 값에 대한 로그 비(log ratio)를 로그 가 능도 비(log-likelihood ratio, LLR)이라고 하며 식 (3)과 같이 나타낼 수 있으며 심벌 노드 메시지의 초기 값이 된다.

$$Z_{n \rightarrow m}(x_n) = \log \left(\frac{P_{X|Y}(x_n = 1 | y_n)}{P_{X|Y}(x_n = 0 | y_n)} \right) = L(x_n | y_n) \quad (3)$$

초기화 과정이 끝나면 체크노드 갱신(check-node update) 과정과 심벌노드 갱신(symbol-node update) 과정을 거치게 되며 체크노드 갱신 과정에서는 식 (4)와 (5), 심벌노드 갱신과정에서는 식 (6), (7) 및 (8) 과 같은 메시지 값을 계산하게 된다^{[5][6]}.

$$\gamma_{m \rightarrow n}(0) = \frac{1}{2} + \frac{1}{2} \prod_{n' \in \mathcal{N}(m) \setminus n} (1 - 2q_{n' \rightarrow m}(1)) \quad (4)$$

여기에서 $\gamma_{m \rightarrow n}(1) = 1 - \gamma_{m \rightarrow n}(0)$ 이므로 체크노드의 메시지의 로그 비는 식 (5)와 같이 나타낼 수 있다.

$$L_{m \rightarrow n}(x_n) = \ln \left(\frac{\gamma_{m \rightarrow n}(0)}{\gamma_{m \rightarrow n}(1)} \right) = \prod_{n' \in N(m) \setminus n} \alpha_{n'm} \times \phi \left(\sum_{n' \in N(m) \setminus n} \phi(\beta_{n'm}) \right) \quad (5)$$

$\alpha_{n'm}$, $\phi(x)$ 및 $\beta_{n'm}$ 은 다음과 같이 정의된다.

$$Z_{m \rightarrow n}(x_n) = \alpha_{nm} \beta_{nm} \quad (6)$$

$$\alpha_{nm} = \text{sign}(Z_{m \rightarrow n}(x_n)) \quad (7)$$

$$\beta_{nm} = |Z_{m \rightarrow n}(x_n)| \quad (8)$$

$$\phi(x) = \ln \left(\frac{e^x + 1}{e^x - 1} \right) \quad (9)$$

한편 심벌 x_n 에서 m 번째 체크 노드로 보내지는 메시지 값은 식 (10)과 같으며

$$q_{n \rightarrow m}(i) = \mu_{n \rightarrow m} P(x_n = i | y_n) \prod_{m' \in M(n) \setminus m} \gamma_{m' \rightarrow n}(i), \quad i = 0 \text{ or } 1. \quad (10)$$

식 (3)과 (10)을 이용하면 심벌 노드 메시지의 로그 비는 식 (11)과 같이 나타낼 수 있다.

$$Z_{n \rightarrow m}(x_n) = \log \left(\frac{q_{n \rightarrow m}(1)}{q_{n \rightarrow m}(0)} \right) = L(x_n | y_n) + \sum_{m' \in M(n) \setminus m} L_{m' \rightarrow n}(x_n) \quad (11)$$

이 때 $L(x_n | y_n) = \log \left(\frac{P_{X|Y}(x_n = 1 | y_n)}{P_{X|Y}(x_n = 0 | y_n)} \right)$ 을 의미한다.

심벌 x_n 에 대한 APP 값은 식 (12)과 같이 계산할 수 있으며 이를 이용하여 심벌 x_n 의 값을 잠정적으로 추정하게 된다.

$$Z_n(x_n) = L(x_n | y_n) + \sum_{m \in M(n)} L_{m \rightarrow n}(x_n) \quad (12)$$

체크 노드와 심벌 노드 메시지의 로그 비를 식 (5), (11) 과 각 각 같이 정의하면 LLR-SPA 복호 과정은 다음과 같이 정리될 수 있다.

(1 단계) 초기화 과정 : LDPC 부호의 패리티 체크

행렬 H 에 대해 $H_{mn} = 1$ 인 경우에 대한 $Z_{n \rightarrow m}(x_n)$ 은 식 (3)으로부터 식 (13)과 같이 초기화 된다.

$$Z_{n \rightarrow m}(x_n) = \log \left(\frac{P_{X|Y}(x_n = 1 | y_n)}{P_{X|Y}(x_n = 0 | y_n)} \right) = L(x_n | y_n) \quad (13)$$

(2 단계) 체크 노드 갱신 : $n \in N(m)$ 인 경우에 대해 체크노드 LLR 메시지는 식 (14)와 같이 계산하여 갱신한다.

$$L_{m \rightarrow n}(x_n) = \ln \left(\frac{\gamma_{m \rightarrow n}(0)}{\gamma_{m \rightarrow n}(1)} \right) = \prod_{n' \in N(m) \setminus n} \alpha_{n'm} \times \phi \left(\sum_{n' \in N(m) \setminus n} \phi(\beta_{n'm}) \right) \quad (14)$$

(3 단계) 심벌노드 갱신 : 모든 n 값에 대해 다음을 계산하여 메시지 값을 갱신한다.

$$Z_{n \rightarrow m}(x_n) = \log \left(\frac{q_{n \rightarrow m}(1)}{q_{n \rightarrow m}(0)} \right) = L(x_n | y_n) + \sum_{m' \in M(n) \setminus m} L_{m' \rightarrow n}(x_n) \quad (15)$$

또한 $m \in M(n)$ 인 모든 체크노드 메시지를 이용하여 심벌 n 의 APP 값은 식 (16)와 같이 계산된다.

$$Z_n(x_n) = L(x_n | y_n) + \sum_{m \in M(n)} L_{m \rightarrow n}(x_n) \quad (16)$$

(4 단계) 복호 결정 : $Z_n(x_n) > 0$ 이면 $\hat{x}_n = 0$ 이고 $Z_n(x_n) < 0$ 이면 $\hat{x}_n = 1$ 로 $\hat{\mathbf{x}} = [\hat{x}_1, \hat{x}_2, \hat{x}_3, \dots, \hat{x}_N]$ 을 결정한다. 만일 $\hat{\mathbf{x}}\mathbf{H}^T = \mathbf{0}$ 이면 복호 과정을 완료하고 $\hat{\mathbf{x}}$ 를 전송 부호로 복호한다. $\hat{\mathbf{x}}\mathbf{H}^T \neq \mathbf{0}$ 이면 (2 단계)로 돌아가 복호과정을 반복한다. 만일 최대 반복 회수인 I_{\max} 까지도 복호가 끝나지 않으면 복호는 실패한 것으로 판단하고 복호 과정을 종료한다.

2.2 MSA 복호 기법과 NMSA 복호 기법의 체크 노드 메시지

식 (5)와 같이 표현되는 체크 노드 메시지는 함수 $\phi(x)$ 자체가 식 (9)와 같이 대단히 복잡한 형태를 가지고 있다. 체크 노드 메시지를 갱신할 때 마다 $\phi(x)$ 함수를 이중으로 호출한다는 것은 매우 큰 연산량을 필요로 한다. 이러한 체크노드 메시지 함수를 식 (17)과 같이 근사화하여 체크 노드 메시지 연산량을 크게 줄인 복호 기법을 MSA(min-sum algorithm)이라고 한다^[4].

$$L_{m \rightarrow n}^{MSA}(x_n) = \prod_{n' \in N(m) \setminus n} \alpha_{n'm} \times \min_{n' \in N(m) \setminus n} \beta_{n'm} \quad (17)$$

MSA 알고리즘은 복잡한 $\phi(x)$ 함수 연산을 피함으로서 복잡 도를 크게 줄였지만 이로 인해 발생하는 성능 열화는 SPA 기법에 비해 약 0.5[dB] 정도로 무시하지 못하는 값이다. MSA의 복잡 도를 유지 하면서도 성능 열화를 보완하고자 제시된 알고리즘이 NMSA(normalized MSA)이다.

MSA의 체크 노드 메시지 값과 SPA의 체크 노드 값은 항상 식 (18)의 관계에 있음은 잘 알려진 사실이다^[2].

$$L_{m \rightarrow n}^{MSA}(x_n) > L_{m \rightarrow n}^{SPA}(x_n) \quad (18)$$

따라서 MSA의 체크 노드 메시지 값을 일정한 상수 값으로 정규화 함으로서 MSA에 의해 발생된 성능 열화를 개선하고자 하는 것이 NMSA 기법이다.

$$L_{m \rightarrow n}^{NMSA}(x_n) = \prod_{n' \in N(m) \setminus n} \alpha_{n'm} \times \frac{\min_{n' \in N(m) \setminus n} \beta_{n'm}}{c} \quad (19)$$

단 c 는 1보다 큰 상수이다.

그림 1은 (8000, 4000, 3) 균일 LDPC 부호의 오류 성능을 MSA 복호 기법과 NMSA 복호 기법에 따라 모의실험 결과를 통해 나타낸 것이다. 그림에서 NMSA 복호 기법의 오류 성능은 MSA 복호 기법의 오류 성능에 비해 약 0.31[dB]의 부호 이득을 보여준다.

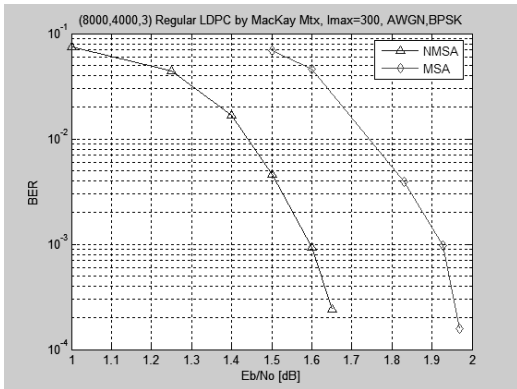


그림 1. 복호 기법에 따른 (8000,4000,3) 균일 LDPC 부호의 오류 성능
Fig. 1. BER performance of LDPC code, (8000,4000) regular, with NMSA, MSA

III. 체크 노드 메시지의 근사 화와 이를 이용한 복호 기법

로그 계에서 동작되는 SPA 알고리즘의 체크 노드 메시지 값은 식 (5)~(9)와 같이 지수함수와 로그 함수가 결합된 복잡한 형태의 $\phi(x)$ 함수 계산을 통해 이루어진다. $\phi(x) = -\log[\tanh(x/2)]$ 이며 이를 그래프로 나타내면 그림 2와 같다.

그림에서 볼 수 있는 바와 같이 $\phi(x)$ 함수는 $1/x$ 또는 $1/x^2$ 함수와 유사함을 알 수 있으며 식 (20)과 같이 근사 화 할 수 있다.

$$\phi(x) \approx f(x) = \begin{cases} \frac{1}{(x+a)}, & x < 1 \\ \frac{1}{(x+b)^2}, & else \end{cases} \quad (20)$$

여기에서 a, b 는 상수이며, 그림 2는 $a=b=0.24$ 를 이용하여 근사 화한 결과를 나타낸 것이다. 함수 $\phi(x)$ 에 비해 근사 화된 함수 $f(x)$ 는 $x < 1$ 일 때에는 나뭇셈 한번으로 계산되고 $x > 1$ 일 때에는 곱셈 한 번과 나뭇셈 한 번이면 모든 연산이 끝남을 알 수 있다. 따라서 $\phi(x)$ 를 사용할 때 보다 $f(x)$ 를 사용하여 체크 노드 메시지 값을 계산하게 되면 연산량이 크게 줄어 들 수 있음을 알 수 있다. 식 (21)은 근사 화된 함수 $f(x)$ 를 이용하여 체크 노드 메시지를 나타낸 것이다.

$$L_{m \rightarrow n}^{Proposed}(x_n) = \prod_{n' \in N(m) \setminus n} \alpha_{n'm} \times f\left(\sum_{n' \in N(m) \setminus n} f(\beta_{n'm})\right) \quad (20)$$

체크 노드 메시지 갱신과정을 제외한 나머지 과정은 SPA 혹은 MSA 기법과 동일하다.

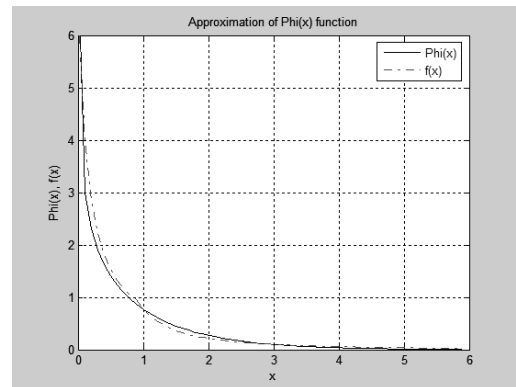


그림 2. $\phi(x)$ 와 근사 화된 $f(x)$ 함수의 비교
Fig. 2. comparison between $\phi(x)$ and approximated $f(x)$

IV. 모의실험 및 결과 분석

그림 3은 AWGN 채널에서 각 복호 기법에 대해 LDPC 부호의 오류성능을 모의 실험하여 얻은 결과를 나타낸 것이다. 변조 방식은 BPSK 방식을 가정하였으며 LDPC 부호는 (8000,4000,3) 균일 LDPC 부호를 선택하였고 시뮬레이션 방식은 Monte-Carlo 방식을 사용하였다. 전송된 정보 비트 수는 최소 10^6 개의 비트를 전송하였으며 각 복호 방식의 최대 반복 복호 회수는 $I_{max} = 300$ 번으로 제한하였다. LDPC 부호의 패리티 체크 행렬에 길이가 짧은 사이클이 존재하는 경우 MSA 알고리즘은 발진할 가능성이 있는데 이를 방지하기 위해 검증된 Mackay 행렬을 이용하여 실험을 수행하였다.

그림에서 알 수 있듯이 SPA 방식과 MSA 방식은 약 0.5[dB]의 부호 이득 차이를 보이며 MSA를 개선한 NMSA의 경우 MSA 보다는 약 0.3[dB]의 부호 이득 개선을 보여 주지만 SPA에 비해 여전히 0.2[dB] 이상의 성능 저하를 나타냄을 알 수 있다.

그림 4는 AWGN 채널에서 제안된 복호 기법에 대해 LDPC 부호의 오류성능을 모의 실험하여 얻은 결과를 나타낸 것이다. 변조 방식은 BPSK 방식을 가정하였으며 LDPC 부호는 (8000,4000,3) 균일 LDPC 부호를 선택하였고 최대 반복 복호 회수는 $I_{max} = 200$ 번으로 제한하였다. 그림에서 SPA 방식의 오류 성능과의 이득 차이는 약 0.1[dB] 이하로 개선되었음을 볼 수 있으며 MSA 및 NMSA와의 이득 차이는 각각 0.45[dB] 및 0.15[dB]의 부호 이득 차이가 존재함을 알 수 있다.

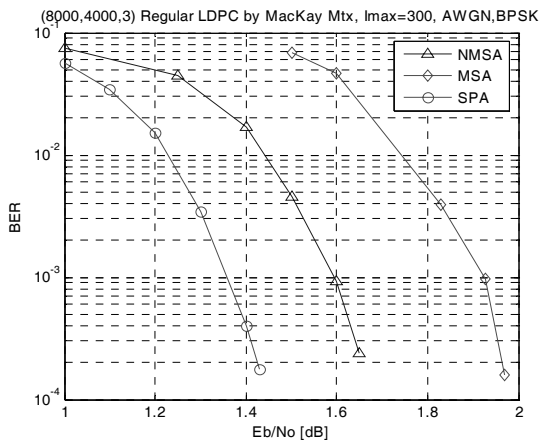


그림 3. 복호 기법에 따른 (8000,4000,3) 균일 LDPC 부호의 오류 성능
 Fig. 3. BER performance of LDPC code, (8000,4000) regular, by decoding algorithms

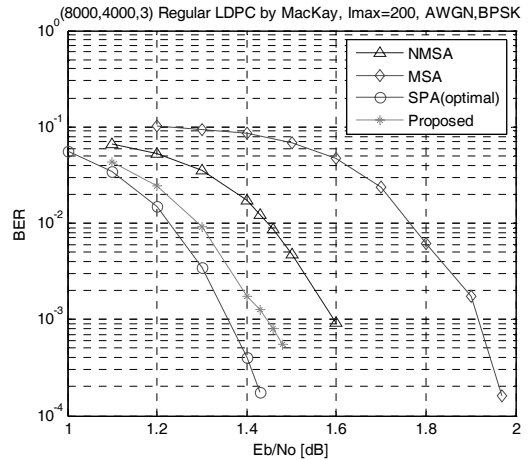


그림 4. (8000,4000,3) 균일 LDPC 부호의 오류 성능 (Imax = 200, AWGN, BPSK)
 Fig. 4. BER performance of (8000,4000) regular LDPC code (Imax = 200, AWGN, BPSK)

V. 결론

본 논문에서는 체크 노드 메시지 함수를 역함수 형태로 근사 화하여 복잡 도를 개선한 복호 알고리즘을 제안하고 Monte-Carlo 시뮬레이션 기법을 이용하여 AWGN 채널에서 제안된 복호 알고리즘의 성능을 모의실험 하였다. SPA, MSA 및 NMSA 알고리즘에 대해서도 모의실험을 수행하여 그 결과를 비교 분석하였다.

실험 결과 SPA 방식과 MSA 방식은 약 0.5[dB]의 부호 이득 차이를 보였으며 MSA를 개선한 NMSA의 경우 MSA 보다는 약 0.3[dB]의 부호 이득 개선을 보여 주지만 SPA에 비해 여전히 0.2[dB] 이상의 성능 저하를 나타냄을 알 수 있었다. 본 논문에서 제안한 복호 방식은 SPA 방식에 비해 부호 이득 차이가 약 0.1[dB] 이하로 개선되었음을 볼 수 있었으며 MSA 및 NMSA와의 이득 차이는 각각 0.45[dB] 및 0.15[dB]의 부호 이득 차이가 존재함을 알 수 있었다.

향 후 불 균일 LDPC 부호의 경우에 대한 제안된 알고리즘의 적용이 필요하며 길이가 짧은 LDPC 부호에 대한 적용과 성능 실험이 요구된다.

참고 문헌

[1] Valentin Savin, "Self-Corrected Min-Sum Decoding of LDPC Codes," ISIT-08, July 7, 2008.

- [2] J. Jhang and Marc Fossorier, "Improved Min-Sum Decoding of LDPC Codes Using 2-Dimensional Normalization," Global Telecommunications Conference-2005, GLOBECOM , Volume 3, Issue, 28 Nov.-2 Dec. pp. 6, 2005.
- [3] J. Chen and M. P. Fossorier, "Near Optimum Universal Belief Propagation Based Decoding of Low Density Parity Check Codes," IEEE Trans. on Comm., 50(3) : 406-414, 2002.
- [4] Jinghu Chen, Ajay dholakia, Evangelos Eleftheriou, M. P. C. Fossorier, and Xiao-Yu Hu, "Reduced-Complexity Decoding of LDPC codes," IEEE Transactions on Communications, Vol.53, No.8, August 2005.
- [5] R. G. Gallager, Low-Density Parity-Check Codes. Cambridge, MA:M.I.T. Press, 1963.
- [6] William E. Ryan, "An Introduction to LDPC Codes", in CRC Handbook for Coding and Signal Processing for Recoding Systems (B. Vasic, ed.), CRC Press, 2004.

정 호 영 (Ho-Young Cheong)

정회원



1986년 2월 충남대학교 전자공학
교육학과

1989년 8월 연세대학교 본 대학
원 전자공 학과(석사)

1994년 2월 연세대학교 본 대학
원 전자공학과(공학박사)

1995년 4월~현재 남서울대학교
정보통신공학과 부교수

<관심분야> 부호이론, 이동통신, RFID 등

김 신 령 (Sin-Ryeong Kim)

정회원



1983년 2월 경북대학교 전자공
학과(학사)

1985년 2월 연세대학교 본 대학
원 전자공학과(공학석사)

1990년 2월 연세대학교 본 대학
원 전자공학과(공학박사)

1992년 9월~현재 동서울대학 전
자통신과 교수

<관심분야> 부호이론, 위성통신 등