An Improvement of UMP-BP Decoding Algorithm Using the Minimum Mean Square Error Linear Estimator

Namshik Kim, Jaebum Kim, Hyuncheol Park, and Seung-Bum Suh

In this paper, we propose the modified uniformly most powerful (UMP) belief-propagation (BP)-based decoding algorithm which utilizes multiplicative and additive factors to diminish the errors introduced by the approximation of the soft values given by a previously proposed UMP BP-based algorithm. This modified UMP BP-based algorithm shows better performance than that of the normalized UMP BP-based algorithm, i.e., it has an error performance closer to BP than that of the normalized UMP BP-based algorithm on the additive white Gaussian noise channel for low density parity check codes. Also, this algorithm has the same complexity in its implementation as the normalized UMP BP-based algorithm.

Keywords: Low density parity check (LDPC) codes, belief propagation (BP), uniformly most powerful (UMP)-BP.

Manuscript received Dec. 18, 2003; revised July 13, 2004.

Namshik Kim (phone: +82 42 866 6809, email: nskim@icu.ac.kr), Jaebum Kim (email: kjbum@icu.ac.kr), and Hyuncheol Park (email: hpark@icu.ac.kr) are with School of Engineering, Information and Communications University (ICU), Daejeon, Korea.

Seung-Bum Suh (email: sbsuh@samsung.com) is with Samsung Advanced Institute of Technologies (SAIT), Yongin, Gyeonggi-do, Korea.

I. Introduction

Low-density parity check (LDPC) codes [1], first proposed by Gallager in the 1960s and later rediscovered by MacKay and Meal [2], have been of great academic interest recently. LDPC codes can achieve near a Shannon limit error performance [3] and represent a very promising prospect for error-control coding. LDPC codes appear as a class of codes that can yield a very good performance on the binary symmetric channel (BSC) as well as in the additive white Gaussian noise (AWGN) channel.

For the decoding of LDPC codes, both soft decoding and hard decision decoding can be used. The original Gallager's decoding method is a typical hard decoding with low complexity. However, soft decoding achieves a much better performance and can be implemented by iterative decoding based on the belief propagation (BP) algorithm [4]. The probabilistic decoding proposed by Gallager [1] in 1962 is essentially the same as the BP algorithm. Unfortunately, the hardware implementation of the BP algorithm was limited at that time because of its complexity. Other algorithms with less complexity, including the iterative a posteriori probability (APP)-based algorithm, can also be considered in soft decoding. However, severe degradations in performance may result because correlated values are updated at each iteration after the first iteration. Recently, it has been shown that the BP algorithm provides a powerful tool for iterative decoding of LDPC codes. The BP algorithm is a kind of message passing algorithm that works on the bipartite graph consisting of bit nodes and check nodes. We can simplify the processing in either bit nodes or check nodes and obtain different simplified versions of the BP algorithm. These different versions are called the uniformly most powerful (UMP) BP-based and

UMP APP-based algorithms [5]. These two algorithms actually simplify some parts of the BP decoding algorithm. Because of these simplifications, there must be a degradation in performance, especially for LDPC codes with sums of large weight check nodes. In [6], the authors suggest a method to improve the UMP BP-based algorithm using normalization. The normalized BP-based algorithm can achieve a better error performance than that of the UMP BP-based decoding algorithm. And they show that the degradation of the UMP BP-based algorithm is due to the inaccuracy of the soft values delivered from the first iteration. However, the normalization factor is not optimum since the approximation of the check node updating part of first iteration does not produce the minimum mean square error. In [9], the authors proposed the modified UMP BP-based algorithm which can improve the performance of the normalized UMP BP-based one. We propose to improve the error performance of the UMP BP-based algorithm by introducing new factors (multiplicative and additive factors) in which the approximation of a check node yields the minimum mean square error at the first iteration. The new factors for the first iteration can be obtained using Monte Carlo simulations. And we will show that the proposed algorithm has the better performance when compared with that of the normalization UMP BP-based one.

II. Standard BP and UMP BP-Based Algorithms

1. Standard BP-Based Decoding Algorithm

This part briefly describes the BP algorithm. In the following, we assume binary phase shift keying modulation, which maps a codeword, $\mathbf{c}=(c_1,\cdots,c_n)$, $c_i \in \{0,1\}$, into a transmitted sequence, $\mathbf{x}=(x_1,\cdots,x_n)$. Then, $\mathbf{x}$ is transmitted over a channel corrupted by additive white Gaussian noise, i.e., $\mathbf{y}=\mathbf{x}+\mathbf{n}$, where $\mathbf{y}$ is the received sequence and each component of $\mathbf{n}$ is a random variable with zero mean and variance $N_0/2$. The decoding problem consists of finding the most likely vector $\tilde{\mathbf{c}}$ (the conditional probability $P(\tilde{\mathbf{c}}\,|\,\mathbf{y})$ is maximum) such that $\mathbf{H}\cdot\tilde{\mathbf{c}}^T=0$ (mod 2). The likelihood of $\mathbf{c}$ is given by $\prod_n f_n^x$ with $f_n^x=P(X_n=x)$, so that $f_n^1=1-f_n^0$. Let the parity check matrix be $\mathbf{H}=[h(m,n)]$. We denote the set of bits that participate in the *m*-th check by $N(m)=\{n\,|\,h(m,n)=1\}$. Similarly, we define the set of checks in which the *n*-th bit participates as $M(n)=\{m\,|\,h(m,n)=1\}$. The cardinalities of sets $N(m)$ and $M(n)$ are denoted by $|N(m)|$ and $|M(n)|$, respectively.

The iterative decoding algorithm consists of two alternating parts, in which certain quantities, L_{mn} and z_{mn}, associated with each nonzero element in the matrix $\mathbf{H}$, are iteratively updated. Quantity z_{mn} is the log likelihood ratio (LLR) of the *n*-th bit of $\mathbf{x}$, given the information obtained via checks other than the *m*-th check. Quantity L_{mn} is the LLR of the *n*-th bit that is sent from the *m*-th check to *n*-th bit. It is obtained from the a priori LLR of the *n*-th bit and the information, $\{L_{m'n}\,|\,m'\in M(n)\setminus m\}$, where $M(n)\setminus m$ denotes the set $M(n)$ with the *m*-th check excluded and $N(m)\setminus n$ denotes the set $N(m)$ with the *n*-th bit excluded. Quantity z_n is the a posteriori LLR of the *n*-th bit.

The following steps are comprised of the standard iterative decoding algorithm based on the BP approach.

- Initialization: For each *m* and *n*, $z_{mn}=(4/N_0)y_n$.
- Iterative processing:

i) For each *m*, *n*,

$$T_{mn}=\prod_{n'\in N(m)\setminus n}\frac{1-\exp(z_{mn'})}{1+\exp(z_{mn'})}, \quad \text{and} \tag{1}$$

$$L_{mn}=\ln\frac{1-T_{mn}}{1+T_{mn}}. \tag{2}$$

ii) For each *n* and *m*, update

$$z_{mn}=\left(\frac{4}{N_0}\right)y_n+\sum_{m'\in M(n)\setminus m}L_{m'n}. \tag{3}$$

For each *n*, update the pseudo posterior probabilities, z_n, given by

$$z_n=\left(\frac{4}{N_0}\right)y_n+\sum_{m\in M(n)}L_{mn}. \tag{4}$$

iii) Determine $\hat{\mathbf{c}}=[\hat{c}_n]$ such that $\hat{c}_n=1$ if $z_n\ge 0$, and $\hat{c}_n=0$ if $z_n<0$.

iv) - If $\mathbf{H}\hat{\mathbf{c}}=\mathbf{0}$, then the decoding algorithm stops, and $\hat{\mathbf{c}}$ is considered as a valid decoding result.
- Otherwise, the algorithm repeats from step 1.
- A failure is declared if some maximum number of iteration stages occurs without a valid decoding.

2. UMP BP-Based Decoding Algorithm [6]

Some approximation can be made to simplify the BP algorithm. We can reduce a lot of computations by simplifying T_{mn} and L_{mn}. First, for $n\in N(m)$, define σ_{mn} as the hard decision according to z_{mn} and define σ_n as the modulo-2 sum of the hard decisions of all the bits of the *m*-th check:

$$\sigma_{mn}=\begin{cases}1, & \text{if } z_{mn}>0,\\ 0, & \text{if } z_{mn}\le 0,\end{cases} \quad \text{and}$$

$$\sigma_m = \sum_{n \in N(m)} \sigma_{mn} \mod 2 . \quad (5)$$

Then, $\sigma_m \oplus \sigma_{mn}$ represents the modulo-2 sum of the hard decision of all the bits, $n' \in N(m) \setminus n$, in the m-th check except for the n-th bit. Based on the approximation $\prod q_n \cong \min q_n$ for $0 < q_n < 1$ and the fact that the sign of T_{mn} is $(-1)^{\sigma_m \oplus \sigma_{mn}}$, we then have

$$\begin{aligned} &\prod_{n' \in N(m) \setminus n} \frac{1-\exp(z_{mn'})}{1+\exp(z_{mn'})} \\ &\cong (-1)^{\sigma_m \oplus \sigma_{mn}} \min_{n' \in N(m) \setminus n} \left| \frac{1-\exp(z_{mn'})}{1+\exp(z_{mn'})} \right| \\ &= (-1)^{\sigma_m \oplus \sigma_{mn}} \frac{\exp\left(\min |z_{mn'}|\right) - 1}{\exp\left(\min |z_{mn'}|\right) + 1} . \end{aligned}$$

Based on this approximation, (2) can be simplified into

$$L_{mn} \cong (-1)^{\overline{\sigma_m \oplus \sigma_{mn}}} \min_{n' \in N(m) \setminus n} |z_{mn'}| , \quad (6)$$

where $\overline{\sigma_m \oplus \sigma_{mn}}$ means the binary complementary of $\sigma_m \oplus \sigma_{mn}$. The positive factor $4/N_0$ in z_{mn} has no effect on the decoding and can be omitted, in which no a priori information about the AWGN channel is required. The resultant UMP BP-based algorithm is described below.

- Initialization: For each m and n, $z_{mn} = y_n$.
- Iterative processing:

i) For each m and n, σ_{mn} and σ_m are defined as in (5).
And for m and n,

$$L_{mn} = (-1)^{\overline{\sigma_m \oplus \sigma_{mn}}} \min_{n' \in N(m) \setminus n} |z_{mn'}| . \quad (7)$$

ii) For each m and n, update

$$z_{mn} = y_n + \sum_{m' \in M(n) \setminus m} L_{m'n} . \quad (8)$$

For each n, update the pseudo posterior probabilities z_n given by

$$z_n = y_n + \sum_{m \in M(n)} L_{mn} . \quad (9)$$

iii) Determine $\hat{\mathbf{c}} = [\hat{c}_n]$ such that $\hat{c}_n = 1$ if $z_n \geq 0$, and $\hat{c}_n = 0$ if $z_n < 0$.

iv) - If $\mathbf{H}\hat{\mathbf{c}} = 0$ then the decoding algorithm stops, and $\hat{\mathbf{c}}$ is considered as a valid decoding result.
- Otherwise, the algorithm repeats from step 1.
- A failure is declared if some maximum number of iteration stages occurs without a valid decoding.

III. Modified UMP BP-Based Decoding Algorithm

Since the above approximation in (6) must have a relative error for any signal-to-noise ratio (SNR), we should adjust the approximated value to make it close to the true value. In [6], Chen and others found the normalization factor, α, which makes the relative error small. For the BP and UMP algorithms, the LLR of the n-th bit can be computed as the following:

$$L_1 := L_{BP} = \ln \frac{1-T_{mn}}{1+T_{mn}}, \quad T_{mn} = \prod_{n' \in N(m) \setminus n} \frac{1-\exp(z_{mn'})}{1+\exp(z_{mn'})}$$

$$L_2 := L_{UMP} = (-1)^{\overline{\sigma_m \oplus \sigma_{mn}}} \min_{n' \in N(m) \setminus n} |z_{mn'}| .$$

Then, L_1 and L_2 denote the values of L_{mn} used in the BP and UMP BP-based algorithms, respectively. Roughly, if we substitute L_1 with L_2, then the UMP BP-based algorithms are led directly. Then, the following property was proved obviously in [6].

The magnitude of L_2 is greater than that of L_1, i.e., $|L_2| > |L_1|$.

To determine normalization factor α [6], Chen and others considered the criterion to force the mean of the normalized magnitude of $L_1 \cdot \alpha$ to equal the mean of L_2:

$$\hat{\alpha} = \frac{E(|L_2|)}{E(|L_1|)} .$$

However, this value, $\hat{\alpha}$, which makes $L_1 \cdot \hat{\alpha}$ equal to L_2 in the average sense may not be optimum. In [7], the authors have proposed the two BP-based algorithms. The first algorithm uses a normalization factor which is multiplied by L_2. However, the second algorithm exploits the factor which is added to L_2. Both factors are determined by the density evolution regardless of the SNR. We propose the BP-based decoding algorithm which exploits two factors (multiplicative and additive factors). These two factors are chosen by minimizing the mean square errors between the LLR values from the BP algorithm and the proposed one. Now for the first iteration, we define the error function as the following:

$$\Delta(\alpha, \beta) = E\left[\left(|L_1| - (\alpha |L_2| + \beta)\right)^2\right].$$

We try to find the factors $\tilde{\alpha}, \tilde{\beta}$ such that $\Delta(\tilde{\alpha}, \tilde{\beta}) = \min \Delta(\alpha, \beta)$. Obviously, if we find $\tilde{\alpha}$ and $\tilde{\beta}$, then the performance of the proposed algorithm with $\tilde{\alpha}$ and $\tilde{\beta}$ is similar to that of the BP decoding algorithm with same maximum iteration number as shown in Fig. 2. In

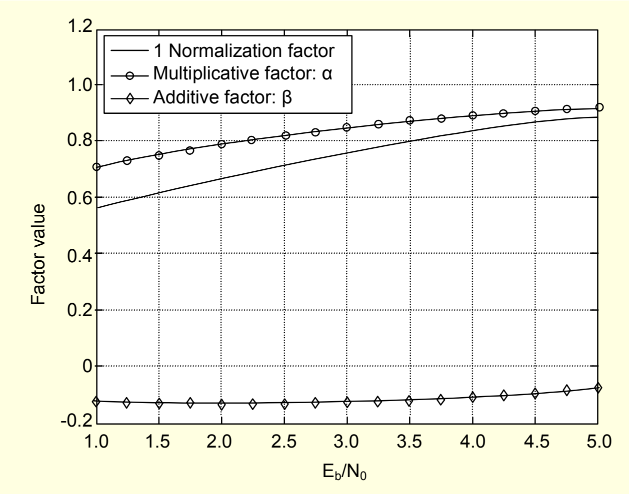


Fig. 1. The new factors for the first iteration which make the minimum mean square error for (1008, 504) a regular LDPC code.

(*j*, *k*)-regular LDPC codes of length *N*, the multiplication number of the proposed algorithm is *jN* in each iteration, whereas there are real additions in the UMP BP-based algorithm. Thus, the complexity of the proposed algorithm is increased when compared with the UMP BP-based one. But the complexity of the proposed algorithm is much lower than that of the BP algorithm.

Theorem. For the first iteration, let $\tilde{\alpha} = \dfrac{\mathrm{Cov}(|L_1|,|L_2|)}{\mathrm{Var}(|L_2|)}$ and $\tilde{\beta} = E[|L_1|] - \tilde{\alpha} \cdot E[|L_2|]$. Then $\tilde{\alpha}$ and $\tilde{\beta}$ produce the minimum value of $\Delta(\alpha, \beta)$.

Proof. Let $Y = |L_1|$ and $X = |L_2|$. Then, the following are trivial. Now consider estimating Y by $\alpha X + \beta$:

$$\min_{\alpha,\beta} E\left[(Y - (\alpha X + \beta))^2\right]. \tag{10}$$

Equation (10) can be viewed as the approximation of $Y - \alpha X$ by the constant, β. So, the best $\tilde{\beta}$ is

$$\tilde{\beta} = E[Y - \alpha X] = E[Y] - \alpha E[X].$$

Substituting $\tilde{\beta}$ into (10) implies that the best $\tilde{\alpha}$ is found by

$$\min_{\alpha} E\left[((Y - E[Y]) - \alpha(X - E[X]))^2\right].$$

We once again differentiate with respect to α, set the result to zero, and solve for α :

$$\begin{aligned} 0 &= \frac{d}{d\alpha} E\left[((Y - E[Y]) - \alpha(X - E[X]))^2\right] \\ &= -2\left(\mathrm{Cov}(X,Y) - \alpha \ \mathrm{Var}(X)\right) \end{aligned}.$$

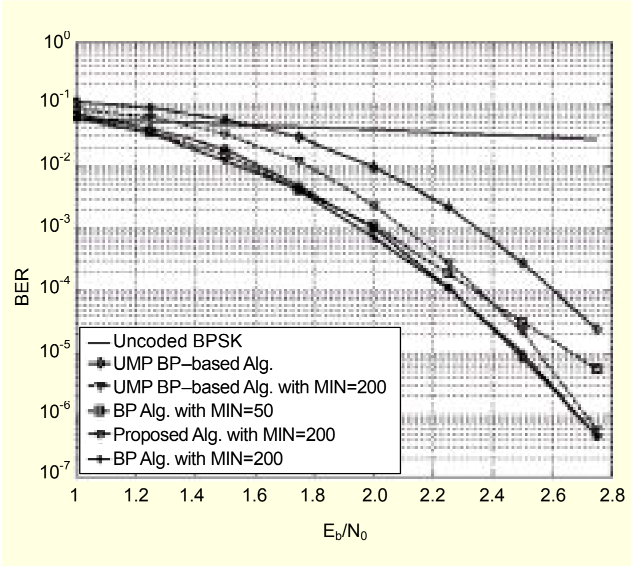


Fig. 2. Error performance of the (1008, 504) regular LDPC code with BP, UMP BP-based, normalized BP-based and proposed BP-based algorithms.

The best $\tilde{\alpha}$ is found to be

$$\tilde{\alpha} = \frac{\mathrm{Cov}(X,Y)}{\mathrm{Var}(X)}.$$

Therefore, the minimum mean square error linear estimator for *Y* in terms of *X* is

$$\hat{Y} = \tilde{\alpha} \ X + \tilde{\beta} = \frac{Cov(X,Y)}{Var(X)}(X - E[X]) + E[Y]. \qquad \square$$

Since $\tilde{\beta}$ is the optimum factor associated with the first iteration, there are errors for all subsequent iterations. If we keep on adding $\tilde{\beta}$ for all these subsequent iterations, the errors that are made from $\tilde{\beta}$ are increased exponentially with respect to the number of iterations, although the first iteration error is very small. Thus, we alter $\tilde{\beta}$ to zero for all subsequent iterations. Also, we should find the new factor, $\tilde{\alpha}$, after the first iteration by using a similar method. However this is not so straightforward to derive. The simulation shows that the performance remains very good if we continue using optimum factor $\tilde{\alpha}$ of the first iteration instead of all subsequent $\tilde{\alpha}$s. Thus we determine not to derive them.

The new factors, $\tilde{\alpha}$ and $\tilde{\beta}$, can be determined based on the Monte Carlo simulations. We use a (3,6)-regular LDPC code [8] of length 1008 and rate 0.5 under various decoding algorithms. Figure 1 shows that the difference between $\tilde{\alpha}$ and $1/\hat{\alpha}$ is decreased as the SNR is increased. Then, the difference between the performances of the normalization UMP-BP and the proposed algorithm is decreased as the SNR is increased. The approximated values used in the two algorithms are close enough to the true value so that, from a particular SNR, the performances of the proposed and normalized UMP-BP algorithms are superior to the BP algorithm with a maximum iteration number (MIN) of 50 because the two algorithms have an MIN of more than 50. In our result, the BP with a 50 MIN is initially inferior to the proposed algorithm at about 2.0 dB and the normalized UMP-BP at about 2.5 dB. Furthermore, both of these algorithms coincide with the BP with a 200 MIN from these SNRs. Also, their complexities are almost the same to each other and are much smaller than that of the BP algorithms. The proposed algorithm is more desirable than the normalized UMP-BP regardless of the block length of the LDPC codes based on the results of the simulation in this article. Figure 2 shows that the proposed BP-based algorithm surpasses the normalized UMP-BP [6] for a (3,6)-regular LDPC code of block length 1008.

IV. Conclusions

We have proposed the new modified UMP BP-based algorithm in which the new factors produce the minimum of mean square error for the first iteration. Finally, we demonstrated the new factors, $\tilde{\alpha}$ and $\tilde{\beta}$, using the Monte Carlo simulation. We showed that for an LDPC code of length 1008, if we choose new factors, $\tilde{\alpha}$ and $\tilde{\beta}$, while keeping $\tilde{\alpha}$ and setting $\tilde{\beta} = 0$ for all subsequent iterations, then the achieved result is superior to that of the normalized UMP BP-based algorithm.

References

[1] R.G Gallager, *Low-Density Parity-Check Codes*, M.I.T. Press, Cambridge, MA, 1963.

[2] D.J.C. Mackay and R.M. Neal, "Near Shannon Limit Performance of Low Density Parity Check Codes," *Electron. Lett.*, vol. 32, no. 18, Aug. 1996, pp. 1645-1646.

[3] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of Capacity Approaching Irregular Low-Density Parity Check Codes," *IEEE. Inform. Theory*, vol. 47, Feb. 2001, pp. 619-637.

[4] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, San Mateo, CA, 1988.

[5] M. 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, May. 1999, pp. 673-680.

[6] Jinghu Chen and M. Fossorier, "Near Optimum Universal Belief Propagation Based Decoding of Low-Density Parity Check Codes," *IEEE Trans. Commun.*, vol. 50, Mar. 2002, pp. 406-414.

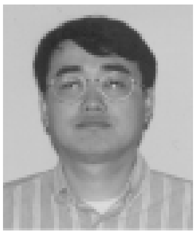
[7] Jinghu Chen and M. Fossorier, "Density Evolution for Two Improved BP-Based Decoding Algorithm of LDPC Codes," *IEEE. Commun. Lett*, vol. 6, May 2002, pp. 208-210.

[8] D.J. Mackay, *Online Database of Low-Density Parity Check Codes*, http://wol.ra.phy.cam.uk/ mackay/codes/data.html.

[9] Namshik Kim and Hyuncheol Park, "Modified UMP BP Decoding Algorithm Based on the Mean Square Error," *Electron. Lett.*, vol. 40, no. 13, June 2004, pp. 816-817.

Namshik Kim received the BS and MS degrees in mathematics from Sung Kyun Kwan in 1996 and from Postech in 2001, respectively. He is currently working toward the PhD degree at the Information and Communications University. His research interests include channel coding (LDPC codes and STBC) and iterative decoding algorithms for linear codes.

Jaebum Kim received the BS and MS degrees from Korea Maritime University of Radio Science & Engineering, Busan, Korea, in 1996 and 1998. He is currently working toward the PhD degree at the Information and Communications University. His research interests include channel coding (Turbo, LDPC codes), iterative decoding algorithm for linear codes, and FPGA implementations.



Hyuncheol Park received the BS and MS degrees in electronics engineering from Yonsei University, Seoul, Korea, in 1983 and 1985, and the PhD degree in electrical engineering from the Georgia Institute of Technology, Atlanta, in 1997. He was a Senior Engineer from 1985 to 1991 and a Principal Engineer from 1997 to 2002 at Samsung Electronic Co., Korea. Since 2002, he has been with the School of Engineering, Information and Communication University, Daejeon, Korea, where he is an Assistant Professor. His research interests include high-speed wireless communications and channel coding.

Seung-Bum Suh received the BS and MS degrees in electrical engineering from Seoul National University, Seoul, Korea in 1998 and from University of Michigan, Ann Arbor, MI, USA, in 1999, respectively. He is currently working at Samsung Electronics.