[2] R. G. Gallager, "Low density parity check codes," *IEEE Trans. Inf. Theory*, vol. IT-8, no. 1, pp. 21–28, Jan. 1962.
[3] M. Sipser and D. A. Spielman, "Expander codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1660–1686, Nov. 1996.
[4] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *IEE Electron. Lett.*, vol. 32, no. 18, pp. 1645–1646, Aug. 1996.
[5] N. Wiberg, "Codes and Decoding on General Graphs," Ph.D. dissertation, Linköping University, Linköping, Sweden, 1996.
[6] N. Wiberg, H.-A. Loeliger, and R. Kötter, "Codes and iterative decoding on general graphs," in *Proc. IEEE Symp. Information Theory*, Adelaide, Australia, Sep. 1995, p. 468.
[7] H. Jin and R. J. McEliece, "General coding theorems for turbo-like codes," in *Proc. IEEE Symp. Information Theory*, Sorrento, Italy, Jun./Jul. 2000, p. 120.
[8] Y. Mao and A. H. Banihashemi, "A heuristic search for good low-density parity-check codes at short block lengths," in *Proc. Int. Conf. Communications*, vol. 1, Helsinki, Finland, Jun. 2001, pp. 41–44.
[9] S. Benedetto and G. Montorsi, "Design of parallel concatenated convolutional codes," *IEEE Trans. Communun.*, vol. 44, no. 5, pp. 591–600, May 1996.
[10] K. M. Chugg, A. Anastasopoulos, and X. Chen, *Iterative Detection: Adaptivity, Complexity Reduction, and Applications*. Norwell, MA: Kluwer, 2001.
[11] S. Crozier, "New high-spread high-distance interleavers for turbo-codes," in *Proc. 20th Biennial Symp. Communications*, Kingston, ON, Canada, May 2000, pp. 3–7.
[12] T. Richardson, M. A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity check codes," *IEEE Trans. Information Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.
[13] J. Flum and M. Grohe, "The parameterized complexity of counting problems," in *Proc. IEEE Symp. Foundations of Computer Science*, Vancouver, BC, Canada, Nov. 2002, pp. 538–547.
[14] N. Alon, R. Yuster, and U. Zwick, "Finding and counting given length cycles," *Algorithmica*, vol. 17, no. 3, pp. 209–223, 1997.
[15] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 533–547, Sep. 1981.
[16] 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.
[17] R. Diestel, *Graph Theory*, 2nd ed. New York: Springer-Verlag, 2000.
[18] A. G. Thomason, "Hamiltonian cycles and uniquely edge-colorable graphs," *Ann. Discr. Math.*, vol. 3, pp. 259–268, 1978.
[19] H. Zhang and J. M. F. Moura, "The design of structured regular LDPC codes with large girth," in *Proc. GLOBECOM Conf.*, Taipei, Taiwan, Dec. 2003, pp. 4022–4027.
[20] D. J. C. MacKay. Encyclopedia of Sparse Graph Codes. [Online]. Available: http://www.inference.phy.cam.ac.uk/mackay/codes/data.html
[21] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.
[22] L. S. Blackford, J. Demmel, J. Dongarra, I. Duff, S. Hammarling, G. Henry, M. Heroux, L. Kaufman, A. Lumsdaine, A. Petitet, R. Pozo, K. Remington, and R. C. Whaley, "An updated set of basic linear algebra subprograms (BLAS)," *ACM Trans. Math. Software*, vol. 28, no. 2, pp. 135–151, June 2002.

Performance of Low-Density Parity-Check Codes With Linear Minimum Distance

Hossein Pishro-Nik, *Member, IEEE*, and
Faramarz Fekri, *Senior Member, IEEE*

***Abstract*—This correspondence studies the performance of the iterative decoding of low-density parity-check (LDPC) code ensembles that have linear typical minimum distance and stopping set size. We first obtain a lower bound on the achievable rates of these ensembles over memoryless binary-input output-symmetric channels. We improve this bound for the binary erasure channel. We also introduce a method to construct the codes meeting the lower bound for the binary erasure channel. Then, we give upper bounds on the rate of LDPC codes with linear minimum distance when their right degree distribution is fixed. We compare these bounds to the previously derived upper bounds on the rate when there is no restriction on the code ensemble.**

***Index Terms*—Bipartite graphs, erasure channel, error floor, iterative decoding, low-density parity-check (LDPC) codes, minimum distance, performance bound.**

I. Introduction

In some applications, it is necessary to design codes that do not suffer from the error floor problem at the desired bit error rates (BERs), while their rates are close to the channel capacity. For example, in some page-oriented memories, low-density parity-check (LDPC) codes can result in very efficient coding schemes [1]. In these memory systems, we can use large block lengths and thus we get performance close to the Shannon limit. However, BER's less than 10^{-12} are required. Since the storage capacity of the system is directly proportional to the code rate, it is very important that the code rate be close to the capacity of the channel. Thus, we need to design LDPC codes that do not show error floor for the BERs higher than 10^{-12}, and at the same time, have a threshold near the Shannon limit.

One method to solve the error floor problem is to use an outer code. In this method we use the outer code to reduce the BER. This method slightly increases the complexity of the system. This is specifically undesirable in page-oriented memories where simple and fast decoding algorithms are required. Moreover, using an outer code results in a rate loss; however, the rate loss is usually small. There are also methods for decreasing the error-floor effect for the capacity-approaching codes [2]; however, these methods are sometimes not effective for the BERs required by the storage systems. Depending on the application, the above methods may or may not be suitable. As it will be described in more detail, an alternative option is to use codes with linear minimum distance. These codes also have some desirable properties other than good error floor performance. Thus, in this paper our aim is to study codes with linear minimum distance and to find bounds on their achievable rates.

Manuscript received February 12, 2004; revised June 27, 2005. This work was supported in part by the Air Force Office of Scientific Research under Grant F49620-02-1-0053.

H. Pishro-Nik is with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01003-9292 USA (e-mail: pishro@ecs.umass.edu).

F. Fekri is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332-0250 USA (e-mail: fekri@ece.gatech.edu).

Communicated by A. E. Ashikhmin, Associate Editor of Coding Theory.
Digital Object Identifier 10.1109/TIT.2005.860439

Here we use the ensemble of LDPC codes described in [3]. The ensemble (d_v, d_c) of LDPC codes is an ensemble that consists of regular LDPC codes in which variable nodes have degree d_v and check nodes have degree d_c. In order to construct a graph from the ensemble we do the following. To each variable or check node we assign d_v or d_c sockets, respectively. We label the variable nodes and check nodes sockets separately with the set $\{1, 2, \ldots, nd_v\}$. We then pick a random permutation π on $E = nd_v$ letters. For each i, we put an edge between the socket i and $\pi(i)$. Two, vertices are connected if there is an edge between their sockets. For irregular ensembles, we use a degree distribution that is defined by the pair (λ, ρ), in which λ and ρ are polynomials. In particular, we have

$$\lambda(x) = \sum \lambda_i x^{i-1}, \quad \rho(x) = \sum \rho_i x^{i-1}$$

where λ_i is the fraction of edges connected to a variable node of degree i and ρ_i is the fraction of edges connected to a check node of degree i. The ensemble (λ, ρ) is defined similar to the regular ensembles. It has been shown in [3] and [4] that any ensemble (λ, ρ) has a threshold under the iterative decoding. If the noise level of the channel is bellow the threshold, the BER of the iterative decoder tends to zero as the code block length tends to infinity. On the other hand, if the noise level is above the threshold, the BER is bounded away from zero. Throughout the paper, by threshold we mean the the threshold of the code ensemble under the iterative decoding.

The error floor problem is related to the minimum distance and the minimum stopping set size of the code. As it is shown in [5], [6], and [7], a suitably expurgated ensemble (λ, ρ) of LDPC codes has a linear typical minimum distance and minimum stopping set size if $\lambda'(0)\rho'(1) < 1$. Here, a constant fraction of the codes in the ensemble with low minimum stopping set size are removed in the expurgation. On the other hand, if $\lambda'(0)\rho'(1) > 1$ the size of the minimum stopping set and the minimum distance is sublinear with high probability. The codes with small minimum distance and small minimum stopping set (the ones with $\lambda'(0)\rho'(1) > 1$) suffer from the error floor problem. On the other hand, if the minimum distance is linear, the error-floor effect is reduced substantially. For the binary erasure channel (BEC) with low enough channel erasure probability, using a simple union bound we can show that the BER of an expurgated ensemble with $\lambda'(0)\rho'(1) < 1$ decreases exponentially with respect to the code length and the channel erasure probability [8], [9]. Thus, the code shows a lower error floor effect for the corresponding erasure probability range. Although this has not been shown for other channels, simulations clearly show the superiority of these codes in terms of the error-floor effect over the codes having a sublinear minimum distance. It is shown in [10] that (assuming that the first two derivatives of $1 - \rho^{-1}(1 - x)$ are positive in $(0, 1)$) capacity-achieving LDPC codes over the BEC satisfy $\lambda'(0)\rho'(1) > 1$ and hence have sublinear minimum distance. Thus, they are very likely to suffer from the error-floor problem. Code ensembles satisfying $\lambda'(0)\rho'(1) < 1$ present other good properties such as having a strictly positive relative erasure correction radius. In other words, if the size of the minimum stopping set is greater than δn, where n is the code length and δ is a positive constant, then the code is guaranteed to recover all the erased bits provided that the number of erased bits is less than or equal to δn.

The question that arises here is how close we can get to the Shannon limit while the minimum distance is maintained linear with respect to the code length. In other words, how much do we possibly lose by restricting to codes with linear minimum distance? This paper is concerned with this question.

In this paper, we find lower bounds on the achievable rates over memoryless binary-input output-symmetric (MBIOS) channels using LDPC codes with linear minimum distance when decoded using the belief propagation algorithm. Then, we obtain upper bounds for the rate of these ensembles over the BEC. We give upper bounds similar to [11] for codes with a given right degree distribution. We will compare these bounds with the ones given in [11] to estimate the rate loss due to restricting to codes with the linear minimum distance property. We think that, like almost any other properties of LDPC codes, the study of this question over the BEC can provide better understanding of the problem over other channels.

II. Lower Bounds on the Achievable Rates

In this section we provide lower bounds on the achievable rates of LDPC codes with linear minimum distance over MBIOS channels. Consider a MBIOS channel with parameter θ, where $\theta \in [\theta_{\min}, \theta_{\max}]$ and $\theta_{\min}, \theta_{\max} \in \mathbb{R} \cup \{-\infty, +\infty\}$. For example, for the binary-input additive white Gaussian noise (BIAWGN) channel, θ can be considered as the variance σ of the noise. Let $\mathcal{C}$ be a class of channels with parameter θ. Thus, any channel C_θ in $\mathcal{C}$ is uniquely determined by its variable θ. A channel in $\mathcal{C}$ with parameter θ_0 is called C_{θ_0}. The capacity of the channel C_{θ_0} is denoted by c_{θ_0}. For simplicity, we assume that c_θ is a continuous function of θ. Similar to [3], we consider physically degraded channels. For clarity of exposition we assume that if $\theta_1 < \theta_2$, then C_{θ_2} is physically degraded with respect to C_{θ_1}. For the channel C_{θ_0} we define the random variable Z_{θ_0} as

$$Z_{\theta_0} = \ln \frac{p(x=1|y, \theta=\theta_0)}{p(x=-1|y, \theta=\theta_0)} = \ln \frac{p(y|x=1, \theta=\theta_0)}{p(y|x=-1, \theta=\theta_0)}$$

where x and y are the input and output of the channel, respectively. Let $F_0(x; \theta)$ be the distribution function of Z_θ under the assumption that a "1" is transmitted. Similar to [4], we define

$$r(\theta) = -\ln\left(\int_{\mathbb{R}} e^{-\frac{x}{2}} d(F_0(x; \theta))\right).$$

For any $\theta \in [\theta_{\min}, \theta_{\max}]$, let α_θ be the supremum value of R/c_θ for which there exists an ensemble (λ, ρ) of LDPC codes that has rate R and threshold (under belief propagation decoding) higher than or equal to θ. For the BEC we have $\alpha_\theta = 1$ where θ is the erasure probability [12], [10], [13], [14]. For other MBIOS channels we know $0 \le \alpha_\theta \le 1$ and it is conjectured that $\alpha_\theta = 1$ for all θ. Let R_θ be the supremum value of R, the rate of an ensemble (λ, ρ) of LDPC codes with the threshold higher than or equal to θ satisfying $\lambda'(0)\rho'(1) < 1$. Shokrollahi's flatness theorem [10] implies that, under certain conditions, $R_\theta < c_\theta$ for the BEC. Thus, unlike the general class of LDPC codes, the LDPC codes with linear typical minimum distance are not capacity-achieving. Moreover, it is conjectured in [10] that the stability condition is satisfied with equality for capacity-achieving LDPC codes over other MBIOS channels. If this is the case, then $R_\theta < c_\theta$ for all MBIOS channels. However, one of the results of this paper is that we do not lose too much by restricting to the codes with the linear minimum distance constraint. We first prove two lemmas.

Lemma 1: Let (λ, ρ) be an ensemble of LDPC codes having the threshold $\theta_{\rm th}$ under belief propagation decoding. For $0 \le \tau < \lambda_2$ define λ^τ and ρ^τ as follows:

$$\lambda^\tau(x) = (\lambda_2 - \tau)x + (\lambda_3 + \tau)x^2 + \sum_{i>3} \lambda_i x^{i-1}$$

$$\rho^\tau(x) = \rho(x) = \sum_i \rho_i x^{i-1}.$$

Then the threshold of the ensemble $(\lambda^\tau, \rho^\tau)$ is greater than or equal to $\theta_{\rm th}$.

Proof: Let $\theta < \theta_{\rm th}$ and P_0 be the density function of Z_θ. Then the density evolution formulas for the ensemble (λ, ρ) can be described as [4]

$$P_l = P_0 \bigotimes \lambda(Q_l) \quad (1)$$

$$Q_l = \Gamma^{-1}(\rho(\Gamma(P_{l-1}))). \quad (2)$$

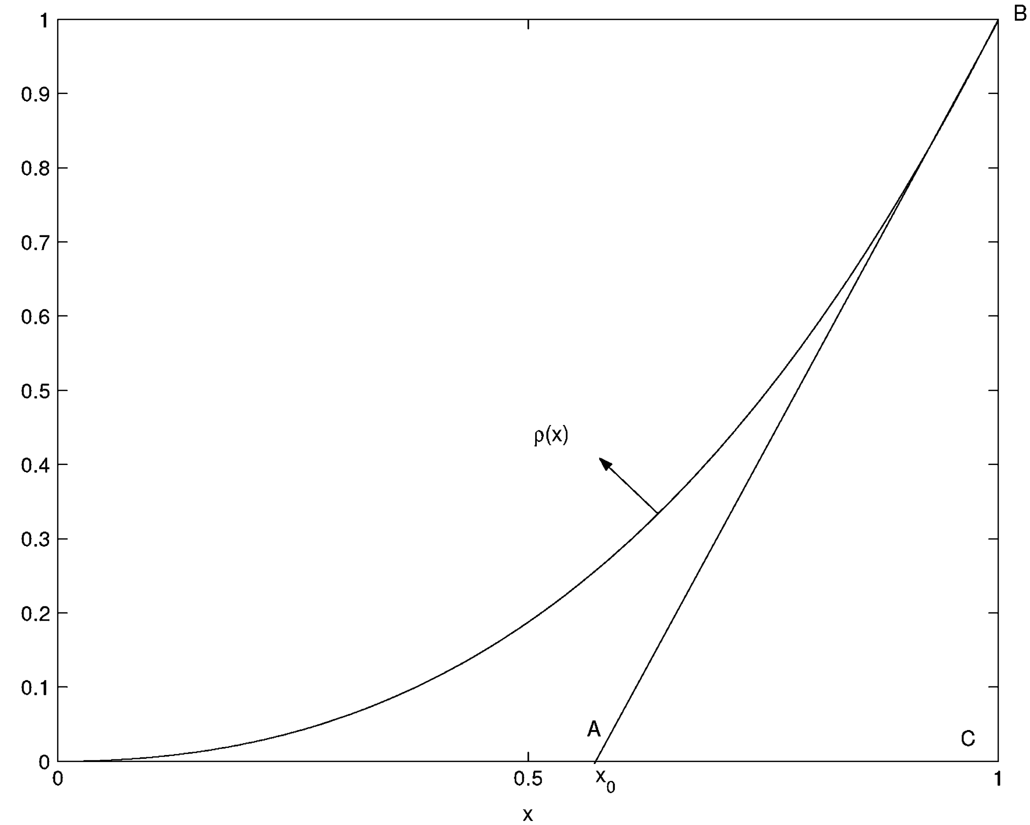

Fig. 1. Plot of the function $\rho(x)$.

For the ensemble $(\lambda^\tau, \rho^\tau)$, we introduce a message-passing decoding algorithm named Algorithm B. In this algorithm, for any edge e that connects a variable node v and a check node c, the messages are computed in the following way in each iteration. The message from c to v is computed the same way as the standard belief propagation algorithm. If the degree of v is not equal to 3, then the message from v to c is also computed the same way as the standard belief propagation algorithm. However, if the degree of v is equal to 3 then there are two other edges (e_1 and e_2) incident with v. In this case, with probability $\frac{\tau}{\lambda_3^\tau} = \frac{\tau}{\lambda_3+\tau}$, we choose one of the edges e_1 and e_2 at random. Suppose we choose e_1. Then, we compute the message from v to c similar to the belief propagation algorithm except that we disregard e_1 in the computation. In other words, the message from v to c is computed based on the observation from the channel and the message transmitted to v by e_2 in the previous iteration. Now if we obtain the density evolution formulas for Algorithm B on the ensemble $(\lambda^\tau, \rho^\tau)$, we get the same equations as (1) and (2). This shows that when $\theta < \theta_{\text{th}}$, the error probability of Algorithm B on the ensemble $(\lambda^\tau, \rho^\tau)$ tends to zero as the number of iteration goes to infinity. But, based on the cycle-free-neighborhood lemma in [3], the belief propagation algorithm has an asymptotic error rate less than or equal to Algorithm B. Thus we conclude when $\theta < \theta_{\text{th}}$, the error probability of the belief propagation decoding on the ensemble $(\lambda^\tau, \rho^\tau)$ tends to zero as the number of iteration goes to infinity. Therefore, the threshold of the ensemble $(\lambda^\tau, \rho^\tau)$ under belief propagation decoding is greater than or equal to θ_{th}. □

The intuition behind Lemma 1 is that we change degree-two variable nodes into degree-three variable nodes without changing the check node degree distribution. We note that the lemma states that the threshold can only improve. The reason for this improvement is that the rate of the code is getting worse, as more bits receive more information.

Lemma 2: For any ensemble (λ, ρ) of LDPC codes, we have

$$\frac{1}{2\rho'(1)} < \int_0^1 \rho(x)\, dx.$$

Proof: The function $\rho(x)$ has the following properties:

$$\rho(0) = 0, \quad \rho(1) = 1, \quad \rho^{(n)}(x) > 0, \qquad \text{for } x \in (0,1] \text{ and } 0 \le n \le d_{c_{\max}}$$

where $\rho^{(n)}(x)$ is the n'th derivative of the function ρ and $d_{c_{\max}}$ is the largest degree of check nodes. Fig. 1 shows the plot of a typical $\rho(x)$. The tangent line to the curve at point $(1,1)$ is also shown in the figure. We have

$$1 - x_0 = \frac{1}{\rho'(1)}.$$

Therefore, the area of the triangle ABC in Fig. 1 is equal to $\frac{1}{2\rho'(1)}$. Since $\rho(x)$ is a convex function in $[0,1]$, the area of the triangle ABC is less than the area under the curve. That is, we have

$$\frac{1}{2\rho'(1)} < \int_0^1 \rho(x)\, dx.$$ □

Theorem 1: For any MBIOS channel with parameter θ and capacity c_θ, we have

$$R_\theta \ge 1 - \frac{1 - \alpha_\theta c_\theta}{1 - \frac{(1-\alpha_\theta c_\theta)(e^{r(\theta)}-1)}{3}}.$$

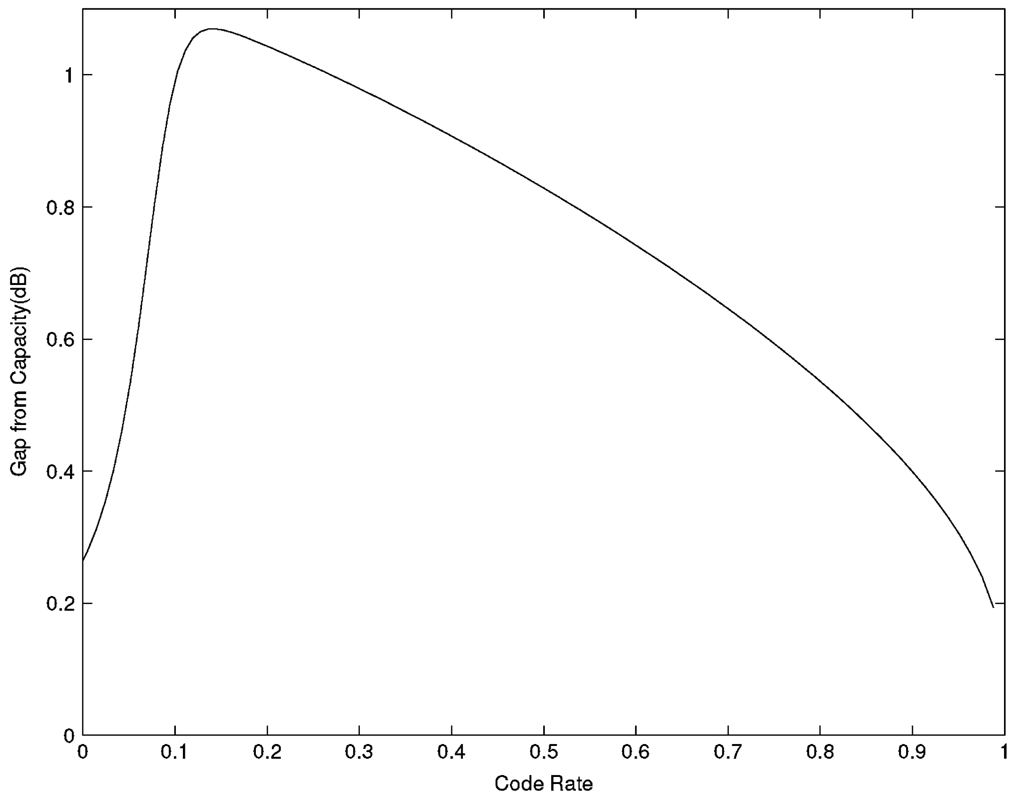

Fig. 2. Upper bound on the gap between the ensemble threshold and the Shannon limit of the BIAWGN channel for LDPC code ensembles with linear typical minimum distance. The bound is obtained using the lower bound on the rate given by (4).

Proof: Let (λ, ρ) be an ensemble of LDPC codes with $\lambda'(0)\rho'(1) \geq 1$ with the threshold θ_{th}. Similar to Lemma 1, define λ^τ and ρ^τ as follows:

$$\lambda^\tau(x) = (\lambda_2 - \tau)x + (\lambda_3 + \tau)x^2 + \sum_{i>3} \lambda_i x^{i-1}$$
$$\rho^\tau(x) = \rho(x) = \sum_i \rho_i x^{i-1}$$
$$\tau > \frac{\lambda'(0)\rho'(1) - 1}{\rho'(1)}. \tag{3}$$

Then by Lemma 1, the ensemble $(\lambda^\tau, \rho^\tau)$ has a threshold greater than or equal to θ_{th}. It also satisfies ${\lambda'}^{\tau}(0){\rho'}^{\tau}(1) < 1$. Now we claim that for any $\xi > 0$, by a suitable choice of τ, the ensemble has the rate R^τ satisfying

$$R^\tau \geq 1 - \frac{1 - R}{1 - \frac{(1-R)(e^{r(\theta)} - 1)}{3}} - \xi.$$

Assuming the above claim, and using the fact that for any θ there exists an ensemble (λ, ρ) of LDPC codes with the rate arbitrary close to $\alpha_\theta c_\theta$ and threshold higher than θ, we conclude the theorem. It should be noted that if the ensemble that achieves the rate $\alpha_\theta c_\theta$ satisfies $\lambda'(0)\rho'(1) < 1$, then the assertion of the theorem is trivial. Thus we may assume without loss of generality that $\lambda'(0)\rho'(1) \geq 1$. It remains to prove the claim. The rate R^τ can be expressed as

$$\begin{aligned} R^\tau &= 1 - \frac{\int \rho^\tau}{\int \lambda^\tau} \\ &= 1 - \frac{(1-R)\int \lambda}{\int \lambda - \frac{\tau}{6}}, \end{aligned}$$

where the integrals are on $[0, 1]$. Using the stability condition [4] and Lemma 2, we have

$$\begin{aligned} \frac{\lambda'(0)\rho'(1) - 1}{\rho'(1)} &\leq \frac{(e^{r(\theta)} - 1)}{\rho'(1)} \\ &\leq 2(e^{r(\theta)} - 1)\int \rho = 2(1-R)(e^{r(\theta)} - 1)\int \lambda. \end{aligned}$$

Thus, by choosing τ close enough to $\frac{\lambda'(0)\rho'(1)-1}{\rho'(1)}$, we can ensure that

$$R^\tau \geq 1 - \frac{1 - R}{1 - \frac{(1-R)(e^{r(\theta)} - 1)}{3}} - \xi. \qquad \square$$

It is worth noting that Theorem 1 not only gives a lower bound on the achievable rate, but also gives a distribution meeting the lower bound. However, we can find this distribution only if we know codes that approach the optimal rate $\alpha_\theta c_\theta$. We also note that, the basic idea behind Theorem 1 is to start with an optimized degree distribution without any constraint on $\lambda'(0)\rho'(1)$. Then using Lemma 1 we transform the degree distribution into one with $\lambda'(0)\rho'(1) < 1$. Using this method we can find an analytical lower bound on the achievable rate. However, in practice, one may try optimize the degree distribution while imposing $\lambda'(0)\rho'(1) < 1$ as a constraint.

For the BIAWGN channel we let θ be σ, the variance of noise, and the lower bound becomes

$$R_\sigma \geq 1 - \frac{1 - \alpha_\sigma c_\sigma}{1 - \frac{(1-\alpha_\sigma c_\sigma)(e^{\frac{1}{2\sigma'^2}} - 1)}{3}}. \tag{4}$$

Using the lower bound on the rate, we can find an upper bound on the gap between the ensemble threshold and the Shannon limit for

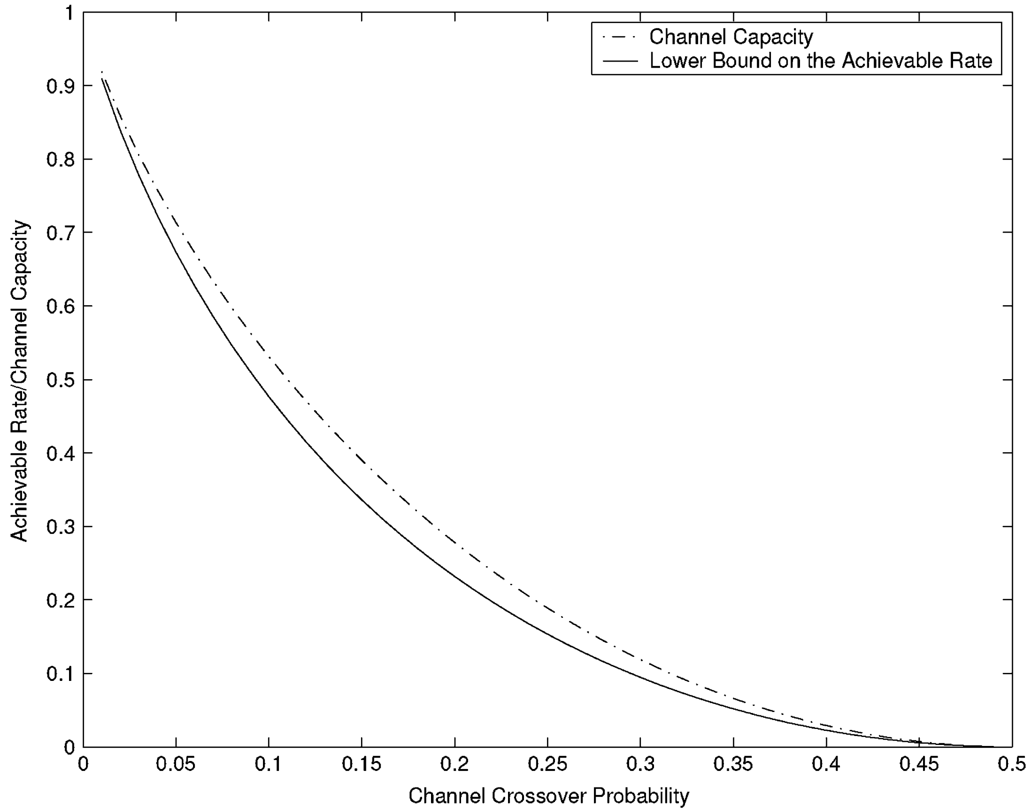

Fig. 3. Lower bound on the achievable rate for LDPC codes with linear minimum distance on the BSC.

the BIAWGN channels. Fig. 2 shows this upper bound for the BIAWGN channel assuming $\alpha_\theta = \alpha_\sigma = 1$ for any $\sigma \in [0, \infty)$ (i.e., assuming that LDPC codes are capacity-achieving over BIAWGN channels). Therefore, as shown in the figure, by restricting to LDPC codes with the linear minimum distance property, we lose at most 1.1 dB. It is worth noting that in storage systems we usually use high-rate codes [1]. Examining Fig. 2 reveals that the gap is very small at these rates. For example, the gap is less than .4 dB for the rate $R = .9$. This is important from the practical point of view.

For the binary symmetric channel (BSC) channel, we let θ be the crossover probability p. Thus, using Theorem 1, the lower bound becomes

$$R_p \geq 1 - \frac{1 - \alpha_p c_p}{1 - \frac{(1-\alpha_p c_p)\left(\frac{1}{2\sqrt{p(1-p)}} - 1\right)}{3}}. \qquad (5)$$

Fig. 3 shows this lower bound for the BSC assuming $\alpha_\theta = \alpha_p = 1$ for any $p \in [0, 1)$ (i.e., assuming LDPC codes are capacity-achieving over the BSC). The figure suggests that the rate loss due to the linear minimum distance property is small.

For the binary erasure channel (BEC), it is possible to improve the bound given by Theorem 1. In the following, we exploit the developed theory on the capacity-achieving sequences to obtain a tighter bound. Furthermore, we can explicitly find sequences of LDPC codes meeting this lower bound.

Theorem 2: For any BEC with erasure probability δ we have

$$R_\delta \geq \frac{5(1-\delta)}{\delta + 5}.$$

Proof: For any BEC with erasure probability δ, we construct a sequence of LDPC code ensembles with linear typical minimum distance and threshold greater than or equal to δ whose rates approach $\frac{5(1-\delta)}{\delta+5}$. Our construction is based on right-regular LDPC codes. Choose $R < 1 - \delta$. As it is shown in [13] and [14], there exists a sequence $\{(\lambda_n, \rho_n)\}_{n=1}^{\infty}$ of right-regular LDPC codes of rate R and thresholds $\delta_{n,\mathrm{th}}$ as follows:

$$\begin{aligned}\lambda_n(x) &= \sum \lambda_{i,n} x^{i-1}\\ \rho_n(x) &= x^{a_n}\\ \lim_{n \longrightarrow \infty} a_n &= \infty\\ \lim_{n \longrightarrow \infty} \delta_{n,\mathrm{th}} &= 1 - R.\end{aligned}$$

Using the flatness theorem, we obtain

$$\begin{aligned}\lim_{n \longrightarrow \infty} \lambda_{2,n} \rho_n'(1) &= \lim_{n \longrightarrow \infty} \lambda_{2,n} a_n\\ &= \frac{1}{1-R}.\end{aligned}$$

Now we construct the sequence $\{(\lambda_n^{\tau_n}, \rho_n^{\tau_n})\}_{n=1}^{\infty}$ of LDPC code ensembles with thresholds $\delta_{\mathrm{th}}^{\tau_n}$ and rates $R_n^{\tau_n}$ as follows:

$$\begin{aligned}\lambda_n^{\tau_n}(x) &= \sum \lambda_{i,n}^{\tau_n} x^{i-1}\\ &= (\lambda_{2,n} - \tau_n)x + (\lambda_{3,n} + \tau_n)x^2 + \sum_{i>3} \lambda_{i,n} x^{i-1}\\ \rho_n^{\tau_n}(x) &= \rho_n(x) = x^{a_n}\\ \tau_n &= \frac{\lambda_{2,n} a_n - 1}{a_n} + \frac{1}{n(a_n + 1)}.\end{aligned}$$

First by Lemma 1, we have $\delta_{\mathrm{th}}^{\tau_n} \geq \delta_{n,\mathrm{th}}$. Since

$$\lim_{n \longrightarrow \infty} \delta_{n,\mathrm{th}} = 1 - R > \delta, \qquad \text{for some } N > 0$$

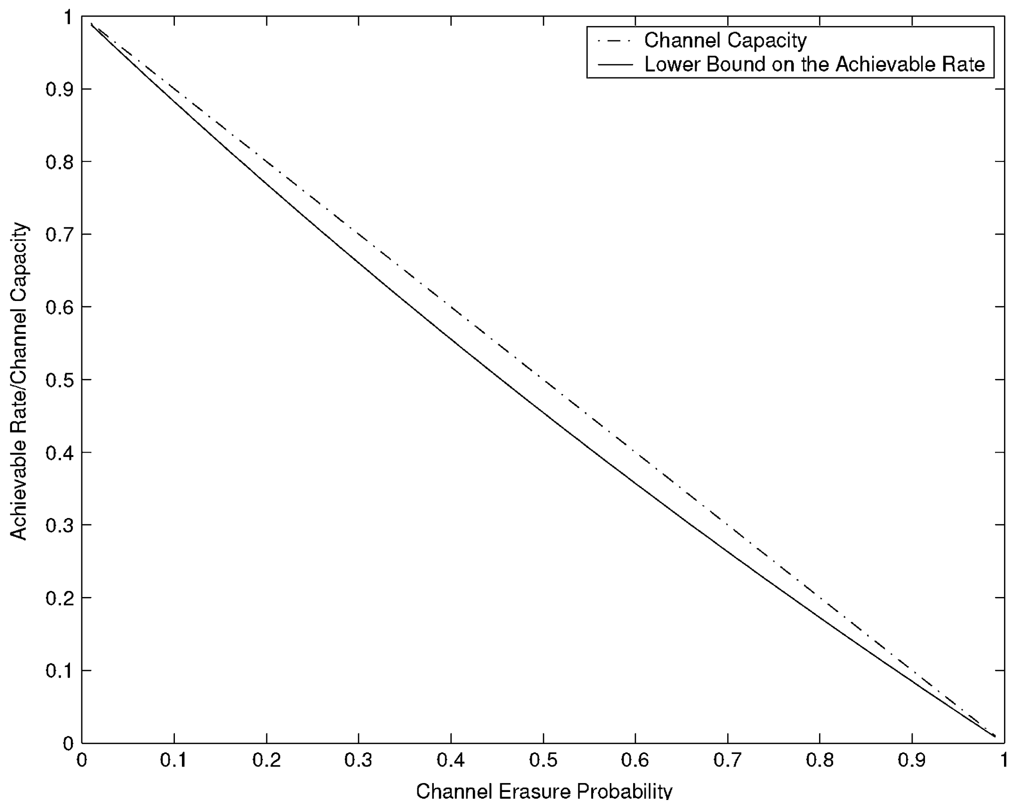

Fig. 4. Lower bound on the achievable rate for LDPC codes with linear minimum distance on the BEC.

we conclude

$$n > N \Longrightarrow \delta_{\rm th}^{\tau_n} \geq \delta.$$

We also note that

$$\begin{aligned} &0 \leq \tau_n \leq \lambda_{2,n} \\ &\lambda_{2,n}^{\tau_n} \rho_n^{\prime \tau_n}(1) = 1 - \frac{a_n}{n(a_n+1)} < 1 \\ &\lim_{n \longrightarrow \infty} \tau_n(a_n+1) = \frac{1}{1-R} - 1. \end{aligned}$$

The rate $R_n^{\tau_n}$ of the ensemble $(\lambda_n^{\tau_n}, \rho_n^{\tau_n})$ is given by

$$R_n^{\tau_n} = 1 - \frac{1-R}{1 - \frac{\tau_n}{6}(a_n+1)(1-R)}.$$

Thus, we obtain

$$\lim_{n \longrightarrow \infty} R_n^{\tau_n} = 1 - \frac{1-R}{1 - \frac{(\frac{1}{1-R}-1)(1-R)}{6}}.$$

If we let R tend to $1-\delta$, we get $R_n^{\tau_n} \longrightarrow \frac{5(1-\delta)}{\delta+5}$, which concludes the theorem □.

Fig. 4 shows this lower bound for the BEC. We note that the lower bound on the achievable rate is very close to the capacity. Since some capacity-achieving right-regular sequences are known [13] and [14], we can explicitly construct the sequences of LDPC codes satisfying the bound given by Theorem 2. It is also easy to see that applying the above procedure to the Tornado sequence [12] will result in the same bound. More generally, we have the following corollary.

Corollary 1: If $\{(\lambda_n, \rho_n)\}_{n=1}^{\infty}$ is a capacity-achieving sequence of rate R, and $b = \limsup_{n \longrightarrow \infty} \frac{\lambda_{2,n}}{\int \lambda_n}$, then applying the procedure in the proof of Theorem 2, we can find a sequence of LDPC codes satisfying the linear-minimum-distance property having rates $R_n^{\tau_n}$ such that

$$R_n^{\tau_n} \longrightarrow 1 - \frac{6\delta}{6-(1-\delta)b}.$$

We now show that we can tighten the lower bound of Theorem 2 for the BEC by including the ensemble of punctured LDPC codes. This can be done by choosing an optimized parent LDPC code that has the linear minimum distance property. Since there is no loss of $\frac{R}{c}$ due to puncturing [15], we can obtain higher rate LDPC codes with the linear distance property if the puncturing fraction q is less than P defined in Theorem 3. It can be concluded that the resulting bound on $\frac{R}{c}$ can improve Theorem 2.

Let us define the performance of any ensemble $\mathcal{C}$ of LDPC codes over the erasure channel by

$$\eta_{\mathcal{C}} = \frac{R}{C} = \frac{R}{1-\delta_{\rm th}}$$

where $\delta_{\rm th}$ is the threshold of the code under the standard iterative decoding over the BEC. For $\nu \in (0,1)$, let b_ν be the asymptotic average distance distribution defined in [16]. Then, we have the following theorem.

Theorem 3: Let (λ, ρ) be an ensemble of LDPC codes of rate R with typical relative minimum distance ν^* (i.e., $d_{\min} \geq \nu^* n$ with high probability for the expurgated ensemble, where n is the block length) and $\frac{R}{C} = \frac{R}{1-\delta_{\rm th}} = \eta_0$. Let

$$P = \sup\{p : b_\nu + \nu \ln(p) < 0,\ \forall \nu \in [\nu^*, 1]\}. \quad (6)$$

Then for rates r satisfying $R \leq r < \frac{R}{1-P}$, there exist punctured LDPC codes whose performance over the erasure channel satisfies $\eta \geq \eta_0$ and has linear typical minimum distance.

Proof: Let $q < P = \sup\{p : b_\nu + \nu \ln(p) < 0, \quad \forall \nu \in [\nu^*, 1]\}$. We perform the following experiment. We choose a code from the expurgated ensemble (λ, ρ) at random. Let h_i be the ith column of the corresponding $m \times n$ parity-check matrix H. We then puncture each bit in the codeword independently with probability q [17]. Puncturing a bit in the codeword can be viewed as erasing the corresponding column of the matrix. Let $A \subset \{1, 2, \ldots, n\}$ with $|A| = l = \gamma n, 0 < \gamma < 1$, and E_A be the event that $\sum_{i \in A} h_i = 0$. Let also Q_A be the number of erased columns in the set A. Then for $0 \leq \zeta < \gamma$, we have

$$\begin{aligned}\Pr\{Q_A \geq (\gamma - \zeta)n\} &= \sum_{i=(\gamma-\zeta)n}^{l} \binom{l}{i} q^i (1-q)^{l-i} \\ &\leq \frac{1}{\sqrt{2\pi}} \frac{1 - \frac{\zeta}{\gamma}}{(1 - \frac{\zeta}{\gamma} - q)\sqrt{n(\gamma - \zeta)\frac{\zeta}{\gamma}}} \left[\frac{1 - \frac{\zeta}{\gamma}}{q}\right]^{-(1-\frac{\zeta}{\gamma})\gamma n} \\ &\quad \times \left[\frac{(1-q)\gamma}{\zeta}\right]^{\zeta n}\end{aligned}$$

where we used [18, Theorem 1.1]. If p_d is the probability that the minimum distance d is sublinear, then p_d is upper-bounded by

$$o(1) + \sum_{A \subset \{1,2,\ldots,n\}, |A| = \gamma n \geq \nu^*} \Pr\{E_A\} \Pr\{Q_A \geq (\gamma - \zeta)n\}.$$

Let $c_s = \sup\{b_\nu + \nu \ln(q), \nu \in [\nu^*, 1]\}$. Since $q < P$, we have $c_s < 0$. Applying (7), and letting ζ tend to zero we obtain

$$p_d = o(1) + O(e^{\frac{nc_s}{2}}) \rightarrow \quad 0 \quad \text{as} \quad n \rightarrow \infty. \qquad \square$$

Using the $(3, 6)$ regular ensemble as an example, we find that for the rates $0.5 \leq r < 0.8469$, there exist punctured LDPC codes with $\eta \geq 0.8763$ and linear typical minimum distance. By finding good degree distributions we can tighten the lower bound on the achievable rates using Theorem 3.

As we mentioned, for ordinary LDPC code ensembles, the conditions for linear typical minimum distance and linear typical minimum stopping set size are the same. However, for a punctured ensemble this may not be the case. Thus, it would be desirable to obtain similar results to Theorem 3 for the codes with linear minimum stopping set size, rather than the linear minimum distance. In fact, this can be done by replacing the b_v function with the stopping set distribution of the ensemble found in [7].

III. Upper Bounds on the Achievable Rates

In this section we provide upper bounds on the achievable rates using LDPC codes with linear typical minimum distance over the BEC. In [11], authors derived upper bounds on the achievable rates of LDPC codes over the BEC given their right-degree distribution. We derive similar bounds for LDPC codes with linear minimum distance. By comparing our bounds with the bounds in [11], we get an estimate of the rate loss due to the linear minimum distance constraint. As in [11], it suffices to consider only the case $\delta\rho'(1) > 1$, where δ is the channel erasure probability.

Theorem 4: Let (λ, ρ) be an ensemble of LDPC codes with fixed $\lambda'(0) = \lambda_2$ and $\rho'(1)$, whose threshold over the BEC is higher than or equal to δ. Then, we have

$$R \leq 1 - \frac{\delta}{1 - (1-\delta)^{2\rho'(1)}} \left[1 + \frac{(1 - \lambda_2\rho'(1)\delta)^3}{3\delta^3\rho'(1)^3(1-\lambda_2)^2}\right]. \tag{7}$$

Proof: For a given right-degree distribution function $\rho(x)$ we define $y_\rho(x)$ as

$$y_\rho(x) = \frac{1 - \rho^{-1}(1-x)}{\delta}.$$

As it is shown in [11], we have

$$\frac{1}{\delta} - \frac{1}{1-R} = \frac{1}{\int \rho} \int (y - \lambda)$$

where the integrals are taken over the interval $[0, 1]$. Let $t(x)$ be the tangent line to $y(x)$ at the origin. Moreover, we define

$$\alpha(x) = \lambda_2 x + (1 - \lambda_2)x^2.$$

Then we have $\alpha(x) \geq \lambda(x)$ for $x \in [0, 1]$. Computing the shaded area in Fig. 5 and applying Lemma 2, we obtain the bound in the theorem. $\square$

Now if we consider the ensemble (λ, ρ) of LDPC codes having the linear minimum distance property, we would have $\rho'(1) < \frac{1}{\lambda_2}$. Thus, we have the followingcorollary.

Corollary 2: For any ensemble of LDPC codes with $\lambda'(0) = \lambda_2$, a linear typical minimum distance, and a threshold over the BEC that is higher than or equal to δ, we have

$$R \leq 1 - \frac{\delta}{1 - (1-\delta)^{\frac{2}{\lambda_2}}} \left[1 + \frac{(1-\delta)^3\lambda_2^3}{3\delta^3(1-\lambda_2)^2}\right].$$

We note that this inequality is similar to the bound given by [13] and the zero-order bound of [11]; however, it has an extra term which is due to the linear-minimum distance property. Now, as in [11f], we consider the ensemble of LDPC codes with a fixed given right degree distribution and obtain an upper bound on the achievable rate.

Theorem 5: Consider an ensemble (λ, ρ) of LDPC codes with threshold higher than δ over the BEC that has a linear typical minimum distance. Define

$$b(x) = \frac{1}{\rho'(1)}x + (1 - \frac{1}{\rho'(1)})x^2. \tag{8}$$

Let $c(x) = \min\{y_\rho(x), b(x)\}$ in $[0, 1]$. Let also $f_\rho(x) = y_\rho(x) - c(x)$. Then, we have

$$R \leq 1 - \frac{\delta}{1 - \frac{\delta}{\int \rho} \int f_\rho}$$

where the integrals are taken over the interval $[0, 1]$.

Proof: The condition $\lambda'(0)\rho'(1) < 1$ implies that $b(x) \geq \alpha(x)$. Thus $b(x) \geq \lambda(x)$. Computing the area between $y_p(x)$ and $b(x)$ concludes the theorem. $\square$

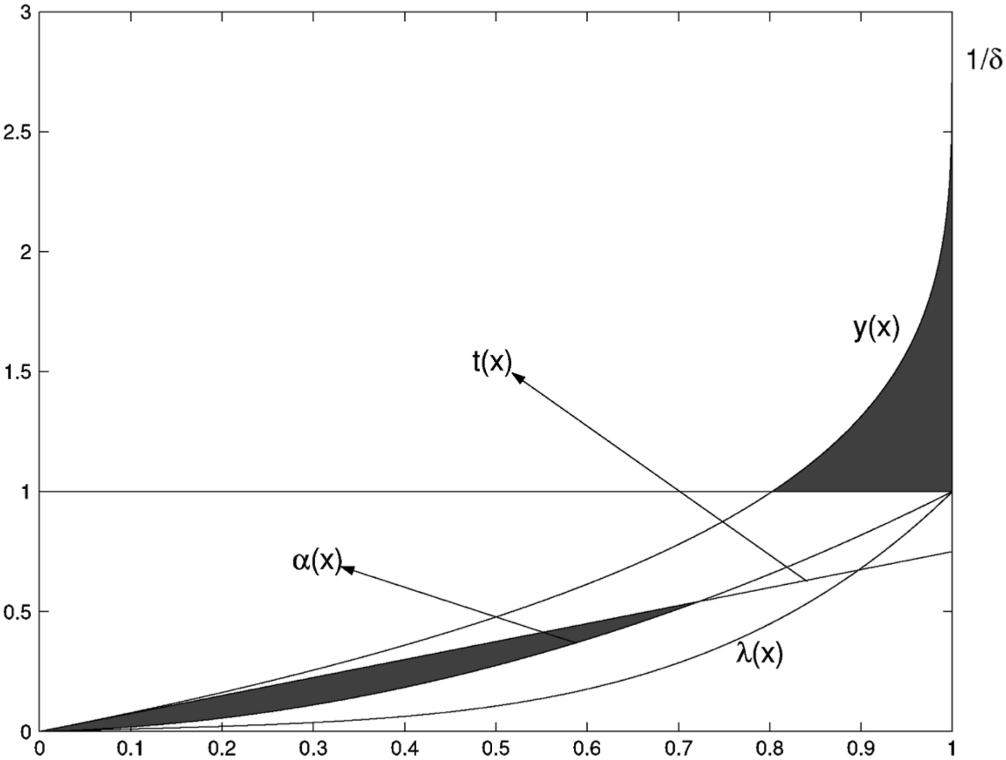

Fig. 5. Upper bound on the achievable rate for the LDPC codes with the linear minimum distance property.

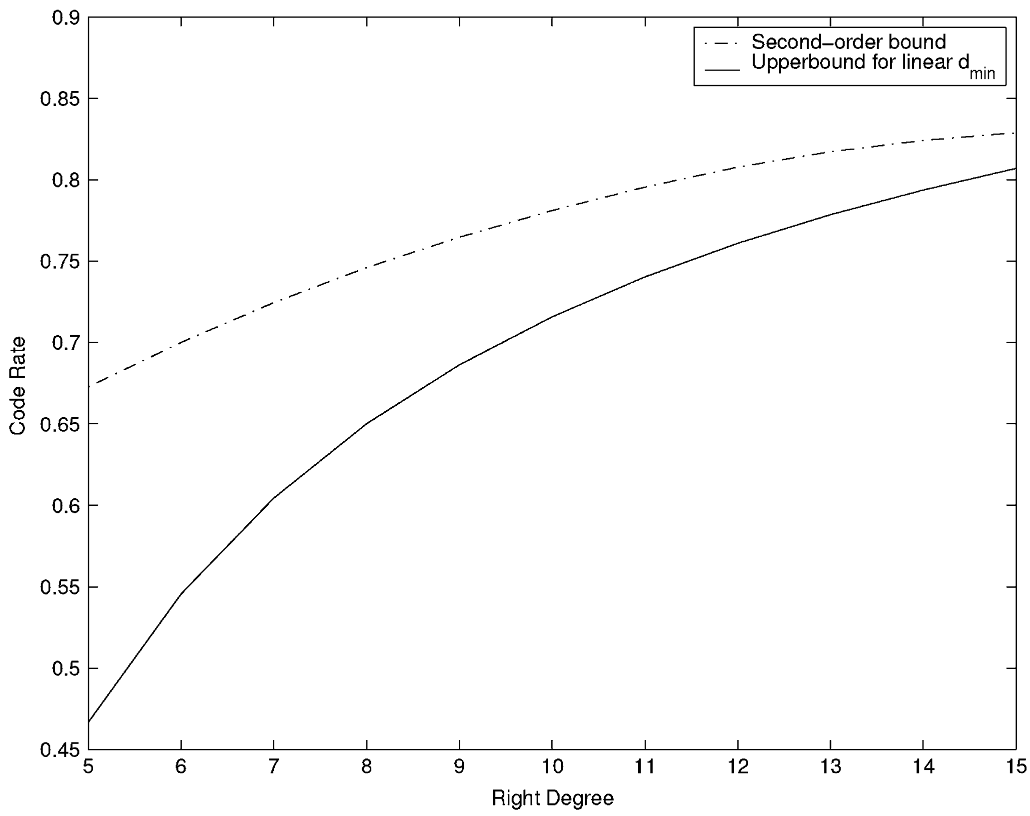

Fig. 6. Comparison between the upper bound on the achievable rate for the LDPC codes with the linear minimum distance property and the bound for the unconstrained codes.

Similar to the arguments in the second-order bound of [11], the bound in Theorem 5 can be improved. However, to compare the performance of the code ensembles having the linear typical minimum distance property with ones with no restriction, it suffices to work with this simple bound. Fig. 6 shows the upper bound of Theorem 5 and the second-order bound of [11] for right-regular codes over the BEC with erasure probability $\delta = 0.15$. As it is shown in [11], the second-order bound is tight, at least for our example. Thus, the difference between the two curves shows the rate loss because of the linear minimum distance constraint.

In the end, we would like to emphasize that all the results in the paper can be easily generalized for the condition $\lambda'(0)\rho'(1) \leq a$, where a is a given constant. For example, if we want to avoid degree-two variable nodes completely, we should have $\lambda_2 = 0$ (i.e., $a = 0$, in this case there is no need for expurgation since the ensemble has linear minimum distance with high probability). Thus, using bounds similar to the ones in the paper we can estimate the achievable rates.

IV. Conclusion

We derived lower and upper bounds on the achievable rates of the iterative decoding of LDPC code ensembles having linear typical minimum distance and linear typical minimum stopping set. These bounds were obtained for MBIOS channels and were improved for the BEC. We also gave a design methodology to construct codes meeting the lower bound for the binary erasure channel. We showed that practically the rates of the linear-minimum-distance codes are close enough to the Shannon limit. For example, on the BIAWGN channel, there is at most 1.1-dB loss due to the linear minimum distance property. Moreover, the loss is much smaller at higher rates. This result implies that it is possible to design codes with low error floors whose rates are close to capacity. On the other hand, our results on the upper bound for the BEC indicate that if the average right degree is not large enough, the loss can be considerable. This was shown by comparing the upper bound derived in this correspondence with a known tight bound on the rate of LDPC codes.

References

[1] H. Pishro-Nik, N. Rahnavard, J. Ha, F. Fekri, and A. Adibi, "Low-density parity-check codes for volume holographic memory systems," *Appl. Opt.*, vol. 42, pp. 861–870, 2003.

[2] T. Tian, C. Jones, J. D. Villasenor, and R. D. Wesel, "Construction of irregular LDPC codes with low error floor," in *Proc. IEEE Int. Conf. Communications*, vol. 5, Anchorage, AK, May 2003, pp. 3125–3129.

[3] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[4] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 619–637, 2001.

[5] C. Di, T. Richardson, and R. Urbanke, "Weight distributions: How deviant can you be?," in *Proc. IEEE Int. Symp. Information Theory*, Washington, DC, Jun./Jul. 2001, p. 50.

[6] C. Di, D. Proietti, İ. E. Telatar, T. Richardson, and R. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.

[7] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 929–953, Mar. 2005.

[8] H. Pishro-Nik and F. Fekri, "On decoding of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 439–454, Mar. 2004.

[9] D. Burshtein and G. Miller, "Asymptotic enumeration method for analyzing LDPC codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1115–1131, Jun. 2004.

[10] M. A. Shokrollahi, *Codes, Systems, and Graphical Models*. New York: Springer-Verlag, 2001, ch. Capacity-Achieving Sequences, pp. 153–166.

[11] O. Barak, D. Burshtein, and M. Feder, "Bounds on achievable rates of LDPC codes used over the binary erasure channel," *IEEE Trans. Inf.. Theory*, vol. 50, no. 10, pp. 2483–2492, Oct. 2004.

[12] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 569–584, Feb. 2001.

[13] M. A. Shokrollahi, "New sequences of linear time erasure codes approaching the channel capacity," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proc. 13th Int. Symp. (AAECC-13) (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1719.

[14] P. Oswald and M. A. Shokrollahi, "Capacity-achieving sequences for the erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 12, pp. 3017–3028, Dec. 2002.

[15] H. Pishro-Nik and F. Fekri, "Results on punctured LDPC codes," in *Proc. IEEE Information Theory Workshop*, San Antonio, TX, Oct. 2004, pp. 215–219.

[16] S. Litsyn and V. Shevelev, "On ensembles of low-density parity-check codes: Asymptotic distance distributions," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 887–908, Apr. 2002.

[17] J. Ha and S. McLaughlin, "Optimal puncturing of low-density parity-check codes," in *Proc. IEEE Int. Conf. Communications*, vol. 5, Anchorage, AK, 2003, pp. 3110–31114.

[18] B. Bollobás, *Random Graphs*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.

Timing Metrics for Constrained Codes

Ara Patapoutian, *Member, IEEE*

***Abstract*—The effect of data constraints on synchronization is quantified by the use of three simple timing metrics that respectively measure the ensemble average, the worst, and the best timing qualities attainable with a given binary pulse amplitude modulation (PAM) waveform. These timing metrics are computed with the help of a graph which represents the constrained PAM system. The timing metrics of the $(0, k)$ constraint are studied in detail for selected PAM pulses.**

***Index Terms*—Constrained coding, Cramer–Rao bound, Fisher information, magnetic recording, run-length-limited systems, shortest route, synchronization, timing-error detector.**

I. Introduction

A common approach to improve the performance of a symbol synchronizer is to impose a set of constraints on the data sequence that is transmitted or stored. The (d, k) constraint is such an example that limits the number of consecutive zeros in a binary data sequence to $d \geq 0$ at least and at most $k > d$ consecutive bits.[1] In the last 50 years, an enormous amount of research has been devoted to the understanding of constrained sequences and their constructions [1]–[4]. In parallel to these efforts, timing synchronization was interpreted and represented as a parameter estimation problem and bounds on its performance were derived, such as the Cramer–Rao lower bound [5]–[8]. However, the two areas of constrained coding and symbol synchronization have not interacted much, with coding theorists taking a (d, k) constraint as their starting point while researchers in the theory of synchronization assuming the data bits to be uncorrelated. Hence, little effort, if any, has been devoted in quantifying the synchronization improvements due to a constraint, a topic that we will discuss in this correspondence. The k parameter of a (d, k) constraint, for example, trades off timing quality with code-rate loss. With the availability of a timing metric, the guesswork in determining the k parameter can be minimized.

Manuscript received February 21, 2002; revised October 5, 2005.
The author is with Maxtor Corporation, Shrewsbury, MA 01545 USA (e-mail: ara@ieee.org).
Communicated by G. Battail, Associate Editor At Large.
Digital Object Identifier 10.1109/TIT.2005.860473

[1]Constraints imposed on sequences for applications other than timing are beyond the scope of this correspondence.