

Capacity-Achieving Codes for Noisy Channels with Bounded Graphical Complexity and Maximum Likelihood Decoding

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

Submitted: February 2006

Abstract

In this paper, capacity-achieving codes for memoryless binary-input output-symmetric (MBIOS) channels under maximum-likelihood (ML) decoding with bounded graphical complexity are investigated. The graphical complexity of a code is defined as the number of edges in the graphical representation of the code per information bit and is proportional to the decoding complexity per information bit per iteration under iterative decoding.

Irregular repeat-accumulate (IRA) codes are studied first. By deriving their asymptotic average weight distribution (AAWD) it is shown that simple nonsystematic IRA ensembles outperform systematic IRA and regular low-density parity-check (LDPC) ensembles with the same graphical complexity, and are only 0.124 dB away from the Shannon limit for the binary-input additive white Gaussian noise (BIAWGN) channel. However, a conclusive result as to whether these nonsystematic IRA codes can really achieve capacity cannot be reached.

Motivated by this inconclusive result, a new family of codes is proposed, called low-density parity-check and generator matrix (LDPC-GM) codes, which are serially concatenated codes with an outer LDPC code and an inner low-density generator matrix (LDGM) code. It is proved that these codes can achieve capacity on any MBIOS channel using ML decoding and also achieve capacity on any BEC using belief propagation (BP) decoding, both with bounded graphical complexity. Moreover, these codes are shown to have linearly increasing minimum distances and achieve the asymptotic Gilbert-Varshamov bound for all rates.

I. 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]–[5]. Another example is the irregular repeat-accumulate (IRA) codes, whose systematic [6] and nonsystematic [7] versions were both proved to be capacity-achieving. One common feature shared by these codes is that they are defined on bipartite graphs with variable and check nodes [8], and thus they can be decoded using iterative decoding (also known as message passing or belief propagation (BP)) algorithms, having complexity (per iteration) proportional to the number of edges in their graphical representations.

In view of the capacity-achieving property of these graph-based code ensembles on the BEC, and the connection between decoding complexity and graph representation, a fundamental question arises: “how simple can the graphs be as a function of the corresponding code performance?”

In [9], the authors give an information theoretical lower bound to show that if all variable nodes are transmitted, then the graphical complexity (defined as the number of edges per information bit in the graph) should grow indefinitely as the multiplicative gap to capacity decreases to zero on any memoryless binary-input output-symmetric (MBIOS) channel. This is true even when maximum-likelihood (ML) decoding is used. On the other hand, allowing state nodes in the graph, the authors in [7] show that nonsystematic IRA codes can achieve capacity on the BEC using BP decoding with **bounded** graphical complexity. However, since the density evolution (DE) method used in the proofs of [7] becomes analytically intractable on channels other than the BEC, it is still unknown whether there exist capacity-achieving codes (even when ML decoding is used) with bounded graphical complexity on general MBIOS channels. Due to the difficulty in estimating the performance of BP on noisy channels, all research activity in this direction follows one of two basic approaches. In the first approach, approximations to DE are utilized (e.g., Gaussian approximation) or numerical evaluation of the densities is performed, such as in the work of [10]–[12]. In the second approach the performance of ML decoding is evaluated, as in [13]–[16]. In this paper we follow the latter approach. It is noted that, although good ML performance does not imply sufficiently good iterative decoding performance, the value of studying the ML performance is twofold. First, there are improved iterative decoding

algorithms that approach closely the ML performance [17], [18]. Thus, it is conceivable that the ML performance can be achieved with decoding algorithms having complexity close to that of iterative decoding. Moreover, achieving capacity with ML decoding gives a necessary condition for achieving capacity with suboptimal iterative decoding algorithms without resorting to the DE method, which becomes an infinite dimensional problem on channels other than the BEC as mentioned above.

We first investigate the ML performance of IRA codes on MBIOS channels. This ensemble is a reasonable candidate for achieving capacity on MBIOS channels with bounded graphical complexity, since it is proved to have this property on the BEC. ML analysis is performed via deriving the average weight distribution (AWD) of systematic and nonsystematic versions of the ensembles. The asymptotic growth rate of the AWD (in the following we refer to this quantity as the asymptotic average weight distribution (AAWD)) of IRA ensembles is also calculated, and used to obtain various ML performance bounds as in [14], [19], [20]. In the process, the AAWD of low-density generator matrix (LDGM) ensembles [21] is also derived. Furthermore, the role of the inner accumulator in spectral thinning is demonstrated. Our approach shows that simple nonsystematic IRA codes have a better guaranteed performance than systematic IRA and LDPC codes with the same graphical complexity, which is only 0.124 dB away from the Shannon limit when Divsalar's bound [14] is used on the binary input additive white Gaussian noise (BIAWGN) channel. However, a conclusive answer as to whether these nonsystematic IRA ensembles achieve capacity was not reached. The reason lies in the fact that their AAWD cannot be proved to be strictly negative in the region of normalized weights closed to zero. As a result, it cannot be guaranteed that the number of low weight codewords in these ensembles decreases exponentially fast. This further implies that their polynomial growth behavior has to be estimated; a seemingly more difficult task.

Motivated by the inconclusive result regarding the capacity-achieving property of IRA ensembles using ML decoding, we introduce a new family of codes, namely the concatenated low-density parity-check and generator matrix (LDPC-GM) codes, which are constructed by serially concatenating an outer LDPC code and an inner LDGM code. We prove that LDPC-GM codes can achieve capacity using ML decoding on any MBIOS channel with bounded graphical complexity. By deriving and analyzing the AWD and AAWD of the LDPC-GM codes with a rate-1 LDGM inner code, we show that the inner rate-1 LDGM code helps eliminate high weight

LDPC codewords while maintaining a vanishing small amount of low weight codewords. In addition to being capacity achieving, it is also shown that these ensembles achieve the asymptotic Gilbert-Varshamov bound [22], [23]. As a supportive fact on the potential of these ensembles under iterative decoding, we also show that LDPC-GM ensembles can achieve capacity on the BEC with bounded decoding complexity (per information bit) for all erasure probabilities in $(0, 1)$. This fact can also be viewed as an instance of symmetry observed in [24].

The remaining of this paper is structured as follows. We derive and analyze the AWD, AAWD of IRA and LDGM codes in Section II. The derived AAWD are then utilized to numerically evaluate the ML performance of these codes. In Section III, we introduce the LDPC-GM codes and prove that they are capacity-achieving with bounded graphical complexity on MBIOS channels. 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 any BEC with bounded decoding complexity in Section IV. Finally, we conclude this work in Section V.

II. AVERAGE WEIGHT DISTRIBUTION OF IRA CODES

One commonly used approach to analyze the ML performance of some code, is via deriving its input-output weight enumerator (IOWE) as in [13]. A general method for computing the IOWE of 1-input- t -output convolutional encoders is proposed in [25], which can then be used to analyze the ML performance of several concatenated code ensembles. However, if we view IRA codes as a serial concatenation of an outer repetition code and an inner convolutional code, then the inner convolutional encoder will have more than 1 input bits when the check node degree is greater than 3 as shown in Fig. 1(a). Therefore, the method in [25] unfortunately can not be directly applied to the general scenario of IRA ensembles with arbitrary check node degrees¹. In this paper, we solve this problem by viewing an IRA code as a serial concatenated code with an outer LDGM code and an inner accumulator code. Based on this decomposition, we derive the average input-parity weight enumerator (AIPWE) of IRA ensembles. Upper bounds on the AWD and AAWD of the systematic and nonsystematic versions of the IRA and LDGM ensembles are then obtained from their AIPWE, which can be used to obtain various ML performance bounds

¹However, when the check node degree is small, this problem can be circumvented by further decomposing the inner convolutional code into a regular check code and an accumulator code, and using the IOWE of check codes with small check degrees derived in [16].

as in [14], [19], [20]. As an example, we use Divsalar’s bound to compare the performances of systematic and nonsystematic IRA ensembles under ML decoding on the BIAWGN channel.

A. Background: LDGM and IRA Codes

Consider the LDGM and IRA codes as shown in Fig. 1. As can be seen in the figure, both of them have two different sets of variable nodes, i.e., the information nodes and the parity nodes. The systematic version of them uses all the variable nodes as its codeword, while the nonsystematic one uses only the parity nodes. Therefore, letting m denote the number of information bits and n denote the number of parity bits, the rate R of the systematic and nonsystematic codes is $m/(n + m)$ and m/n , respectively.

Let λ_i be the fraction of edges between the information and check nodes that are connected to an information node with i check node neighbors, and ρ_i be the fraction of the same edges that are connected to a check node with i information node neighbors. Furthermore, define

$$\lambda(x) \triangleq \sum_{i=1}^{\infty} \lambda_i x^{i-1}, \text{ and } \rho(x) \triangleq \sum_{i=1}^{\infty} \rho_i x^{i-1} \quad (1)$$

to be the generating functions of λ_i ’s and ρ_i ’s. These two functions are used to specify the ensembles of LDGM and IRA codes assuming random permutation of edges between information and check nodes within each ensemble, and are known as the “degree distribution” pair. A special case is the “ (c, d) regular” code ensemble defined by $\lambda(x) = x^{c-1}$ and $\rho(x) = x^{d-1}$.

The above degree distribution pair (λ, ρ) is from the edge perspective. It will facilitate our following analysis if we also have an equivalent description from the node perspective. Let $\tilde{\lambda}_i$ (respectively $\tilde{\rho}_i$) be the fraction of information (respectively check) nodes that are connected to i check (respectively information) nodes. Then we have

$$\tilde{\lambda}_i = \frac{\lambda_i/i}{\sum_{j=1}^{\infty} \lambda_j/j}, \text{ and } \tilde{\rho}_i = \frac{\rho_i/i}{\sum_{j=1}^{\infty} \rho_j/j}. \quad (2)$$

B. Average Input-Parity Weight Enumerator of LDGM and IRA Ensembles

The input-output weight enumerator (IOWE) $A_{w,h}$ of a binary linear block code \mathcal{C} is defined to be the number of codewords in \mathcal{C} with input Hamming weight w and output Hamming weight h . Similarly, we can define the input-parity weight enumerator (IPWE) $Z_{w,h}$ for LDGM and IRA codes to denote the number of codewords with input weight w and parity weight h . Note

that IPWE and IOWE are the same for nonsystematic LDGM and IRA codes, but different for systematic ones.

In this section, we calculate the AIPWE $\overline{Z_{w,h}}$ of LDGM and IRA ensembles, which is then used in the next section to obtain the AWD of systematic and nonsystematic versions of the respective ensembles.

1) *AIPWE of LDGM Ensembles:* Consider the (λ, ρ) LDGM ensemble. Let W and H be the random variables denoting the input and parity weight, respectively, of a randomly chosen codeword of a code drawn randomly from the ensemble. Furthermore, let E be the random variable denoting the total number of edges emanated from the information nodes that are equal to 1 in the aforementioned codeword. Moreover, define

$$t \triangleq m \sum_{i=1}^{\infty} i \tilde{\lambda}_i \quad (3)$$

to be the total number of edges between information and parity nodes. We have

$$\overline{Z_{w,h}^{(LDGM)}} = 2^k P(H = h, W = w) \quad (4a)$$

$$= 2^k P(W = w) \sum_{e=0}^t P(H = h, E = e | W = w) \quad (4b)$$

$$= \binom{k}{w} \sum_{e=0}^t P(H = h | E = e, W = w) P(E = e | W = w) \quad (4c)$$

The number of ways of having exactly e edges emanated from w information nodes, out of a total of $\binom{k}{w}$ possibilities, is equal to $\text{coef}(\prod_{u=1}^{\infty} (1 + x^u y)^{m \tilde{\lambda}_u}, x^e y^w)$, where $\text{coef}(f(x, y), x^a y^b)$ denotes the coefficient of $x^a y^b$ in the polynomial $f(x, y)$. Therefore, we have

$$P(E = e | W = w) = \frac{\text{coef}\left(\prod_{u=1}^{\infty} (1 + x^u y)^{m \tilde{\lambda}_u}, x^e y^w\right)}{\binom{k}{w}}. \quad (5)$$

On the other hand, given that the number of edges from the information nodes equal to 1 is e , the output weight is h if and only if exactly h check nodes are connected to an odd number of such edges, and the remaining $n - h$ check nodes are connected to an even number of them. Counting the number of ways of connecting e edges to t check node sockets such that exactly h check nodes have an odd number of connections, we see that the value is equal to

$\text{coef}(\prod_{v=1}^{\infty} [f_{-}(x, v)y + f_{+}(x, v)]^{n\tilde{\rho}_v}, x^e y^h)$, where

$$f_{-}(x, v) \triangleq \frac{1}{2}[(1+x)^v - (1-x)^v] \quad (6a)$$

$$f_{+}(x, v) \triangleq \frac{1}{2}[(1+x)^v + (1-x)^v]. \quad (6b)$$

Since the total number of ways of connecting e edges to t sockets is equal to $\binom{t}{e}$, we have

$$P(H = h | E = e, W = w) = \frac{\text{coef}(\prod_{v=1}^{\infty} [f_{-}(x, v)y + f_{+}(x, v)]^{n\tilde{\rho}_v}, x^e y^h)}{\binom{t}{e}}, \quad (7)$$

which is not related to the exact input weight w . Combining (4), (5) and (7), we obtain the AIPWE of the (λ, ρ) LDGM ensemble

$$\overline{Z_{w,h}^{(LDGM)}} = \sum_{e=0}^t \frac{1}{\binom{t}{e}} \text{coef} \left(\prod_{u=1}^{\infty} (1 + x^u y)^{m\tilde{\lambda}_u}, x^e y^w \right) \text{coef} \left(\prod_{v=1}^{\infty} [f_{-}(x, v)y + f_{+}(x, v)]^{n\tilde{\rho}_v}, x^e y^h \right). \quad (8)$$

In particular, if $\lambda(x) = x^{c-1}$ and $\rho(x) = x^{d-1}$, we have $t = cm$, and

$$\text{coef}((1 + x^c y)^m, x^e y^w) = \begin{cases} \binom{m}{w} & \text{if } e = cw, \\ 0 & \text{else.} \end{cases} \quad (9)$$

$$\text{coef}([f_{-}(x, d)y + f_{+}(x, d)]^n, x^e y^h) = \binom{n}{h} \text{coef}(f_{-}(x, d)^h f_{+}(x, d)^{n-h}, x^e). \quad (10)$$

Hence (8) simplifies to the following AIPWE for the (c, d) regular LDGM ensemble

$$\overline{Z_{w,h}^{(LDGM)}} = \frac{\binom{m}{w}}{\binom{cm}{cw}} \binom{n}{h} \text{coef}(f_{-}(x, d)^h f_{+}(x, d)^{n-h}, x^{cw}). \quad (11)$$

2) *AIPWE of IRA Ensembles*: A (λ, ρ) IRA code can be viewed as a serially concatenated code with an outer nonsystematic (λ, ρ) LDGM code and an inner accumulator code. In addition, the randomness of the LDGM ensemble construction is equivalent to having a uniform

interleaver² [26] between the inner and outer codes. Based on the above, we have

$$\overline{Z_{w,h}^{(IRA)}} = \sum_{s=0}^n \frac{\overline{Z_{w,s}^{(LDGM)}} A_{s,h}^{(acc)}}{\binom{n}{s}}, \quad (12)$$

where $A_{w,h}^{(acc)}$ denotes the IOWE of the accumulator code, which is given in [13] to be

$$A_{w,h}^{(acc)} = \begin{cases} \binom{n-h}{\lfloor w/2 \rfloor} \binom{h-1}{\lceil w/2 \rceil - 1} & \text{if } \lfloor w/2 \rfloor \leq n-h \text{ and } \lceil w/2 \rceil \leq h, \\ 0 & \text{else.} \end{cases} \quad (13)$$

Hence, from (12), (13) and (8), we obtain the AIPWE of the (λ, ρ) IRA ensemble as

$$\begin{aligned} \overline{Z_{w,h}^{(IRA)}} &= \sum_{\substack{s \geq 0, \lfloor s/2 \rfloor \leq h \\ \lceil s/2 \rceil \leq n-h}} \left\{ \frac{\binom{n-h}{\lfloor s/2 \rfloor} \binom{h-1}{\lceil s/2 \rceil - 1}}{\binom{n}{s}} \right. \\ &\times \left. \sum_{e=0}^t \frac{1}{\binom{t}{e}} \text{coef} \left(\prod_{u=1}^{\infty} (1 + x^u y)^{m \tilde{\lambda}_u}, x^e y^w \right) \text{coef} \left(\prod_{v=1}^{\infty} [f_-(x, v) y + f_+(x, v)]^{n \tilde{\rho}_v}, x^e y^s \right) \right\}. \quad (14) \end{aligned}$$

Similarly, from (12), (13) and (11), we obtain the AIPWE of the (c, d) regular IRA ensemble as

$$\overline{Z_{w,h}^{(IRA)}} = \frac{\binom{m}{w}}{\binom{cm}{cw}} \sum_{\substack{s \geq 0, \lfloor s/2 \rfloor \leq h \\ \lceil s/2 \rceil \leq n-h}} \binom{n-h}{\lfloor s/2 \rfloor} \binom{h-1}{\lceil s/2 \rceil - 1} \text{coef} (f_-(x, d)^s f_+(x, d)^{n-s}, x^{cw}). \quad (15)$$

C. AAWD of LDGM and IRA Ensembles

Consider an LDGM or IRA ensemble with AIPWE $\overline{Z_{w,h}}$. Let $\overline{N(l)}$ be the average number of codewords of weight l in a randomly drawn code from the ensemble. Then for the systematic ensembles, their AWD is given by

$$\overline{N(l)} = \sum_{w=\max(0, l-n)}^{\min(m, l)} \overline{Z_{w, l-w}} \quad (16)$$

However, for the nonsystematic ensembles, different input words can result in the same output codeword in a nonsystematic code. Such codewords should not be counted more than once in the weight distribution. As a result, the AWD of non-systematic ensembles can not be obtained

²A uniform interleaver of length n is a probabilistic device that maps any given input of weight w to all $\binom{n}{w}$ possible permutations of it with equal probability.

as directly as that for the systematic ones. For example, for a nonsystematic regular LDGM code with even d , both the all-0 and the all-1 input word result in the all-0 output word. If we just overcount the repeated codewords in a code, then we obtain the following upper bound for the AWD of nonsystematic ensembles

$$\overline{N}(l) \leq \overline{N^{ub}}(l) \triangleq \sum_{w=0}^m \overline{Z_{w,l}} \quad (17)$$

To analyze the asymptotic behavior of the AWD's, we use the following two equations proved in [27]

$$\lim_{\substack{n \rightarrow \infty \\ \text{coef}(f(x), x^{an}) \neq 0}} \frac{1}{n} \ln \text{coef}(f(x)^n, x^{an}) = \inf_{x>0} \ln \frac{f(x)}{x^a} \quad (18a)$$

$$\lim_{\substack{n \rightarrow \infty \\ \text{coef}(f(x,y), x^{an}y^{bn}) \neq 0}} \frac{1}{n} \ln \text{coef}(f(x,y)^n, x^{an}y^{bn}) = \inf_{x>0, y>0} \ln \frac{f(x,y)}{x^a y^b} \quad (18b)$$

where $0 < a, b < 1$, and $f(x)$ and $f(x, y)$ are polynomials with nonnegative coefficients. Also, we use the well known property of binomial coefficients (see, e.g., [28, Lemma 18.9] for a proof),

$$\lim_{n \rightarrow \infty} \frac{1}{n} \ln \binom{n}{an} = H(a) \quad (19)$$

where $0 \leq a \leq 1$, and $H(a) \triangleq -a \ln a - (1-a) \ln(1-a)$ is the binary entropy function evaluated with natural logarithms. Note that the convergence of (19) is uniform in a , and the convergence of (18a) ((18b), respectively) is uniform in a (and b) at the vicinity of any point such that $\inf_{x>0} \frac{f(x)}{x^a} \neq 0$ ($\inf_{x>0, y>0} \frac{f(x,y)}{x^a y^b} \neq 0$) as pointed out in [27].

Define the AAWD of an ensemble with AWD $\overline{N}(l)$ to be

$$w(a) \triangleq \lim_{n \rightarrow \infty} \frac{1}{n} \ln \overline{N}(an). \quad (20)$$

We have the following result.

Theorem 1 *The AAWD of the nonsystematic (c, d) regular LDGM, nonsystematic (c, d) regular IRA, systematic (c, d) regular LDGM, and systematic (c, d) regular IRA ensembles, respectively,*

satisfy

$$w(a) \leq H(a) + \max_{0 \leq b \leq 1} \left\{ R(1-c)H(b) + \inf_{x>0} \ln \frac{f_-(x,d)^a f_+(x,d)^{1-a}}{x^{bd}} \right\} \triangleq w^{ub}(a) \quad (21)$$

$$w(a) \leq \max_{0 \leq r \leq \min(2(1-a), 2a)} \left\{ (1-a)H\left(\frac{r}{2(1-a)}\right) + aH\left(\frac{r}{2a}\right) + \max_{0 \leq b \leq 1} \left[R(1-c)H(b) + \inf_{x>0} \log \frac{f_-(x,d)^r f_+(x,d)^{1-r}}{x^{bd}} \right] \right\} \triangleq w^{ub}(a) \quad (22)$$

$$w(a) = \max_{\max(0, \frac{a-1+R}{R}) \leq b \leq \min(1, \frac{a}{R})} \left\{ R(1-c)H(b) + (1-R) \left[H\left(\frac{a-bR}{1-R}\right) + \inf_{x>0} \log \frac{f_-(x,d)^{\frac{a-bR}{1-R}} f_+(x,d)^{1-\frac{a-bR}{1-R}}}{x^{bd}} \right] \right\} \quad (23)$$

$$w(a) = \max_{\max(0, \frac{a-1+R}{R}) \leq b \leq \min(1, \frac{a}{R})} R(1-c)h(b) + \max_{0 \leq r \leq \min(2(1-\frac{a-bR}{1-R}), 2(\frac{a-bR}{1-R}))} \left\{ (1-R) \left[\left(1 - \frac{a-bR}{1-R}\right) H\left(\frac{r}{2(1-\frac{a-bR}{1-R})}\right) + \frac{a-bR}{1-R} H\left(\frac{r}{2(\frac{a-bR}{1-R})}\right) \inf_{x>0} \log \frac{f_-(x,d)^r f_+(x,d)^{1-r}}{x^{bd}} \right] \right\} \quad (24)$$

Proof: From (17) and (11), the AAWD of the nonsystematic (c, d) regular LDGM ensemble with $R \triangleq d/c$ and AWD $\overline{N}(l)$ can be calculated as follows³

$$w(a) = \lim_{n \rightarrow \infty} \frac{1}{n} \log \overline{N}(an) \quad (25a)$$

$$\leq \lim_{n \rightarrow \infty} \frac{1}{n} \log \overline{N^{ub}}(an) \quad (25b)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} \ln \sum_{w=0}^m \overline{Z_{w,an}^{(LDGM)}} \quad (25c)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} \ln \sum_{bm=0}^m \frac{\binom{m}{bm} \binom{n}{an} \text{coef}(f_-(x,d)^{an} f_+(x,d)^{(1-a)n}, x^{bcm})}{\binom{cm}{bcm}} \quad (25d)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} \ln \left[\binom{n}{an} \max_{0 \leq b \leq 1} \frac{\binom{\frac{d}{c}n}{\frac{bd}{c}n} \text{coef}(f_-(x,d)^{an} f_+(x,d)^{(1-a)n}, x^{bdn})}{\binom{dn}{bdn}} \right] + o(1) \quad (25e)$$

³ R may not be the true guaranteed rate of the nonsystematic (c, d) regular LDGM ensemble since nonsystematic codes with repeated codewords can undergo a rate reduction.

where $o(1)$ is a function of n that converges to 0 as n approaches infinity. Now, (21) follows from (18a) and (19).

Similarly, (22), (23) and (24) can be derived from (11), (15), (16), (17), (18a) and (19). ■ Analogous results for the irregular LDGM and IRA ensembles can also be obtained in a straightforward manner from (8), (14), (16), (17), (18b) and (19), and are omitted here.

The derived upper bounds on the AAWD of nonsystematic ensembles are sufficient for obtaining various ML performance upper bounds. However, we still have to determine the guaranteed (design) rate of these codes due to the possible occurrence of rate reduction. In the following, we will show that regular nonsystematic LDGM and IRA codes indeed suffer no rate reduction with asymptotically high probability.

Let R_1 be the true rate of a randomly drawn code from the nonsystematic (c, d) regular LDGM ensemble. Let $N^{ub}(0)$ be the random variable denoting the number of input words that result in all-0 codeword in a randomly drawn code. Then, we have by the linearity of the LDGM codes and Markov's inequality that

$$P(R_1 < R - r) = P(2^{nR}/2^{nR_1} > 2^{nr}) = P(N^{ub}(0) > 2^{nr}) \leq \frac{\overline{N^{ub}(0)}}{2^{nr}} \leq O\left(2^{n\left(\frac{w^{ub}(0)}{\ln 2} - r\right)}\right) \quad (26)$$

which converges to 0 as n approaches infinity for all $r > \frac{w^{ub}(0)}{\ln 2}$. Therefore, if $w^{ub}(0) \leq 0$, the nonsystematic (c, d) regular LDGM ensemble essentially suffers no rate reduction with asymptotically high probability. This last inequality is shown to be true in the following theorem.

Theorem 2 *For the (c, d) nonsystematic regular LDGM ensembles, $R = d/c$ is the guaranteed rate with asymptotically high probability in the ensemble, i.e., these ensembles suffer no rate reduction.*

Proof: Following the above discussion, it is sufficient to show that $w^{ub}(0) \leq 0$ for these ensembles. Starting from the expression in (21) we have for every $b \in [0, 1]$

$$R(1 - c)H(b) + \inf_{x>0} \ln \frac{f_+(x, d)}{x^{bd}} \leq (1 - d)H(b) + \inf_{x>0} \ln \frac{f_+(x, d)}{x^{bd}}. \quad (27)$$

However, the last expression is exactly the AAWD of a Gallager's (n, d, d) ensemble of codeword length n , variable node degree d , and check node degree d as defined in [1] with rate 0 (the

expression for the AAWD of Gallager's (n, c, d) ensemble was derived in [29] and it appears as an upper bound in [1]). Thus

$$w^{ub}(0) = \max_{0 \leq b \leq 1} \left\{ R(1-c)H(b) + \inf_{x>0} \ln \frac{f_+(x, d)}{x^{bd}} \right\} \quad (28a)$$

$$\leq \max_{0 \leq b \leq 1} \left\{ (1-d)H(b) + \inf_{x>0} \ln \frac{f_+(x, d)}{x^{bd}} \right\} \quad (28b)$$

$$= \max_{b \in \{0, 1/2, 1\}} \left\{ (1-d)H(b) + \inf_{x>0} \ln \frac{f_+(x, d)}{x^{bd}} \right\} \quad (28c)$$

$$= 0 \quad (28d)$$

where the last two equalities follow directly from [1, Appendix A, Theorem A.1]. ■

Since the accumulator code maps distinct input words to distinct output words, we have the following corollary.

Corollary 1 *The nonsystematic (c, d) regular IRA ensemble suffers no rate reduction, and its guaranteed rate is given by $R = c/d$ with asymptotically high probability.*

D. Numerical Results

Although the AAWD's given in Theorem 1 do not assume close forms, we can still numerically evaluate these expressions to acquire some intuition and insight on the performance of the LDGM and IRA ensembles. Fig. 2 depicts the AAWD of the nonsystematic (10,5) regular LDGM and IRA ensembles, and compares them with those of the (7,14) regular LDPC ensemble given in [27] and the rate-1/2 random ensemble. As can be seen in the figure, the IRA ensemble has a more concentrated AAWD than the LDGM ensemble. This demonstrates how the rate-1 accumulator code helps eliminate low weight codewords in the nonsystematic LDGM codes. Moreover, this figure shows that the AAWD of the nonsystematic (10,5) regular IRA ensemble well approximates that of the random ensemble with the same rate for positive values of the AAWD.

A similar comparison is shown in Fig. 3. The effect of the accumulator code is also evident for both the systematic (12,12) and the nonsystematic (10,5) regular IRA ensembles. It is also evident in this figure that the AAWD of the nonsystematic IRA ensemble is better than that of the systematic one with the same graphical complexity. This finding is consistent with the results of [7] for the BEC.

Motivated by the above numerical examples, we now focus on the nonsystematic regular IRA ensembles and investigate their AAWD's with different check node degrees and the same rate. Fig. 4 shows that the AAWD of the rate 1/2 nonsystematic regular IRA ensembles approaches that of the random code ensemble (for positive values of the AAWD) with increasing check node degrees. In particular, the AAWD of the nonsystematic (12,6) regular IRA ensemble almost coincides with that of the random ensemble for all growth exponent values greater than 0 with a moderate check node degree equal to $6 + 2 = 8$. Compared with LDPC ensembles, which are proved in [9] to have a random-ensemble-like AAWD only at the limit when the check node degree goes to infinity, IRA ensembles appear to have a great potential of achieving capacity with bounded (small) check node degrees.

However, it is proved in [30] that if a code can be encoded in linear time using sub-linear memory (IRA codes fall in this category) then this code can not have minimum distance growing linearly with n . This result explains why the AAWD of IRA ensembles is always nonnegative as can be seen in the figures, and imposes a difficulty on proving IRA codes to be capacity-achieving on MBIOS channels even with ML decoding. For instance, the ML bound in [15] cannot be used in the same way used to prove that regular LDPC codes can achieve capacity on MBIOS channels with ML decoding [9]. In the next section, we introduce a new family of codes that circumvent this problem and are proved to be capacity-achieving on MBIOS channels with ML decoding.

To further investigate how regular IRA ensembles perform on the BIAWGN channel with ML decoding, we invoke Divsalar's bound [14] on the minimum bit signal to noise ratio (SNR) $(\frac{E_b}{N_0})^*$ required for reliable communication as follows

$$\left(\frac{E_b}{N_0}\right)^* \leq \frac{1}{R} \max_{0 \leq a \leq 1} \left\{ \frac{(1 - e^{-2w(a)})(1 - a)}{2a} \right\}. \quad (29)$$

This bound is shown in [14] to have the same error exponent as the tangential sphere bound of Poltyrev [19], which often happens to be the tightest reported upper bound for block codes transmitted over the BIAWGN channel (see [31]). The results for rate-1/2 nonsystematic regular IRA, systematic regular IRA and regular LDPC ensembles are summarized in Table I. The comparison is based on the same graphical complexity, denoted by \bar{e} in the table. As can be seen, all nonsystematic regular IRA ensembles with a check node degree greater than 3 yield

the same performance bound, which is better than that of their corresponding systematic regular IRA and regular LDPC ensembles, and is only 0.124 dB away from the Shannon limit. This result seems to suggest that nonsystematic regular IRA codes with small check node degrees can come very close to the BIAWGN channel capacity.

III. LDPC-GM CODES

In this section, we introduce the LDPC-GM codes, which are serially concatenated codes with an outer LDPC code and an inner LDGM code. In particular, we show that if the outer code is Gallager's LDPC code and the inner code is a rate-1 regular LDGM code, then this LDPC-GM ensemble can achieve capacity on MBIOS channels using ML decoding with bounded graphical complexity.

A. Gallager's LDPC Ensemble

Consider Gallager's (n, j, k) LDPC ensemble of codeword length n , variable node degree j , and check node degree k as introduced in [1] 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 [29] (it appears as an upper bound in [1]) to be

$$w_o(a) \triangleq \lim_{n \rightarrow \infty} \frac{1}{n} \ln \overline{N_o(an)} = (1 - R_o) \inf_{x > 0} \left\{ \ln \frac{(1+x)^k + (1-x)^k}{2x^{ak}} \right\} - (j-1)H(a) \quad (30)$$

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 that⁴*

- 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 $a \in (\delta_o, 1/2]$, 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 $l \in \{0, 1, \dots, n\}$.

In Fact 1, item 1 to 4 are either proved explicitly in [1, Appendix A] or directly result from there, and item 5 follows from the linearity of the LDPC codes and the fact that the all-1

⁴Suppose $f(n)$ and $g(n)$ are two functions of n . We say $f(n) = O(g(n))$ if there exist N and $c > 0$ such that $|f(n)| < c|g(n)|$ for all $n > N$.

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.

In the remaining of this section, 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 of $w_o(a)$, which is tight especially when a is around $1/2$.

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

Proof: Bounding the infimum term of (30) by substituting $x = \frac{a}{1-a}$, we have

$$\inf_{x>0} \left\{ \ln \frac{(1+x)^k + (1-x)^k}{2x^{ak}} \right\} \leq \ln \frac{(1+x)^k + (1-x)^k}{2x^{ak}} \Big|_{x=\frac{a}{1-a}} \quad (31a)$$

$$= \ln[1 + (1 - 2a)^k] - \ln 2 + kH(a), \quad (31b)$$

from which the lemma follows straightforwardly. ■

The next lemma gives a sufficient condition on k for any desired lower bound of δ_o .

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

$$k > \frac{\ln \left(1 - \frac{H(\delta)}{(1 - R_o) \ln 2} \right)}{\ln(1 - 2\delta)}, \quad (32)$$

then $\delta_o > \delta$, where we denote by $H^{-1}(x)$ the unique $a \in [0, 1/2]$, such that $H(a) = x$.

Proof:

$$(1 - R_o) \ln[1 + (1 - 2\delta)^k] + [H(\delta) - (1 - R_o) \ln 2] < 0 \quad (33a)$$

$$\Leftrightarrow \ln[1 + (1 - 2\delta)^k] < \left(1 - \frac{H(\delta)}{(1 - R_o) \ln 2} \right) \ln 2 \quad (33b)$$

$$\Leftrightarrow (1 - 2\delta)^k < 1 - \frac{H(\delta)}{(1 - R_o) \ln 2} \quad (33c)$$

$$\Leftrightarrow k > \frac{\ln \left(1 - \frac{H(\delta)}{(1 - R_o) \ln 2} \right)}{\ln(1 - 2\delta)} \quad (33d)$$

where we have used the facts that $\ln(1+x) < x$, $\forall x \geq 0$ and $1 - 2\delta < 1$ in the last two steps.

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

B. 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. 5. 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 and from (11), the AWD $\overline{N_c(l)}$ of this LDPC-GM ensemble can be bounded by

$$\overline{N_c(l)} \leq \overline{N_c^{ub}(l)} \triangleq \sum_{s=0}^n \frac{\overline{N_o(s)} \overline{Z_{s,l}^{(LDGM)}}}{\binom{n}{s}} \quad (34a)$$

$$= \binom{n}{l} \sum_{s=\lceil l/k \rceil}^{\lfloor n-l/k \rfloor} \frac{\overline{N_o(s)}}{\binom{kn}{ks}} \text{coef}(f_-(x, k)^l f_+(x, k)^{n-l}, x^{ks}) \quad (34b)$$

where the change of the range of the 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 $\overline{N_c^{ub}(l)}$, we employ (18a) and (19) to get

$$w_c(a) \triangleq \lim_{n \rightarrow \infty} \frac{1}{n} \ln \overline{N_c(an)} \quad (35a)$$

$$\leq \lim_{n \rightarrow \infty} \frac{1}{n} \ln \overline{N_c^{ub}(an)} \quad (35b)$$

$$= H(a) + \max_{\frac{a}{k} \leq b \leq 1 - \frac{a}{k}} w_o(b) - kH(b) + \inf_{x>0} \ln \frac{f_-(x, k)^a f_+(x, k)^{1-a}}{x^{bk}} \quad (35c)$$

$$\stackrel{(a)}{\leq} H(a) + \max_{\frac{a}{k} \leq b \leq 1 - \frac{a}{k}} w_o(b) + a \ln[1 - (1 - 2b)^k] + (1 - a) \ln[1 + (1 - 2b)^k] - \ln 2 \quad (35d)$$

$$\triangleq w_c^{ub}(a) \quad (35e)$$

where (a) follows by substituting $x = \frac{b}{1-b}$ in the infimum expression. Since Theorem 2 shows that regular LDGM ensembles are free of rate reduction with asymptotically high probability, we conclude that the guaranteed rate R of this LDPC-GM ensemble is R_o with asymptotically high probability.

C. Analysis of ML decoding of LDPC-GM Codes on MBIOS channels

In this section, we will first characterize $w_c^{ub}(a)$, and then use the derived results to prove that LDPC-GM codes can be capacity-achieving on MBIOS channels using ML decoding with

bounded graphical complexity. Although $w_c^{ub}(a)$ is not symmetric about $a = 1/2$, the following lemma shows that we can focus on analyzing $w_c^{ub}(a)$ for $a \in [0, 1/2]$ and bound $w_c^{ub}(a)$ by $w_c^{ub}(1-a)$ for $a \in [1/2, 1]$.

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

Proof: Since

$$\ln[1 - (1 - 2b)^k] \leq 0 \leq \ln[1 + (1 - 2b)^k] \quad \forall b \in [0, 1] \quad (36)$$

and $1-a \leq a$ for all $a \in [1/2, 1]$, it follows from (35) that for all $a \in [1/2, 1]$, we have

$$w_c^{ub}(a) = H(a) + \max_{\frac{a}{k} \leq b \leq 1 - \frac{a}{k}} w_o(b) + a \ln[1 - (1 - 2b)^k] + (1-a) \ln[1 + (1 - 2b)^k] - \ln 2 \quad (37a)$$

$$\leq H(1-a) + \max_{\frac{1-a}{k} \leq b \leq 1 - \frac{1-a}{k}} w_o(b) + (1-a) \ln[1 - (1 - 2b)^k] + a \ln[1 + (1 - 2b)^k] - \ln 2 \quad (37b)$$

$$= w_c^{ub}(1-a) \quad (37c)$$

■

In the next theorem, we prove that given any R_1 in $[0, 1]$, the positive part of $w_c^{ub}(a)$ can be upper bounded by the AAWD of the random ensemble for any rate $R \leq R_1$ if k is sufficiently large. In this case, we also prove that $\overline{N_c(l)}$ decreases at least polynomially with n in the negative part of $w_c^{ub}(a)$ when $j \geq 3$.

Theorem 3 For any $R_1 \in [0, 1]$, there exists an integer $M < \infty$ such that for all $k > M$ and for all LDPC-GM codes with design rate $R \in [0, R_1]$, there exists a $\delta' < H^{-1}((1-R) \ln 2)$ such that the following two statements are true.

1)

$$w_c^{ub}(a) \begin{cases} \leq 0 & \text{if } a = 0, \\ < 0 & \text{if } a \in (0, \delta'], \\ \leq H(a) - (1-R) \ln 2 & \text{if } a \in (\delta', 1/2]. \end{cases} \quad (38)$$

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

Proof: See Appendix I. ■

One important point in the above theorem is that, M only depends on R_1 , and does not vary with the design rate R . Therefore, given any MBIOS channel with capacity C , if we let $R_1 = C$, then a fixed and finite $k > M$ (e.g., $k = M + 1$) depending only on C is sufficient for all LDPC-GM codes of design rate $R \in [0, C]$ to satisfy the two statements of Theorem 3. On the contrary, if M were also dependent on R (as proved in [9] for the case for regular LDPC codes), then M (and thus the graphical complexity) could approach infinity as R approaches the capacity C . Indeed, this is the essence of our bounded graphical complexity result as will be proved in Theorem 4.

If we let d_{min} and $N_c(l)$ be the random variables denoting the minimum distance and number of codewords of weight l , respectively, of a randomly drawn code from the LDPC-GM ensemble, and if we denote by $\delta_{GV} = H^{-1}((1 - R) \ln 2)$ the normalized Gilbert-Varshamov distance, then from Markov's inequality, we have for all $\epsilon > 0$,

$$P(d_{min} \leq (\delta_{GV} - \epsilon)n) = P\left(\sum_{l \in (0, (\delta_{GV} - \epsilon)n]} N_c(l) \geq 1\right) \quad (39a)$$

$$\leq \sum_{l \in (0, (\delta_{GV} - \epsilon)n]} \overline{N_c(l)} \quad (39b)$$

$$\leq n \max_{l \in (0, \delta' n]} \overline{N_c^{ub}(l)} + n \exp\left\{n \sup_{a \in (\delta', \delta_{GV} - \epsilon]} w_c^{ub}(a) + o(n)\right\} \quad (39c)$$

$$= O(n^{-j+3}). \quad (39d)$$

The last equality follows from the facts proved in Theorem 3. In particular, for the first term in (39c) we have $\overline{N_c^{ub}(l)} = O(n^{-j+2})$ for all $l \in (0, \delta' n]$ and for the second term we have

$$w_c^{ub}(a) < 0 \text{ for all } a \in [\delta', \delta_{GV} - \epsilon] \quad (40a)$$

$$\Rightarrow n \exp\left\{n \sup_{a \in (\delta', \delta_{GV} - \epsilon]} w_c^{ub}(a) + o(n)\right\} \text{ decreases exponentially for large } n, \quad (40b)$$

where $o(n)$ denotes some value that converges to 0 as n approaches infinity. Equation (39) implies that $P(d_{min} > (\delta_{GV} - \epsilon)n)$ approaches 1 asymptotically as n approaches infinity when $j \geq 4$. Since ϵ can be arbitrarily small, we have proved the following corollary.

Corollary 2 *For any $R_1 \in [0, 1]$, there exists an integer $M < \infty$ such that for all $k > M$, and for all $j \geq 4$, all LDPC-GM codes with design rate $R \in [0, R_1]$ have a normalized minimum distance, which is arbitrarily close to the Gilbert-Varshamov bound with asymptotically high probability.*

In Fig. 6, we compare the AAWD 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 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, the number of low weight codewords still becomes vanishingly small as n goes to infinity.

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

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

Proof: See Appendix II. ■

As can be seen in Fig. 5, the graphical complexity Δ of these LDPC-GM codes can be evaluated as follows

$$\Delta = \frac{n(j+k) + n}{Rn} = \frac{(2-R)k + 1}{R}. \quad (41)$$

Since Theorem 4 guarantees that k does not approach infinity, we can deduce that these LDPC-GM codes with any rate $R \in (0, 1)$ can be capacity-achieving on any MBIOS channel with bounded graphical complexity.

IV. 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 and inner LDGM codes to be more generally irregular, the LDPC-GM

ensemble can be capacity-achieving on any BEC under BP decoding with bounded decoding complexity per information bit. Although this is not a proof that the same might be true for 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 [32]. Note that this LDPC-GM ensemble has guaranteed rate

$$R = 1 - \frac{\int_0^1 \rho(t) dt}{\int_0^1 \lambda(t) dt}. \quad (42)$$

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. 5. Then, assuming we are operating at some fixed point, we have the following density evolution equations.

$$x_1 = 1 - (1 - q)(1 - x_4) \quad (43a)$$

$$x_2 = x_1^2 \lambda(x_3) \quad (43b)$$

$$x_3 = 1 - \rho(1 - x_2) \quad (43c)$$

$$x_4 = x_1 \tilde{\lambda}(x_3) \quad (43d)$$

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

$$\tilde{\lambda}_i = \frac{\lambda_i/i}{\int_0^1 \lambda(t) dt}, \quad (44)$$

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

$$\tilde{\lambda}(x) = \frac{\int_0^x \lambda(t) dt}{\int_0^1 \lambda(t) dt}. \quad (45)$$

Note that equations (43) are also the density evolution equations for the serially concatenated codes with an outer LDPC code and an inner differentiator code⁵. Solving these equations for

⁵A differentiator code with input a_k and output b_k is defined by the input-output relation $b_k = a_{k-1} + a_k$

x_3 , we have

$$x_3 = 1 - \rho(1 - x_2) \quad (46a)$$

$$= 1 - \rho(1 - x_1^2 \lambda(x_3)) \quad (46b)$$

$$= 1 - \rho \left(1 - \left[\frac{q}{1 - (1 - q) \tilde{\lambda}(x_3)} \right]^2 \lambda(x_3) \right). \quad (46c)$$

If (46) 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 approaches infinity. Therefore, if we have

$$1 - \rho \left(1 - \left[\frac{q}{1 - (1 - q) \tilde{\lambda}(x_3)} \right]^2 \lambda(x_3) \right) < x_3, \quad \forall x_3 \in (0, 1] \quad (47)$$

then the BP decoding is successful. Note that, (46) is essentially the same as equation (6) in [7] except for the following changes: $x_0 \rightarrow 1 - x_3$, $p \rightarrow 1 - q$, $\lambda(\cdot) \rightarrow \rho(\cdot)$, $\rho(\cdot) \rightarrow \lambda(\cdot)$, and $R(\cdot) \rightarrow \tilde{\lambda}(\cdot)$. More generally, (46) is an instance of the symmetry introduced in [24]. So, in the following, we will use the results proved in [7] to show two particular degree distribution pairs are capacity-achieving under BP decoding.

Theorem 5 (Check-regular ensemble) *Let*

$$\lambda(x) = \frac{1 - (1 - x)^{\frac{1}{k-1}}}{\left[1 - (1 - q) \left(1 - kx + (k - 1) \left[1 - (1 - x)^{\frac{k}{k-1}} \right] \right) \right]^2} \quad (48)$$

$$\rho(x) = x^{k-1} \quad (49)$$

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 that⁶

$$\sum_{i=M(\epsilon)+1}^{\infty} \frac{\lambda_i}{i} < \frac{\epsilon(1 - q)}{qk} \quad (50)$$

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.

⁶ $M(\epsilon)$ 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 $M(\epsilon)$.

Proof: See Appendix III-A. ■

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

$$\Delta < \frac{knq + 2n + n}{(1-q)(1-\epsilon)n} = \frac{qk + 3}{(1-q)(1-\epsilon)}, \quad (51)$$

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

Theorem 6 (Variable-regular ensemble) *Let*

$$\lambda(x) = x^2 \quad (52)$$

$$\rho(x) = 1 + \frac{2(1-q)(1-x)^2 \sin\left(\frac{1}{3} \arcsin\left(\sqrt{-\frac{27(1-q)(1-x)^{\frac{3}{2}}}{4q^3}}\right)\right)}{\sqrt{3}q^4 \left[-\frac{(1-q)(1-x)^{\frac{3}{2}}}{q^3}\right]^{\frac{3}{2}}} \quad (53)$$

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 that⁷

$$\sum_{i=M(\epsilon)+1}^{\infty} \rho_i < \frac{\epsilon(1-q)}{3} \quad (54)$$

and let

$$\rho_\epsilon(x) \triangleq \left(1 - \sum_{i=1}^{M(\epsilon)} \rho_i\right) + \sum_{i=1}^{M(\epsilon)} \rho_i x^{i-1} \quad (55)$$

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 III-B. ■

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

$$\Delta < \frac{3n + 2n + n}{(1-q)(1-\epsilon)n} = \frac{6}{(1-q)(1-\epsilon)} \quad (56)$$

⁷ $M(\epsilon)$ 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 $M(\epsilon)$.

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

One drawback of these capacity-achieving degree distribution pairs is that they are not guaranteed to be valid, i.e., with only nonnegative coefficients, for all $q \in (0, 1)$. Thus, it is not clear if there exist capacity-achieving check-regular ensembles with bounded complexity for the BEC with erasure probability $q \leq 12/13$ (respectively, variable-regular ensembles for the BEC with erasure probability $q \leq 0.05$). However, since this is true for q in the vicinity of 1 (which is not true for the capacity-achieving IRA codes in [7]), it is possible to construct capacity-achieving ensembles with bounded complexity for any q by considering punctured LDPC-GM codes. The idea is to construct a low-rate capacity-achieving code for a bad (i.e., q close to 1) BEC channel, and then use puncturing to increase its rate. In [33], it is shown that random puncturing results in no performance loss on the gap to capacity for codes on the BEC. It follows that puncturing can be used to increase the rate of LDPC-GM codes without affecting their capacity-achievability, a fact that was also observed by Pfister and Sason [24]. Furthermore, since a punctured LDPC-GM ensemble can also be viewed as another unpunctured LDPC-GM ensemble with inner irregular LDGM code (which is no longer rate-1 in general), we have the following theorem.

Theorem 7 *Let (λ, ρ) be a degree distribution pair implied by Theorem 5 or Theorem 6 for some given ϵ and q' . Consider the LDPC-GM ensemble, whose outer LDPC code has degree distribution pair (λ, ρ) , and inner LDGM code has degree distribution pair (f, g) . Then for any given $p \in [0, q']$, if*

$$f(x) = x(1 - p) + p \tag{57a}$$

$$g(x) = x \tag{57b}$$

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 III-C. ■

According to this theorem, 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 produce capacity-achieving LDPC-GM ensembles for all BECs with bounded decoding complexity.

V. CONCLUSION

In this paper, we first studied some fundamental properties of IRA codes, and then introduced LDPC-GM codes, which were proved to be capacity-achieving on the BEC and MBIOS channels using BP and ML decoding, respectively, with bounded graphical complexity. These LDPC-GM codes are the first reported ensembles that achieve capacity on MBIOS channels with bounded graphical complexity.

For the IRA codes, we derived their AIPWE by viewing an IRA code as a serially concatenated code with an outer LDGM code and an inner accumulator code. The resulting AIPWE was then used to derive the AWD for systematic and nonsystematic versions of IRA codes, and their asymptotic growth rate was also calculated. In the process, we also derived the AAWD of the systematic and nonsystematic LDGM codes, and proved that nonsystematic regular LDGM codes are free of rate reduction with asymptotically high probability. By numerically evaluating the AAWD of the ensembles, we concluded that: (a) the accumulator code plays an important role in eliminating low weight codewords for IRA ensembles; (b) the nonsystematic regular IRA ensembles have more concentrated AAWD's than their corresponding systematic ones with the same graphical complexity; (c) the nonsystematic regular IRA ensembles with moderate check node degrees have AAWD's very close to that of the random ensemble for all growth rate values greater than zero. The bit SNR thresholds on the BIAWGN channel based on Divsalar's bound were obtained to show that nonsystematic regular IRA ensembles with small check node degrees have a better guaranteed ML performance than the corresponding systematic regular IRA and regular LDPC ensembles with the same graphical complexity, which is only 0.124 dB away from the Shannon limit. However, although these promising results made nonsystematic IRA ensembles strong candidates for capacity-achieving codes on noisy channels with bounded graphical complexity, the fact that they do not have linearly increasing minimum distance as proved in [30] prevented this statement from being rigorously proved.

Motivated by this reason, LDPC-GM codes codes, i.e., concatenated codes with an outer LDPC code and an inner LDGM code, were introduced. In the case that the outer code is a Gallager's (n, j, k) LDPC code and the inner code is a rate-1 (k, k) regular LDGM code, we proved that

for any desired range of rates R , there always exists an integer $M < \infty$ such that if $k > M$, then the resulting AAWD of the LDPC-GM codes has a positive part, which can be upper bounded by the AAWD of the random ensemble, and a negative part, where the number of codewords vanishes at least polynomially in n when $j \geq 4$. This result was attributed to the presence of the rate-1 LDGM encoder, which helps eliminate high weight codewords while maintaining a vanishingly small amount of low weight codewords in the LDPC code. The implication of the above statement is that these codes achieve the Gilbert-Varshamov bound with asymptotically high probability. Furthermore, after applying the ML performance bound given in [15] to these LDPC-GM codes, we proved that they can achieve capacity on any MBIOS channel using ML decoding. Since all these results hinged on the only condition that k is greater than some finite number, we have proved that these LDPC-GM codes are capacity-achieving codes with bounded graphical complexity on any MBIOS channel. Finally, if the outer LDPC code is allowed to be irregular, then invoking the density evolution method, we showed two particular ensembles of the LDPC-GM codes to be capacity-achieving 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 were also presented.

These favorable results could suggest a high potential for the LDPC-GM codes to achieve capacity on MBIOS channels with bounded decoding complexity per iteration. This remains an open problem mainly due to the fact that the only available method for studying the performance of turbo-like codes under BP is density evolution, which becomes ineffective as an analytical tool in MBIOS channels. Even if this problem could be solved another open problem arises: since the required number of iterations for successful iterative decoding for the LDPC-GM codes as a function of the gap to capacity remains unknown (a fact that is true also for all other known capacity-achieving codes), it is not clear whether bounded graphical complexity property implies bounded decoding complexity using iterative decoding.

APPENDIX I

PROOF OF THEOREM 3

Fix an R_1 and pick an arbitrary $\delta \in (0, H^{-1}((1 - R_1) \ln 2))$.

1) Define

$$f(b) \triangleq w_o(b) + a \ln \frac{1 - (1 - 2b)^k}{2} + (1 - a) \ln \frac{1 + (1 - 2b)^k}{2}. \quad (58)$$

We will bound $f(b)$ in two cases.

Case (a): Let

$$M'_1 \triangleq \frac{\ln \left[1 - \frac{H(\delta)}{(1-R_1) \ln 2} \right]}{\ln(1 - 2\delta)} \geq \frac{\ln \left[1 - \frac{H(\delta)}{(1-R) \ln 2} \right]}{\ln(1 - 2\delta)} \quad (59)$$

and $M_1 = \max\{M'_1, 1/\delta\}$. By Lemma 2, if $k > M_1$ then $w_o(\delta) < 0$ for all $R \in [0, R_1]$. Therefore, for $k > M_1$ and $b \in [a/k, \delta] \cup [1 - \delta, 1 - a/k]$, we have

$$f(b) \leq w_o(b) - H(a) \leq \max\{w_o(a/k), w_o(\delta)\} - H(a), \quad (60)$$

where the first inequality follows from the fact that relative entropy is always nonnegative [34, Theorem 2.6.3], and the second inequality follows from Fact 1.

Case (b): $b \in (\delta, 1 - \delta)$. We have from Lemma 1 that

$$\begin{aligned} f(b) &\leq (1 - R) \ln[1 + (1 - 2b)^k] + H(b) - (1 - R) \ln 2 + \\ &\quad + a \ln \frac{1 - (1 - 2b)^k}{2} + (1 - a) \ln \frac{1 + (1 - 2b)^k}{2} \end{aligned} \quad (61a)$$

$$\leq - (1 - R) \ln 2 - \ln 2 + \{H(b) + 2 \ln[1 + (1 - 2b)^k]\} \quad (61b)$$

where the last inequality follows from (36). Since

$$\frac{\partial^2 H(b)}{\partial b^2} = -\frac{1}{(1 - b)b} \leq -4, \quad (62)$$

and

$$\frac{\partial^2 2 \ln[1 + (1 - 2b)^k]}{\partial b^2} = \frac{8k[k - 1 - (1 - 2b)^k](1 - 2b)^{k-2}}{[1 + (1 - 2b)^k]^2} \quad (63a)$$

$$\leq 8k(k - 1)(1 - 2b)^{k-2} \quad (63b)$$

$$\leq 8k(k - 1)(1 - 2\delta)^{k-2}, \quad (63c)$$

which can be made arbitrarily close to 0 for a large enough k , there exists an M_2 such that

$$k > M_2 \Rightarrow \frac{\partial^2 H(b) + 2 \ln[1 + (1 - 2b)^k]}{\partial b^2} < 0, \quad \forall b \in (\delta, 1 - \delta). \quad (64)$$

Furthermore, since

$$\left. \frac{\partial H(b) + 2 \ln[1 + (1 - 2b)^k]}{\partial b} \right|_{b=1/2} = \left\{ \ln \frac{1-b}{b} + \frac{-4k(1-2b)^{k-1}}{1+(1-2b)^k} \right\} \Big|_{b=1/2} = 0 \quad (65)$$

it follows that the maximum of $H(b) + 2 \ln[1 + (1 - 2b)^k]$ is attained at $b = 1/2$, and thus

$$f(b) \leq -(1 - R) \ln 2, \quad \forall b \in (\delta, 1 - \delta). \quad (66)$$

Based on the above two cases, we have shown that for a fixed R_1 and an arbitrary $\delta \in (0, H^{-1}((1 - R_1) \ln 2))$, there exists an $M \triangleq \max\{M_1, M_2\}$ such that for all $k > M$ and for all LDPC-GM ensembles with $R \leq R_1$ we have

$$w_c^{ub}(a) = H(a) + \max_{\frac{a}{k} \leq b \leq 1 - \frac{a}{k}} f(b) \leq \max\{H(a) - (1 - R) \ln 2, w_o(a/k), w_o(\delta)\}. \quad (67)$$

For $a = 0$ we have $\max\{w_o(a/k), w_o(\delta)\} = 0$ and $H(a) - (1 - R) \ln 2 = -(1 - R) \ln 2 < 0$, which implies $w_c^{ub}(0) = 0$. For $a = 1/2$ we have $\max\{w_o(a/k), w_o(\delta)\} < 0$ and $H(a) - (1 - R) \ln 2 = R \ln 2 > 0$. Since $\max\{w_o(a/k), w_o(\delta)\} < 0$ for all $a > 0$, $H(a) - (1 - R) \ln 2$ must intersect with $\max\{w_o(a/k), w_o(\delta)\}$ at some $a = \delta' < H^{-1}((1 - R) \ln 2)$. This is true since $\max\{w_o(a/k), w_o(\delta)\}$ is a non-increasing function w.r.t a for all $a \in [0, 1/2]$.

Thus for all $a \in (0, \delta']$, $w_c^{ub}(0) = \max\{w_o(a/k), w_o(\delta)\} < 0$. In addition, for all $a \in [\delta', 1/2]$, $w_c^{ub}(0) = H(a) - (1 - R) \ln 2$. This concludes the proof of the first statement of the theorem.

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

$$\overline{N_c^{ub}(l)} = \sum_{s=\lceil l/k \rceil}^{\lfloor n-l/k \rfloor} \frac{\overline{N_o(s)} \overline{Z_{s,l}^{(LDPG)}}}{\binom{n}{s}} \quad (68a)$$

$$\stackrel{(a)}{\leq} \sum_{s=\lceil l/k \rceil}^{\delta n} \overline{N_o(s)} + \sum_{s=n-\delta n}^{\lfloor n-l/k \rfloor} \overline{N_o(s)} + \sum_{s=\delta n}^{n-\delta n} \frac{\overline{N_o(s)} \overline{Z_{s,l}^{(LDPG)}}}{\binom{n}{s}} \quad (68b)$$

$$\stackrel{(b)}{\leq} O(n^{-j+2}) + n \exp\{n[H(l/n) + \max_{\delta \leq b \leq 1-\delta} f(b)] + o(n)\} \quad (68c)$$

$$\stackrel{(c)}{\leq} O(n^{-j+2}) + n \exp\{n[H(l/n) - (1-R) \ln 2] + o(n)\} \quad (68d)$$

$$\stackrel{(d)}{=} O(n^{-j+2}) \quad (68e)$$

where $o(n)$ denotes some value that converges to 0 as n approaches infinity. In (68), (a) follows from the fact that $\overline{Z_{s,l}^{(LDPG)}}/\binom{n}{s} \leq 1$ since it is a probability as shown in (4); (b) follows from Fact 1; (c) follows from (66); (d) follows from the fact that $\delta' < H^{-1}((1-R) \ln 2)$.

APPENDIX II

PROOF OF THEOREM 4

Let M be as defined in Theorem 3 for $R_1 = C$. Moreover, let $U \subset \{1, 2, \dots, n\}$, and U^c be its complementary set. The following upper bound on the average block error probability under ML decoding is given in [15]

$$P_B \leq \sum_{l \in U} \{\overline{N_c(l)} D^l\} + 2^{-n E_r(R + \frac{\ln \alpha}{n \ln 2})} \quad (69)$$

where

$$\alpha \triangleq \max_{l \in U^c} \frac{\overline{N_c(l)}}{2^{nR} - 1} \frac{2^n}{\binom{n}{l}} \quad (70)$$

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

$$D \triangleq \sum_y \sqrt{p(y|0)p(y|1)} \leq 1 \quad (71)$$

is the Bhattacharya parameter, where $p(y|0)$ and $p(y|1)$ are the conditional probability density functions of the output of the MBIOS channel given the input. We will apply this bound to the

LDPC-GM ensemble with $k > M$, $R < C$, and

$$U \triangleq \left\{ l : \frac{l}{n} \in (0, \delta'] \cup [1 - \delta', 1] \right\}, \quad (72)$$

where δ' is as defined in Theorem 3. Regarding the first term, we have from Theorem 3 that

$$\sum_{l \in U} \{\overline{N_c(l)} D^l\} \leq \sum_{l \in U} \overline{N_c^{ub}(l)} \leq n O(n^{-j+2}) = O(n^{-j+3}) \quad (73)$$

Regarding the second term, we have from the same theorem and Lemma 3 that

$$\lim_{n \rightarrow \infty} \frac{\ln a}{n} = \max_{a \in (\delta', 1 - \delta')} w_c(a) - [H(a) - (1 - R) \ln 2] \quad (74a)$$

$$\leq \max_{a \in (\delta', 1/2]} w_c^{ub}(a) - [H(a) - (1 - R) \ln 2] \quad (74b)$$

$$\leq 0. \quad (74c)$$

Hence

$$P_B \leq O(n^{-j+3}) + 2^{-nE_r(R)} \quad (75)$$

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

APPENDIX III

PROOFS OF SECTION IV

First, we need a lemma.

Lemma 4 *If the degree distribution pair (λ, ρ) satisfies $\rho(0) = 0$, $\rho(1) = 1$, and satisfies (46) for all $x_3 \in [0, 1]$, then $R = 1 - q$.*

Proof: [7, Lemma 1] shows that under the assumed conditions, we have

$$\frac{\int_0^1 \rho(t) dt}{\int_0^1 \lambda(t) dt} = q. \quad (76)$$

■

A. Proof of Theorem 5

The facts that (λ, ρ) satisfies (46) 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 [7, Theorem 1]. By the definition of λ_ϵ , we have effectively

$$\lambda_\epsilon(x) = \sum_{i=1}^{M(\epsilon)} \lambda_i x^{i-1} \quad (77)$$

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, (47) is satisfied, which implies that the BP decoding is successful. To find the rate of this ensemble of codes, let

$$\delta \triangleq \sum_{M(\epsilon)+1}^{\infty} \tilde{\lambda}_i \quad (78)$$

be the fraction of pilot nodes. Then, we have

$$R = \frac{(1 - \delta) \int_0^1 \lambda(t) dt - \int_0^1 \rho(t) dt}{\int_0^1 \lambda(t) dt} \quad (79a)$$

$$= 1 - \delta - \frac{\int_0^1 \rho(t) dt}{\int_0^1 \lambda(t) dt} \quad (79b)$$

$$= 1 - q - \delta \quad (79c)$$

where the last equality follows from the facts that $\rho(0) = 0$, $\rho(1) = 1$, and Lemma 4. But, from (44)

$$\delta = \sum_{M(\epsilon)+1}^{\infty} \frac{\lambda_i/i}{\int_0^1 \lambda(t) dt} = q \sum_{M(\epsilon)+1}^{\infty} \frac{\lambda_i/i}{\int_0^1 \rho(t) dt} = qk \sum_{M(\epsilon)+1}^{\infty} \lambda_i/i < \epsilon(1 - q) \quad (80)$$

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

B. Proof of Theorem 6

The facts that (λ, ρ) satisfies (46) for all $x \in [0, 1]$ and that $\rho(x)$ has only non-negative coefficients for $q \in [0.05, 1]$ are proved in [7, Theorem 2]. Since $\rho_\epsilon(x) > \rho(x)$ for all $x \in (0, 1]$, (47) is satisfied and the BP decoding is successful. As for the rate of this ensemble of codes,

we have

$$R = 1 - \frac{\int_0^1 \rho_\epsilon(t) dt}{\int_0^1 \lambda(t) dt} \quad (81a)$$

$$= 1 - \frac{\sum_{i=1}^{M(\epsilon)} \frac{\rho_i}{i} + 1 - \sum_{i=1}^{M(\epsilon)} \rho_i}{\int_0^1 \lambda(t) dt} \quad (81b)$$

$$> 1 - \frac{\sum_{i=1}^{\infty} \frac{\rho_i}{i} + 1 - \sum_{i=1}^{M(\epsilon)} \rho_i}{\int_0^1 \lambda(t) dt} \quad (81c)$$

$$= 1 - \frac{\int_0^1 \rho(t) dt + \sum_{i=M(\epsilon)+1}^{\infty} \rho_i}{\int_0^1 \lambda(t) dt} \quad (81d)$$

$$\stackrel{(a)}{=} 1 - q - 3 \sum_{i=M(\epsilon)+1}^{\infty} \rho_i \quad (81e)$$

$$> (1 - \epsilon)(1 - q) \quad (81f)$$

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

C. Proof of Theorem 7

Let F be the degree distribution from the node perspective⁸ corresponding to f . We have

$$F(x) = \frac{\int_0^x f(t) dt}{\int_0^1 f(t) dt} = [x(1 - p) + p]^2 \quad (82)$$

and the following set of density evolution equations

$$x_1 = 1 - (1 - q)(1 - x_4) \quad (83a)$$

$$x_2 = F(x_1)\lambda(x_3) \quad (83b)$$

$$x_3 = 1 - \rho(1 - x_2) \quad (83c)$$

$$x_4 = f(x_1)\tilde{\lambda}(x_3) \quad (83d)$$

⁸That is, $F(x) = \sum_{i=0}^{\infty} F_i x^i$, where F_i denotes the fraction of input nodes that have i neighboring check nodes in the LDGM code.

where q denotes the channel erasure probability. After some algebraic manipulations, the fixed point equation can be shown to be

$$x_3 = 1 - \rho \left(1 - \left[\frac{q(1-p) + p}{1 - (1-q)(1-p)\tilde{\lambda}(x_3)} \right]^2 \lambda(x_3) \right) \quad (84)$$

which is the same as (46) if we let the erasure probability be $q' = q(1-p) + p$. Hence, from Theorem 5 and Theorem 6, the decoding is successful under BP decoding on the BEC with erasure probability q . Moreover, the rate of this ensemble is given by

$$R = \{\text{rate of the outer LDPC code}\} \times \frac{\{\text{number of input nodes in the LDGM code}\}}{\{\text{number of check nodes in the LDGM code}\}} \quad (85a)$$

$$= \{\text{rate of the outer LDPC code}\} \times \frac{G'(1)}{F'(1)} \quad (85b)$$

$$> (1 - \epsilon)(1 - q') \frac{1}{1 - p} \quad (85c)$$

$$= (1 - \epsilon)(1 - q), \quad (85d)$$

which then proves this theorem.

REFERENCES

- [1] R. G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA, 1963.
- [2] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. A. Spielman, and V. Stemann, "Practical loss-resilient codes," in *Proc. ACM Symposium on Theory of Computing*, El Paso, Texas, May 1997, pp. 150–159.
- [3] 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.
- [4] A. Shokrollahi, "Capacity-achieving sequences," in *Codes, Systems, and Graphical Models*, B. Marcus and J. Rosenthal, Eds., vol. 123 of *IMA Volumes in Mathematics and its Applications*, pp. 153–166. Springer-Verlag, 2000.
- [5] P. Oswald and A. Shokrollahi, "Capacity-achieving sequences for the erasure channel," *IEEE Trans. Information Theory*, vol. 48, no. 12, pp. 3017–3028, Dec. 2002.
- [6] 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.
- [7] 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.
- [8] N. Wiberg, *Codes and Decoding on General Graphs*, Ph.D. thesis, Linköping University, Linköping, Sweden, 1996.
- [9] I. Sason and R. Urbanke, "Parity-check density versus performance of binary linear block codes over memoryless symmetric channels," *IEEE Trans. Information Theory*, vol. 49, no. 7, pp. 1611–1635, July 2003.
- [10] T. J. Richardson S.-Y. Chung and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation," *IEEE Trans. Information Theory*, vol. 47, no. 2, pp. 657–670, Feb. 2001.

- [11] S.-Y. Chung, D. Forney, T. J. Richardson, and R. L. Urbanke, "On the design of low-density parity-check codes within 0.0045db of the shannon limit," *IEEE Commun. Lett.*, vol. 5, no. 2, pp. 58–60, Feb. 2001.
- [12] J. Ha, J. Kim, and S. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Trans. Information Theory*, vol. 50, no. 11, pp. 2824–2836, Nov. 2004.
- [13] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for 'turbo-like' codes," in *Proc. Allerton Conf. Commun., Control, Comp.*, Illinois, Sept. 1998, pp. 201–210.
- [14] D. Divsalar, "A simple tight bound on error probability of block codes with application to turbo codes," Tech. Rep. TMO Progress Report 42-139, Jet Propulsion Labs., Pasadena, CA, Nov. 1999.
- [15] 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.
- [16] A. Abbasfar, D. Divsalar, and K. Yao, "Accumulate repeat accumulate codes," in *Proc. International Symposium on Information Theory*, Chicago, USA, June 2004, p. 505.
- [17] 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.
- [18] 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.
- [19] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Information Theory*, vol. 40, no. 4, pp. 1284–1292, July 1994.
- [20] N. Shulman and M. Feder, "Random coding techniques for nonrandom codes," *IEEE Trans. Information Theory*, vol. 45, no. 6, pp. 2101–2104, Sept. 1999.
- [21] J. Garcia-Frias and W. Zhong, "Approaching shannon performance by iterative decoding of linear codes with low-density generator matrix," *IEEE Commun. Lett.*, vol. 7, no. 6, pp. 266–268, June 2003.
- [22] A. Brown, M. Luby, and A. Shokrollahi, "Repeat-accumulate codes that approach the Gilbert-Varshamov bound," in *Proc. International Symposium on Information Theory*, Adelaide, Australia, Sept. 2005, pp. 169–173.
- [23] A. Barg and G. Zemor, "Distance properties of expander codes," *IEEE Trans. Information Theory*, vol. 52, no. 1, pp. 78–90, Jan. 2006.
- [24] 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>.
- [25] I. Sason, E. Telatar, and R. Urbanke, "On the asymptotic input-output weight distributions and thresholds of convolutional and turbo-like encoders," *IEEE Trans. Information Theory*, vol. 48, no. 12, pp. 3052–3061, Dec. 2002.
- [26] S. Benedetto and G. Montorsi, "Unveiling turbo codes: Some results on parallel concatenated coding schemes," *IEEE Trans. Information Theory*, vol. 42, no. 2, pp. 409–428, Mar. 1996.
- [27] 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.
- [28] O. Pretzel, *Error-Correcting Codes and Finite Fields*, Oxford University Press, New York, 1992.
- [29] 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.

- [30] L. M. J. Bazzi and S. K. Mitter, "Encoding complexity versus minimum distance," *IEEE Trans. Information Theory*, vol. 51, no. 6, pp. 2103–2112, June 2005.
- [31] S. Shamai and I. Sason, "Variations on the gallager bounds, connections, and applications," *IEEE Trans. Information Theory*, vol. 48, no. 12, pp. 3029–3051, Dec. 2002.
- [32] 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.
- [33] 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.
- [34] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, New York, 1991.

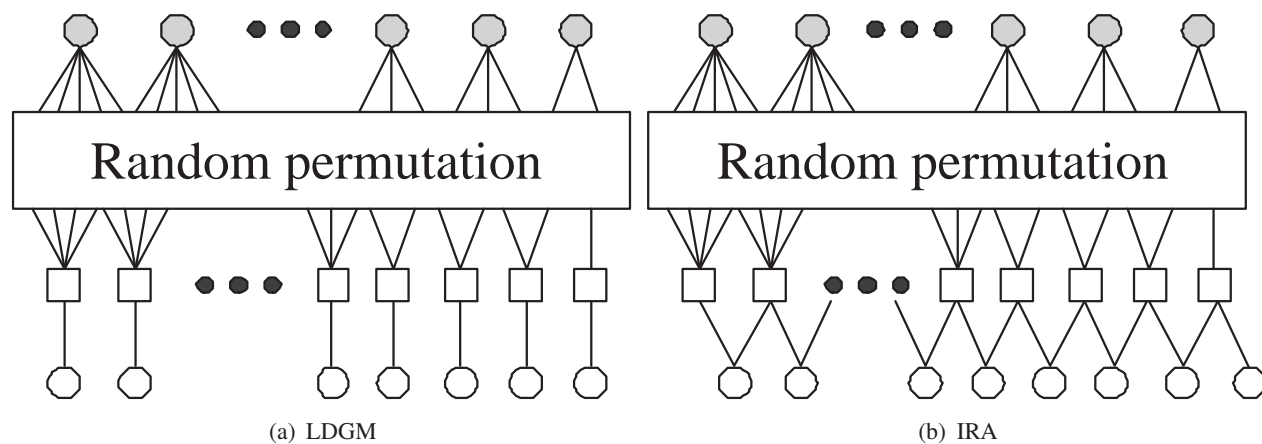


Fig. 1. Factor graph for LDGM and IRA codes. Information bits are denoted by filled gray circles, parity bits by open circles, and check nodes by squares.

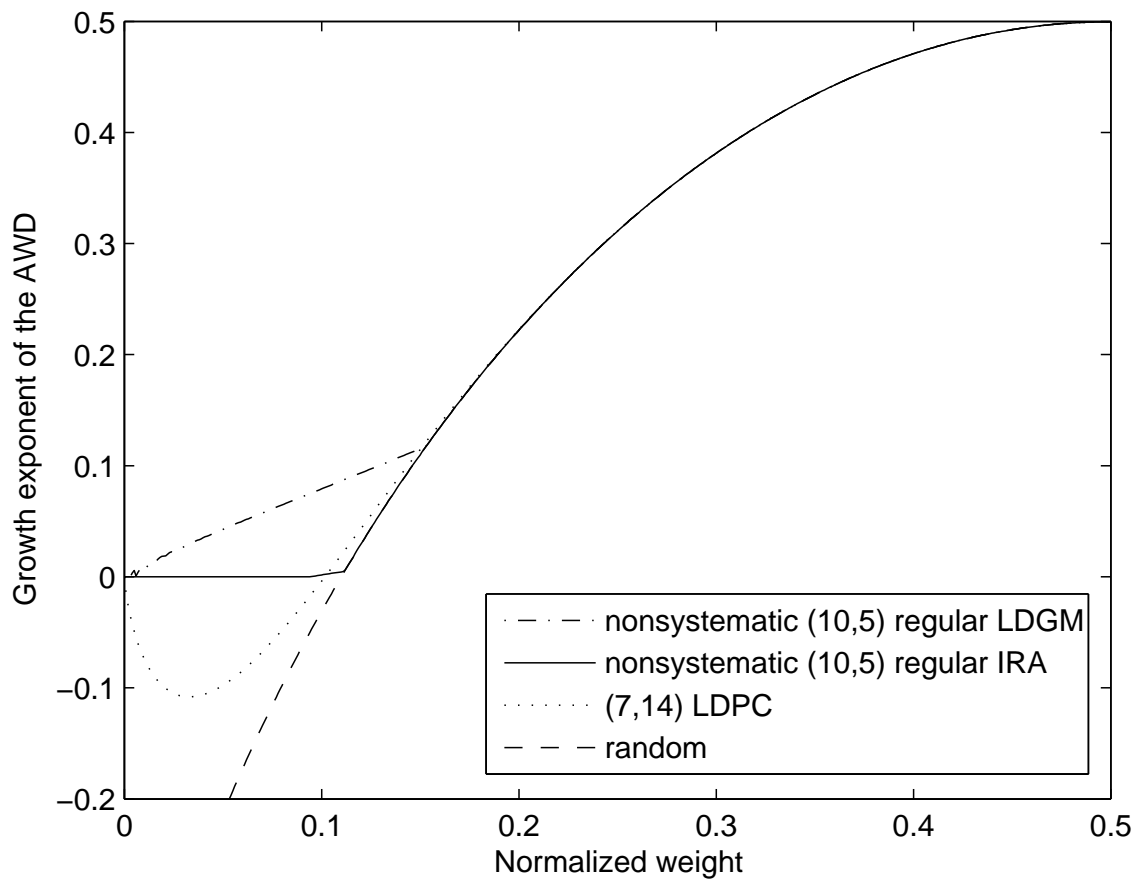


Fig. 2. The AAWD of the nonsystematic (10,5) regular LDGM ensemble, nonsystematic (10,5) regular IRA ensemble, (7,14) regular LDPC ensemble, and the random ensemble. All of them have rate 1/2, and the logarithm is to the base 2.

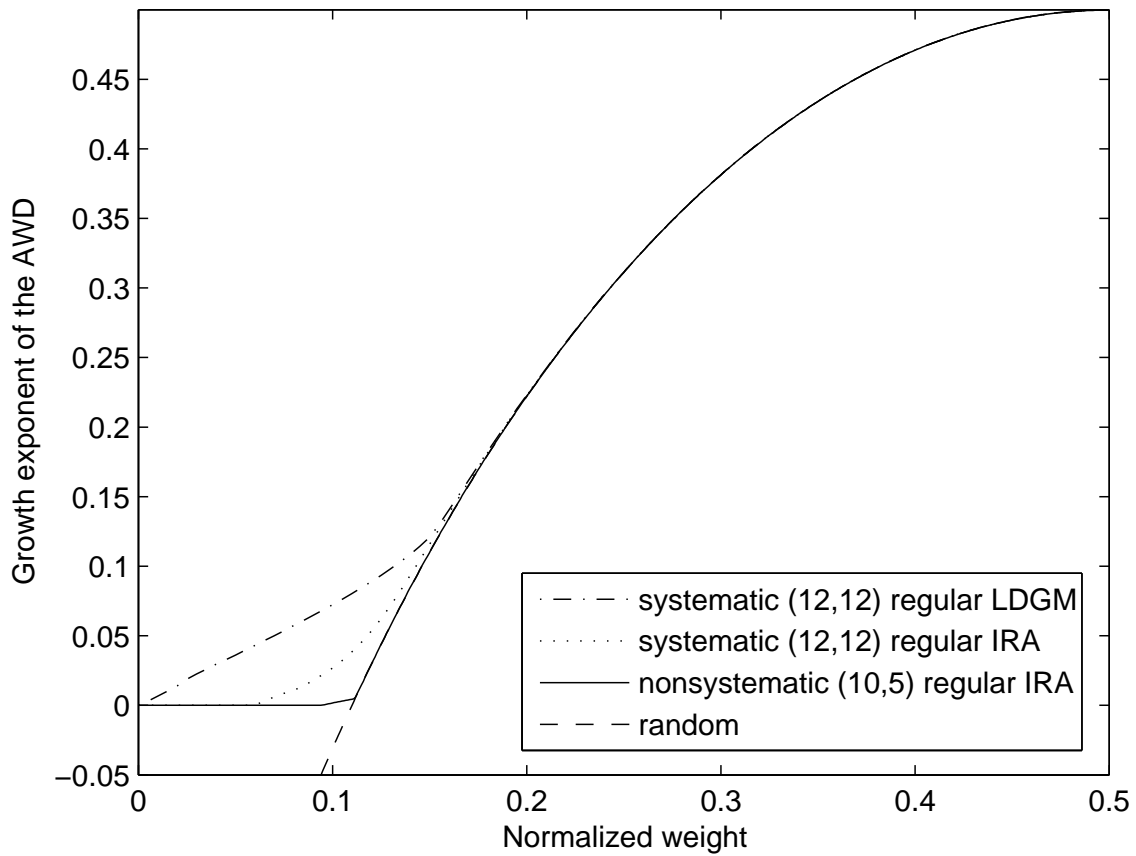


Fig. 3. The AAWD of the systematic (12,12) regular LDGM ensemble, systematic (12,12) regular IRA ensemble, nonsystematic (10,5) regular IRA ensemble, and the random ensemble. All of them have rate $1/2$, and the logarithm is to the base 2.

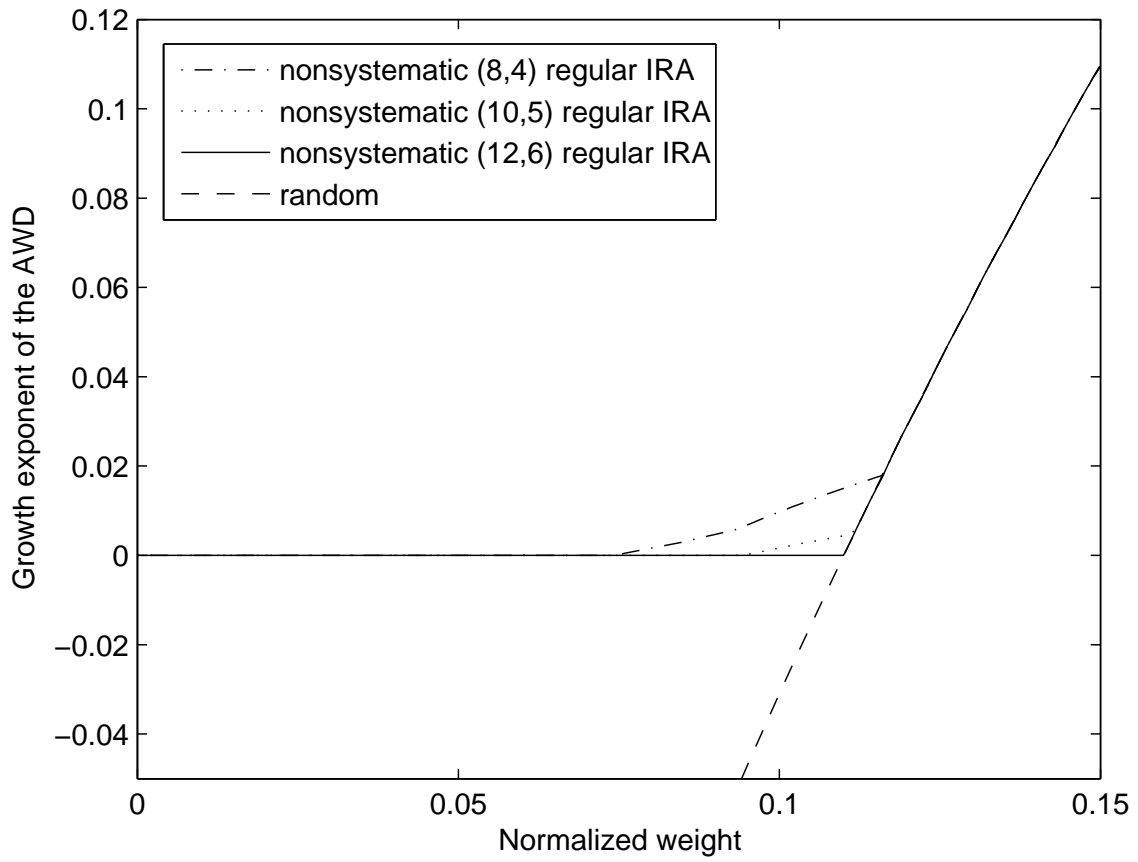


Fig. 4. Comparison for the AAWD of nonsystematic regular IRA ensembles with different right degrees. All of them have rate $1/2$, and the logarithm is to the base 2.

TABLE I
COMPARISON OF $(\frac{E_b}{N_0})^*$ AS GIVEN IN (29) FOR SEVERAL ENSEMBLES WITH RATE 1/2.

Ensemble	\bar{e}	$(\frac{E_b}{N_0})^*(dB)$
nonsystematic (4,2) regular IRA	8	0.308
Systematic (6,6) regular IRA	8	0.444
(4,8) regular LDPC	8	0.426
nonsystematic (6,3) regular IRA	10	0.308
Systematic (8,8) regular IRA	10	0.343
(5,10) regular LDPC	10	0.341
nonsystematic (8,4) regular IRA	12	0.308
Systematic (10,10) regular IRA	12	0.318
(6,12) regular LDPC	12	0.318
nonsystematic (10,5) regular IRA	14	0.308
Systematic (12,12) regular IRA	14	0.311
(7,14) regular LDPC	14	0.311
Shannon limit		0.184

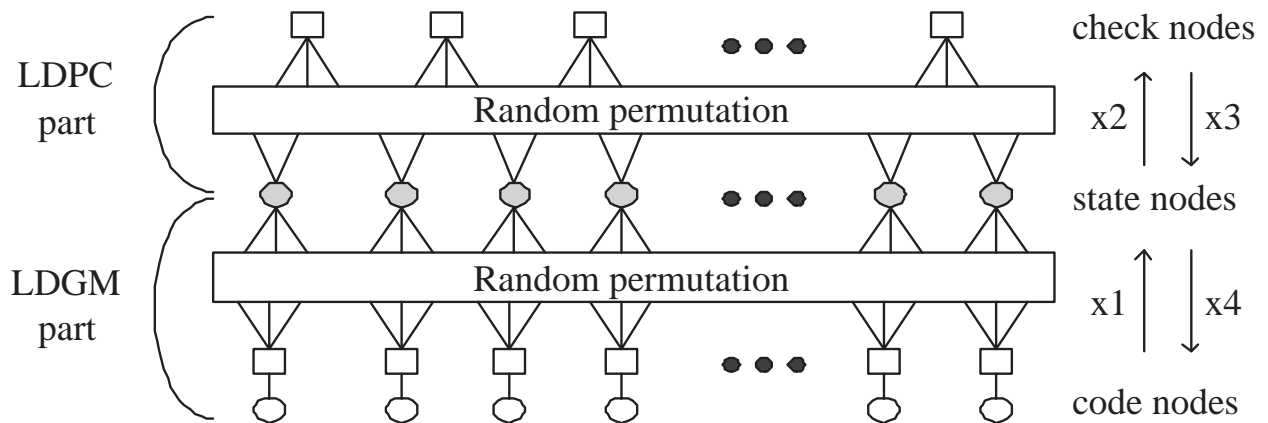


Fig. 5. The factor graph of the LDPC-GM codes

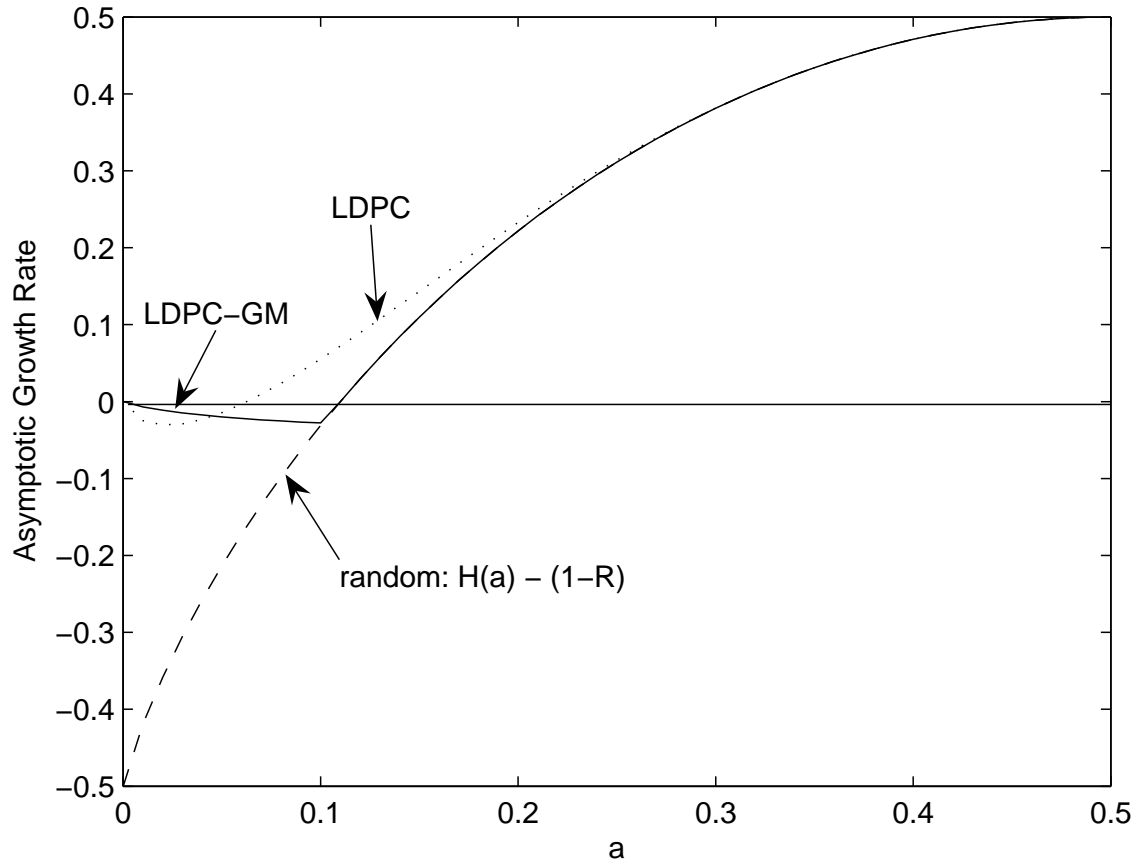


Fig. 6. Comparison of $w_o(a)$, $w_c^{ub}(a)$ and $H(a) - (1 - R)$ with $R = 0.5$ and $k = 8$. The logarithm is to the base 2 in this figure.