Capacity-Achieving Codes with Bounded Graphical Complexity on Noisy Channels

Chun-Hao Hsu and Achilleas Anastasopoulos
Electrical Engineering and Computer Science Department
University of Michigan
Ann Arbor, MI, 48109-2122
email: {chhsu, anastas}@umich.edu

Abstract

We introduce a new family of concatenated codes with an outer low-density parity-check (LDPC) code and an inner low-density generator matrix (LDGM) code, and prove that these codes can achieve capacity under any memoryless binary-input output-symmetric (MBIOS) channel using maximum-likelihood (ML) decoding with bounded graphical complexity, i.e., the number of edges per information bit in their graphical representation is bounded. We also show that these codes can achieve capacity for the special case of the binary erasure channel (BEC) under belief propagation (BP) decoding with bounded decoding complexity per information bit for all erasure probabilities in (0, 1). By deriving and analyzing the average weight distribution (AWD) and the corresponding asymptotic growth rate of these codes with a rate-1 inner LDGM code, we also show that these codes achieve the Gilbert-Varshamov bound with asymptotically high probability. This result can be attributed to the presence of the inner rate-1 LDGM code, which is demonstrated to help eliminate high weight codewords in the LDPC code while maintaining a vanishingly small amount of low weight codewords.

1 Introduction

During the last decade, several codes have been found to achieve capacity on the binary erasure channel (BEC) under iterative decoding. The first well-known example is the low-density parity-check (LDPC) codes, which were introduced by Gallager [1] and proved to be capacity-achieving about forty years later [2, 3]. Another prominent example is the irregular repeat-accumulate (IRA) codes, whose systematic [4] and nonsystematic [5] versions have both been proved to be capacity-achieving. One common feature shared by these codes is that they can be understood to be codes defined on bipartite graphs with variable nodes and check nodes [6], and their iterative decoding complexity is closely related to the number of edges in their graphical representations. A fundamental question arises: "How simple can the graphs be as a function of their performance?"

In [7], the authors give an information theoretical lower bound to show that if all variable nodes are transmitted, then the graphical complexity, i.e., the number of edges per information bit in the graph, should grow indefinitely as the multiplicative gap to capacity decreases to 0 on any memoryless binary-input output-symmetric (MBIOS)

hand, allowing state nodes in the graph, the authors in [5] show that nonsystematic IRA codes can achieve capacity on the BEC with bounded graphical complexity by using the density evolution method [8]. However, partially due to the limitation of the density evolution method, whether graphs with state nodes can achieve capacity with bounded graphical complexity on more general channels other than the BEC still remains unknown. It should be noted that graphical complexity does not translate directly to decoding complexity for a general MBIOS channel when an iterative decoder is utilized. Indeed, it has been conjectured in [9] that for an LDPC code which achieves a fraction $1-\epsilon$ of the channel capacity, the number of iterations for achieving vanishing bit error probability grows as $1/\epsilon$ while the average right degree grows as $\ln(1/\epsilon)$, and thus the average decoding complexity per information bit scales as $1/\epsilon \ln(1/\epsilon)$. It is thus unclear whether by reducing the graphical complexity to a constant the conjectured number of iterations will be influenced. This is an open problem for general MBIOS channels. Fortunately, at least for the BEC, this question is resolved, since edges in the graph need only be visited once when iterative decoding is performed.

In this paper, we introduce a new family of concatenated codes defined on graphs, namely the concatenated low-density parity-check and generator matrix (LDPC-GM) codes, and prove that these codes can achieve capacity using ML decoding on any MBIOS channels with bounded graphical complexity. These codes are constructed by serially concatenating an outer LDPC code and an inner low-density generator matrix (LDGM) code. By deriving and analyzing the average weight distribution (AWD) and its corresponding asymptotic growth rate of these codes with a rate-1 LDGM inner code, we show that the inner rate-1 LDGM code can help eliminate high weight codewords in the LDPC code while maintaining a vanishing small amount of low weight codewords. The resulting AWD of these codes thus has an asymptotic growth spectrum, which can be upper bounded by that of the random ensemble in the positive region of the curve while the number of codewords in negative region vanishes at least polynomially in n. The ML performance bound given in [10] is then used to prove our main result. Note that, although the ML performance does not translate directly to the iterative decoding performance of the codes, the value of this result is twofold. First, there are improved iterative decoding algorithms that approach closely the ML performance [11, 12]. Thus, it is conceivable that the ML performance can be achieved with decoding algorithms having complexity close to that of iterative decoding. Moreover, this finding gives a necessary condition for achieving capacity with suboptimal iterative decoding algorithms without resorting to the density evolution method, which becomes an infinite dimensional problem on channels other than the BEC. As a supportive fact on the potential of these ensembles under iterative decoding, we also show that these codes can achieve capacity on the BEC with bounded decoding complexity per information bit for all erasure probabilities in (0, 1).

The remaining of this paper is organized as follows. We review and prove some basic properties of the AWD of Gallager's LDPC ensemble in Section 2 and derive the average input-output weight enumerator of the LDGM codes in Section 3. Then, in Section 4, we introduce a family of the LDPC-GM codes and give their AWD and the associated asymptotic growth rate based on the previous two sections. Detailed analysis on these LDPC-GM codes is done and the main result is presented in Section 5. Allowing the outer LDPC code and inner LDGM code to be more generally irregular, we prove that the LDPC-GM codes can achieve capacity on the BEC with bounded decoding complexity in Section 6. Finally, we conclude this work in Section 7.

LDPC Ensemble

Consider Gallager's (n, j, k) LDPC ensemble as introduced in [13] with guaranteed rate $R_o = 1 - j/k$. Let $\overline{N_o(l)}$ be the average number of codewords of weight l in a randomly drawn code from the ensemble. The asymptotic growth rate of $\overline{N_o(l)}$ is given in [14] (it appears as an upper bound in [13]) to be

$$w_o(a) \triangleq \lim_{n\to\infty} \frac{1}{n} \ln \overline{N_o(an)} = \frac{j}{k} \inf_{x>0} \left\{ \ln \frac{(1+x)^k + (1-x)^k}{2x^{ak}} \right\} - (j-1)H(a) \qquad (1)$$

where $H(a) \triangleq -a \ln a - (1-a)\ln(1-a)$ is the binary entropy function evaluated with natural logarithms. Some useful characterizations of $\overline{N_o(l)}$ and $w_o(a)$ are summarized below.

Fact 1 *There exists a $\delta_o \in (0, 1/2)$, such that*

1. $\sum_{l=1}^{n\delta_o} \overline{N_o(l)} = O(n^{-j+2})$.
2. $w_o(a) < 0$ *and has exactly one local minimum, but no local maximum for all* $a \in (0, \delta_o)$.
3. $w_o(a) > 0$ *for all* $a \in (\delta_0, 1/2]$, *and* $w_o(\delta_o) = 0$.
4. $w_o(a)$ *has exactly one local maximum at* $a = 1/2$, *and* $w_o(1/2) = R_o \ln 2$.
5. *When k is even,* $\overline{N_o(l)} = \overline{N_o(n-l)}$, *for all* $l \in \{0, 1, \ldots, n\}$.

In Fact 1, item 1 to 4 are proved in [13, Appendix A], and item 5 follows from the linearity of the LDPC codes and the fact that the all-1 word is always a codeword when k is even. In order to use item 5, and for other mathematical convenience, we will assume throughout this paper that k is even.

We would like to prove two more results, which will help our later analysis involving LDPC codes. The first lemma gives a close-form upper bound on $w_o(a)$, which is tight especially when a is around $1/2$.

Lemma 1 $w_o(a) \le (1 - R_o)\ln[1 + (1-2a)^k] + [H(a) - (1-R_o)\ln 2]$.

Proof: Bounding the infimum term of (1) by substituting $x = \frac{a}{1-a}$ proves the lemma. ■

The next lemma gives a sufficient condition on k for any desired lower bound of δ_o, where we denote by $H^{-1}(x)$ the unique $a \in [0, 1/2]$, such that $H(a) = x$.

Lemma 2 *Given any $\delta_l \in (0, H^{-1}((1-R_o)\ln 2))$, if*

$$k > \frac{\ln\left[1 - \frac{H(\delta_l)}{(1-R_o)\ln 2}\right]}{\ln(1-2\delta_l)}, \qquad (2)$$

then $\delta_o > \delta_l$.

Proof: After some algebraic manipulations, it can be shown that

$$k > \frac{\ln\left[1 - \frac{H(\delta_l)}{(1-R_o)\ln 2}\right]}{\ln(1-2\delta_l)} \Rightarrow (1-R_o)\ln(1 + (1-2\delta_l)^k) + [H(\delta_l) - (1-R_o)\ln 2] < 0 \qquad (3)$$

Now, the lemma follows from Lemma 1 and Fact 1. ■

the LDGM Ensemble

Consider the regular LDGM ensemble with codeword length n such that each input node is connected to c check nodes, and each check node is connected to d input nodes. Let $\overline{Z_{w,h}}$ be the average number of codewords with input weight w and output weight h in a code drawn randomly from the ensemble. We have

$$\overline{Z_{w,h}} = \binom{R_i n}{w} P(H = h|W = w), \tag{4}$$

where $R_i \triangleq d/c$ is the rate of the LDGM codes, and H and W are random variables denoting the input and output weight, respectively, of a randomly drawn codeword. Now, given the input weight of the codeword is w, the output weight is h if and only if exactly h check nodes are connected to an odd number of edges emanated from "1" input nodes, and the remaining $n - h$ check nodes are connected to an even number of them. Counting the number of ways of connecting cw edges to dn check node sockets such that exactly h check nodes have an odd number of connections, we see that the value is equal to

$$\binom{n}{h} \mathrm{coef}(f_-(x,d)^h f_+(x,d)^{n-h}, x^{cw}), \tag{5}$$

where $\mathrm{coef}(f(x), x^a)$ denotes the coefficient of x^a in the polynomial $f(x)$, and $f_-(x,d) \triangleq \frac{1}{2}[(1+x)^d - (1-x)^d]$ and $f_+(x,d) \triangleq \frac{1}{2}[(1+x)^d + (1-x)^d]$ are defined to simplify notation. Since the total number of ways of connecting cw edges to nd sockets is equal to $\binom{nd}{cw}$, we have

$$P(H = h|W = w) = \frac{\binom{n}{h}}{\binom{nd}{cw}} \mathrm{coef}(f_-(x,d)^h f_+(x,d)^{n-h}, x^{cw}) \tag{6}$$

Combining (4) and (6), we obtain the average input-output weight enumerator of the (c, d) regular LDGM ensemble

$$\overline{Z_{w,h}} = \frac{\binom{nd/c}{w}}{\binom{nd}{cw}} \binom{n}{h} \mathrm{coef}(f_-(x,d)^h f_+(x,d)^{n-h}, x^{cw}). \tag{7}$$

4 Concatenation of LDPC and Rate-1 LDGM Codes

Consider the concatenation of an outer Gallager's (n, j, k_1) LDPC code and an inner rate-1 (k_2, k_2) regular LDGM code as shown in Fig. 1. For simplicity, we assume that $k = k_1 = k_2$ throughout this paper. If we ignore the possibility that different LDPC codewords can become the same codeword after further encoded by the inner LDGM code and just overcount them, then due to the randomness of the LDPC code construction (although we do not assume a uniform interleaver between the inner and outer codes), the AWD of the overall code $\overline{N(l)}$ can be bounded by

$$\overline{N(l)} \le \overline{N^{ub}(l)} \triangleq \sum_{s=0}^{n} \frac{\overline{N_o(s)}\,\overline{Z_{s,l}}}{\binom{n}{s}} = \binom{n}{l} \sum_{s=\lceil l/k \rceil}^{\lfloor n-l/k \rfloor} \frac{\overline{N_o(s)}}{\binom{kn}{ks}} \mathrm{coef}(f_-(x,k)^l f_+(x,k)^{n-l}, x^{ks}), \tag{8}$$

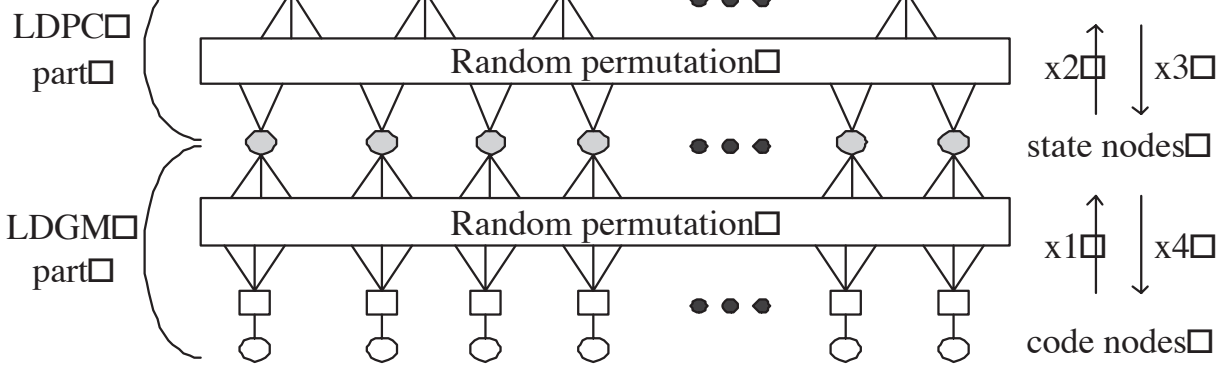

Figure 1: The factor graph of the LDPC-GM codes

where the change of the range of summation in the last equality is due to the fact that $\text{coef}(f_-(x,k)^l f_+(x,k)^{n-l}, x^{ks}) = 0$ for $s < \lceil l/k \rceil$ and $s > \lfloor n - l/k \rfloor$. To calculate the asymptotic growth rate of $\overline{N^{ub}(l)}$, we use the following important equation given in [15]

$$\lim_{\substack{n\to\infty \\ \text{coef}(f(x),x^{an})\neq 0}} \frac{1}{n} \ln \text{coef}(f(x)^n, x^{an}) = \inf_{x>0} \ln \frac{f(x)}{x^a} \tag{9}$$

where $0 < a < 1$, and $f(x)$ is a polynomial with nonnegative coefficients. Also used is the well known property of binomial coefficients

$$\lim_{n\to\infty} \frac{1}{n} \ln \binom{n}{an} = H(a), \quad \forall a \in [0,1] \tag{10}$$

(8), (9) and (10) then give

$$\begin{aligned} w(a) &\triangleq \lim_{n\to\infty} \frac{1}{n} \ln \overline{N(an)} \\ &\leq \lim_{n\to\infty} \frac{1}{n} \ln \overline{N^{ub}(an)} \\ &= H(a) + \max_{\frac{a}{k} \leq b \leq 1-\frac{a}{k}} w_o(b) - kH(b) + \inf_{x>0} \ln \frac{f_-(x,k)^a f_+(x,k)^{1-a}}{x^{bk}} \\ &\overset{(a)}{\leq} H(a) + \max_{\frac{a}{k} \leq b \leq 1-\frac{a}{k}} w_o(b) + a \ln[1-(1-2b)^k] + (1-a)\ln[1+(1-2b)^k] - \ln 2 \\ &\triangleq w^{ub}(a) \end{aligned} \tag{11}$$

where (a) follows by substituting $x = \frac{b}{1-b}$ in the infimum expression. To investigate the true rate R_1 of a randomly drawn LDPC-GM code from this ensemble, let $N(0)$ be the random variable denoting the number of LDPC codewords which after encoded by the inner LDGM encoder becomes the all-0 word. Then, we have by linearity of the LDPC-GM codes and Markov's inequality that

$$P(R_1 < R_o - r) = P(N(0) > 2^{nr}) \leq \frac{\overline{N(0)}}{2^{nr}} \leq O(2^{n(w^{ub}(0)-r)}) \tag{12}$$

which goes to 0 as n goes to infinity for all $r > w^{ub}(0)$. Therefore we can define the guaranteed rate of these LDPC-GM codes with asymptotically high probability to be

$$R \triangleq R_o - \max\{w^{ub}(0), 0\} \tag{13}$$

In this section, we will first characterize $w^{ub}(a)$, and then use the derived results to prove that LDPC-GM codes can be capacity-achieving on the MBIOS channels using ML decoding with bounded graphical complexity. Although $w^{ub}(a)$ is not symmetric about $a = 1/2$, the following lemma shows that we can focus on analyzing $w^{ub}(a)$ for $a \in [0, 1/2]$ and bound $w^{ub}(a)$ by $w^{ub}(1-a)$ for $a \in [1/2, 1]$.

Lemma 3 *$w^{ub}(a) \leq w^{ub}(1-a)$ for all $a \in [0, 1/2]$.*

Proof: It follows from the facts that

$$\ln[1-(1-2b)^k] \leq 0 \leq \ln[1+(1-2b)^k] \quad \forall b \in [0,1] \tag{14}$$

and $a \leq 1-a$ for all $a \in [0, 1/2]$. ■

In the next theorem, we prove that given any R' in [0, 1], the positive part of $w^{ub}(a)$ can be upper bounded by $H(a) - (1-R_o)\ln 2$ if k is sufficiently large for all $R_o \in [0, R']$. In this case, we also prove that $\overline{N^{ub}(l)}$ at least decreases polynomially with n in the negative part of $w^{ub}(a)$ when $j \geq 3$.

Theorem 1 *For any $R' \in [0,1]$, there exists an integer $M < \infty$ such that for all $k > M$ and $R_o \in [0, R']$, there exists a $\delta' < H^{-1}((1-R_o)\ln 2)$ such that the followings are true.*

1.

$$w^{ub}(a) \begin{cases} \leq 0 & \text{if } a = 0, \\ < 0 & \text{if } a \in (0, \delta'], \\ \leq H(a) - (1-R_o)\ln 2 & \text{if } a \in (\delta', 1/2]. \end{cases} \tag{15}$$

2. $\overline{N^{ub}(l)} = O(n^{-j+2})$ for all $l \in (0, \delta' n] \cup [n - \delta' n, n]$.

Proof: See Appendix A ■

From the above theorem and the definition of the guaranteed rate of the LDPC-GM codes in (13), we have the following corollary, which says that the conditions implied by the above theorem also guarantee no rate reduction for the LDPC-GM codes.

Corollary 1 *If $k > M$, where M is as defined in Theorem 1 for some $R' \in [0,1]$, then $R = R_o$ for all $R_o \in [0, R']$.*

Moreover, if we let d_{min} and $N(l)$ be the random variables denoting the minimum distance and number of codewords of weight l, respectively, of a randomly drawn code from the concatenated ensemble, and let $\delta_{GV} = H^{-1}((1-R)\ln 2)$ be the normalized Gilbert-Varshamov distance, then from Markov's inequality and Theorem 1, we have

$$\begin{aligned} P(d_{min} < \delta_{GV} n) =& P\left(\sum_{l \in (0, \delta_{GV} n)} N(l) \geq 1\right) \\ \leq& \sum_{l \in (0, \delta_{GV} n)} \overline{N(l)} \\ \leq& n \max_{l \in (0, \delta' n]} \overline{N^{ub}(l)} + n \exp\{n \max_{a \in (\delta', \delta_{GV})} w^{ub}(a) + o(n)\} \\ =& O(n^{-j+3}) \end{aligned} \tag{16}$$

following corollary.

Corollary 2 *If $k > M$, where M is as defined in Theorem 1 for some rate R and $j \geq 4$, then the LDPC-GM codes have a normalized minimum distance greater than or equal to the Gilbert-Varshamov bound with asymptotically high probability.*

In Fig. 2, we compare the asymptotic growth rate of the LDPC, the LDPC-GM and the random ensemble with $R = 0.5$ and $k = 8$. It is evident that the rate-1 LDGM inner code really helps eliminate high weight codewords in the outer LDPC code. As a trade-off, the growth rate of some low weight codewords increases slightly. However, as long as the growth rate of the low weight codewords remains negative, Theorem 1 shows that they still vanish as n goes to infinity.

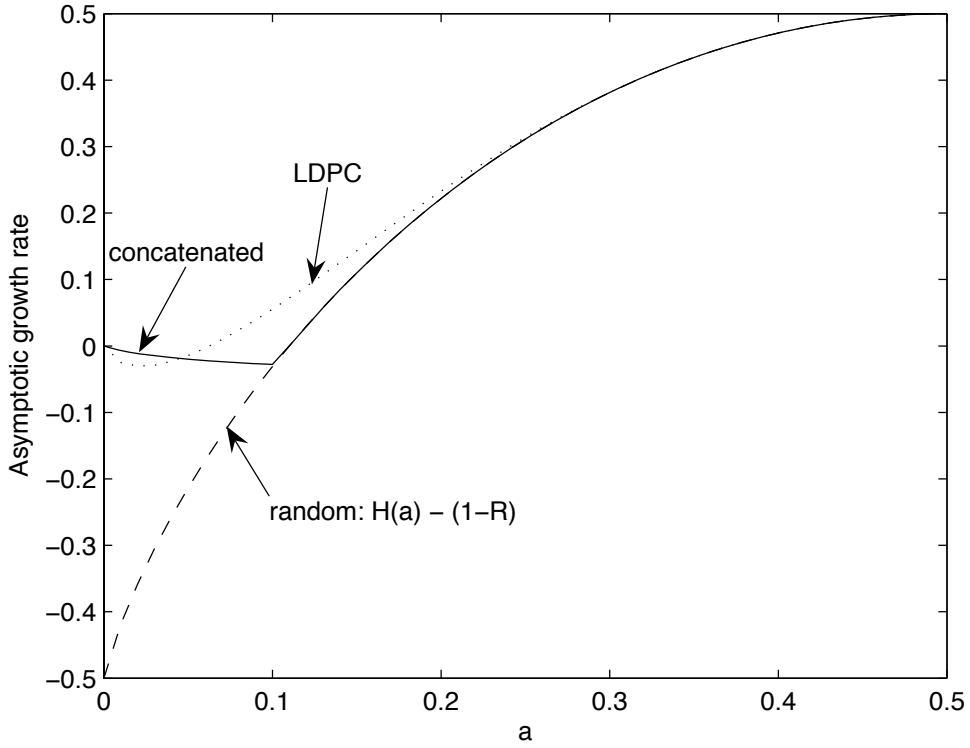

Figure 2: Comparison of $w_o(a)$, $w^{ub}(a)$ and $H(a) - (1 - R)$ with $R = 0.5$ and $k = 8$. The logarithm is to the base 2 in this figure.

We are now ready to state our main theorem, which shows that given any MBIOS channel, there always exists a finite value M such that these LDPC-GM codes with $k > M$ is capacity-achieving.

Theorem 2 *Given any MBIOS channel with capacity C, there exists an integer $M < \infty$ such that if $k > M$, then $R = R_o$ for the LDPC-GM ensembles with $R_o < C$. Moreover, for the given channel, the average block error probability P_B of the LDPC-GM ensembles with $k > M$, $j \geq 4$ and $R < C$ is vanishingly small when ML decoding is used.*

Proof: See Appendix B. ■

be evaluated as follows.

$$\Delta = \frac{n(j+k)+n}{Rn} = \frac{(2-R)k+1}{R} \tag{17}$$

Since Theorem 2 says that k need not go to infinity to achieve capacity, we can deduce that these LDPC-GM codes with any rate $R \in (0,1)$ can be capacity achieving with bounded graphical complexity.

6 Density Evolution for LDPC-GM Codes on the BEC

Although the aforementioned LDPC-GM ensembles have finite graphical complexity, the decoding complexity under ML decoding is still exponential. In this section, we show that by allowing the outer LDPC codes to be more generally irregular, the LDPC-GM ensemble can be capacity-achieving on the BEC under BP decoding with bounded decoding complexity per information bit. Although this is not a proof that the same might be true for the MBIOS channels, it is a good indication of the potential of the LDPC-GM codes.

Consider the concatenation of a (λ, ρ) irregular LDPC code and a $(2,2)$ regular LDGM code, where λ and ρ are the standard variable and check node degree distributions, respectively, from the edge perspective as defined in [16]. Note that this LDPC-GM ensemble has guaranteed rate

$$R = 1 - \frac{\int_0^1 \rho(t)dt}{\int_0^1 \lambda(t)dt} \tag{18}$$

and our task is to successfully decode the non-transmitted LDPC codewords. Let q be the channel erasure probability, and let x_1, x_2, x_3 and x_4 be the probabilities of erasure on edges from check to variable(LDGM), variable to check(LDPC), check to variable(LDPC) and variable to check(LDGM), respectively as shown in Fig. 1. Then, assuming we are operating at some fixed point, we have the following density evolution equations.

$$x_1 = 1 - (1-q)(1-x_4) \tag{19a}$$
$$x_2 = x_1^2 \lambda(x_3) \tag{19b}$$
$$x_3 = 1 - \rho(1-x_2) \tag{19c}$$
$$x_4 = x_1 \tilde{\lambda}(x_3) \tag{19d}$$

where $\tilde{\lambda}(x) = \sum_{i=1}^{\infty} \tilde{\lambda}_i x^i$ and

$$\tilde{\lambda}_i = \frac{\lambda_i / i}{\int_0^1 \lambda(t)dt}, \tag{20}$$

which denotes the fraction of variable nodes in the LDPC code with degree i. Equivalently, we have

$$\tilde{\lambda}(x) = \frac{\int_0^x \lambda(t)dt}{\int_0^1 \lambda(t)dt} \tag{21}$$

nated codes with an outer LDPC code and an inner differentiator code. Solving these equations for x_3, we have

$$x_3 = \rho\left(1 - \left[\frac{q}{1-(1-q)\tilde{\lambda}(x_3)}\right]^2 \lambda(x_3)\right) \tag{22}$$

If (22) has no solution in $(0,1]$, then x_3 must converge to 0 and thus x_4 must converge to 0 as the number of iterations goes to infinity. Therefore, if we have

$$1 - \rho\left(1 - \left[\frac{q}{1-(1-q)\tilde{\lambda}(x_3)}\right]^2 \lambda(x_3)\right) < x_3, \quad \forall x_3 \in (0,1] \tag{23}$$

then the BP decoding is successful. Note that (22) is essentially the same as equation (6) in [5] except for the following changes: $x_0 \to 1 - x_3$, $p \to 1 - q$, $\lambda(\cdot) \to \rho(\cdot)$, $\rho(\cdot) \to \lambda(\cdot)$, and $R(\cdot) \to \tilde{\lambda}(\cdot)$. More generally, (22) is an instance of the symmetry introduced in [17]. So, in the following, we will use the results proved in [5] to show two particular degree distribution pairs are capacity-achieving under BP decoding.

Theorem 3 (Check-regular ensemble) *Let*

$$\lambda(x) = \frac{1-(1-x)^{\frac{1}{k-1}}}{\left[1-(1-q)\left(1-kx+(k-1)\left[1-(1-x)^{\frac{k}{k-1}}\right]\right)\right]^2} \tag{24}$$

$$\rho(x) = x^{k-1} \tag{25}$$

Then for $k = 3$ and $q \in [\frac{12}{13}, 1)$, $\lambda(x)$ has only non-negative coefficients. Moreover, for any $\epsilon \in (0,1)$, let $M(\epsilon)$ be the smallest positive integer such that[1]

$$\sum_{i=M(\epsilon)+1}^{\infty} \frac{\lambda_i}{i} < \frac{\epsilon(1-q)}{qk} \tag{26}$$

and let $\lambda_\epsilon(x)$ be the truncated degree distribution of $\lambda(x)$ by treating all variable nodes with degree greater than $M(\epsilon)$ as pilot bits. Then the degree distribution pair (λ_ϵ, ρ) achieves a fraction $1-\epsilon$ of the channel capacity with vanishing bit error probability under BP decoding.

Proof: See Appendix C.1. ■

The decoding complexity per information bit of this check-regular ensemble can be calculated as follows

$$\Delta < \frac{knq + 2n + n}{(1-q)(1-\epsilon)n} = \frac{qk+3}{(1-q)(1-\epsilon)}, \tag{27}$$

which approaches the bounded value $\frac{qk+3}{1-q}$ as ϵ goes to 0.

[1] $M(\epsilon)$ exists for all $\epsilon \in (0,1)$ since $\sum_{i=1}^{\infty} \frac{\lambda_i}{i} = \int_0^1 \lambda(t)dt = \frac{1}{qk}$, which means $\sum_{i=M(\epsilon)+1}^{\infty} \frac{\lambda_i}{i}$ can be made arbitrarily close to 0 by increasing $M(\epsilon)$.

$$\lambda(x) = x^2 \tag{28}$$

$$\rho(x) = 1 + \frac{2(1-q)(1-x)^2 \sin\left(\frac{1}{3}\arcsin\left(\sqrt{-\frac{27(1-q)(1-x)^{\frac{3}{2}}}{4q^3}}\right)\right)}{\sqrt{3}q^4\left[-\frac{(1-q)(1-x)^{\frac{3}{2}}}{q^3}\right]^{\frac{3}{2}}} \tag{29}$$

Then for $q \in [0.05, 1]$, $\rho(x)$ has only non-negative coefficients. Moreover, for any $\epsilon \in (0,1)$, let $M(\epsilon)$ be the smallest positive integer such that[2]

$$\sum_{i=M(\epsilon)+1}^{\infty} \rho_i < \frac{\epsilon(1-q)}{3} \tag{30}$$

and let

$$\rho_\epsilon(x) \triangleq \left(1 - \sum_{i=1}^{M(\epsilon)} \rho_i\right) + \sum_{i=1}^{M(\epsilon)} \rho_i x^{i-1} \tag{31}$$

be the truncated degree distribution of $\rho(x)$. Then the degree distribution pair (λ, ρ_ϵ) achieves a fraction $1-\epsilon$ of the channel capacity with vanishing bit error probability under BP decoding.

Proof: See Appendix C.2. ■

The decoding complexity per information bit of this variable-regular ensemble can be calculated as follows

$$\Delta < \frac{3n + 2n + n}{(1-q)(1-\epsilon)n} = \frac{6}{(1-q)(1-\epsilon)} \tag{32}$$

which approaches the bounded value $\frac{6}{1-q}$ as ϵ goes to 0.

One drawback of the these capacity-achieving degree distribution pairs is that they are not guaranteed to be valid, i.e., with only nonnegative coefficients, for all $q \in (0,1)$. However, since they are valid for q close 1 (which is not true for the capacity-achieving IRA codes in [5]), this problem can be solved by considering punctured LDPC-GM codes. In [18], it is shown that random puncturing results in no performance loss on the gap to capacity for codes on the BEC. Hence, it follows that puncturing can be used to increase the rate of the LDPC-GM codes without affecting its capacity-achievability, a fact that was also observed by Pfister and Sason [17]. Furthermore, since a punctured LDPC-GM ensemble can also be viewed as another unpunctured LDPC-GM ensemble with inner irregular LDGM codes (which is no longer rate-1 in general), we have the following theorem.

Theorem 5 *Let (λ, ρ) be a degree distribution pair implied by Theorem 3 or Theorem 4 for some given ϵ and q'. Consider the LDPC-GM ensemble, whose outer LDPC code has*

[2] $M(\epsilon)$ exists for all $\epsilon \in (0,1)$ since $\sum_{i=1}^{\infty} \rho_i = 1$, which means $\sum_{i=M(\epsilon)+1}^{\infty} \rho_i$ can be made arbitrarily close to 0 by increasing $M(\epsilon)$.

distribution pair (F, G) from the node perspective[3]*. Then for any given $p \in [0, q']$, if*

$$F(x) = [x(1-p)+p]^2 \tag{33}$$
$$G(x) = x^2 \tag{34}$$

then this LDPC-GM ensemble achieves a fraction of $1-\epsilon$ of the channel capacity on the BEC with erasure probability $q \triangleq \frac{q'-p}{1-p}$ under BP decoding.

Proof: See Appendix C.3. ■

This theorem says that, given any capacity-achieving degree distribution pair (λ, ρ) for some erasure probability q', we can generate capacity-achieving LDPC-GM ensembles for all erasure probabilities $q \in [0, q']$ by adjusting p. Since q' can be arbitrarily close to 1, and the maximum degrees of F and G are bounded for all p, this construction can be done to produce capacity-achieving LDPC-GM ensembles for all rate in (0, 1) on the BEC with bounded decoding complexity.

7 Conclusion

In this paper, the LDPC-GM codes, i.e., the concatenated codes with an outer LDPC code and an inner LDGM code, are introduced. In the case that the outer code is Gallager's (n, j, k) LDPC code and the inner code is a rate-1 (k, k) regular LDGM code, we prove that for any desired range of rates R_o, there always exists an integer $M < \infty$ such that if $k > M$ then the inner LDGM encoder results in no rate reduction for the outer LDPC code. Moreover, the LDGM encoder helps eliminate high weight codewords while maintaining a vanishingly small amount of low weight codewords in the LDPC code. The resulting asymptotic growth spectrum of the LDPC-GM codes has a positive part, which can be upper bounded by the asymptotic growth spectrum of the random ensemble, and a negative part, where the number of codewords vanishes at least polynomially in n when $j \geq 4$. Note that, the condition $j \geq 4$ is automatically satisfied when k is big enough. It then follows easily that these codes achieve the Gilbert-Varshamov bound with asymptotically high probability. Furthermore, after applying the ML performance bound given in [10] to these LDPC-GM codes, we prove that they can achieve capacity on any MBIOS channels using ML decoding. Since all these results are implied by the only condition that k is greater than some finite number, which shows that the number of edges per information bit in the graph need not go to infinity to achieve capacity, we have proved that these LDPC-GM codes are capacity-achieving codes with bounded graphical complexity on any MBIOS channels.

On the other hand, if the outer LDPC code is allowed to be irregular, then invoking the density evolution method, we use the results in [5] to show two particular ensembles of the LDPC-GM codes can achieve capacity on the BEC under BP decoding with bounded decoding complexity. Moreover, extensions valid for all erasure probabilities of the BEC using inner irregular LDGM codes are also presented. These favorable results could suggest high potential of the LDPC-GM codes to achieve capacity on the MBIOS channels with bounded decoding complexity per iteration. However, since the scaling on the required number of iterations for successful iterative decoding for the LDPC-GM codes

[3]That is, $F(x) = \sum_{i=0}^{\infty} F_i x^i$ and $G(x) = \sum_{i=1}^{\infty} G_i x^i$, where F_i and G_i denote the fraction of input and check nodes that have i neighboring check and input nodes, respectively, in the LDGM code.

complexity property implies bounded decoding complexity using iterative decoding is still an open problem on MBIOS channels.

A Proof of Theorem 1

1. Define

$$f(b) \triangleq w_o(b) + a \ln \frac{1-(1-2b)^k}{2} + (1-a) \ln \frac{1+(1-2b)^k}{2} \tag{35}$$

We will bound $f(b)$ in two cases. By Lemma 2, for any $\delta_l \in (0, H^{-1}((1-R')\ln 2)) \subset (0, H^{-1}((1-R_o)\ln 2))$, if

$$k > M_1 \triangleq \frac{\ln\left[1 - \frac{H(\delta_l)}{(1-R')\ln 2}\right]}{\ln(1-2\delta_l)} \geq \frac{\ln\left[1 - \frac{H(\delta_l)}{(1-R_o)\ln 2}\right]}{\ln(1-2\delta_l)}, \tag{36}$$

then $w_o(\delta_l) < 0$ for all $R_o \in [0, R']$. Therefore, for $k > M_1$ and $b \in [a/k, \delta_l] \cup [1-\delta_l, 1-a/k]$ (we assume without loss of generality that $a/k \leq \delta_l$. otherwise, we just skip this step), we have

$$f(b) \leq w_o(b) - H(a) \leq \max\{w_o(a/k), w_o(\delta_l)\} - H(a), \tag{37}$$

where the first inequality follows from the fact that relative entropy is always non-negative, and the second inequality follows from Fact 1. On the other hand, when $b \in (\delta_l, 1-\delta_l)$, we have from Lemma 1 that

$$\begin{aligned} f(b) \leq & (1-R_o)\ln[1+(1-2b)^k] + H(b) - (1-R_o)\ln 2 + \\ & + a \ln \frac{1-(1-2b)^k}{2} + (1-a)\ln\frac{1+(1-2b)^k}{2} \\ \leq & -(1-R_o)\ln 2 - \ln 2 + \{H(b) + (2-R_o-a)\ln[1+(1-2b)^k]\} \\ \leq & -(1-R_o)\ln 2 - \ln 2 + \{H(b) + 2\ln[1+(1-2b)^k]\} \end{aligned} \tag{38}$$

where the last two inequalities follow from (14). Since

$$\frac{\partial^2 H(b)}{\partial b^2} = -\frac{1}{(1-b)b} \leq -4, \tag{39}$$

and

$$\begin{aligned} \frac{\partial^2 2\ln[1+(1-2b)^k]}{\partial b^2} = & \frac{8k[k-1-(1-2b)^k](1-2b)^{k-2}}{[1+(1-2b)^k]^2} \\ \leq & 8k(k-1)(1-2b)^{k-2} \\ \leq & 8k(k-1)(1-2\delta_l)^{k-2}, \end{aligned} \tag{40}$$

which can be made arbitrarily close to 0 for a large enough k, there exists a M_2 such that $k > M_2$ implies that the maximum of $H(b) + 2\ln[1+(1-2b)^k]$ is attained at $b = 1/2$, and thus

$$f(b) \leq -(1-R_o)\ln 2, \quad \forall b \in (\delta_l, 1-\delta_l) \tag{41}$$

$$w^{ub}(a) = H(a) + \max_{\frac{a}{k} \le b \le 1-\frac{a}{k}} f(b) \le \max\{H(a) - (1-R_o)\ln 2, w_o(a/d), w_o(\delta_l)\} \quad (42)$$

Since $\max\{w_o(a/d), w_o(\delta_l)\} < 0$ for all $a > 0$, there must exist a $\delta' < H^{-1}((1 - R_o)\ln 2)$ such that this part of the theorem is true.

2. For all $l \in (0, \delta' n] \cup [n - \delta' n, n]$ and $k > M$, we have

$$\begin{aligned}
\overline{N_c^{ub}(l)} &= \sum_{s=\lceil l/k \rceil}^{\lfloor n-l/k \rfloor} \frac{\overline{N_o(s)}\,\overline{Z_{s,l}^{(LDPG)}}}{\binom{n}{s}} \\
&\overset{(a)}{\le} \sum_{s=\lceil l/k \rceil}^{\delta_l n} \overline{N_o(s)} + \sum_{s=n-\delta_l n}^{\lfloor n-l/k \rfloor} \overline{N_o(s)} + \sum_{s=\delta_l n}^{n-\delta_l n} \frac{\overline{N_o(s)}\,\overline{Z_{s,l}^{(LDPG)}}}{\binom{n}{s}} \\
&\overset{(b)}{\le} O(n^{-j+2}) + n\exp\{n[H(l/n) + \max_{\delta_l \le b \le 1-\delta_l} f(b)] + o(n)\} \\
&\overset{(c)}{\le} O(n^{-j+2}) + n\exp\{n[H(l/n) - (1-R)\ln 2] + o(n)\} \\
&\overset{(d)}{=} O(n^{-j+2})
\end{aligned} \quad (43)$$

where $o(n)$ denotes some value that converges to 0 as n goes to infinity. In (43), (a) follows from the fact that $\overline{Z_{s,l}^{(LDPG)}}/\binom{n}{s} \le 1$ since it is a probability as shown in (4), (b) follows from Fact 1, (c) follows from (41), and (d) follows from the fact that $\delta' < H^{-1}((1-R)\ln 2)$.

B Proof of Theorem 2

Let M be as defined in Theorem 1 for $R' = C$. Then by Corollary 1, we have $R = R_o$ for all $k > M$ and $R_o < C$. Let $U \subset \{1, 2, \ldots, n\}$, and U^c be its complementary set. The following upper bound on the average block error probability under ML decoding is given in [10]

$$P_B \le \sum_{l \in U} \{\overline{N(l)} D^l\} + 2^{-nE_r(R + \frac{\ln \alpha}{n \ln 2})} \quad (44)$$

where

$$\alpha \triangleq \max_{l \in U^c} \frac{\overline{N(l)}}{2^{nR} - 1} \frac{2^n}{\binom{n}{l}} \quad (45)$$

$E_r(\cdot)$ is the random coding exponent, and

$$D \triangleq \sum_y \sqrt{p(y|0)p(y|1)} \le 1 \quad (46)$$

where $p(y|0)$ and $p(y|1)$ are the conditional probability density functions of the output of the MBIOS channel given the input. If we apply this bound to the LDPC-GM ensemble with $k > M$ and $R_o < C$, and let

$$U \triangleq \left\{ l : \frac{l}{n} \in (0, \delta'] \cup [1 - \delta', 1] \right\}, \quad (47)$$

$$\sum_{l\in U}\{\overline{N(l)}D^l\} \le \sum_{l\in U}\overline{N^{ub}(l)} \le nO(n^{-j+2}) = O(n^{-j+3}) \tag{48}$$

But we have from the same theorem and Lemma 3 that

$$\begin{aligned}\lim_{n\to\infty}\frac{\ln\alpha}{n} &= \max_{a\in(\delta',1-\delta')} w(a) - [H(a) - (1-R)\ln 2] \\ &\le \max_{a\in(\delta',1/2]} w^{ub}(a) - [H(a) - (1-R)\ln 2] \\ &\le 0\end{aligned} \tag{49}$$

Hence we have

$$P_B \le O(n^{-j+3}) + 2^{-nE_r(R)} \tag{50}$$

which goes to 0 as n goes to infinity for all $R < C$ and $j \ge 4$. Thus, the theorem is proved.

C Proofs of Section 6

First, we need a lemma.

Lemma 4 *If the degree distribution pair (λ, ρ) satisfies $\rho(0) = 0$, $\rho(1) = 1$, and satisfies (22) for all $x_3 \in [0, 1]$, then $R = 1 - q$.*

Proof: [5, Lemma 1] shows that under the assumed conditions, we have

$$\frac{\int_0^1 \rho(t)dt}{\int_0^1 \lambda(t)dt} = q \tag{51}$$

■

C.1 Proof of Theorem 3

The facts that (λ, ρ) satisfies (22) for all $x \in [0, 1]$ and that $\lambda(x)$ has only non-negative coefficients for $k = 3$ and $q \in [\frac{12}{13}, 1)$ are proved in [5, Theorem 1]. By the definition of λ_ϵ, we have effectively

$$\lambda_\epsilon(x) = \sum_{i=1}^{M(\epsilon)} \lambda_i x^{i-1} \tag{52}$$

in the density evolution equations. Hence, it follows that $\lambda_\epsilon(x) < \lambda(x)$, and the corresponding $\tilde{\lambda}_\epsilon(x) < \tilde{\lambda}(x)$ for all $x \in (0, 1]$. Therefore, (23) is satisfied, which implies that the BP decoding is successful. To find the rate of this ensemble of codes, let

$$\delta \triangleq \sum_{M(\epsilon)+1}^{\infty} \tilde{\lambda}_i \tag{53}$$

$$\begin{aligned} R =& \frac{(1-\delta)\int_0^1 \lambda(t)dt - \int_0^1 \rho(t)dt}{\int_0^1 \lambda(t)dt} \\ =& 1-\delta-\frac{\int_0^1 \rho(t)dt}{\int_0^1 \lambda(t)dt} \\ =& 1-q-\delta \end{aligned} \tag{54}$$

where the last equality follows from the facts that $\rho(0) = 0$, $\rho(1) = 1$, and Lemma 4. But, from (20)

$$\delta = \sum_{M(\epsilon)+1}^{\infty} \frac{\lambda_i/i}{\int_0^1 \lambda(t)dt} = q \sum_{M(\epsilon)+1}^{\infty} \frac{\lambda_i/i}{\int_0^1 \rho(t)dt} = qk \sum_{M(\epsilon)+1}^{\infty} \lambda_i/i < \epsilon(1-q) \tag{55}$$

Therefore, it follows that $R > (1-\epsilon)(1-q)$, and the theorem is proved.

C.2 Proof of Theorem 4

The facts that (λ, ρ) satisfies (22) for all $x \in [0,1]$ and that $\rho(x)$ has only non-negative coefficients for $q \in [0.05, 1]$ are proved in [5, Theorem 2]. Since $\rho_\epsilon(x) > \rho(x)$ for all $x \in (0,1]$, (23) is satisfied and the BP decoding is successful. As for the rate of this ensemble of codes, we have

$$\begin{aligned} R =& 1-\frac{\int_0^1 \rho_\epsilon(t)dt}{\int_0^1 \lambda(t)dt} \\ =& 1-\frac{\sum_{i=1}^{M(\epsilon)} \frac{\rho_i}{i} + 1 - \sum_{i=1}^{M(\epsilon)} \rho_i}{\int_0^1 \lambda(t)dt} \\ >& 1-\frac{\sum_{i=1}^{\infty} \frac{\rho_i}{i} + 1 - \sum_{i=1}^{M(\epsilon)} \rho_i}{\int_0^1 \lambda(t)dt} \\ =& 1-\frac{\int_0^1 \rho(t)dt + \sum_{i=M(\epsilon)+1}^{\infty} \rho_i}{\int_0^1 \lambda(t)dt} \\ \overset{(a)}{=}& 1-q-3\sum_{i=M(\epsilon)+1}^{\infty} \rho_i \\ >& (1-\epsilon)(1-q) \end{aligned} \tag{56}$$

where (a) follows from the facts that $\rho(0) = 0$, $\rho(1) = 1$, and Lemma 4. Hence, the theorem is proved.

C.3 Proof of Theorem 5

Let f be the degree distribution corresponding to F from the edge perspective. We have

$$f(x) = \frac{F'(x)}{F'(1)} = x(1-p) + p \tag{57}$$

$$x_1 = 1 - (1 - q')(1 - x_4) \tag{58a}$$
$$x_2 = F(x_1)\lambda(x_3) \tag{58b}$$
$$x_3 = 1 - \rho(1 - x_2) \tag{58c}$$
$$x_4 = f(x_1)\tilde{\lambda}(x_3) \tag{58d}$$

After some algebraic manipulations, the fixed point equation can be shown to be

$$x_3 = 1 - \rho\left(1 - \left[\frac{q'(1-p)+p}{1-(1-q')(1-p)\tilde{\lambda}(x_3)}\right]^2 \lambda(x_3)\right) \tag{59}$$

which is the same as (22) if we let q be as defined in this theorem. Hence, from Theorem 3 and Theorem 4, the decoding is successful under BP decoding on the BEC with erasure probability q. Moreover, the rate of this ensemble is given by

$$\begin{aligned} R =& \{\text{rate of the outer LDPC code}\} \times \frac{\{\text{number of input nodes in the LDGM code}\}}{\{\text{number of check nodes in the LDGM code}\}} \\ =& \{\text{rate of the outer LDPC code}\} \times \frac{G'(1)}{F'(1)} \\ >& (1-\epsilon)(1-q')\frac{1}{1-p} \\ =& (1-\epsilon)(1-q), \end{aligned} \tag{60}$$

which then proves this theorem.

References

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

[2] M. A. Shokrollahi, "New sequences of linear time erasure codes approaching channel capacity," in *Proc. International Symposium on Information Theory and its Applications*, Honolulu, Hawaii, Nov. 1999, pp. 65–76.

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

[4] H. Jin, A. Khandekar, and R. J. McEliece, "Irregular repeat-accumulate codes," in *Proc. International Symposium on Turbo Codes and Related Topics*, Brest, France, Sept. 2000, pp. 1–8.

[5] H. D. Pfister, I. Sason, and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity," *IEEE Trans. Information Theory*, vol. 51, no. 7, pp. 2352–2379, July 2005.

[6] N. Wiberg, *Codes and Decoding on General Graphs*, Ph.D. thesis, Linköping University, Linköping, Sweden, 1996.

ear block codes over memoryless symmetric channels," *IEEE Trans. Information Theory*, vol. 49, no. 7, pp. 1611–1635, July 2003.

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

[9] A. Khandekar and R. J. McEliece, "On the complexity of reliable communication on the erasure channel," in *Proc. International Symposium on Information Theory*, Washinton, DC, June 2001, p. 1.

[10] G. Miller and D. Burshtein, "Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes," *IEEE Trans. Information Theory*, vol. 47, no. 7, pp. 2696–2710, Nov. 2001.

[11] N. Varnica and M. Fossorier, "Belief-propagation with information correction: improved near maximum-likelihood decoding of low-density parity-check codes," in *Proc. International Symposium on Information Theory*, Chicago, USA, June 2004, p. 343.

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

[13] R. G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA, 1963.

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

[15] D. Burshtein and G. Miller, "Asymptotic enumeration methods for analyzing ldpc codes," *IEEE Trans. Information Theory*, vol. 50, no. 6, pp. 1115–1131, June 2004.

[16] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Information Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[17] H. D. Pfister and I. Sason, "Accumulate-repeat-accumulate codes: Systematic codes achieving the binary erasure channel with bounded complexity," in *Proc. Allerton Conf. Commun., Control, Comp.*, Monticello, IL, Sept. 2005, [Online]. Available: http://www.arxiv.org/abs/cs.IT/0509044.

[18] H. Pishro-Nik, N. Rahnavard, and F. Fekri, "Nonuniform error correction using low-density parity-check codes," *IEEE Trans. Information Theory*, vol. 51, no. 7, pp. 2702–2714, July 2005.