높은 무게 LDPC 부호의 저복잡도 고성능 복호 알고리즘

정회원 조 준 호*, 성 원 용*

High-Performance and Low-Complexity Decoding of High-Weight LDPC Codes

Junho Cho*, Wonyong Sung* *Regular Members*

요 약

Low-density parity-check (LDPC) 부호의 복호에는 성능이 좋은 합곱 알고리즘(sum-product algorithm; SPA)과 하드웨어가 간단한 비트 반전(bit-flipping; BF) 알고리즘이 많이 쓰이고 있다. 본 논문은 이들 두 가지 방법의 장점을 가지는 저복잡도 고성능 복호 알고리즘을 제안한다. 본 제안된 유연 비트 반전(soft bit-flipping) 알고리즘은 비트와 체크 노드 사이에 전달되는 메시지를 계산하는 데 단순한 비교와 덧셈 연산만을 필요로 하며 연산량이 적다는 장점이 있다. 또한 연산이 완료된 메시지의 활용률을 높이고 비균등 양자화(non-uniform quantization)를 채용하여 1000 내외의 부호 길이에서 SPA 에 0.4dB 근접하는 신호대 잡음비(signal-to-noise ratio)를 달성하였다. 본 논문에서 제안된 알고리즘을 이용하면, 행 무게(row weight)와 열 무게(column weight)가 높아서 종래의 SPA로 구현하기 어려웠던 부호를 비교적 좋은 오율 성능을 유지하면서 실용적으로 구현할 수 있다.

Key Words : LDPC codes, Decoding, Low complexity, Soft bit-flipping, Sum-product.

ABSTRACT

A high-performance low-complexity decoding algorithm for LDPC codes is proposed in this paper, which has the advantages of both bit-flipping (BF) algorithm and sum-product algorithm (SPA). The proposed soft bit-flipping algorithm requires only simple comparison and addition operations for computing the messages between bit and check nodes, and the amount of those operations is also small. By increasing the utilization ratio of the computed messages and by adopting nonuniform quantization, the signal-to-noise ratio (SNR) gap to the SPA is reduced to 0.4dB at the frame error rate of 10-4 with only 5-bit assignment for quantization. LDPC codes with high column or row weights, which are not suitable for the SPA decoding due to the complexity, can be practically implemented without much worsening the error performance

Ⅰ. 서 론

1960년대 초 Gallager에 의하여 고안된 low-density parity-check(LDPC) 부호[1]는 MacKay 등에 의하여 채널 용량에 근접하는 우수한 복호 성능을 보임이 밝혀짐에 따라[2] 최근 오류 정정 부호의 분야에서 중요한 연구 주제로 부각되었다. 전통적인 LDPC 부호의 복호 방식을 신호의 검출 방법에 따라 크게 두 가지로 분류하면, 0이나 1로 엄격하게 결정(hard-decision)된 신호에 대하여 복호를 시도하는 비트 반전(bit-flipping; BF) 방식과 실수(real number) 범위에서 다단계의 값을 가지는(soft-decision) 신호에 대하여 복호를 시도하는 합곱 알고리즘(sum-product algorithm; SPA)으로 나눌 수 있다. BF 알고리즘은 비트 노드와 체크 노드를

※ 본 연구는 교육과학기술부의 BK21 사업, 그리고 하이닉스 반도체 주식회사의 지원으로 수행되었습니다.
* 서울대학교 전기컴퓨터공학부 멀티미디어시스템 연구실(juno@dsp.snu.ac.kr, wysung@snu.ac.kr)
논문번호 : KICS2008-12-559, 접수일자 : 2008년 12월 7일, 최종논문접수일자 : 2009년 4월 13일

갱신(update)하는 방식이 매우 간단하고 두 노드 사이에 교환되는 메시지의 크기가 1 비트에 불과하기 때문에 구현이 매우 쉽지만 에러 정정 성능이 SPA 에 비하여 크게 뒤떨어진다. 반면 SPA 는 일반적으로 LDPC 부호의 복호 알고리즘 가운데 가장 우수한 오류 정정 성능을 보이는 것으로 알려져 있으나 체크 노드 업데이트에 쌍곡선 삼각함수(hyperbolic trigonometric function)를 이용해야 하며 이상적인 메시지는 무한대의 정밀도를 가져야 하기 때문에 구현의 복잡도가 지나치게 높다는 단점이 있다.

이에 따라 오류 정정 성능을 크게 저하시키지 않으면서도 구현 상의 복잡도를 줄이기 위하여 다양한 연구가 지속적으로 수행되고 있다. BF 알고리즘의 성능을 개선하는 시도로서 가중치 비트 반전(weighted bit-flipping; WBF) 알고리즘 등[3]-[5]이 제안되었고, 다른 한편으로 SPA의 복잡도를 줄이기 위하여 최소값합(min-sum; MS) 알고리즘 등[6]-[7]에 대한 연구도 수행되었다. 지금까지의 연구 결과를 보면, 이상적인 SPA 에 필적하는 높은 에러 정정 성능을 얻을 수 있었던 알고리즘들은 기본적으로 신뢰 전파(belief propagation)를 위한 외부(extrinsic) 메시지를 연산할 때 메시지를 전달받을 노드로부터 오는 메시지를 제외하고 나머지 유입되는(incoming) 모든 메시지들에 합이나 곱의 연산을 수행하기 때문에 패리티 행렬의 열 무게(column weight) d_v와 행 무게(row weight) d_c의 제곱에 비례하는 $O(d_v^2+d_c^2)$의 연산 복잡도를 요구하고 있다[9]. 따라서 구현에 관한 모든 문헌은 전체 유입 메시지의 합과 곱을 먼저 계산하고 나중에 전달 대상 노드로부터의 메시지를 제외하는 방식의 연산량 최적화를 통하여 $O(d_v+d_c)$의 선형적인 연산 복잡도를 달성하는 구현 방법을 사용하고 있다[9]. 그러나 이러한 최적화를 위해서는 SPA에서는 추가적으로 나눗셈기나 뺄셈기가 필요하며[8], MS 알고리즘에서는 두 개의 최소값을 빠른 시간 안에 찾는 하드웨어의 구현이 쉽지 않고 저장 공간도 추가로 필요하다는 단점이 있다[9]. 이러한 까닭으로 기존의 SPA 또는 MS 방식의 LDPC 복호는 3이나 6 정도의 매우 낮은 열 무게 또는 행 무게를 가지는 경우로 실시간 구현이 제한이 되어 왔다.

본 논문에서는 SPA 와 BF 알고리즘의 장점을 고루 반영하여 유연한 비트 반전(soft bit-flipping; SBF)을 이용한 LDPC 의 복호 알고리즘을 제안하고자 한다. 제안된 알고리즘은 외부 메시지로부터 전달되는 정보를 내부(intrinsic) 메시지에 유연하게 결합하여 이후의 반복 복호(iterative decoding) 과정에서 계속해서 이용함으로써 성능을 높이는 SPA 의 장점을 가지고 있다. 또한 비트 노드와 체크노드에서 상대편 노드로 전달하는 메시지가 단일하기 때문에 패리티 행렬의 행 무게와 열 무게에 선형적으로 비례하는 $O(d_v+d_c)$의 연산 복잡도를 갖는 BF 알고리즘의 장점도 가지고 있다.

본 논문은 다음과 같은 순서로 SBF 알고리즘을 제안하고 그 성능을 검증하고자 한다. 제 II장은 WBF 알고리즘과 improved modified WBF (IMWBF) 알고리즘에 대하여 소개한다. 그리고 이를 더욱 개선하기 위하여 본 논문에서 제안하는 SBF 알고리즘을 제 III 장에서 설명한다. 제 IV장에서는 다양한 LDPC 복호 알고리즘의 성능 실험 결과를 비교하고, 제 V장에서 결론을 제시한다.

II. WBF와 IMWBF 알고리즘

Gallager에 의해 제안된 BF 알고리즘은 패리티 체크 방정식에 모두 동일한 가중치를 부여했지만, 이를 개선한 WBF 알고리즘[3]은 각 체크에 관여되는 비트 가운데 신호의 크기가 가장 작은 것을 방정식의 가중치로 부여함으로써 패리티 체크 방정식의 신뢰성을 차등화하는 방법을 사용하였다. WBF 알고리즘을 개선한 IMWBF 알고리즘[5]은 WBF와 마찬가지로 체크 방정식에 가중치를 부여하여 복호를 수행하지만 가중치의 값을 결정하는 방법이 다르다. 다시 말해 WBF는 각 체크에 연결된 비트의 정보를 모두 이용하는 반면에, IMWBF는 자기 자신으로부터 제공된 정보를 제거한 후에 메시지를 전달받는 것이다.

IMWBF 알고리즘을 소개하기 위하여 먼저 M 행 N열의 패리티 체크 행렬 $H=[h_{m,n}]$에 의하여 정의된 (d_v, d_c) 규칙 LDPC 부호를 가정하자. 신호는 AWGN(additive white Gaussian noise) 채널에서 BPSK(binary phase-shift keying) 변조를 이용하여 전송하며, 부호어 $c=(c_1,c_2,\cdots,c_N)$은 $x_n=2c_n-1, n\in[1,N]$의 규칙에 의하여 이진 벡터 $x=(x_1,x_2,\cdots,x_N)$으로 변환된다고 하자. 만약 채널에 평균이 0이고 분산이 $N_0/2$인 백색 가우시안 잡음(white Gaussian noise) v_n이 존재한다면 수신된 신호 $y=(y_1,y_2,\cdots,y_N)$은 $y_n=x_n+v_n, n\in[1,N]$로 표현할 수 있다. 이 때 m번째 체크에 관여하는 비트의 집합을 $B(m)=\{n|h_{m,n}=1\}$이라 하고 n번째 비트에 관여하는 체크의 집합을 $A(n)=\{m|h_{m,n}=1\}$이라 하자. 그러면 엄격결정 벡터

(hard-decision vector) $z=(z_1,z_2,\cdots,z_N)$의 값은 y_n이 양수이면 z_n=1, 음수이면 z_n=0으로 정해지며, 신드롬 $s=(s_1,s_2,\cdots,s_N)=zH^t$는 다음의 식 (1)에 의하여 정의된 체크로부터 구할 수 있다.

$$s_m=\sum_{n\in B(m)} z_n h_{m,n}. \quad (1)$$

또한 IMWBF 알고리즘에서 n번째 비트로부터 m번째 체크로 전달되는 메시지의 가중치 $w_{n\to m}$은 다음과 같이 정의된다.

$$w_{n\to m}=\min_{i\in B(m)\setminus n}|y_i|,\ m\in[1,M];n\in B(m). \quad (2)$$

관여된 비트의 최소값으로 체크에 부여되는 가중치를 결정하는 것은, 이상적인 SPA 에서 tanh(hyperbolic tangent) 법칙에 의해 정의되는 체크의 LLR(log-likelihood ratio) 값이 비트의 최소값으로 근사화된다는 사실에 기인한다[6].

위에서 설명한 가정과 정의를 기반으로 하여, IMWBF 알고리즘은 다음 순서에 따라 복호를 수행한다.

초기화 : 반복 회수 k를 0으로 초기화하고 최대 반복 회수 K_{MAX}를 설정한다. 수신된 신호로부터 $n\in[1, N]$, $m\in[1, M]$에 대하여 가중치 $w_{n\to m}$를 모두 구한다.

1단계 : 신드롬 벡터 $s^k=z^kH^t$를 계산한다. 만약 s^k가 영벡터이면 z^k를 부호어로 출력하고 복호를 성공적으로 종료한다.

2단계 : 모든 비트에 대하여 다음과 같이 정의된 반전 함수 (flipping function) 를 계산한다.

$$e_n^k=\sum_{m\in A(n)}(2s_m^k-1)w_{n\to m}-\alpha|y_n|.$$

3단계 : 다음의 비트 n^*를 반전함으로써 엄격결정 벡터 z^{k+1}을 갱신한다.

$$n^*=\arg\max_{n\in[1,N]} e_n^k.$$

4단계 : 반복 회수 k를 $k+1$로 증가시키고 1단계로 돌아간다. 만약 $k>K_{MAX}$가 되어 반복 회수 제한을 넘으면 복호 실패를 선언하고 복호를 종료한다.

여기서 복호 과정 2단계의 가중치 인수 α는 신호대 잡음비(signal-to-noise ratio; SNR)에 따라 다른 최적값을 갖는 양의 실수이다.

Ⅲ. SBF 알고리즘의 제안

IMWBF 알고리즘은 WBF의 체크 연산 과정에 SPA의 방법론을 적용함으로써 성능 향상을 도모하고 있지만 몇 가지 한계를 가지고 있다. 첫 번째는 복호의 반복 과정 전반에 걸쳐서 수신된 벡터 y가 그대로 유지되고 단지 엄격결정 벡터 z만이 매번 갱신된다는 점이다. 따라서 복호 반복 도중에 각 비트가 외부로부터 새로 얻게 되는 정보가 매우 제한적이며 최초에 내부에 가지고 있던 정보가 지배적인 영향을 계속 유지하게 된다. 두 번째로, 한 번의 복호 반복에서는 가장 큰 반전 함수값을 갖는 한 개나 소수 개의 엄격결정 비트만이 반전될 뿐이고 나머지 비트들은 어떠한 영향도 받지 않는다는 점이다. 체크 연산에 의해 이미 알게 된 추가 정보의 상당부분이 그대로 낭비되는 셈이다. 세 번째로 Gallager의 BF 알고리즘이 가지고 있던 장점인, 작은 저장 공간과 간단한 연산이라는 성질을 상당 부분 잃게 되어, 강력한 복호 성능을 보이면서도 구현이 상당히 용이한 MS 알고리즘에 대한 비교 우위가 불확실하다.

이러한 단점들을 극복하기 위하여 본 논문이 제안하는 복호 알고리즘은 다음과 같다. 먼저 각 패리티 체크 방정식에 부여되는 가중치는, 그에 관여되는 비트의 최소값이 아니라 비트의 총합으로서 결정된다. 즉 m번째 체크에 부여되는 가중치는 다음 식 (3)과 같이 정의된다.

$$w'_m=\sum_{i\in B(m)}|y_i|,\ m\in[1,M]. \quad (3)$$

이것은, SPA 에 주로 쓰이는 LLR 을 사용하지 않고 LD(likelihood difference)를 사용하면 비트로부터 오는 메시지의 곱에 의해 체크의 값을 계산할 수 있다는 데에 이론적 근거를 두고 있다[7]. LD로부터 식 (3)을 유도하는 더욱 자세한 과정은 본 논문의 부록에 수록되어 있다. 식 (3)과 같이 변경된 가중치를 이용하면, Gallager의 BF 알고리즘처럼 체크 하나는 한 종류의 메시지만 보내기 때문에 복잡도가 낮아진다. 예를 들어 행 무게와 열 무게가 모두 33인 부호를 사용한다면 SPA나 IMWBF를 최적화 없이 바로 구현하기 위해서는 비트와 체크 노드 당 32(연산/메시지)×33(메시지/노드)=1056(연산/노드)회의 연산이 필요하지만, SBF에서는 노드 당 32회의 연산이 필요할 뿐이다. 이 경우 기존의 MS 알고리즘에서는 트리(tree) 구조로 최소값 두 개를 찾는 방식으로 노드 당 연산 수를 37회로 줄일 수 있지만[9], 트리 구조를 탐색 (traverse)하

는 하드웨어의 구현이 어렵고 체크 노드 한 개에 최소값 두 개가 저장되어야 하기 때문에 체크 노드를 위한 저장 공간이 SBF보다 두 배 소요된다. 한편, SBF의 반전 함수는 IMWBF와 동일한 것을 사용하지만, 반전 함수의 계산 결과를 이용하여 수신 벡터의 신뢰도를 향상시키는 방법은 차이가 있다. 즉, 가장 큰 반전 함수값을 가지는 엄격결정 비트만이 반전되는 방식이 아니고, 반전 함수값을 미리 정의된 순차적인 크기의 여러 임계값과 비교하여 y_i 자체를 변경하는 방식이다. 이 때, 반전 함수가 크면 클수록 y_i 가 반대편 신호 방향으로 이동되는 정도가 크도록 한다. 반대로 반전 함수가 매우 작다면 y_i 는 자신의 신호 크기를 강화하는 방향으로 갱신된다. 이처럼 반전 함수가 수신 신호의 갱신에 반영되는 정도가 비례적이기 때문에, 즉 유연하기 때문에 본 알고리즘을 '유연한 비트 반전(soft bit-flipping) 알고리즘'이라 지칭하기로 한다. 유연한 비트 반전 방식은 IMWBF가 가지는 두 가지 단점, 즉 비트 노드 반전 결과가 다음 체크 값 계산에 불완전하게 전파되고 상당 부분 단절된다는 점과 반전 함수가 제공하는 정보가 비트 반전 과정에서 극소량 반영되고 대부분 손실된다는 점을 동시에 극복할 수 있다. SBF 의 동작 원리는 SPA 가 외부 정보를 이용하여 수신 신호의 신뢰도를 반복적으로 높여나가는 것과 근본적으로 일맥상통한다.

SBF 알고리즘을 실제 회로로 구현할 때, 수신된 신호와 비트 노드, 체크 노드에 저장되는 신호를 모두 q 비트로 양자화하는 상황을 가정하자. 이 때 비트 노드와 체크 노드는 2^q-1개의 임계값 $\delta_1^b < \cdots < \delta_{2^{q-2}}^b = 0 < \cdots < \delta_{2^q-1}^b$과 $\delta_1^c < \cdots < \delta_{2^{q-2}}^c = 0 < \cdots < \delta_{2^q-1}^c$를 경계로 하여 ± 0을 제외한 부호-크기(sign-magnitude)의 방식으로 각각 양자화되며, 비트 반전의 강도는 임계값 $\delta_1^f < \delta_2^f < \delta_3^f$에 의해 정해진다고 하자. 그러면 SBF 알고리즘은 다음 순서에 따라 복호를 수행한다.

초기화 : 반복 회수 k를 0으로 초기화하고 최대 반복 회수 K_{MAX}를 설정한다.

1단계 : 신드롬 벡터 $s^k = z^k H^t$를 계산한다. 만약 s^k가 영벡터이면 z^k를 부호어로 출력하고 복호를 성공적으로 종료한다.

2단계 : 경계값 $\delta_i^b (i \in [1, 2^q-1])$에 따라 $y_n^k (n \in [1, N])$을 q비트로 양자화한 후, 식 (3)에 의해 정의된 체크 노드 m의 가중치 $w_m^{k'} (m \in [1, M])$를 계산하고 $\delta_i^c (i \in [1, 2^q-1])$를 경계로 하여 양자화한다.

3단계 : 모든 비트에 대하여 다음과 같이 정의된 반전 함수를 계산한다.

$$e_n^{k'} = \sum_{m \in A(n)} (2s_m^k - 1) w_m^{k'} - \alpha |y_n^k|.$$

4단계 : 반전 함수에 따라 각 비트 노드에 다음과 같이 유연한 반전을 수행한다.

i) $e_n^{k'} \in (\delta_3^f, \infty)$일 때

$y_n^{k+1} = \mathrm{sgn}(y_n^k - 2.5) \cdot \max(1, |y_n^k| - 2)$ (비트의 강한 반전),

ii) $e_n^{k'} \in (\delta_2^f, \delta_3^f]$일 때

$y_n^{k+1} = \mathrm{sgn}(y_n^k - 1.5) \cdot \max(1, |y_n^k| - 1)$ (비트의 약한 반전),

iii) $e_n^{k'} \in (\delta_1^f, \delta_2^f]$일 때

$y_n^{k+1} = \mathrm{sgn}(y_n^k) \cdot |y_n^k|$ (비트의 유지),

iv) $e_n^{k'} \in (-\infty, \delta_1^f]$일 때,

$y_n^{k+1} = \mathrm{sgn}(y_n^k) \cdot \min(2^q, |y_n^k| + 1)$ (비트의 강화).

어떤 비트 노드에서도 반전이 일어나지 않는다면 $\delta_3^f = \max_n e_n^{k'}$, $\delta_2^f = \delta_3^f - \beta$로 조정한다.

5단계 : 반복 회수 k를 $k+1$로 증가시키고 1단계로 돌아간다. 만약 $k > K_{MAX}$가 되어 반복 회수 제한을 넘으면 복호 실패를 선언하고 복호를 종료한다.

여기서 복호 과정 4단계의 임계값 조정 상수 β는 q에 따라 다른 최적값을 갖는 양의 정수이다.

Ⅳ. 모의 실험 결과

본 논문에서는 유한체(finite field) 위의 사영 기하학(projective geometry; PG)에 존재하는 점과 선, 면에 의하여 생성되는 PG-LDPC 부호[3]를 이용하여 SBF의 성능을 검증하였다. PG-LDPC 부호는 생성 과정에서 본질적으로 주기성을 내포하게 된다. PG-LDPC 부호는 패리티 행렬의 행 무게와 열 무게가 큰 단점이 있지만 비슷한 길이와 부호율을 갖는 LDPC 부호 가운데 가장 좋은 오류 정정 성능을 보이는 것으로 알려져 있다. 특히 BF 알고리즘과 WBF 알고리즘에서 Gallager

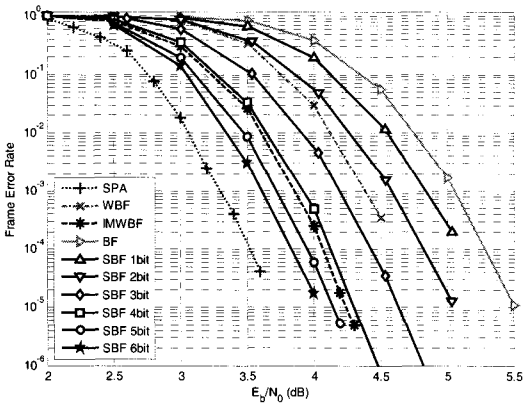


그림 1. 부호율 0.77 인 (1057, 813) PG-LDPC 부호의 블록 오율 성능 (Block error rate of rate 0.77 (1057, 813) PG-LDPC code)

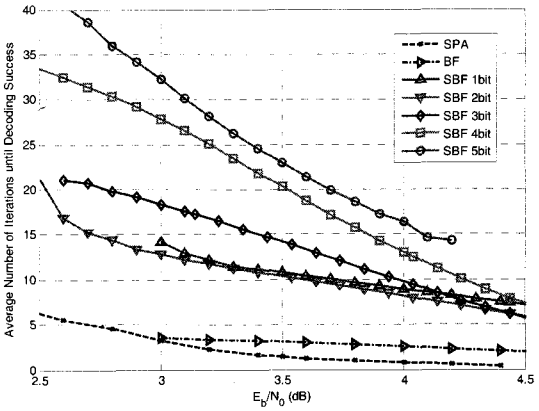


그림 2. (1057, 813) PG-LDPC 부호의 복호 성공까지 필요한 평균 반복 회수 (Average number of iterations until decoding success of (1057, 813) PG-LDPC code)

부호보다 월등한 성능을 보이는데, 두 알고리즘에서는 행과 열의 무게가 구현의 복잡도에 중대한 영향을 미치지 않기 때문에, 주기성을 갖는 특성과 더불어 구현이 용이하면서도 복호 성능이 매우 뛰어난 부호이다.

그림 1은 부호율이 0.77이고 행 무게와 열 무게가 모두 33인 (1057, 813) PG-LDPC 부호의 블록 오율 (frame error rate; FER)성능을 보여준다. 그래프에서 WBF와 IMWBF 알고리즘, 3~6비트 SBF 알고리즘은 복호의 최대 반복 회수를 200회로 제한하였고 SPA와 1~2비트 SBF 알고리즘은 50회로 제한하였다. SBF는 양자화에 할당된 비트 수를 1비트에서 6비트까지 변화시키며 오율을 측정하였고, 다른 복호 알고리즘들은 부동 소수점(floating point)을 이용한 결과이다. SBF의 양자화에 할당된 비트 수를 점차 늘릴 때 2비트 이하에서는 SBF가 WBF 보다 좋지 않은 성능을 보이나, 불과 3비트 만으로도 부동 소수점의 WBF를 능가하는 성능을 보이기 시작한다. 5비트에 도달하면 IMWBF 보다 좋은 성능을 보이고, 10^{-4}의 블록 오율에서 SPA 에 약 0.4dB 정도까지 근접하는 성능을 나타낸다. 비트 수를 증가시켜도 지속적으로 성능 향상이 이루어지고 있으나 4비트 이상에서는 다소 향상의 정도가 줄어든다.

다음은 SBF 의 복호 속도에 대한 분석이다. 복호가 성공할 때까지 필요한 평균 반복 회수를 t_{avg}라 하자. 최대 반복 회수를 t_{max}라 하고 블록 에러율을 ϵ_f라 하면, 복호의 성공과 실패를 모두 포함하여 소요되는 총 소요시간의 기대값은 $\epsilon_f \cdot t_{max} + (1-\epsilon_f) \cdot t_{avg}$로 계산할 수 있다. 따라서 복호에 소요되는 시간은 복호의 성공률과 복호 수렴 속도에 동시에 영향을 받는다. SBF 알고리즘을 이용하여 (1057, 813) PG-LDPC 부호를 복호할 때 복호가 성공할 때까지 소요되는 반복 회수(t_{avg})를 그림 2에 도시하였다. 그림에서 볼 수 있듯이 SBF 알고리즘은 BF 알고리즘이나 SPA 에 비하여 복호 수렴 속도가 훨씬 느리며, 할당된 비트 수가 늘어날수록 더욱 더 느려진다. 이것은 SBF 복호 중 비트 반전 단계 (제 4단계) 에서 양자화 비트 수에 따라 비트의 동적 영역 (dynamic range)이 $[-2^{q-1}, 2^{q-1}]$으로 지수적으로 증가하는 반면에 비트 반전의 강도는 1이나 2 정도로 유지되기 때문이다. 즉 SBF 알고리즘은 비트가 포함하고 있는 정보를 보수적으로 변화시킴으로써, 에러일 가능성이 매우 높은 비트부터 반전하기 시작하여 복호 반복이 진행되면서 순차적으로 반전하는 방식으로 복호의 성공률을 높이는 것이다. 복호 수렴 시간이 길다는 단점은 문헌 [3]에서 제시한 방법과 유사하게 BF와 SBF를 모두 이용하는 2 단계

표 1. 오율 성능 실험에 사용한 임계값 (Threshold values used in the error performance simulation)

(a) $q = 2\ (\alpha = 6, \beta = 5)$

	δ^b	δ^c	δ^f
δ_1	-0.767	-53	-41
δ_2	0	0	25
δ_3	0.767	53	32

(b) $q = 3\ (\alpha = 10, \beta = 5)$

	δ^b	δ^c	δ^f
δ_1	-1.140	-99	-94
δ_2	-0.710	-95	34
δ_3	-0.315	-90	60
δ_4	0	0	·
δ_5	0.315	90	·
δ_6	0.710	95	·
δ_7	1.140	99	·

(c) $q = 4\ (\alpha = 23, \beta = 5)$

	δ^b	δ^c	δ^f
δ_1	-1.436	-197	-259
δ_2	-1.120	-191	42
δ_3	-0.880	-187	98
δ_4	-0.666	-183	·
δ_5	-0.459	-179	·
δ_6	-0.258	-174	·
δ_7	-0.091	-168	·
δ_8	0	0	·
δ_9	0.091	168	·
δ_{10}	0.258	174	·
δ_{11}	0.459	179	·
δ_{12}	0.666	183	·
δ_{13}	0.880	187	·
δ_{14}	1.120	191	·
δ_{15}	1.436	197	·

혼성 복호(2-stage hybrid decoding)를 통하여 극복이 가능하다. 즉, 수렴 속도가 매우 빠른 BF 알고리즘으로 최대 5회 이하의 반복 회수를 부여하여 먼저 복호를 시도한 후에 실패하는 경우에만 느리지만 복호 성공률이 높은 SBF 알고리즘으로 2차 복호를 시도하는 방식이다. BF와 SBF 두 가지 알고리즘은 매우 비슷한 구조로 동작하기 때문에 복호 회로를 공유하면서 약간의 추가 제어 신호 만을 이용하여 복호 시간을 단축시킬 수 있을 것으로 예측된다.

표 1에는 양자화 비트가 2~4인 경우의 성능 모의 실험에 사용한 여러 가지 임계값을 정리하였다. 표에서 보는 바와 같이 SBF 알고리즘에는 $2\times(2^q-1)+5$개의 파라미터가 필요하기 때문에 비트 수가 늘어나면 필요한 파라미터의 수가 많아진다. 이 가운데 하나의 파라미터를 변경하면 다른 파라미터들이 영향을 받기 때문에 여러 파라미터의 최적 조합을 찾는 것은 시간을 요하는 일이다. 파라미터 값을 결정하기 위해서는 먼저 SBF의 복호 과정에서 비트와 체크 노드가 어떤 분포를 갖는가를 알아야 하고, 파라미터의 이동으로 인하여 그 분포가 어떻게 변화되는가를 알아야 한다. 그러나 통계적으로 조사된 비트와 체크의 분포에 Lloyd-Max의 양자화 방법을 적용하여 구한 임계값이 실험 결과 좋은 복호 성능을 보이지는 않았는데, 이것은 일반적인 양자화의 효율성이 필연적으로 복호 성능의 향상을 가져오지는 않기 때문으로 보인다. 본 논문에서는 부록에 유도된 바와 같이 LD의양자화를 위하여 지수 함수 a^{x_p}를 쓰는 대신에, 양의 구간에서 x_p가 증가할수록 지수함수처럼 기울기가 증가하면서도 x_p가 1에 접근할수록 함수 값이 무한대로 발산하는 역 오류 함수(inverted error function) $erf^{-1}(x_p)$를 사용하였다. 여기서 오류 함수는 $erf(x)=\frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$로 정의된다. 지수 함수 a^{x_p}가 밑 $a>1$를 어떤 값으로 선택하더라도 x_p가 충분히 작은 음의 정수가 되면 a^{x_p}와 a^{x_p+1} 사이의 구간이 너무 좁아져서 양자화 효율이 떨어지는 단점이 있는 반면에, 역 오류 함수는 x축에 정의된 구간이 $[-1,1]$로 한정되어 있기 때문에 양자화 비트수가 늘어나서 x축을 따라 많은 구간으로 양자화가 되어도 양자화 효율이 크게 줄어들지 않는다. 목적 함수(objective function)를 오율 성능으로 두고 모의 담금질(simulated annealing)을 통하여 파라미터의 최적 조합을 찾는 방법도 있겠지만 이 또한 너무 많은 시간을 필요로 하여 실용성이 없었다. 따라서 SBF 알고리즘에 사용되는 비균등 양자화의 양자화 구간을 효율적으로 설정하는 분석적인(analytic) 방법이 연구된다면 장시간의 모의 실험을 하지 않고도 좋은 오율 성능에 도달할 수 있을 것이다.

V. 결 론

본 논문에서는 오율(error rate) 성능이 좋으면서도 하드웨어 복잡도가 낮은 SBF (soft bit-flipping) 알고리즘을 제안하였다. SBF 알고리즘을 이용하면 비트와 체크 노드가 상대 노드에 보내는 메시지가 단일하고 메시지 연산이 간단하기 때문에 PG-LDPC 부호와 같이 행 무게와 열 무게가 높은 부호라도 충분히 실용적으로 구현할 수 있다. 이와 동시에 노드 간 상호 전달 메시지의 이용 효율을 높임으로써 BF 알고리즘에 비하여 SPA 에 상당히 근접한 오율 성능을 보임이 PG-LDPC 부호를 통하여 검증되었다. 그러나 SBF 알고리즘은 메시지의 비균등 양자화(non-uniform quantization)에 필요한 여러 가지 양자화 임계값들을 찾는 방법이 명확하게 밝혀지지 않았기 때문에 높은 오율 성능을 얻기 위해서는 최적 임계값을 많은 모의 실험을 통해 구하는 것이 필요하다. 비균등 양자화가 회로 구현에 미치는 영향도 분석될 필요가 있다. 또한 부호의 길이가 1057인 PG-LDPC 부호에 대해서만 성능 검증이 이루어졌기 때문에 차후 다양한 부호에 대한 추가의 실험을 통하여 일반적인 성능의 검증이 필요하다.

부 록
SBF 알고리즘의 가중치 유도

비트 노드 p가 0 과 1일 확률을 각각 p_0, p_1이라 하자. 이 때 노드 p의 LD는 $\delta_p=p_0-p_1$로 정의된다. 이 때 노드 p와 q를 포함한 3개의 비트 노드와 연결된 체크 노드가 p와 q로부터 나머지 하나의 비트 노드로 전파하는 LD 값은 다음과 같이 유도할 수 있다.

$$\begin{aligned} CHK(p,q) &= \Pr[\text{check}=0]-\Pr[\text{check}=1] \\ &= (p_0q_0+p_1q_1)-(p_0q_1+p_1q_0) \\ &= (p_0-p_1)\times(q_0-q_1) \\ &= \delta_p\times\delta_q. \end{aligned} \tag{4}$$

한 편, $|\delta_p|\le 1$이므로, δ_p를 q비트로 양자화할 때 임의의 실수 $a>1$ 정수 $|x_p|\in[-(2^{q-1}-1),0]$에 대하여 $\hat{\delta}_p=sgn(\delta_p)\cdot a^{x_p}$를 δ_p의 양자화 대표값

(representation level)으로 정할 수 있다. 따라서 두 비트 노드의 양자화된 LD δ_p, δ_q로부터 계산되는 체크 노드의 값은 다음과 같다.

$$\begin{aligned} CHK(p,q) &= \hat{\delta_p} \times \hat{\delta_q} \\ &= sgn(\delta_p) \cdot sgn(\delta_q) \cdot \{a^{x_p} \times a^{x_q}\} \\ &= sgn(\delta_p) \cdot sgn(\delta_q) \cdot a^{x_p + x_q}. \end{aligned} \quad (5)$$

비트 노드와 체크 노드에 지수적인 방식으로 양자화된 LD의 밑 a를 미리 정의해 둔다면 비트 노드 p와 q는 LD의 부호 $sgn(\delta_p)$, $sgn(\delta_q)$와, 양의 방향으로 평행 이동시킨 지수의 값 $x'_p = x_p + (2^{q-1}-1)$, $x'_q = x_q + (2^{q-1}-1)$만 전송하면 된다. 따라서 $x'_c = x'_p + x'_q \in [0, 2(2^{q-1}-1)]$일 때 $a^{x'_c}$는 x'_c에 대하여 단조증가함수이므로 $a^{x'_c} \approx x'_c$로 근사화할 수 있다. 즉, 체크 노드의 신뢰도는 다음과 같이 근사화될 수 있다.

$$CHK(p,q) = a^{x'_p + x'_q} \approx x'_p + x'_q. \quad (6)$$

여기서 지수 함수를 선형 함수로 근사화할 때 발생하는 오차는 체크 노드의 비균등 양자화를 통하여 감소시킬 수 있다.

참 고 문 헌

[1] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21-28, Jan. 1962.7

[2] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399-432, Mar. 1999.

[3] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711-2736, Nov. 2001.

[4] J. Zhang and M. P. C. Fossorier, "A modified weighted bit-flipping decoding of low-density parity-check codes," *IEEE Commun. Lett.*, vol. 8, no. 3, pp. 165-167, Mar. 2004.

[5] M. Jiang, C. Zhao, Z. Shi, and Y. Chen, "An improvement on the modified weighted bit flipping decoding algorithm for LDPC codes," *IEEE Commun. Lett.*, vol. 9, no. 9, pp. 814-816, Sep. 2005.

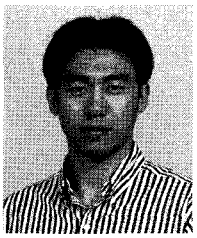
[6] M. P. C. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE Trans. Commun.*, vol. 47, no. 5, pp. 673-680, May 1999.

[7] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498-519, Feb. 2001.

[8] A. Darabiha, A. C. Carusone, F. R. Kschischang, "Block-interlaced LDPC decoders with reduced interconnect complexity," *IEEE Trans. Circuits and Systems II*, vol. 55, no. 1, pp. 74-78, Jan. 2008.

[9] J. Chen, A. Dholakia, E. Eleftheriou, M. P. C. Fossorier, and X-Y. Hu, "Reduced-complexity decoding of LDPC codes," *IEEE Trans. Commun*, vol. 53, no. 8, pp. 1288-1299, Aug. 2005.

조 준 호 (Junho Cho) 정회원



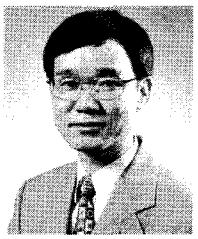
2004년 2월 서울대학교 전기공학부 졸업

2006년 2월 서울대학교 전기컴퓨터공학부 석사

2006년 3월~현재 서울대학교 전기컴퓨터공학부 박사과정

<관심분야> 오류정정부호, 알고리즘 설계 및 구현

성 원 용 (Wonyong Sung) 정회원



1978년 2월 서울대학교 전자공학과 졸업

1980년 2월 한국과학기술원 전기전자공학과 석사

1987년 6월 미국 University of California, Santa Barbara (UCSB) Electrical and Computer Engineering Department 박사

1989년 2월~현재 서울대학교 전기컴퓨터공학부 교수