© 2003 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

[24] K. H. Rosen, Ed., *Handbook of Discrete and Combinatorial Mathematics*. Boca Raton, FL: CRC, 2000.
[25] B. Rudner, "Construction of minimum-redundancy codes with an optimum synchronization property," *IEEE Trans. Information Theory*, vol. IT-17, pp. 478–487, July 1971.
[26] P. F. Swaszek and P. DiCicco, "More on the error recovery for variable-length codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2064–2071, Nov. 1995.
[27] Y. Takishima, M. Wada, and H. Murakami, "Error states and synchronization recovery for variable length codes," *IEEE Trans. Commun.*, vol. 42, pp. 783–792, Feb. 1994.
[28] M. R. Titchener, "The synchronizaation of variable-length codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 683–691, Mar. 1997.
[29] V. K. W. Wei and R. A. Scholtz, "On the characterization of statistically synchronizable codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 733–735, Nov. 1980.
[30] G. Zhou and Z. Zhang, "Synchronization receovery of variable-length codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 219–227, Jan. 2002.

A Coding Theorem for Lossy Data Compression by LDPC Codes

Yuko Matsunaga and Hirosuke Yamamoto, *Member, IEEE*

***Abstract*—In this correspondence, low-density parity-check (LDPC) codes are applied to lossy source coding and we study how the asymptotic performance of MacKay's LDPC codes depends on the sparsity of the parity-check matrices in the source coding of the binary independent and identically distributed (i.i.d.) source with $\Pr\{x = 1\} = 0.5$. In the sequel, it is shown that an LDPC code with column weight $O(\log n)$ for code length n can attain the rate-distortion function asymptotically.**

***Index Terms*—Lossy data compression, low-density parity-check (LDPC) codes, rate-distortion function.**

I. Introduction

Recently, low-density parity-check (LDPC) codes, which were originally discovered by Gallager [1], [2] in 1962, have been studied actively because of their very good performance in error correction. It was shown by many researchers [3]–[8] that LDPC codes can attain high performance near the Shannon limit by iterative decoding with belief propagation [9], [10]. Furthermore, MacKay [3] and Miller and Burshtein [11] proved that the LDPC codes can asymptotically achieve channel capacity.

On the other hand, it is well known that channel coding can be considered as the dual problem of lossy source coding in rate-distortion theory [12], and a good error-correcting code can be used for efficient lossy data compression. Csiszár and Körner [13] showed that the rate-distortion function can be achieved by an error-correcting code that can attain error probability $P_e = 1 - \epsilon$ with rate close to the rate-distortion function for any sufficiently small fixed $\epsilon > 0$. However, for LDPC codes or other practical error-correcting codes, the existence of such codes is not obvious, and hence we have to prove the existence if we want to use such codes for lossy data compression. Actually, for example, Goblick [14] and Berger [15] showed that a general linear error-correcting code can attain the rate-distortion function asymptotically for a binary independent and identically distributed (i.i.d.) source with $\Pr\{x = 1\} = 0.5$. Furthermore, Viterbi and Omura [16] proved a lossy source coding theorem for i.i.d. sources by using trellis codes with Viterbi decoding. However, no *practically good* lossy source coding scheme has been found because the encoding methods used in the lossy source coding schemes are not practical in the sense of memory and time complexity.

Based on the good performance of the LDPC codes and the practically feasible belief propagation decoding, we may expect that LDPC codes are good candidates for practical lossy source coding. However, it is known that belief propagation decoding does not work well in lossy source coding because the noise level of the test channel in lossy source coding is much larger than that of usual channels used in practical error correction. Nevertheless, it is still worth to clarify if the LDPC codes can attain the rate-distortion function asymptotically because some cleverly modified version of belief propagation decoding or an entirely new decoding algorithm may be devised exploiting the sparsity of parity-check matrix in the future.

In this correspondence, we treat LDPC codes on MacKay's ensemble [3] for the binary i.i.d. source with $\Pr\{x = 1\} = 0.5$, and we consider the relation between the sparsity of parity-check matrices and the asymptotic performance in LDPC codes. Furthermore, we show that for code length n, an LDPC code with column weight $O(\log n)$ can attain the rate-distortion function asymptotically.

The correspondence is organized as follows. Section II is devoted to some preliminaries of the rate-distortion theory and the lossy source coding by LDPC codes. The main coding theorem is also described in Section II, but the proof is given in Section III. It is also shown in Section III how the sparsity of parity-check matrices affects the performance of LDPC codes in the lossy source coding.

II. Lossy Data Compression by LDPC Codes

Let source X be a binary i.i.d. source which takes values in $\mathcal{X} = \{0, 1\}$ with $q = \Pr\{x = 1\}$. The distortion between single letters is measured by the Hamming distortion defined by

$$d_{\mathrm{H}}(x, \hat{x}) = \begin{cases} 0, & \text{if } x = \hat{x} \\ 1, & \text{if } x \neq \hat{x} \end{cases}$$

and the distortion between n-bit sequences[1] $\boldsymbol{x} = x_1, x_2, \cdots, x_n^T$ and $\hat{\boldsymbol{x}} = \hat{x}_1, \hat{x}_2, \cdots, \hat{x}_n^T$ is measured by the averaged single-letter distortion as follows:

$$d(\boldsymbol{x}, \hat{\boldsymbol{x}}) = \frac{1}{n} \sum_{i=1}^{n} d_{\mathrm{H}}(x_i, \hat{x}_i).$$

Then the rate-distortion function $R(D)$ of the binary i.i.d. source is given by

$$R(D) = \min_{\hat{X}:\, \mathrm{E}[d_{\mathrm{H}}(X, \hat{X})] \leq D} I(X; \hat{X})$$
$$= h(q) - h(D), \qquad 0 \leq D \leq q \leq 0.5$$

[1]In this correspondence, a bold-faced letter represents a column vector and $\boldsymbol{T}$ stands for transposition of a vector or a matrix

Manuscript received November 21, 2002; revised May 13, 2003. The work of H. Yamamoto was supported in part by JSPS under Grant-in-Aid for Scientific Research 14550347. The material in this correspondence was presented at the IEEE International Symposium on Information Theory, Lausanne, Switzerland, June/July 2002.

Y. Matsunaga is with Internet Systems Research Laboratories, NEC Corporation, 4-1-1 Miyazaki, Miyamae-ku, Kawasaki, Kanagawa, 216-8555, Japan (e-mail: y-matsunaga@da.jp.nec.com).

H. Yamamoto is with the Department of Mathematical Informatics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-8656, Japan (e-mail: Hirosuke@ieee.org).

Communicated by R. Koetter, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.815805

0018-9448/03$17.00 © 2003 IEEE

where $\mathrm{E}[d_{\mathrm{H}}(X, \hat{X})]$ stands for the expected value of the distortion and $h(x) = -x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy function. When $q = 0.5$, $R(D)$ becomes

$$R(D) = 1 - h(D), \qquad 0 \le D \le 0.5.$$

An LDPC code is a linear error-correcting code defined by a very sparse parity-check matrix H. First we define a lossy data compression scheme based on a linear error-correcting code with a generator matrix G and the corresponding parity-check matrix H.

Lossy Encoding by a Linear Code: Let G be a $k \times n$ generator matrix and H be the corresponding $m \times n$ parity-check matrix that satisfies $k = n - m$ and $HG^T = 0$, where 0 is the $m \times k$ zero matrix. Encoding in lossy data compression can be processed like decoding in error correction. We calculate the syndrome vector $\boldsymbol{s}$ of a source sequence $\boldsymbol{x}$ by $\boldsymbol{s} = H\boldsymbol{x}$, and we derive a reproductive sequence $\hat{\boldsymbol{x}}$ from $\boldsymbol{s}$ such that $\hat{\boldsymbol{x}}$ satisfies $H\hat{\boldsymbol{x}} = \boldsymbol{0}$ and $d(\boldsymbol{x}, \hat{\boldsymbol{x}}) \le D$. The compressed codeword is obtained as the k-bit vector $\boldsymbol{u}$ that satisfies $\hat{\boldsymbol{x}} = G^T\boldsymbol{u}$. The rate R of the code is defined by $R =$ (the length of $\boldsymbol{u}$)/(the length of $\boldsymbol{x}$), i.e., $R = k/n = (n - m)/n$.

Now we define (m, n, t)-LDPC codes which can be applied to lossy data compression.

Definition 1: An (m, n, t) parity-check matrix H is an $m \times n$ matrix such that the Hamming weight of each column is not larger than t. An (m, n, t)-LDPC code is a code represented by an (m, n, t) parity-check matrix satisfying $t \ll m$.

Definition 2 (MacKay's Ensemble [3]): MacKay's ensemble is the ensemble of LDPC codes with $m \times n$ parity-check matrices, each of which is constructed as follows. For every column of H, first, set the column to all 0's and repeat the following procedure t times. Choose an index uniformly and independently from $\{1, 2, \ldots, m\}$ and flip the corresponding bit of the column. If an index is chosen an odd number of times in t repetitions, the corresponding element of the column becomes 1, and otherwise, the element becomes 0.

Then, by applying the random coding argument to MacKay's code ensemble of (m, n, t)-LDPC codes, we can prove the following theorem.

Theorem 1: There exists an (m, n, t)-LDPC code with $t = O(\log n)$ that can attain the rate-distortion function for the binary i.i.d. source with $\Pr\{x = 1\} = 0.5$ asymptotically if t is odd. Furthermore, in the case that $t = O(n)$ for any $R > R(D)$, the distortion of the code converges to D exponentially as n becomes large.

In the proof of Theorem 1, we use following two lemmas.

Lemma 1: Let $W_{\mathrm{H}}(\boldsymbol{x})$ be the Hamming weight of an n-bit vector $\boldsymbol{x}$, and let $P(w) = \Pr\{\boldsymbol{x} : H\boldsymbol{x} = \boldsymbol{0} | W_{\mathrm{H}}(\boldsymbol{x}) = w\}$, which is the probability that $\boldsymbol{x}$ satisfies $H\boldsymbol{x} = \boldsymbol{0}$ under the condition $W_{\mathrm{H}}(\boldsymbol{x}) = w$. Then $P(w)$ satisfies the following equations on MacKay's ensemble. If wt is odd

$$P(w) = 0 \tag{1}$$

and if wt is even

$$P(w) = 2^{-m}\sum_{j=0}^{m}\binom{m}{j}\left(1 - \frac{2j}{m}\right)^{wt} \tag{2}$$

$$\le \exp\left[m(e^{-2wt/m} - \ln 2) + \ln 2\right] \tag{3}$$

$$= \frac{1}{2^{m-1}}\exp\left[me^{-2wt/m}\right] \tag{4}$$

where $\ln x = \log_e x$.

Lemma 2: The binomial coefficient $\binom{N}{K}$ satisfies

$$\frac{1}{N+1}2^{Nh(K/N)} \le \binom{N}{K} \le 2^{Nh(K/N)}. \tag{5}$$

Furthermore, it holds for $K' < N/2$ that

$$\sum_{K=0}^{K'}\binom{N}{K} \le 2^{Nh(K'/N)}. \tag{6}$$

We note that $P(w)$ is the probability that the wtth step of the random walk on the m-dimensional hypercube, starting from the origin, brings us back to the origin, which is given by the right-hand side of (2) for the case of even wt. Furthermore, (1) holds because we cannot come back to the origin when wt is odd. See [17] and [18] for more details of the random walk and the derivations of (1) and (2). The bound (3), which is tight for sufficiently large wt, is given by [3, eq. (23)]. Since Lemma 2 is well known, we omit the proof (see [12, Ch. 12, Theorem 12.1.3]).

III. Proof of Theorem 1

Assume that D, $0 < D \le 0.5$, is given. Then, we first fix constants η_j, $j = 1, \ldots, 5$, that satisfy the following relations:

$$h(D) > \eta_1 > \eta_2 > \eta_3 > 0 \tag{7}$$

$$\eta_2 - \eta_3 > \eta_5 > \eta_4 > 0. \tag{8}$$

Then, when the code length n is sufficiently large, they satisfy

$$\eta_2 > \eta_3 + \frac{1}{n}\log(n+1)$$

$$\eta_2 - \eta_3 > \eta_5 + \frac{1}{n}\log(n+1). \tag{9}$$

Furthermore, when n is sufficiently large, there exist integers m, d_0, and d_1 that satisfy the following inequalities:

$$2^{n(h(D)-\eta_1)} < 2^m < 2^{n(h(D)-\eta_2)} \tag{10}$$

$$2^{n(h(D)-\eta_3)} < 2^{nh(d_0/n)} < 2^{nh((d_0+1)/n)} < 2^{nh(D)} \tag{11}$$

$$2^{n\eta_4} < 2^{nh(d_1/n)} < 2^{n\eta_5}. \tag{12}$$

Note that $d_1 < d_0$ holds from (11) and (12) because we have $\eta_5 < h(D) - \eta_3$ from $h(D) > \eta_2$ in (7) and $\eta_2 - \eta_3 > \eta_5$ in (8).

For the above m, we consider an (m, n, t) parity-check matrix H and the corresponding code defined by H. For simplicity, we assume that the rank of H is equal to m[2] and the total number of syndrome vectors of H is given by 2^m.

Then, the rate of the code $R = (n - m)/n$ satisfies from (10) that

$$1 - h(D) + \eta_2 < R < 1 - h(D) + \eta_1. \tag{13}$$

Next, based on the integer d_0, we construct a distortion dictionary $\mathcal{S}$ that consists of n-bit vectors with the Hamming weight not larger than nD.

Distortion Dictionary: Letting $d = W_{\mathrm{H}}(\boldsymbol{d})$ stand for the Hamming weight of n-bit vector $\boldsymbol{d}$, the distortion dictionary $\mathcal{S}$ consists of all n-bit vectors $\boldsymbol{d}$ with $W_{\mathrm{H}}(\boldsymbol{d}) \le d_0$ and some n-bit vectors $\boldsymbol{d}$ with $W_{\mathrm{H}}(\boldsymbol{d}) = d_0 + 1$, i.e.,

$$\mathcal{S} = \{\boldsymbol{d} | 0 \le d = W_{\mathrm{H}}(\boldsymbol{d}) \le d_0\} \cup \mathcal{S}' \tag{14}$$

where $\mathcal{S}'$ is defined as follows.

The auxiliary set $\mathcal{S}'$ consists of different vectors that are chosen randomly from vectors $\boldsymbol{d}$ with $W_{\mathrm{H}}(\boldsymbol{d}) = d_0 + 1$. The size of $\mathcal{S}'$, $|\mathcal{S}'|$, is

[2]For the case of rank smaller than m, see Remark 1.

determined so that the number of vectors $\boldsymbol{d}$ having even weight is equal to the number of vectors $\boldsymbol{d}$ having odd weight in $\mathcal{S}$. That is,

$$|\mathcal{S}'| = \begin{cases} \sum_{d=0}^{\frac{d_0-1}{2}} \left[\binom{n}{2d+1} - \binom{n}{2d} \right], & d_0 \text{ is odd} \\ 1 + \sum_{d=1}^{\frac{d_0}{2}} \left[\binom{n}{2d} - \binom{n}{2d-1} \right], & d_0 \text{ is even.} \end{cases} \tag{15}$$

We note from (5), (11), and (14) that $|\mathcal{S}|$ satisfies

$$|\mathcal{S}| \geq \sum_{d=0}^{d_0} \binom{n}{d} > \binom{n}{d_0} \geq \frac{1}{n+1} 2^{nh(d_0/n)} > \frac{1}{n+1} 2^{n(h(D)-\eta_3)}. \tag{16}$$

For each vector $\boldsymbol{d}$ in $\mathcal{S}$, the syndrome of $\boldsymbol{d}$ is obtained by $H\boldsymbol{d}$. Using the distortion dictionary and the calculation of syndromes, a source sequence $\boldsymbol{x}$ is encoded as follows.

Encoding: Calculate the syndrome $H\boldsymbol{x}$ for a given $\boldsymbol{x}$. If there exists a distortion vector $\boldsymbol{d}$ in $\mathcal{S}$ that has the same syndrome as $\boldsymbol{x}$, i.e., $H\boldsymbol{x} = H\boldsymbol{d}$, then $\boldsymbol{x}$ is encoded by

$$\hat{\boldsymbol{x}} = \boldsymbol{x} - \boldsymbol{d}.$$

If there exist two or more such distortion vectors, we may choice any one of them. If there is no such distortion vector, then $\boldsymbol{x}$ is encoded into an arbitrarily fixed vector $\hat{\boldsymbol{x}}_0$.

Now we consider what distortion the above encoding can attain. Source sequences $\boldsymbol{x}$ can be divided into the following two categories.

1) $\mathcal{X}_1^n = \{\boldsymbol{x}$: There is $\boldsymbol{d} \in \mathcal{S}$ that satisfies $H\boldsymbol{x} = H\boldsymbol{d}.\}$
2) $\mathcal{X}_2^n = \{\boldsymbol{x}$: There is no $\boldsymbol{d} \in \mathcal{S}$ that satisfies $H\boldsymbol{x} = H\boldsymbol{d}.\}$

If $\boldsymbol{x} \in \mathcal{X}_1^n$, then $\boldsymbol{x}$ can be encoded within distortion $(d_0+1)/n$. On the other hand, if $\boldsymbol{x} \in \mathcal{X}_2^n$, then the distortion is bounded by

$$d_{\max} = \min_{\hat{x}} \mathrm{E}[d_{\mathrm{H}}(X, \hat{x})] = 0.5.$$

Hence, letting $\epsilon_H = |\mathcal{X}_2^n|/2^n$, the total expected distortion is bounded by

$$\frac{d_0+1}{n} + \epsilon_H d_{\max}.$$

Since $h(D)$ is an increasing function for $0 < D < 0.5$, d_0 satisfies from (11) that

$$(d_0+1)/n < D.$$

On the other hand, the rate R satisfies (13). Therefore, if ϵ_H satisfies that $\epsilon_H \to 0$ as $n \to \infty$ for any given $\eta_1 > 0$, the above encoding can attain asymptotically the rate $1 - h(D)$ and the distortion D with probability 1.

Next we show by the random coding technique that there exists an (m, n, t)-LDPC code with the desired ϵ_H. For a given H, let $K_s(H)$ be $K_s(H) = |\{\boldsymbol{s}: \boldsymbol{s} = H\boldsymbol{d}$ for some $\boldsymbol{d} \in \mathcal{S}\}|$, i.e., the number of different syndromes $\boldsymbol{s}$ that can be obtained by $\boldsymbol{s} = H\boldsymbol{d}$, $\boldsymbol{d} \in \mathcal{S}$. Then, $K_u(H) = |\mathcal{S}| - K_s(H)$ represents the number of duplicated syndromes obtained from all $\boldsymbol{d} \in \mathcal{S}$. This means that $\mathcal{S}$ contains $K_u(H)$ useless distortion vectors. For a fixed $\boldsymbol{d}$, the number of useless distortion vectors that have the same syndrome as $\boldsymbol{d}$ is given by

$$f(\boldsymbol{d}) = \sum_{\substack{\boldsymbol{d}' \in \mathcal{S} \\ \boldsymbol{d}' \neq \boldsymbol{d}}} \mathbf{1}[H(\boldsymbol{d} - \boldsymbol{d}') = \boldsymbol{0}]$$

where $\mathbf{1}[A]$ is the indicator function that takes 1 if and only if A is true. Hence, $K_u(H)$ can be represented by

$$K_u(H) = \sum_{\boldsymbol{d} \in \mathcal{S}} \frac{f(\boldsymbol{d})}{f(\boldsymbol{d})+1}$$

because for each syndrome, $f(\boldsymbol{d})+1$ distortion vectors have the same syndrome in $\mathcal{S}$.

If $K_s(H) = 2^m$, then every syndrome has the corresponding distortion vectors in $\mathcal{S}$. In case of $K_s(H) < 2^m$, some syndromes have no corresponding vector in $\mathcal{S}$. The number of such missing syndromes $M_s(H)$ is given by

$$\begin{aligned} M_s(H) &= 2^m - K_s(H) \\ &= 2^m + K_u(H) - |\mathcal{S}|. \end{aligned} \tag{17}$$

On the other hand, since the (m, n, t)-LDPC code is a linear code, ϵ_H and $M_s(H)$ satisfy

$$\begin{aligned} \epsilon_H &= \frac{|\mathcal{X}_2^n|}{2^n} = \frac{M_s(H) 2^{(n-m)}}{2^n} \\ &= \frac{M_s(H)}{2^m}. \end{aligned} \tag{18}$$

Now we evaluate $K_u(H)$ by the random coding technique. Letting K_u be the expectation of $K_u(H)$ over MacKay's ensemble in Definition 2, K_u is bounded by

$$\begin{aligned} K_u &= \mathrm{E}_H \left[\sum_{\boldsymbol{d} \in \mathcal{S}} \frac{f(\boldsymbol{d})}{f(\boldsymbol{d})+1} \right] \\ &= \sum_{\boldsymbol{d} \in \mathcal{S}} \mathrm{E}_H \left[\frac{f(\boldsymbol{d})}{f(\boldsymbol{d})+1} \right] \\ &\leq \sum_{\boldsymbol{d} \in \mathcal{S}} \frac{\mathrm{E}_H[f(\boldsymbol{d})]}{\mathrm{E}_H[f(\boldsymbol{d})]+1} \end{aligned} \tag{19}$$

where the inequality follows from Jensen's inequality because $x/(x+1)$ is a concave function for $x \geq 0$. In order to apply Lemma 1 to (19), we represent $\mathrm{E}_H[f(\boldsymbol{d})]$ as

$$\begin{aligned} \mathrm{E}_H[f(\boldsymbol{d})] &= \sum_{\substack{\boldsymbol{d}' \in \mathcal{S} \\ \boldsymbol{d}' \neq \boldsymbol{d}}} \mathrm{E}_H \left[\mathbf{1} \left[H(\boldsymbol{d} - \boldsymbol{d}') = \boldsymbol{0} \right] \right] \\ &= \sum_{w=1}^{2(d_0+1)} \sum_{\substack{\boldsymbol{d}' \in \mathcal{S} \\ w = W_{\mathrm{H}}(\boldsymbol{d} - \boldsymbol{d}')}} \mathrm{E}_H \left[\mathbf{1} \left[H(\boldsymbol{d} - \boldsymbol{d}') = \boldsymbol{0} \right] \right]. \end{aligned}$$

Then, letting $g(w|\boldsymbol{d})$ be the number of distortion vectors $\boldsymbol{d}' \in \mathcal{S}$ that satisfies $w = W_{\mathrm{H}}(\boldsymbol{d} - \boldsymbol{d}')$, and noting that $\mathrm{E}_H \left[\mathbf{1} \left[H(\boldsymbol{d} - \boldsymbol{d}') = \boldsymbol{0} \right] \right]$ is equal to $P(w)$ defined in Lemma 1 for such $\boldsymbol{d}'$, $\mathrm{E}_H[f(\boldsymbol{d})]$ can be represented as

$$\mathrm{E}_H[f(\boldsymbol{d})] = \sum_{w=1}^{2(d_0+1)} g(w|\boldsymbol{d}) P(w). \tag{20}$$

Now we consider the worst case for the right-hand side of (20) in the case of odd t. Since $P(w)$ is a decreasing function for even wt and 0 for odd wt, the right-hand side of (20) is maximized by maximizing $g(w|\boldsymbol{d})$ for smaller even w. We note that $g(w|\boldsymbol{d})$ is bounded by

$$g(w|\boldsymbol{d}) \leq \binom{n}{w}$$

and $g(w|\boldsymbol{d})$ satisfies

$$\sum_{w=1}^{2(d_0+1)} g(w|\boldsymbol{d}) = |\mathcal{S}| - 1$$

because $\sum_{w=1}^{2(d_0+1)} g(w|\boldsymbol{d})$ counts all distortion vectors in $\mathcal{S}$ except $\boldsymbol{d}$. We also note from the Appendix that the sum of $g(w|\boldsymbol{d})$ for all even w is less than $|\mathcal{S}|/2$. Hence, $\mathrm{E}_H[f(\boldsymbol{d})]$ can be bounded as follows:

$$\mathrm{E}_H\left[f(\boldsymbol{d})\right] = \sum_{w=1}^{2(d_0+1)} g(w|\boldsymbol{d})P(w) \le \sum_{w=1}^{2(d_0+1)} g^*(w)P(w) \tag{21}$$

where $g^*(w)$ is defined as

$$g^*(w) = \begin{cases} \binom{n}{w}, & \text{if } w = \text{even and } 1 \le w \le d_0 \\ |\mathcal{S}| - \sum_{d=0}^{d_0}\binom{n}{d}, & \text{if } w = \text{even and } w = d_0+1 \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

Since $x/(x+1)$ is an increasing function for $x \ge 0$, we have from (19) and (21) that

$$K_u \le |\mathcal{S}| \, \frac{\sum_{w=1}^{2(d_0+1)} g^*(w)P(w)}{\sum_{w=1}^{2(d_0+1)} g^*(w)P(w) + 1}. \tag{23}$$

Now we evaluate $\epsilon = \mathrm{E}_H[\epsilon_H]$, the expectation of ϵ_H over MacKay's ensemble. Letting M_s be the expectation of $M_s(H)$ over the ensemble, we obtain from (17), (18), and (23) that

$$\begin{aligned} \epsilon &= E_H\left[\frac{|\mathcal{X}_2^n|}{2^n}\right] \\ &= \frac{E_H[M_s(H)]}{2^m} \\ &= \frac{M_s}{2^m} \\ &= \frac{2^m + K_u - |\mathcal{S}|}{2^m} \\ &\le 1 - \frac{|\mathcal{S}|}{2^m\left(\sum_{w=1}^{2(d_0+1)} g^*(w)P(w) + 1\right)}. \end{aligned} \tag{24}$$

We now evaluate the right-hand side of (21) by dividing the summation into two parts based on the integer d_1. From (6), (12), (22), and the Appendix, we have

$$\begin{aligned} \sum_{w=1}^{2(d_0+1)} g^*(w)P(w) &= \sum_{w=1}^{d_1} g^*(w)P(w) + \sum_{w=d_1+1}^{2(d_0+1)} g^*(w)P(w) \\ &\le \sum_{w=0}^{d_1}\binom{n}{w} + \frac{|\mathcal{S}|}{2}P(d_1) \qquad (25) \\ &\le 2^{nh(d_1/n)} + \frac{|\mathcal{S}|}{2}P(d_1) \\ &< 2^{n\eta_5} + \frac{|\mathcal{S}|}{2}P(d_1). \qquad (26) \end{aligned}$$

Thus, from (4), (10), (16), (24), and (26), ϵ is bounded as follows:

$$\begin{aligned} \epsilon &< 1 - \frac{|\mathcal{S}|}{2^m\left(2^{n\eta_5} + \frac{|\mathcal{S}|}{2}P(d_1) + 1\right)} \\ &\le 1 - \frac{|\mathcal{S}|}{2^m\left(2^{n\eta_5} + \frac{|\mathcal{S}|}{2^m}\exp(me^{-2d_1t/m}) + 1\right)} \\ &= 1 - \frac{1}{\frac{2^m(2^{n\eta_5}+1)}{|\mathcal{S}|} + \exp(me^{-2d_1t/m})} \\ &< 1 - \frac{1}{2^{-n\left(\eta_2-\eta_3-\frac{1}{n}\log(n+1)\right)}(2^{n\eta_5}+1) + \exp(me^{-2d_1t/m})} \\ &= 1 - \frac{1}{\epsilon_2 + e^{\epsilon_3}} \end{aligned} \tag{27}$$

where ϵ_2 goes to zero as n increases because ϵ_2 can be represented by

$$\begin{aligned} \epsilon_2 &= 2^{-n(\eta_2-\eta_3-\log(n+1)/n)}(2^{n\eta_5}+1) \\ &= 2^{-n(\eta_2-\eta_3-\eta_5-\log(n+1)/n)} + 2^{-n(\eta_2-\eta_3-\log(n+1)/n)} \end{aligned} \tag{28}$$

and (9) holds.

On the other hand, we have from (12) and $m/n = 1 - R$ that

$$\begin{aligned} \epsilon_3 &= me^{-2d_1t/m} \\ &= me^{-2(d_1/n)(n/m)t} \\ &< me^{-2h^{-1}(\eta_4)\frac{1}{1-R}t} \\ &= e^{-2h^{-1}(\eta_4)\frac{1}{1-R}t + \ln m}. \end{aligned} \tag{29}$$

Thus, if for a fixed $\lambda > 1$

$$t = \frac{\lambda(1-R)\ln m}{2h^{-1}(\eta_4)} = \frac{\lambda(1-r)(\ln n + \ln(1-R))}{2h^{-1}(\eta_4)}$$

which is $O(\log n)$, ϵ_3 goes to zero as n increases. This means that $\epsilon \to 0$ as $n \to \infty$. Finally, we note that there exists an LDPC code in the ensemble that attains a distortion not larger than the ensemble averaged distortion.

Remark 1: In the proof of Theorem 1, we assumed that each randomly generated H has rank m. But a parity-check matrix H' may have rank m', which is less than m. We note that such codes are included in MacKay's ensemble and the rate R' of a code with H' is given by $R' = (n-m')/n > (n-m)/n = R$. However, we note that when this code is encoded by the distortion dictionary method, (18) still holds and $M_s(H')$ must satisfy from (17) that

$$M_s(H') = 2^m - K_s(H') \ge 2^m - 2^{m'}$$

because the number of different syndrome vectors in the dictionary $K_s(H')$ is not larger than $2^{m'}$. Thus, ϵ_H of this code satisfies from (18) that

$$\begin{aligned} \epsilon_H &= \frac{M_s(H')}{2^m} \\ &\ge \frac{2^m - 2^{m'}}{2^m} \\ &\ge \frac{2^m - 2^{m-1}}{2^m} \ge \frac{1}{2} \end{aligned}$$

which is larger than $\epsilon = \mathrm{E}_H[\epsilon_H]$. This means that any code with H' cannot attain ϵ, and hence, the code attaining ϵ in MacKay's ensemble must have rate $R = (n-m)/n$.

Remark 2: By calculating the Taylor expansion of (27) we can derive a bound on ϵ as follows:

$$\begin{aligned}\epsilon &\le 1 - \frac{1}{\epsilon_2 + e^{\epsilon_3}} \\ &\le 1 - \frac{1}{1 + (\epsilon_2 + \epsilon_3 + O({\epsilon_3}^2))} \\ &\le \epsilon_2 + \epsilon_3 + O({\epsilon_3}^2)\end{aligned}$$

where ϵ_2 and ϵ_3 are given by (28) and (29), respectively.

Letting $\eta_1 \approx \eta_2 \approx h(D) - m/n = h(D) - (1-R) = R - R(D)$, $\eta_4 \approx \eta_5$, η_3 be sufficiently small, and n be sufficiently large in (28), we have $\epsilon_2 \approx 2^{-n[R-R(D)-\eta_4]}$. Hence, ϵ_2 converges to zero with exponent $R - R(D) - \eta_4$ as n goes to infinity. On the other hand, since ϵ_3 is given by (29), ϵ_3 goes to zero with

$$O\left(1/n^{\frac{2h^{-1}(\eta_4)a}{1-R}-1}\right)$$

if $t = a \ln n$ and $a > \frac{1-R}{2h^{-1}(\eta_4)}$. However, in case of $t = bn$ (and $b \ll 1$ in the LDPC codes), ϵ_3 vanishes exponentially with exponent $\frac{2h^{-1}(\eta_4)b}{1-R}$. In the latter case, the exponent of ϵ can be maximized for given $\eta_1 \approx \eta_2 \approx R - R(D) > 0$ by letting η_4 satisfy $R - R(D) - \eta_4 = \frac{2h^{-1}(\eta_4)b}{1-R}$.

Remark 3: In the encoding scheme used to prove Theorem 1, the distortion dictionary requires an exponential size of memory for code length n. Thus, the scheme cannot be used practically when n is large.

In any practical lossy source coding, we need an encoder that works well at rate a little larger than $R(D) = 1 - h(D)$ for distortion D. However, Richardson *et al.* [6] show by the density evolution that a belief propagation decoder does not work well if $R = 1 - h(D)$ for the binary-symmetric channel with bit-error probability D. Thus, the straightforward application of belief propagation methods to the LDPC codes in lossy source coding has no good result. We must devise an encoder that works well even at a noise level larger than the belief propagation method for the same rate.

IV. Conclusion

In this correspondence, we applied LDPC codes to lossy data compression, and proved that LDPC codes with (m, n, t) parity-check matrices for odd t can attain the rate-distortion function asymptotically for the binary i.i.d. source with $\Pr\{x = 1\} = 0.5$. Furthermore, we also considered the relation between the sparsity parameter t and the asymptotic performance of LDPC codes in lossy source coding. We showed that an LDPC code with column weight $O(\log n)$ can attain the rate-distortion function asymptotically. In the proof of error correction by LDPC codes, MacKay [3] used parity-check matrices with both even and odd t. However, we assumed that t is odd. This assumption is necessary in our proof because of the following reason. In the case of odd t, about half of all wt's are odd and we can ignore the half from (1) in Lemma 1. This allows us to bound $\sum_{w=d_1+1}^{2(d_0+1)} g^*(w)P(w)$ by $\frac{|\mathcal{S}|}{2}P(d_1)$ in (25).

The theorem we proved is limited to the case of the binary i.i.d. source with $\Pr\{x = 1\} = 0.5$. For linear codes, it is not simple to prove the source coding theorem by applying the traditional method of typical sequences to linear codes because of the linear space of codewords. Hence, the proof of the general source case with $\Pr\{x = 1\} = q$ remains for future studies.

Although our encoding scheme using the distortion dictionary is not practical from the point of memory size, Theorem 1 justifies the efforts to realize practically good lossy source coding by LDPC codes.

Appendix

For a given $\boldsymbol{d} \in \mathcal{S}$, we consider the number of distortion vectors $\boldsymbol{d}' \in \mathcal{S}$, $\boldsymbol{d}' \neq \boldsymbol{d}$, such that $w = W_{\mathrm{H}}(\boldsymbol{d} - \boldsymbol{d}')$ is even. Assume that $\boldsymbol{d}$ and $\boldsymbol{d}'$ have 1 at the same l positions. Then, letting $d = W_{\mathrm{H}}(\boldsymbol{d})$ and $d' = W_{\mathrm{H}}(\boldsymbol{d}')$, w is given by

$$w = (d - l) + (d' - l) = d + d' - 2l.$$

Thus, the total number of the distortion vectors $\boldsymbol{d}'$ with even w is equal to the number of vectors $\boldsymbol{d}'$ with odd d' or even d' when d is odd or even, respectively. On the other hand, from (14) and (15), the half of distortion vectors in the dictionary $\mathcal{S}$ have even weights $W_{\mathrm{H}}(\boldsymbol{d})$. Hence, the total number of vectors $\boldsymbol{d}'$ with even w is given by $|\mathcal{S}|/2 - 1$.

References

[1] R. G. Gallager, "Low density parity check codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 21–28, Jan. 1962.

[2] ——, *Low Density Parity Check Codes*, ser. Research Monograph. Cambridge, MA: MIT Press, 1963.

[3] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, Mar. 1999. see also the correction: *IEEE Trans. Inform. Theory*, vol. 47, pp. 2101, July, 2001.

[4] 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. Inform. Theory*, vol. 47, pp. 2711–2736, Nov. 2001.

[5] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inform. Theory*, vol. 47, pp. 585–598, Feb. 2001.

[6] T. Richardson, A. Shokrollahi, and R. Urbanke, "The capacity of low-density parity check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599–618, Feb. 2001.

[7] ——, "Design of provably good low-density parity check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619–637, Feb. 2001.

[8] M. Sipser and D. A. Spielman, "Expander codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1710–1722, Nov. 1996.

[9] J. Pearl, *Probabilistic Reasoning in Intelligent Systems*. San Mateo, CA: Morgan Kaufmann, 1988.

[10] B. J. Frey, *Graphical Models for Machine Learning and Digital Communication*. Cambridge, MA: MIT Press, 1998.

[11] G. Miller and D. Burshtein, "Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2696–2710, Nov. 2001.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[13] I. Csiszár and J. Körner, *Information Theroy, Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1981.

[14] T. J. Goblick, "Coding for a discrete information source with a distortion measure," Ph.D. dissertation, Dept. Elec. Eng., MIT, Cambridge, MA, 1962.

[15] T. Berger, *Rate Distortion Theory, A Mathematical Basis for Data Compression*. Englewood Cliffs, NJ: Prentice-Hall, 1971.

[16] A. J. Viterbi and J. K. Omura, "Trellis encoding of memoryless discrete-time sources with a fidelity criterion," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 325–332, May 1974.

[17] M. Kac, "Random walk and the theory of Brownian motion," *Amer. Math. Monthly*, vol. 54, pp. 369–391, 1947.

[18] G. Letac and L. Takacs, "Random walk on the m-dimensional cube," *J. Reine Angrew. Math.*, vol. 310, pp. 187–195, 1979.