New Sequences of Capacity Achieving LDPC Code Ensembles Over the Binary Erasure Channel

Hamid Saeedi, *Student Member, IEEE*, and Amir H. Banihashemi, *Senior Member, IEEE*

***Abstract*—In this paper, new sequences (λ^n, ρ^n) of capacity achieving low-density parity-check (LDPC) code ensembles over the binary erasure channel (BEC) is introduced. These sequences include the existing sequences by Shokrollahi *et al.* as a special case. For a fixed code rate R, in the set of proposed sequences, Shokrollahi's sequences are superior to the rest of the set in that for any given value of n, their threshold is closer to the capacity upper bound $1-R$. For any given δ, $0<\delta<1-R$, however, there are infinitely many sequences in the set that are superior to Shokrollahi's sequences in that for each of them, there exists an integer number n_0, such that for any $n>n_0$, the sequence (λ^n, ρ^n) requires a smaller maximum variable node degree as well as a smaller number of constituent variable node degrees to achieve a threshold within δ-neighborhood of the capacity upper bound $1-R$. Moreover, it is proven that the check-regular subset of the proposed sequences are asymptotically quasi-optimal, i.e., their decoding complexity increases only logarithmically with the relative increase of the threshold. A stronger result on asymptotic optimality of some of the proposed sequences is also established.**

***Index Terms*—Asymptotically optimal sequences, binary erasure channel (BEC), capacity achieving sequences, check regular ensembles, low-density parity-check codes (LDPC).**

I. Introduction

LOW-DENSITY parity-check (LDPC) codes have received much attention in the past decade. Among different binary-input symmetric-output channels, the binary erasure channel (BEC) has been widely considered as the initial step for analysis and design due to the simplicity of the decoder structure [1], [2]. For irregular LDPC codes, the problem of finding ensemble degree distributions that perform well (i.e., have the best threshold for a given rate or have the highest rate with negligible error or erasure probability for a given channel parameter) is called *code design* [3]. More specifically, over the BEC, we can consider the following categories of code design: 1) For a given channel erasure probability ϵ, we look for a code with maximum rate and negligible probability of erasure; 2) For a given rate R, the code capable of providing a reliable transmission for the worst possible channel erasure probability (threshold) is designed. For the first case, the best achievable rate is limited by $1-\epsilon$ and for the second case, the threshold is upper bounded by $1-R$.

For a BEC, a sequence of degree distributions is called capacity achieving with rate R if the largest possible value of ϵ that makes the reliable transmission possible (threshold) can be made arbitrarily close to $1-R$ for sufficiently large maximum variable node and check node degrees [4]–[7]. Two such sequences, Tornado and right-regular sequences, have been introduced in [4] and [6], respectively. In [7], Oswald and Shokrollahi have presented a more general class of capacity achieving sequences that includes Tornado and right-regular sequences. Specifically, they show that right-regular sequences approach the capacity faster than other sequences in the class as the maximum variable node and check node degrees increase. This in turn results in a smaller decoding complexity to achieve a given performance [7].[1] The definition for capacity achieving sequences can be extended to the case of fixed channel parameter. More specifically, a sequence of degree distributions is called capacity achieving for the channel parameter ϵ if the ensemble sequence can provide reliable transmission over a BEC with parameter ϵ and if the corresponding code rate R can be made arbitrarily close to $1-\epsilon$ for sufficiently large maximum variable node and check node degrees.

Construction and analysis of capacity achieving ensemble sequences of codes defined on graphs has also been studied in [8]–[12]. In particular in [10] and [11], explicit constructions of capacity achieving irregular repeat-accumulate (IRA) and accumulate-repeat-accumulate (ARA) code ensembles with bounded complexity were presented, respectively. In the light of the results of [8], such bounded complexity can not be achieved for any capacity achieving sequence of LDPC code ensembles.

In [4]–[7], the constructed LDPC code ensembles are required to have variable node degree distributions for which all variable node degrees from 2 to a maximum degree N are present. In designing code ensembles to achieve a certain performance, and usually driven by implementation considerations, one may be interested in having smaller maximum variable node and check node degrees as well as smaller variety

Manuscript received January 25, 2008; revised September 11, 2009. Date of current version November 19, 2010. This work was supported by the Natural Science and Engineering Research Council of Canada. The material in this paper was presented in part at the International Symposium on Information Theory, Toronto, ON, Canada, July 2008.

H. Saeedi was with the Broadband Communications and Wireless Systems (BCWS) Centre, Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6 Canada. He is now with the Wireless Innovations Lab (WIL), Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran, and also with the Advanced Communications Research Institute (ACRI), Sharif University of Technology, Tehran, Iran (e-mail: hsaeedi@ieee.org).

A. H. Banihashemi is with the BCWS Centre, Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6 Canada (e-mail: ahashemi@sce.carleton.ca).

Communicated by T. Richardson, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2010.2053874

[1]In general, the average variable node or check node degree determine the decoding complexity per iteration. However for the BEC, due to the absolute reliability of the unerased bits, the iterative decoding algorithm can be modified such that every edge in the graph is used only once during the decoding process. In this case, we can replace "decoding complexity per iteration" by just "decoding complexity,"

of constituent variable node and check node degrees. In this paper, we propose sequences of capacity achieving ensembles for which the number of constituent variable node degrees can be reduced to a value $P = [f(N)] < N$, where [.] denotes the closest integer value (in case of a tie, the larger integer would be selected). There is a great deal of freedom in choosing P as the only condition on $f(N)$ is to be a strictly increasing function of N (The special case where $P = f(N) = N - 1$ corresponds to the sequences of [4]–[7].) We show that, similar to the sequences of [4]–[7], all the proposed sequences are also capacity achieving. Moreover, we demonstrate that for $P < N - 1$, the proposed sequences are superior to those of [4]–[7] in the sense that for sufficiently large maximum check node and variable node degrees, they can achieve a target performance within a given neighborhood of the capacity upper bound with a smaller maximum variable node degree and a smaller number of constituent variable node degrees.

As an example, consider rate one-half ensembles with the check node degree of 12. For $R = 1/2$, the best achievable threshold is upper bounded by $1 - R = 1/2$. Using the ensemble construction of [7] with the maximum variable node degree 1059 and a variable node degree distribution which includes all the degrees from 2 to 1059 (1058 different degrees), we can achieve a threshold which is %99.95 of $1 - R$. Practically the same threshold can be achieved based on our proposed sequences with $f(N) = [N/4] + 2$. In this case, the maximum variable node degree is reduced from 1059 to 493 and we only require 267 different variable node degrees instead of 1058 needed for the construction of [7].

To quantify the convergence speed of the proposed sequences as the maximum variable node and check node degrees increase, we prove that with a proper choice of $f(N)$, our proposed sequences can be *asymptotically quasi-optimal* [7], i.e., their decoding complexity increases only logarithmically with the relative increase of the performance with respect to the capacity upper bound. We note that a stronger result for check-regular sequences with $P = N - 1$ has been established in [7]. In particular, it is proved in [7] that these sequences are *asymptotically optimal*, i.e., their decoding complexity increases not only logarithmically with the relative increase of the performance but also the coefficient of this increase, μ, is equal to one. For the other capacity achieving sequences discussed in [7], including Tornado sequences, we have $\mu > 1$. We show that if $f(N)$ is a linear function of N, our proposed check-regular sequences are asymptotically optimal.

Due to the fast convergence speed of check-regular sequences and their simpler structure of having only one constituent check node degree, our focus in this paper will be mainly on check-regular ensembles. The same design principles however can be applied to other capacity achieving sequences including those in [7]. As an example, we also devise new sequences with a smaller maximum variable node degree and smaller number of constituent variable node degrees based on Tornado sequences. Moreover, some of our results and proofs are applicable to a general check node degree distribution.

It is worthwhile to mention that the extrinsic information transfer (EXIT) charts of variable nodes and check nodes of an LDPC code ensemble have been introduced in [13] as an important analysis and design tool. In particular, it is shown that to minimize the gap to capacity, the area between the variable node EXIT curve and the inverse of the check node EXIT curve has to be minimized while avoiding any intersection between the curves (except in the ending points). Using this idea of curve fitting, Paolini *et al.* [14] have proposed a design method based on matching several orders of the derivative of the variable node and the inverse of the check node curves. We note that this result is in-line with the *flatness condition* of [5] for capacity achieving sequences. Also noteworthy is that LDPC code ensembles can be designed by solving constrained optimization problems [15]. The nature of such formulations, however, does not allow for a systematic design of capacity achieving sequences of ensembles.

This paper complements earlier results presented in [16] and [17]. The basic construction of ensemble sequences was presented in [16] and [17] along with simulation results mainly comparing the performance and the decoding complexity of the proposed sequences with those of the ensembles designed by optimization methods for relatively small check and variable node degrees. In this paper, our focus is on asymptotic performance and convergence speed of the sequences. In particular, we prove that the proposed sequences are capacity achieving and that they are asymptotically (quasi-)optimal. Lemma 1 in Appendix B and Theorems 1 and 2 in Section III deal with the basic construction of the proposed sequences. Their proofs can be found in [16] and are not repeated here.

The paper is organized as follows. In the next section, we define some notations that will be used throughout the paper. In Section III, we introduce our proposed ensembles and in Section IV, we prove that they are capacity achieving. Section V is devoted to proving that the proposed sequences are asymptotically quasi-optimal or optimal depending on the choice of $f(N)$. In Section VI, we provide some examples of our sequences and compare their performance with those of [6], [7]. Section VII concludes the paper. Appendix A describes some properties of fractional binomial coefficients useful to the derivations of the paper. Some lemmas, propositions, theorems and their proofs are given in Appendix B.

II. Definitions

We represent a (λ, ρ) LDPC code ensemble with its variable node and check node degree distributions as

$$\rho(x) = \sum_{i=2}^{D_c} \rho_i x^{i-1}$$

and

$$\lambda(x) = \sum_{i=2}^{D_v} \lambda_i x^{i-1}$$

with constraints

$$\sum_{i=2}^{D_c} \rho_i = 1 \quad (1)$$

$$\sum_{i=2}^{D_v} \lambda_i = 1 \quad (2)$$

where the coefficient of x^i represents the fraction of edges connected to the nodes of degree $i+1$, and D_v and D_c represent the maximum variable node degree and the maximum check node degree, respectively. It should be noted that throughout the paper, we sometimes use N to represent the maximum variable node degree. The difference between the two representations is clear from the context. Average check node and variable node degrees are given by: $\overline{d}_c = 1/(\sum_{i=2}^{D_c} \rho_i/i)$ and $\overline{d}_v = 1/(\sum_{i=2}^{D_v} \lambda_i/i)$, respectively.

The code rate R satisfies

$$R = 1 - \overline{d}_v/\overline{d}_c. \tag{3}$$

Consider a BEC with erasure probability ϵ. The capacity of this channel is $C = 1-\epsilon$. For a given code ensemble over a BEC with a given channel parameter ϵ, the sufficient and necessary condition for the zero probability of message erasure after infinite number of iterations is

$$\epsilon\lambda(x) - 1 + \rho^{-1}(1-x) < 0, \quad 0 \le x < 1. \tag{4}$$

We call any code ensemble that satisfies (4) *convergent* for the given ϵ. For a code ensemble, the *threshold* is defined as the supremum of all ϵ values that satisfy (4).

III. Proposed Ensemble Sequences

Consider a check node degree distribution $\rho(x)$. It can be shown that the Taylor series of $\rho^{-1}(1-x)$ around $x=0$ is convergent. Let

$$\rho^{-1}(1-x) = 1 - \sum_{i=2}^{\infty} T_i x^{i-1} \tag{5}$$

where the coefficients T_i are positive.[2] We note that for check-regular ensembles with the check node degree D_c, there exists a closed form expression for T_i

$$T_i = \binom{\alpha}{i-1}(-1)^i, \ \alpha = 1/(D_c - 1) \tag{6}$$

where the fractional binomial expansion $\binom{\alpha}{i}$ is defined as [6]

$$\binom{\alpha}{i} = \frac{\alpha(\alpha-1)\dots(\alpha-i+1)}{i!} = \frac{\alpha}{i}\left(1-\frac{\alpha}{i-1}\right)\cdots \\ \cdots\left(1-\frac{\alpha}{2}\right)(1-\alpha)(-1)^{(i+1)}. \tag{7}$$

Some properties of this expansion are discussed in Appendix A.

In the following, we present our ensemble constructions for the two categories of code design based on a given $\rho(x)$. In Section IV, we prove that the corresponding check-regular ensembles are capacity achieving. The main idea in the construction of the ensembles is to maximize the fraction of the edges connected to lower degree nodes in a greedy fashion [16], [17]. The number of constituent variable node degrees is controlled by the function $f(N)$, where N is the maximum variable node degree. The degrees are selected successively from 2 to $f(N)$, in addition to the maximum node degree N. There are no variable nodes with degrees in the range $[f(N)+1, N-1]$ or larger than N. Starting from degree 2 nodes, edge fractions are assigned to variable nodes of successively larger degrees to achieve a sequences of upper bounds devised based on the convergence condition (4) in the vicinity of $x=0$ [16], [17].

[2]For example, the ensembles defined in [7] all have his property.

A. Ensemble Construction for a Given Channel Erasure Probability

Consider a check node degree distribution $\rho(x)$, a given channel erasure probability ϵ, and a maximum variable node degree N. Also consider the following variable node degree distribution associated with $\rho(x)$:

$$\begin{aligned} \lambda_i &= T_i/\epsilon, \ \ 2 \le i \le f(N), \\ \lambda_i &= 0, \ \ f(N)+1 \le i \le N-1 \\ \lambda_N &= 1 - \sum_{i=2}^{f(N)} \lambda_i. \end{aligned} \tag{8}$$

In (8), f is a strictly increasing function of N and smaller than N, and N must satisfy the following inequalities:

$$\sum_{i=2}^{N} T_i > \epsilon \tag{9}$$

$$\epsilon \ge \sum_{i=2}^{N-1} T_i. \tag{10}$$

We call such an ensemble GC which stands for "Given Channel erasure probability." Note that for brevity, we have omitted the notation '[.]' applied to $f(N)$. It is also important to note that $f(N) = N-1$ corresponds to a special case of GC ensembles where all the λ_i coefficients, $2 \le i \le N$, are nonzero.

Theorem 1: Consider a given check node degree distribution $\rho(x)$, and denote the ith term of the Taylor expansion of $\rho^{-1}(1-x)$ at $x=0$ by T_i, as in (5). For a given channel parameter $\epsilon > T_2$, there always exists a unique N that satisfies (9) and (10). For such N, in (8), $\lambda_N \ge 0$, and the convergence of the ensemble constructed based on (8) is ensured. Also, ϵ is the threshold of the constructed ensemble.

Note that if ϵ does not satisfy the inequality $\epsilon > T_2$, we need to decrease T_2 by increasing $\overline{d}_c$.

Consider now a GC ensemble for a given $\rho(x)$. The maximum variable node degree for this ensemble is N which satisfies (9) and (10). Based on part 1 of Lemma 1 of Appendix B, if we decrease the maximum variable node degree from N to $D_v < N$, with the same fraction of adjacent edges, the newly constructed ensemble has a higher rate but can be nonconvergent. By choosing the smallest D_v which results in a convergent ensemble, we can create a new ensemble, referred to as Modified GC or MGC. Note that the variable node degree distribution for this ensemble is the same as that of the GC ensemble with λ_{Dv} replacing λ_N.

B. Ensemble Construction for a Given Code Rate

Consider a check node degree distribution $\rho(x)$, and a given code rate R. Consider the following variable node degree distribution associated with $\rho(x)$

$$\begin{aligned} \epsilon &= \frac{\sum_{i=2}^{f(N)} T_i(1/i - 1/N)}{\overline{d_v}^{-1} - 1/N} \\ \lambda_i &= T_i/\epsilon, \;\; 2 \leq i \leq f(N), \\ \lambda_i &= 0, \;\; f(N)+1 \leq i \leq N-1 \\ \lambda_N &= 1 - \sum_{i=2}^{f(N)} \lambda_i. \end{aligned} \tag{11}$$

In (11), f is a strictly increasing function of N and smaller than N, and N must satisfy the following inequalities:

$$\overline{d_v}^{-1} \sum_{i=2}^{N} T_i > \sum_{i=2}^{N} T_i/i \tag{12}$$

$$\overline{d_v}^{-1} \sum_{i=2}^{N-1} T_i \leq \sum_{i=2}^{N-1} T_i/i. \tag{13}$$

We refer to such an ensemble as GR, which stands for "Given code Rate." Note that the special case of $f(N) = N-1$, where all the coefficients $\lambda_i, 2 \leq i \leq N$, are nonzero, corresponds to the sequences of [7].

Theorem 2: For a given code rate R and a given check node degree distribution $\rho(x)$ (and thus a given $\overline{d_v}^{-1}$), if $R < 1-2/\overline{d}_c$, there always exists a unique value of N that satisfies (12) and (13). For such N, in (11), $\lambda_N \geq 0$, and the convergence of the ensemble constructed based on (11) is ensured. Also, ϵ in (11) is the threshold of the constructed ensemble.

Note that if the code rate R does not satisfy the inequality, we need to increase $\overline{d}_c$.

Similar to the case in Section III-A, we can decrease the maximum variable node degree of a GR ensemble from N to a smaller value D_v and design a new GR ensemble for a given rate. The convergent ensemble corresponding to the smallest D_v is called Modified GR or MGR. Clearly an MGR ensemble has a larger threshold value compared to the corresponding GR ensemble.

IV. Achieving the Capacity

In this section, we consider check-regular ensembles and show that GC and GR ensembles can achieve capacity as the check node degree D_c and consequently N tend to infinity. To prove the main results, we need lemma 2 from Appendix B.

Theorem 3: GC and GR ensemble sequences achieve the capacity as D_c tends to infinity.

Proof: For both GC and GR ensembles, we have

$$\overline{d_v}^{-1} = \sum_{i=2}^{f(N)} \lambda_i/i + \frac{1}{N}\lambda_N.$$

Using (3), it is then easy to see that the following relationship holds between ϵ (the threshold) and R:

$$\frac{1}{1-R} = \frac{\alpha+1}{\alpha}\left(\frac{1}{\epsilon}\sum_{i=2}^{f(N)} T_i/i + \frac{\lambda_N}{N}\right),$$

where α is defined in (6). We thus have

$$1 - \frac{\epsilon}{1-R} = 1 - \frac{\alpha+1}{\alpha}\left(\sum_{i=2}^{f(N)} T_i/i + \epsilon\frac{\lambda_N}{N}\right) = 1 - \frac{\alpha+1}{\alpha}\left(\frac{\alpha - \left|\binom{\alpha}{f(N)}\right|}{\alpha+1} + \epsilon\frac{\lambda_N}{N}\right)$$

where for the second equality, we have used (A-2). By applying the lower and the upper bounds of (A-4) to $\left|\binom{\alpha}{f(N)}\right|$ in the above equation, we obtain

$$\frac{L(\alpha, f(N))}{f(N)^{\alpha+1}} - \frac{\epsilon(\alpha+1)}{\alpha N}\lambda_N \leqslant 1 - \frac{\epsilon}{1-R} \leqslant \frac{U(\alpha)}{f(N)^{\alpha+1}} - \frac{\epsilon(\alpha+1)}{\alpha N}\lambda_N \tag{14}$$

where $\gamma = .577215\ldots$ is the Euler constant. Taking the limit of both the lower and the upper bounds in (14) as $\alpha \to 0$ (and $N \to \infty$ based on Lemma 2), it is easy to see that both limits are zero. We therefore conclude that

$$\lim_{\alpha \to 0} \frac{\epsilon}{1-R} = 1.$$

In other words, as D_c tends to infinity, for a GC ensemble, R tends to $1-\epsilon$, and for a GR ensemble, ϵ tends to $1-R$. ■

Corollary 1: MGC and MGR ensemble sequences achieve the capacity as D_c tends to infinity.[3]

V. The Choice of $f(N)$ and the Optimality/Quasi-Optimality of the Proposed Sequences

For a capacity achieving sequence, it is important to know how fast it achieves the capacity as the check node degree increases. This indicates how fast the decoding complexity increases as the performance improves. A GR sequence (λ^n, ρ^n) of degree distributions with rate R is called asymptotically *quasi-optimal* [7] if a constant $\mu \geq 1$ exists for which

$$\lim_{n \to \infty} \sup \mu(\lambda^n, \rho^n) = \mu$$

where

$$\mu(\lambda^n, \rho^n) = \frac{\overline{d}_c \log(R)}{\log(\Im(\lambda^n, \rho^n))}$$

and

$$\Im(\lambda^n, \rho^n) = 1 - \frac{\epsilon_n}{1-R}.$$

[3]Note that the assumption that $f(N)$ is an increasing function of N was used to show that the first terms of the lower bound and the upper bound of (14) tend to zero as α tends to zero. The same result could follow from the weaker condition of $\lim_{N\to\infty} 1/f(N) = 0$.

Parameter ϵ_n is the threshold of the ensemble sequence. The closer μ is to 1, the faster ϵ_n approaches $1-R$. A GC sequence (λ^n, ρ^n) of degree distributions constructed for a given channel erasure probability ϵ is called *asymptotically quasi-optimal* if a constant $\mu \geq 1$ exists for which

$$\lim_{n\to\infty} \sup \mu(\lambda^n, \rho^n) = \mu$$

where

$$\mu(\lambda^n, \rho^n) = \frac{\overline{d}_c \log(1-\epsilon)}{\log(\Im(\lambda^n, \rho^n))}$$
and
$$\Im(\lambda^n, \rho^n) = 1 - \frac{\epsilon}{1-R_n}.$$

Parameter R_n is the rate of the ensemble sequence.

A GR sequence (λ^n, ρ^n) of degree distributions giving rise to codes of rate R is called *asymptotically optimal* [7] if a constant Δ exists for which

$$\lim_{n\to\infty} \sup \Delta(\lambda^n, \rho^n) = \Delta$$

where

$$\Delta(\lambda^n, \rho^n) = \frac{\Im(\lambda^n, \rho^n)}{R^{\overline{d}_c}}.$$

Extending this definition to GC sequences, A GC sequence (λ^n, ρ^n) of degree distributions constructed for a given channel erasure probability ϵ is called asymptotically optimal if a constant Δ exists for which

$$\lim_{n\to\infty} \sup \Delta(\lambda^n, \rho^n) = \Delta$$

where

$$\Delta(\lambda^n, \rho^n) = \frac{\Im(\lambda^n, \rho^n)}{(1-\epsilon)^{\overline{d}_c}}.$$

It can be verified that an asymptotically optimal ensemble sequence is asymptotically quasi-optimal with $\mu = 1$.

It is shown in [7] that check-regular GR ensembles with $f(N) = N-1$ are asymptotically optimal. In the sequel, for the proposed check-regular sequences with arbitrary $f(N)$, for both categories of GC and GR sequences, we find conditions on $f(N)$ which are sufficient for the sequences to be asymptotically quasi-optimal and optimal, respectively. In the set of all possible choices for $f(N)$, we focus on a subset for which $\lim_{\alpha\to 0} f(N)/N$ exists.[4] In this subset, we consider two categories: 1) $\lim_{\alpha\to 0} f(N)/N = 0$, and 2) $\lim_{\alpha\to 0} f(N)/N \neq 0$. For the first category, we prove in Theorem 4 that if an additional condition $\lim_{\alpha\to 0} f(N)^\alpha = M$ holds, where for GC ensembles $1 < M < 1/(1-\epsilon)$, and for GR ensembles $1 < M < 1/R$, the sequence is asymptomatically quasi-optimal. For the second category, we prove in Theorem 5 that the resulting sequence is asymptotically optimal. This also implies the asymptotic quasi-optimality of the sequences in the second category. Note that for the second category it can be easily shown that $M = 1/(1-\epsilon)$ and $M = 1/R$ for GC and GR ensembles, respectively. To prove the main results, we need Lemma 3 and Propositions 1 and 2 of Appendix B.

[4]Note that since $0 < f(N) < N$, we necessarily have $0 \leq \lim_{\alpha\to 0} \frac{f(N)}{N} \leq 1$.

Theorem 4: GC and GR ensemble sequences for which the function $f(N)$ is chosen such that $\lim_{\alpha\to 0} f(N)^\alpha = M$, where for GC ensembles $1 < M < 1/(1-\epsilon)$, and for GR ensembles $1 < M < 1/R$, are asymptotically quasi-optimal with parameters $\mu = -\ln(1-\epsilon)/\ln M$, and $\mu = -\ln R/\ln M$, respectively.

Proof: We first consider the GR ensemble sequence with code rate R. From Lemma 3, we have

$$\frac{(1-\epsilon_n)(\alpha+1)}{\alpha N} + \frac{L(\alpha, f(N))}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{U(\alpha)}{f(N)^\alpha} \leq 1 - \frac{\epsilon_n}{1-R} \leq \frac{(1-\epsilon_n)(\alpha+1)}{\alpha N} + \frac{U(\alpha)}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{L(\alpha, f(N))}{f(N)^\alpha}.$$

Taking the logarithm of all terms and multiplying by $D_c^{-1} = \frac{\alpha}{\alpha+1}$, we obtain

$$\frac{\alpha}{\alpha+1} \times \ln\left(\frac{(1-\epsilon_n)(\alpha+1)}{\alpha N} + \frac{L(\alpha, f(N))}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{U(\alpha)}{f(N)^\alpha}\right) \leq D_c^{-1} \ln\left(1 - \frac{\epsilon_n}{1-R}\right) \leq \frac{\alpha}{\alpha+1} \ln\left(\frac{(1-\epsilon_n)(\alpha+1)}{\alpha N} + \frac{U(\alpha)}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{L(\alpha, f(N))}{f(N)^\alpha}\right). \tag{15}$$

Consider now the limit of the upper bound of the above inequality as $\alpha \to 0$:

$$\begin{aligned}\lim_{\alpha\to 0} \frac{\alpha}{\alpha+1} \times & \ln\left(\frac{(1-\epsilon_n)(\alpha+1)}{\alpha N} + \frac{U(\alpha)}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{L(\alpha, f(N))}{f(N)^\alpha}\right) \\ = \lim_{\alpha\to 0} \frac{\alpha}{\alpha+1} & \ln\big((1-\epsilon_n)(\alpha+1) f(N)^{\alpha+1} + U(\alpha)\alpha N \\ & - (\alpha+1) L(\alpha, f(N)) f(N)\big) \\ & - \lim_{\alpha\to 0} \frac{\alpha}{\alpha+1} \ln\left(\alpha N f(N)^{\alpha+1}\right).\end{aligned} \tag{16}$$

Manipulating the limits at the right hand side of (16), for the second limit, we have

$$\lim_{\alpha\to 0} \frac{\alpha}{\alpha+1} \ln\left(\alpha N f(N)^{\alpha+1}\right) = \lim_{\alpha\to 0} \frac{\alpha}{\alpha+1} \ln \alpha + \lim_{\alpha\to 0} \frac{\alpha}{\alpha+1} \ln N + \lim_{\alpha\to 0} \alpha \ln f(N) = -\ln R + \ln M, \tag{17}$$

where for the last equality, we have used $\lim_{\alpha\to 0} \alpha \ln \alpha = 0$, and $\lim_{\alpha\to 0} \alpha \ln N = -\ln R$, based on Proposition 1, and $\lim_{\alpha\to 0} \alpha \ln f(N) = \ln M$, based on theorem's assumption. We now consider the first limit on the right hand side of (16). Based on Proposition 2, we have

$$\lim_{\alpha\to 0} U(\alpha) - \frac{f(N)}{N\alpha}(\alpha+1)(L(\alpha, f(N)) - (1-\epsilon_n) f(N)^\alpha) = 1.$$

Thus

$$\lim_{\alpha\to 0}\frac{\alpha}{\alpha+1}\ln\Big(U(\alpha)-\frac{f(N)}{N\alpha}(\alpha+1)(L(\alpha,f(N)) -(1-\epsilon_n)f(N)^{\alpha})\Big)=0. \quad (18)$$

Therefore, the first limit on the right hand side of (16) can be written as

$$\lim_{\alpha\to 0}\frac{\alpha}{\alpha+1}\ln\Big(N\alpha(U(\alpha)-\frac{f(N)}{N\alpha}(\alpha+1)(L(\alpha,f(N)) -(1-\epsilon_n)f(N)^{\alpha}))\Big)=\lim_{\alpha\to 0}\frac{\alpha}{\alpha+1}\ln N\alpha+\frac{\alpha}{\alpha+1}\ln\Big(U(\alpha) -\frac{f(N)}{N\alpha}(\alpha+1)(L(\alpha,f(N))-(1-\epsilon_n)f(N)^{\alpha})\Big)= \lim_{\alpha\to 0}\frac{\alpha}{\alpha+1}\ln N\alpha=-\ln R, \quad (19)$$

where for the second equality, we have used (18), and for the last equality, Proposition 1 ($\lim_{\alpha\to 0}\alpha\ln N=-\ln R$), and the fact that $\lim_{\alpha\to 0}\alpha\ln\alpha=0$ are used. By replacing (17) and (19) in (16), we conclude that

$$\lim_{\alpha\to 0}\frac{\alpha}{\alpha+1}\ln\left(\frac{(1-\epsilon_n)(\alpha+1)}{\alpha N}+\frac{U(\alpha)}{f(N)^{\alpha+1}} -\frac{\alpha+1}{\alpha N}\frac{L(\alpha,f(N))}{f(N)^{\alpha}}\right)=-\ln M. \quad (20)$$

With a similar approach, one can prove that the limit of the lower bound of (15) is also equal to $-\ln M$ as α tends to zero. We therefore have

$$\lim_{\alpha\to 0}\sup D_c^{-1}\ln\left(1-\frac{\epsilon_n}{1-R}\right)=-\ln M. \quad (21)$$

With similar arguments, one can see that (21) is also valid for GC ensemble sequences where R has to be interpreted as R_n and ϵ_n has to be replaced by ϵ.

Inverting both sides of (21) and multiplying them by -1, we obtain

$$\lim_{\alpha\to 0}\sup\,(-D_c)/\ln\left(1-\frac{\epsilon_n}{1-R}\right)=1/\ln M.$$

For the case of GR sequences, $-\ln R$ is a positive constant. Therefore

$$\lim_{\alpha\to 0}\sup\,D_c\ln R/\ln\left(1-\frac{\epsilon_n}{1-R}\right)=-\ln R/\ln M=\mu.$$

This proves the theorem for GR sequences. For the case of GC sequences, $-\ln(1-\epsilon)$ is a positive constant. Therefore, using (21), we have

$$\lim_{\alpha\to 0}\sup\,D_c\ln(1-\epsilon)/\ln\left(1-\frac{\epsilon}{1-R_n}\right) =-\ln(1-\epsilon)/\ln M=\mu.$$

This proves the theorem for GC sequences. ■

Corollary 2: GC and GR sequences with $f(N)=aN^{\beta}+b$, where $0<a\le 1$ and $0<\beta<1$ and b is an arbitrary constant, are asymptotically quasi-optimal with $\mu=1/\beta$.

Proof: First note that the bounds on β are necessary to ensure that asymptotically $f(N)<N$. For GC and GR ensemble sequences, we have $M=\lim_{\alpha\to 0}f(N)^{\alpha}=\lim_{\alpha\to 0}(aN^{\beta}+b)^{\alpha}=(\lim_{\alpha\to 0}N^{\alpha})^{\beta}$.

Now based on Proposition 1, for GC ensemble sequences, we have $M=(\lim_{\alpha\to 0}N^{\alpha})^{\beta}=1/(1-\epsilon)^{\beta}$ and therefore, $\mu=-\ln(1-\epsilon)/\ln(M)=1/\beta$. For GR ensemble sequences, based on Proposition 1, we have $M=(\lim_{\alpha\to 0}N^{\alpha})^{\beta}=1/R^{\beta}$ and therefore $\mu=-\ln(R)/\ln(M)=1/\beta$. ■

Now we show that if $f(N)$ is chosen such that the limit of its ratio over N tends to a positive constant, the resulting sequence is in fact asymptotically optimal. To prove the main result, in addition to Lemma 3 and Proposition 1, we need Proportions 3 to 5 of Appendix B.

Theorem 5: GC and GR sequences for which function $f(N)$ satisfies $\lim_{\alpha\to 0}\frac{f(N)}{N}=K>0$, are asymptotically optimal with $\Delta=e^{\gamma}(1/K-ln(1/K))$, where γ is the Euler constant.

Proof: We provide the proof for GC sequences. The proof for GR sequences is similar. From Lemma 3, we have

$$\frac{(1-\epsilon)(\alpha+1)}{\alpha N}+\frac{L(\alpha,f(N))}{f(N)^{\alpha+1}}-\frac{\alpha+1}{\alpha N}\frac{U(\alpha)}{f(N)^{\alpha}} \le 1-\frac{\epsilon}{1-R_n}\le \frac{(1-\epsilon)(\alpha+1)}{\alpha N}+\frac{U(\alpha)}{f(N)^{\alpha+1}}-\frac{\alpha+1}{\alpha N}\frac{L(\alpha,f(N))}{f(N)^{\alpha}}.$$

For GC sequences, we multiply both sides by $(1-\epsilon)^{-\overline{d}_c}=(1-\epsilon)^{-(1+1/\alpha)}$, to obtain

$$(1-\epsilon)^{-(1+1/\alpha)}\left(\frac{(1-\epsilon)(\alpha+1)}{\alpha N}+\frac{L(\alpha,f(N))}{f(N)^{\alpha+1}}- \frac{\alpha+1}{\alpha N}\frac{U(\alpha)}{f(N)^{\alpha}}\right)\le(1-\epsilon)^{-\overline{d}_c}\left(1-\frac{\epsilon}{1-R_n}\right)\le (1-\epsilon)^{-(1+1/\alpha)}\left(\frac{(1-\epsilon)(\alpha+1)}{\alpha N}+\frac{U(\alpha)}{f(N)^{\alpha+1}} -\frac{\alpha+1}{\alpha N}\frac{L(\alpha,f(N))}{f(N)^{\alpha}}\right) \quad (22)$$

We now consider the upper bound of (22) and find its limit as $\alpha\to 0$. Rearranging the terms, we have

$$\begin{aligned}
&\lim_{\alpha\to 0}(1-\epsilon)^{-(1+1/\alpha)}\left(\frac{(1-\epsilon)(\alpha+1)}{\alpha N}+\frac{U(\alpha)}{f(N)^{\alpha+1}} -\frac{\alpha+1}{\alpha N}\frac{L(\alpha,f(N))}{f(N)^{\alpha}}\right)\\
&=\lim_{\alpha\to 0}(1-\epsilon)^{-(1+1/\alpha)}\frac{U(\alpha)}{f(N)^{\alpha+1}}\\
&\quad-\lim_{\alpha\to 0}(1-\epsilon)^{-(1+1/\alpha)}\frac{\alpha+1}{\alpha N}\left(\frac{L(\alpha,f(N))}{f(N)^{\alpha}}-(1-\epsilon)\right)\\
&=\lim_{\alpha\to 0}\frac{(1-\epsilon)^{-1/\alpha}}{f(N)}\times\lim_{\alpha\to 0}\frac{(1-\epsilon)^{-1}}{f(N)^{\alpha}}\times\lim_{\alpha\to 0}U(\alpha)\\
&\quad-(1-\epsilon)^{-1}\times\lim_{\alpha\to 0}(1+\alpha)\times\lim_{\alpha\to 0}\frac{(1-\epsilon)^{-1/\alpha}}{N}\\
&\quad\times\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{L(\alpha,f(N))}{f(N)^{\alpha}}-(1-\epsilon)\right)\\
&=e^{\gamma}/K\times 1\times 1-(1-\epsilon)^{-1}\times 1\times e^{\gamma}\times(1-\epsilon)\ln(1/K)\\
&=e^{\gamma}(1/K-\ln(1/K)),
\end{aligned}$$

where in the third equality, the first limit is obtained based on Proposition 4, the second limit based on Proposition 5, the fifth limit based on Proposition 1 and the sixth limit based on Proposition 3. It can be similarly shown that the lower bound of (22) has the same limit as α tends to zero. We therefore conclude that

$$\lim_{\alpha \to 0} \sup \Delta(\lambda^n, \rho^n) = e^{\gamma}(1/K - \ln(1/K)) = \Delta,$$

which completes the proof. ∎

Corollary 3: GC and GR sequences with $f(N) = aN + b$, where b is an arbitrary constant, are asymptotically optimal with $\Delta = \left(\frac{1}{a} - \ln \frac{1}{a}\right) e^{\gamma}$.

Note that for an asymptotically optimal sequence, the smaller the Δ, the faster it achieves the capacity. For GR and GC sequences with $f(N) = aN + b$, the smallest value for Δ is obtained when $a = 1$. This corresponds to the check-regular sequences proposed in [6], [7] with $\Delta = e^{\gamma}$. For other values of a, Δ is larger. Results similar to those of Theorems 4 and 5 also apply to MGC and MGR sequences, although we have not been able to compute the constants μ and Δ for these sequences analytically. In the next section, we show that for MGC and MGR sequences with $f(N) = aN + b$, for a given value of a, the value of Δ tends to a constant between e^{γ} and $e^{\gamma}(1/a - \ln(1/a))$ and is in fact very close to e^{γ}.

Finally, it is important to note that the results obtained in [7] and extended in [12], on the convergence speed of capacity achieving sequences are only applicable to the special case of $f(N) = N - 1$. More specifically, for the check-regular sequences which are the main focus our work, the asymptotic optimality is proved and Δ is derived in [7] for the special case of $f(N) = N - 1$. Our results in Theorems 4 and 5 are, however, more general and apply to the case where $f(N) \leq N - 1$. Our attempt to find clear relationships between the analysis of [7], [12] and that of this paper with the purpose of simplifying our proofs has been unsuccessful.

VI. Simulation Results

In this section, we first consider GR ensembles with rate one-half. For other code rates similar results are obtained. We consider check-regular sequences with different $f(N)$ functions and compute the values of $\Im, \mu$ and Δ. Consider GR ensemble sequences C_1, C_2, C_3, and C_5 with $f_1(N) = [\ln(N)] + 2, f_2(N) = [\sqrt{N}], f_3(N) = [N/4] + 2$, and $f_5(N) = N - 1$, respectively. Also let C_4 be the MGR ensemble with $f_4(N) = [N/4] + 2$. Note that C_5 is the same as the rate one-half check-regular ensemble of [7]. The constant values have been used to ensure that for smaller values of check node degrees (and thus smaller values of N), we have at least 3 constituent variable node degrees. Note that for large values of N, the effect of constant values is negligible. The results have been shown in Table I.

TABLE I
Values of $\Im, \mu$ and Δ for Rate-1/2 GR Ensemble Sequences (C_1, C_2, C_3, C_5) and an MGR Sequence (C_4) With Different Check Node Degrees

D_c	N	$\Im_1$	$\Im_2$	$\Im_3$	$\Im_4$	$\Im_5$
5	6	.1127	.2857	.1127	.1128	.1020
6	13	.0829	.1152	.0829	.0531	.0404
7	29	.1047	.1047	.0452	.0206	.0179
8	61	.0972	.0657	.0233	.0095	.0084
9	126	.0909	.0509	.0113	.0044	.0040
10	257	.0850	.0363	.0057	.0021	.0019
11	523	.0911	.0262	.0028	.0010	.0010
12	1059	.0836	.0188	.0014	.0005	.0005
13	2136	.0771	.0139	.0007	.0002	.0002
14	4301	.0792	.0099	.0003	.0001	.0001
D_c	N	μ_1	μ_2	μ_3	μ_4	μ_5
5	6	1.588	2.765	1.588	1.587	1.518
6	13	1.670	1.924	1.670	1.417	1.297
7	29	2.150	2.150	1.567	1.190	1.207
8	61	2.378	2.036	1.474	1.161	1.159
9	126	2.601	2.094	1.390	1.150	1.130
10	257	2.812	2.090	1.342	1.125	1.111
11	523	3.181	2.093	1.296	1.108	1.097
12	1059	3.351	2.093	1.262	1.096	1.086
13	2136	3.515	2.106	1.234	1.086	1.078
14	4301	3.811	2.100	1.212	1.077	1.071
D_c	N	Δ_1	Δ_2	Δ_3	Δ_4	Δ_5
5	6	3.60	9.14	3.60	3.60	3.26
6	13	5.30	7.37	5.31	3.30	2.59
7	29	13.40	13.40	5.79	2.62	2.29
8	61	24.87	16.82	5.95	2.42	2.14
9	126	46.53	26.04	5.76	2.25	2.05
10	257	87.05	37.18	5.85	2.16	2.00
11	523	186.48	53.61	5.70	2.10	1.96
12	1059	342.32	77.00	5.62	2.07	1.94
13	2136	631.22	113.61	5.54	2.04	1.92
14	4301	1297.81	161.42	5.47	2.01	1.91

TABLE II
Values of P, D_v and ψ for Rate-1/2 MGR Ensemble Sequences With $f(N) = [aN] + b$ for Different Values of a

		$a = 1, (C_5)$			$a = 1/2$		
D_c	N	P	D_v	ψ	P	D_v	ψ
5	6	5	6	.8980	5	6	.8980
6	13	12	13	.9596	9	12	.9576
7	29	28	29	.9821	17	23	.9814
8	61	60	61	.9916	33	45	.9915
9	126	125	126	.9960	65	88	.9960
10	257	256	257	.9981	131	175	.9981
11	523	522	523	.9991	264	352	.9991
12	1059	1058	1059	.9995	532	707	.9995
13	2136	2135	2136	.9998	1070	1442	.9998
14	4301	4300	4301	.9999	2153	2861	.9999
		$a = 1/4, (C_4)$			$a = 1/8$		
D_c	N	P	D_v	ψ	P	D_v	ψ
5	6	4	6	.8873	3	5	.8750
6	13	5	9	.9469	4	8	.9376
7	29	9	16	.9795	6	13	.9716
8	61	17	31	.9905	10	23	.9864
9	126	34	62	.9956	18	45	.9919
10	257	66	122	.9979	34	88	.9959
11	523	133	246	.9990	67	178	.9979
12	1059	267	495	.9995	134	359	.9989
13	2136	536	995	.9998	269	725	.9995
14	4301	1077	1999	.9999	540	1364	.9998

As can be seen in Table I, while all ensembles are capacity achieving, their speed of achieving the capacity is different. Ensemble C_1 achieves the capacity very slowly. It can be seen that μ_1 increases as D_c increases and the ensemble is not asymptotically quasi-optimal. Ensemble C_2 is asymptotically quasi-optimal and the value of μ_2 tends to 2 based on Corollary 2. It can be seen however that μ_2 does not decrease uniformly to its limit as opposed to μ_3, μ_4 and μ_5. Ensembles C_3 and C_4 are asymptotically optimal. Based on Corollary 3, the value of Δ_3 tends to $(4 - \ln 4)e^{\gamma} = 4.65$. By comparing the values of μ and Δ for C_3 and C_4, it can also be seen that C_4 converges much faster to

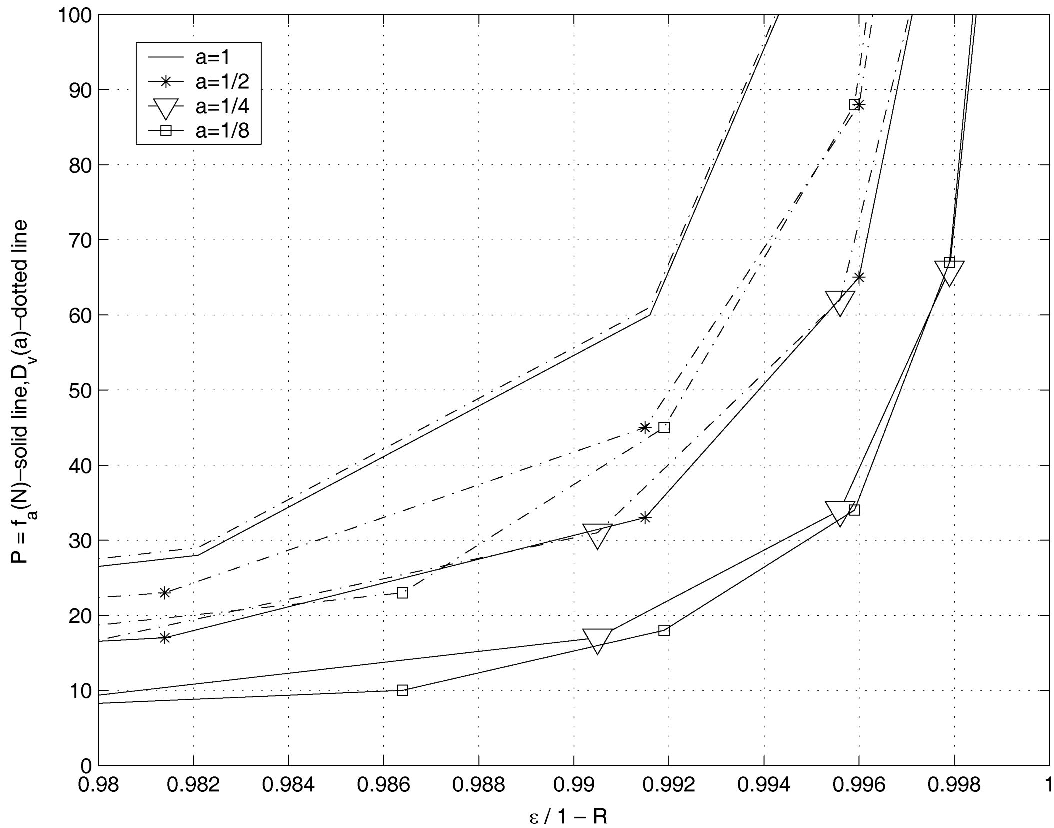

Fig. 1. The maximum variable node degree (dotted lines) and the required number of constituent variable node degrees (solid lines) versus the performance of rate-1/2 MGR ensembles with $f_a(N) = aN + b$ for different values of a.

the capacity compared to C_3. This is in addition to the advantage of C_4 over C_3 in having a smaller maximum variable node degree.

Another important comparison is to see that the values of Δ_4 are very close to those of Δ_5 for a given D_c. This means that the MGR ensembles introduced here have more or less the same speed of convergence to the capacity as the check-regular ensembles of [7] do. This is while C_4 has a much smaller number of constituent variable node degrees (by a factor of about 4 for larger D_c values) and a much smaller maximum variable node degree compared to C_5.

In general, the results of Table I suggest that choosing linear functions of N for $f(N)$ would result in ensembles that perform very closely to those proposed in [7] but with a considerably smaller number of constituent variable node degrees and a smaller maximum variable node degree. Other choices of $f(N)$ may also result in capacity achieving sequences but with a lower speed of convergence. These sequences may still be of interest due to their smaller number of constituent variable node degrees.

In the following, we concentrate on $f_a(N) = [aN] + b$ and study the effect of coefficient a on the performance of the proposed ensembles. Note again that for $a = 1$ and $b = -1$, the resulting ensemble sequence is identical to that of [7]. Consider rate one-half check-regular ensembles corresponding to $a = 1/2, 1/4, \text{and } 1/8$, respectively, and $b = 2$. For each value of a and each check node degree, we construct an MGR ensemble for which N is obtained from (12) and (13). For this ensemble, the number of constituent variable node degrees P is equal to $f_a(N)$, and we use the ratio of the ensemble threshold ϵ_a to the best achievable threshold $1 - R = 1/2$ as the measure of performance ($\psi_a = \epsilon_a/(1 - R)$). The results for these ensembles are reported in Table II along with the ψ values. The results of Table II show that, for a given D_c, the larger the P, the better the performance, and the best performance is achieved for $a = 1$ (some inconsistencies for small values of D_c might be caused by the constant term b). However, an almost similar performance can be achieved by the proposed MGR ensembles with considerably smaller P and D_v for the same value of D_c or with $D_c + 1$.[5]

In Fig. 1, we have shown the values of D_v and P versus the performance of the ensembles with different values of a and for practical values of D_c (D_c values are chosen such that the corresponding values of D_v are less than 100). As can be seen in Fig. 1, compared to the ensemble with $a = 1$, the ensembles corresponding to all other values of a require smaller values of D_v and P to achieve a certain performance. Again note that in Fig. 1, for a given performance, the values of D_c for different ensembles are only slightly different (by zero or one).

Another issue which is important in comparison of the proposed ensembles with those of [7], is the number of iterations required to achieve a certain erasure probability. In Fig. 2 we have shown the number of iterations required to achieve the erasure

[5]We note that for a given D_c, the performance of the proposed MGR ensembles is always upperbounded by that of the right regular sequences of [7]. However, for larger values of D_c, the performance of the proposed MGR ensembles quickly tends to its upperbound such that the performance of both ensemble types can be considered practically identical.

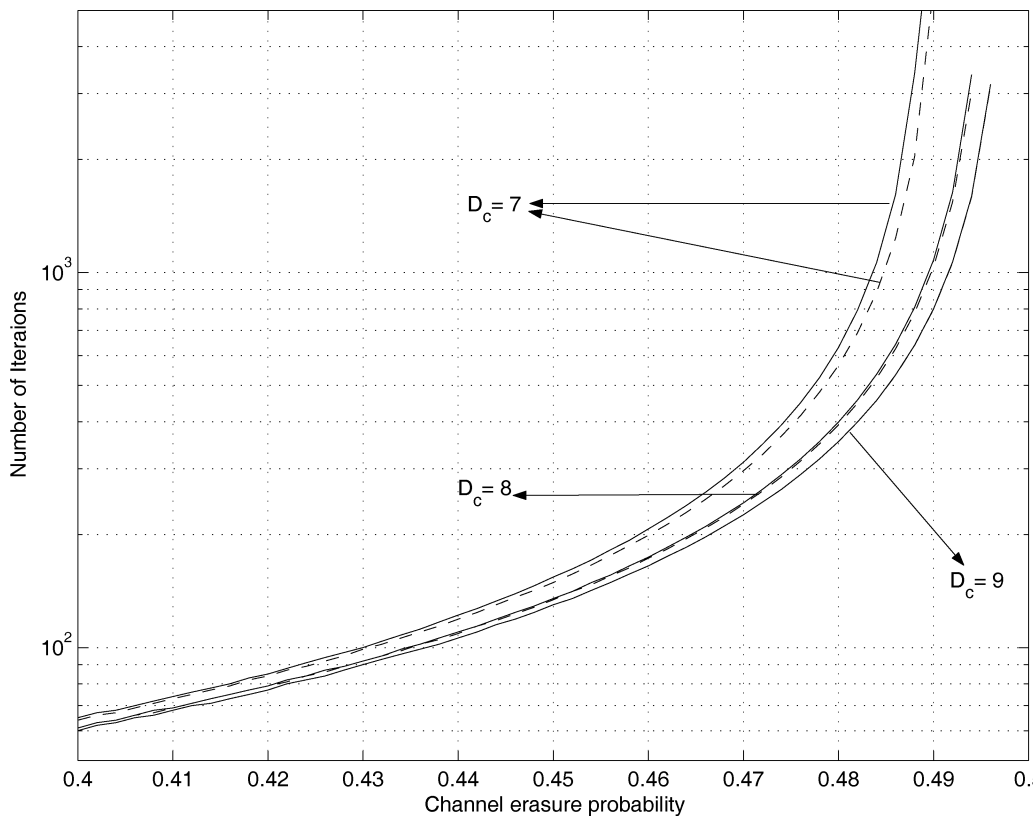

Fig. 2. The required number of iterations required to achieve the erasure rate of 10^{-6} for different values of channel erasure probabilities for rate-1/2 ensembles (Full lines correspond to C_4 and dashed lines correspond to C_5, for $D_c = 9$, the two curves fall on each other).

rate of 10^{-6} for different values of channel erasure probabilities for rate-1/2 ensembles. The full curves correspond to MGR sequence C_4 and the dashed curves correspond to Shokrollahi's sequence C_5. In general, the difference in the number of iterations is directly related to the gap between the ensemble threshold and the channel erasure probability. For larger values of D_c, where the threshold of the proposed ensembles and those of [7] are very close, the convergence speed to zero erasure probability with the increase in the number of iterations, is basically the same across the whole range of channel erasure probabilities. For lower values of D_c however, where there is some non-negligible gap between the two thresholds, although the number of iterations is very close for both cases, Shokrollahi's ensembles converge slightly faster. The difference is predictably more pronounced for larger channel erasure probabilities.

Related to results of Fig. 2, it is worthwhile to note that in [18], the authors have derived lower bounds on the number of iterations required for successful message-passing decoding of LDPC codes over the BEC. These results indicate that if the fraction of degree-2 variable nodes does not vanish, then the number of iterations scales at least like the inverse of the gap to capacity.

It is worthwhile to note that the authors in [18] derive lower bounds on the number of iterations for LDPC, IRA, and ARA codes over the BEC in terms of their achievable gap to capacity. One of the results proved in [18] for the BEC, is that if the fraction of degree-2 variable nodes does not vanish, then the number of iterations grows at least like the reciprocal of the achievable gap to capacity under iterative message-passing decoding. This fact can be confirmed quantitatively by Fig. 2.

As we explained before, the proposed degree distributions have smaller maximum variable node degrees compared to those of [7] for a given check node degree distribution. Consequently, the convergence speed of the performance of finite-length codes from the proposed ensembles to the asymptotic results would be faster than that of [7]. This is a consequence of the well-known result that larger maximum variable node degrees imply slower convergence of the finite length performance to the asymptotic threshold [15] and presents yet another advantage of the proposed sequences. To verify this, we consider the two ensembles with $D_c = 8$ within sequences of C_4 and C_5, and call them E_1 and E_2, respectively. Ensemble E_1 has maximum variable node degree of 31 and threshold of 0.4953 which is slightly worse than 0.4958, the threshold of E_2. Ensemble E_2 has maximum variable node degree of 61. In Fig. 3, we have presented the performances of codes with block length 10 000 from the two ensembles. We have set the maximum number of iterations to 200. Fig. 3 shows that the code from E_1 outperforms the code from E_2 despite E_1 having a worse threshold. We expect that the gap in performance increases by increasing D_c since this makes the threshold difference smaller and the difference between the maximum variable node degrees larger.

Although we proved our results on capacity achieving properties of constructed sequences for check-regular ensembles, the same principles can be applied to other check node degree distributions to construct GC, GR, MGC and MGR ensembles. In Table III, we have used check node degree distributions of Tornado sequences [7] and have constructed an MGR ensemble sequence C_T of rate one-half with $f(N) = [a/4] + 2$. Based on

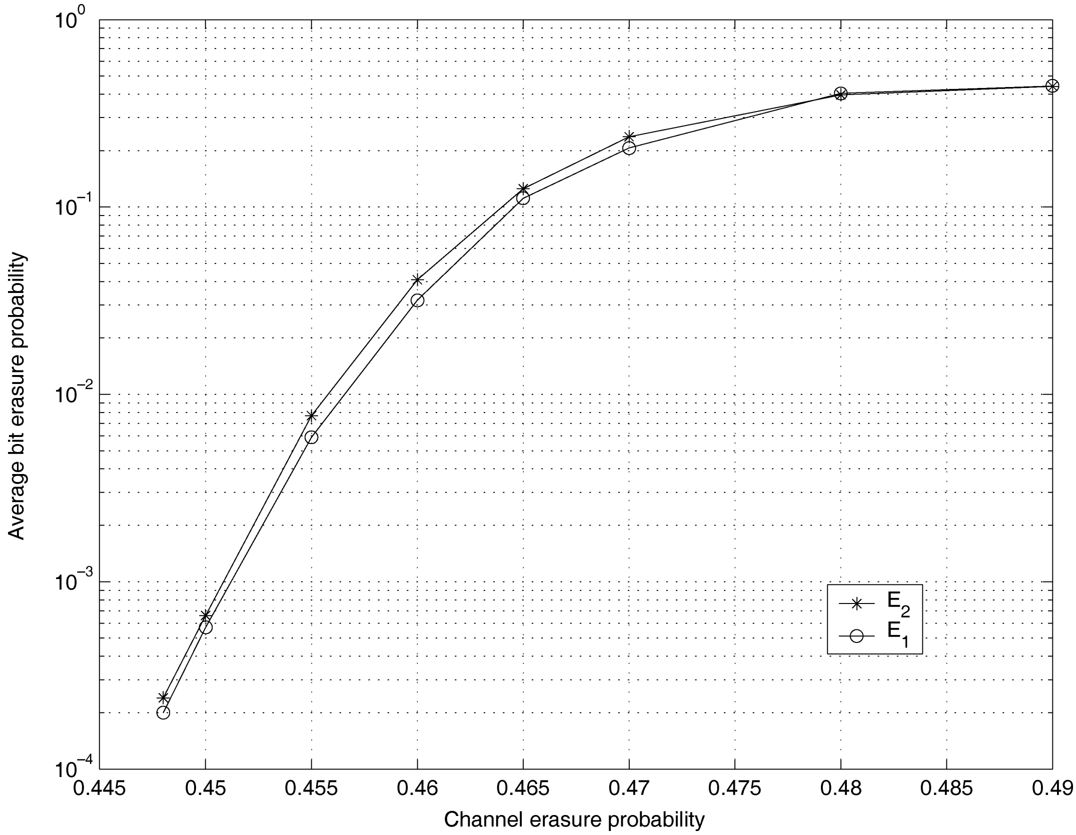

Fig. 3. Performance of codes of block 10 000 from ensembles E_1 and E_2.

TABLE III
VALUES OF D_v, N, $\Im$, μ AND Δ FOR RATE-1/2 MGR ENSEMBLE SEQUENCE C_T, BASED ON THE TORNADO SEQUENCES, FOR DIFFERENT VALUES OF $\overline{d}_c$

$\overline{d}_c$	$\Im_{C_T}$	$\Im_{[7]}$	μ_{C_T}	Δ_{C_T}	$N(D_v$ of [7])	D_v
5	.2437	.2098	2.454	7.8	5	5
6	.1350	.1091	2.077	8.6	9	7
7	.0644	.0610	1.769	8.2	16	10
8	.0393	.0353	1.713	10.0	28	16
9	.0219	.0208	1.632	11.2	47	25
10	.0129	.0124	1.593	13.2	79	40
11	.0079	.0074	1.573	16.1	133	65
12	.0046	.0045	1.548	19.0	222	107
13	.0028	.0027	1.534	23.0	368	175
14	.0017	.0016	1.522	27.9	610	289

the $\Im$ values, the sequence seems to be capacity achieving. The sequence also seems to be asymptotically quasi-optimal as its μ values do not increase as the average check node degree increases. The sequence, however, is not asymptotically optimal. The reason is that our proposed sequences can never perform better than those proposed in [7] for a given check node degree distribution. Since the Tornado sequences of [7] are not asymptotically optimal, we do not expect our sequences to be asymptotically optimal either. The comparison of $\Im$ values between the proposed sequences and Tornado sequences of [7] indicates that roughly the same performance as in [7] can be achieved by the proposed ensembles with much smaller values of D_v and P. In particular, C_T has roughly one fourth of the number of constituent variable node degrees needed for the sequence of [7]. The maximum variable node degrees for C_T ensembles are also much smaller than the corresponding Tornado sequence of [7]. For example, for $\overline{d}_c = 14$, while $D_v = 610$ for the ensemble in [7], it is only equal to 289 for C_T. The D_v values for C_T ensembles with different $\overline{d}_c$ values are given in Table III.

VII. CONCLUSION

In this paper, we presented new sequences of LDPC code ensembles that can achieve the capacity of the BEC. Unlike the sequences proposed by Shokrollahi *et al.* [7], which have nonzero coefficients for each constituent variable node degree $i \in [2, N]$, where N is the maximum variable node degree, the new sequences have only nonzero coefficients for $i \in [2, f(N)]$ and $i = D_v \leq N$ (there are no variable nodes with degrees in the range $[f(N)+1, D_v - 1]$). In terms of performance, the proposed sequences perform similar to those of [7] with a smaller number of constituent variable node degrees and a smaller maximum variable node degree. We also proved that the proposed sequences are asymptotically quasi-optimal or optimal for proper choices of $f(N)$. In particular, asymptotic optimality was proved for a linear $f(N)$.

APPENDIX A
FRACTIONAL BINOMIAL COEFFICIENTS

Based on the properties of the Fractional Binomial Coefficients [6], we have the following relationships for $0 < \alpha < 1$:

$$\sum_{i=1}^{N-1} \binom{\alpha}{i} (-1)^{i+1} = \sum_{i=2}^{N} \binom{\alpha}{i-1} (-1)^{i} = \sum_{i=2}^{N} T_i$$

$$\sum_{i=1}^{N-1} = 1 - \frac{N}{\alpha} \left| \binom{\alpha}{N} \right|. \tag{A-1}$$

$$\sum_{i=1}^{N-1}\binom{\alpha}{i}\frac{(-1)^{i+1}}{i+1}=\sum_{i=2}^{N}\binom{\alpha}{i-1}\frac{(-1)^{i}}{i}=\sum_{i=2}^{N}\frac{T_i}{i}=\frac{\alpha-\left|\binom{\alpha}{N}\right|}{\alpha+1}. \tag{A-2}$$

Also from the proof of Proposition 1 of [6], we have

$$\frac{\alpha}{N^{\alpha+1}}e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2\leq\left|\binom{\alpha}{N}\right|\leq\frac{\alpha}{N^{\alpha+1}}e^{\alpha(1-\gamma)}(1-\alpha) \tag{A-3}$$

where $\gamma=.577215\ldots$ is the Euler constant. This is equivalent to

$$\frac{\alpha}{N^{\alpha+1}}L(\alpha,N)\leq\left|\binom{\alpha}{N}\right|\leq\frac{\alpha}{N^{\alpha+1}}U(\alpha) \tag{A-4}$$

where $L(\alpha,N)=e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2$ and $U(\alpha)=e^{\alpha(1-\gamma)}\times(1-\alpha)$.

Based on (A-2), it is easy to see that

$$\alpha-\left|\binom{\alpha}{N}\right|>0. \tag{A-5}$$

Appendix B
Lemmas 1–3 and Propositions 1–5 and Proofs Theorems 1 and 2

Lemma 1: Consider a given check node degree distribution, a given channel parameter and a given set of constituent variable node degrees. Let C be a convergent code ensemble of rate R with variable node degree distribution $\lambda(x)=\sum_{i=2}^{N}\lambda_i x^{i-1}$. For given integer numbers a and b in $[2,N]$, $a\neq b$, we form a new ensemble C' with rate R' such that $\lambda'_a=\lambda_a-k$, $\lambda'_b=\lambda_b+k$ and $\lambda'_i=\lambda_i$, for $i\neq a,b$ (k is chosen such that $\lambda'_a>0$ and $\lambda'_b<1$). We have:

1) If $a>b$, then $R'>R$.
2) If $a<b$, C' is convergent.

Proof: See [16].

Proof of Theorem 1: See the proofs of Theorems 1 and 2 in [16].

Proof of Theorem 2: See the proofs of Theorems 3, 4, and 5 in [16].

Lemma 2:

For GC and GR ensembles, if D_c tends to infinity, the value of N in Theorems 1 and 2 also tends to infinity. Moreover, N tends to infinity much faster than D_c does. This is such that

$$\lim_{D_c\to\infty}\frac{D_c}{N^\beta}=\lim_{\alpha\to 0}\frac{1}{\alpha N^\beta}=0,\ \ \forall\beta>0\ (\alpha=\frac{1}{D_c-1}).$$

Proof: We first prove the lemma for GC ensembles. Based on (6), it is easy to see that $T_2\geq T_i, 2\leq i\leq N$. This combined with (9) results in $NT_2>\epsilon$. Replacing T_2 with its value α, we then have

$$N>\epsilon/\alpha.$$

If D_c tends to infinity, α tends to zero and N will tend to infinity. To prove $\lim_{\alpha\to 0}\frac{1}{N^\beta\alpha}=0$, we use (9) and (A-1) to obtain

$$1-\frac{N}{\alpha}\left|\binom{\alpha}{N}\right|>\epsilon.$$

Based on the lower bound of (A-3), the above inequality results in $1-\frac{N}{\alpha}\frac{\alpha}{N^{\alpha+1}}e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2>\epsilon$, where γ is the Euler constant. Therefore

$$\frac{1}{N^\alpha}<\frac{1-\epsilon}{e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2}.$$

Taking the power β/α of both sides and then multiplying both sides by $1/\alpha$, we have

$$\frac{1}{N^\beta\alpha}<\frac{1}{\alpha}\left(\frac{1-\epsilon}{e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2}\right)^{\beta/\alpha}. \tag{B-1}$$

Taking the limit of the right hand side of (B-1) as α tends to zero, we obtain

$$\begin{aligned}&\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{1-\epsilon}{e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2}\right)^{\beta/\alpha}\\&=\lim_{\alpha\to 0}e^{-\beta(2-\gamma-1/2N)}\lim_{\alpha\to 0}(1-\alpha)^{-2\beta/\alpha}\lim_{\alpha\to 0}\frac{1}{\alpha}(1-\epsilon)^{\beta/\alpha}\\&=0,\end{aligned}$$

where the limit is derived based on the fact that the first two limits are finite and the third limit is zero. To show that the third limit is zero, we argue as follows. Let $H(\alpha)=\frac{1}{\alpha}(1-\epsilon)^{\beta/\alpha}$. We then have

$$\lim_{\alpha\to 0}\ln(H(\alpha))=\lim_{\alpha\to 0}\frac{-\alpha\ln\alpha+\beta\ln(1-\epsilon)}{\alpha}=\lim_{\alpha\to 0}\frac{\beta\ln(1-\epsilon)}{\alpha}=-\infty,$$

where the second equality is based on $\lim_{\alpha\to 0}\alpha\ln\alpha=0$, and the last one is based on $0<1-\epsilon<1$ and $\alpha>0$. The above limit implies $\lim_{\alpha\to 0}H(\alpha)=0$. Based on (B-1), we therefore have

$$\lim_{\alpha\to 0}\frac{1}{N^\beta\alpha}\leq\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{1-\epsilon}{e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2}\right)^{\beta/\alpha}=0.$$

This completes the proof for GC ensembles.

For GR ensembles, based on (12), N must satisfy $\overline{d_v}^{-1}>\frac{\sum_{i=2}^{N}T_i/i}{\sum_{i=2}^{N}T_i}$. Replacing i with N in the denominator of the terms T_i/i, we obtain

$$\overline{d_v}^{-1}>\frac{\sum_{i=2}^{N}T_i/N}{\sum_{i=2}^{N}T_i}=1/N.$$

By replacing $\overline{d_v}^{-1}$ with $\frac{1}{(1-R)(1+1/\alpha)}$ in this inequality, we have

$$N>(1-R)(1+1/\alpha). \tag{B-2}$$

If D_c tends to infinity, α tends to zero and based on (B-2), N will tend to infinity. To prove that $\lim_{\alpha\to 0}\frac{1}{N^\beta\alpha}=0$, we use (12) along with (A-1) and (A-2) to obtain

$$\frac{\alpha/(\alpha+1)}{1-R}>\frac{\frac{\alpha-\left|\binom{\alpha}{N}\right|}{\alpha+1}}{1-\frac{N}{\alpha}\left|\binom{\alpha}{N}\right|}.$$

By slight manipulation of this inequality, we have

$$R > \frac{(N-1)\left|\binom{\alpha}{N}\right|}{\alpha - \left|\binom{\alpha}{N}\right|}.$$

Considering that both sides of the inequality are positive based on (A-5), we take both sides to the power of $-\beta/\alpha$, and divide them by N^β to obtain

$$\frac{R^{-\beta/\alpha}}{N^\beta} < \frac{1}{N^\beta}\left(\frac{\alpha - \left|\binom{\alpha}{N}\right|}{(N-1)\left|\binom{\alpha}{N}\right|}\right)^{\beta/\alpha}.$$

Using the lower bound of (A-4) in the numerator and the denominator, we have

$$\frac{R^{-\beta/\alpha}}{N^\beta} < \frac{1}{N^\beta}\left(\frac{\alpha - \frac{\alpha}{N^{\alpha+1}}L(\alpha,N)}{(N-1)\frac{\alpha}{N^{\alpha+1}}L(\alpha,N)}\right)^{\beta/\alpha} = \frac{1}{N^\beta}\left(\frac{N^{\alpha+1} - L(\alpha,N)}{(N-1)L(\alpha,N)}\right)^{\beta/\alpha}. \quad \text{(B-3)}$$

Rearranging the terms, dividing the sides by α and replacing the value of $L(\alpha, N)$ from Appendix A, we have

$$\frac{1}{\alpha N^\beta} < \frac{R^{\beta/\alpha}}{\alpha N^\beta}\left(\frac{N^{\alpha+1} - e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2}{(N-1)e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2}\right)^{\beta/\alpha}.$$

Using an argument similar to that of *GC* sequences, one can show that the limit of the right-hand side (RHS) of the above inequality is zero, and, thus

$$\lim_{\alpha\to 0}\frac{1}{N^\beta \alpha} = 0.$$

This completes the proof for GR sequences. ∎

Lemma 3: For GC and GR ensemble sequences, the following relationship holds:

$$\begin{aligned}\frac{(1-\epsilon)(\alpha+1)}{\alpha N} &+ \frac{L(\alpha,f(N))}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{U(\alpha)}{f(N)^\alpha} \\ &\leq 1 - \frac{\epsilon}{1-R} \leq \\ \frac{(1-\epsilon)(\alpha+1)}{\alpha N} &+ \frac{U(\alpha)}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{L(\alpha,f(N))}{f(N)^\alpha}\end{aligned}$$

where ϵ and R should be interpreted as ϵ_n and R_n and for GR and GC sequences, respectively, and $L(\alpha, N) = e^{\alpha(2-\gamma-1/2N)}(1-\alpha)^2$ and $U(\alpha) = e^{\alpha(1-\gamma)}(1-\alpha)$, as also defined in Appendix A.

Proof: For both GC and GR sequences, we have

$$\lambda_N = 1 - \frac{1}{\epsilon}\sum_{i=2}^{f(N)} T_i = 1 - \frac{1}{\epsilon}\left[1 - \frac{f(N)}{\alpha}\left|\binom{\alpha}{f(N)}\right|\right]$$

where for the second equality, (A-1) is used. Inserting the above equation for λ_N into (14), which also applies to both GR and GC sequences, and replacing $\left|\binom{\alpha}{f(N)}\right|$ with its upper and lower bounds, we obtain

$$\begin{aligned}\frac{(1-\epsilon)(\alpha+1)}{\alpha N} &+ \frac{L(\alpha,f(N))}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{U(\alpha)}{f(N)^\alpha} \\ &\leq 1 - \frac{\epsilon}{1-R} \leq \\ \frac{(1-\epsilon)(\alpha+1)}{\alpha N} &+ \frac{U(\alpha)}{f(N)^{\alpha+1}} - \frac{\alpha+1}{\alpha N}\frac{L(\alpha,f(N))}{f(N)^\alpha}.\end{aligned} \quad \text{(B-4)}$$

∎

Proposition 1: Consider check-regular GC and GR ensemble sequences for which the values of N are computed based on the equation pairs (9), (10), and (12), (13), respectively. For the GC ensemble sequence with the channel parameter ϵ, we have

$$\lim_{\alpha\to 0}\frac{(1-\epsilon)^{-1/\alpha}}{N} = e^\gamma$$
and
$$\lim_{\alpha\to 0}\frac{1}{N^\alpha} = 1-\epsilon$$

where γ is the Euler constant, and for the GR ensemble sequence with rate R, we have

$$\lim_{\alpha\to 0}\frac{R^{-1/\alpha}}{N} = e^\gamma$$

and

$$\lim_{\alpha\to 0}\frac{1}{N^\alpha} = R.$$

Proof: For GC sequences, using (9), (A-1) and (A-4), we have

$$\frac{L(\alpha,N)}{N^\alpha} < 1-\epsilon.$$

Moreover, using (10), (A-1) and (A-4), we can see that

$$1-\epsilon \leq \frac{L(\alpha)}{(N-1)^\alpha}.$$

Putting the two bounds together, taking all terms to the power of $-1/\alpha$, and dividing them by N, we obtain

$$L(\alpha,N)^{-1/\alpha} > \frac{(1-\epsilon)^{-1/\alpha}}{N} \geq U(\alpha)^{-1/\alpha}\frac{N-1}{N}. \quad \text{(B-5)}$$

Replacing the values of $L(\alpha, N)$ and $U(\alpha)$ from Appendix A in (B-5) and slightly manipulating the inequality, we obtain

$$e^{-2+\gamma+1/2N}(1-\alpha)^{-2/\alpha} > \frac{(1-\epsilon)^{-1/\alpha}}{N} \geq e^{-1+\gamma}(1-\alpha)^{-1/\alpha}\frac{N-1}{N}.$$

For the upper bound, we have

$$\lim_{\alpha\to 0} e^{-2+\gamma+1/2N}(1-\alpha)^{-2/\alpha} = e^{-2+\gamma}\lim_{\alpha\to 0}(1-\alpha)^{-2/\alpha} = e^\gamma, \quad \text{(B-6)}$$

and for the lower bound, we have

$$\lim_{\alpha\to 0} e^{-1+\gamma}(1-\alpha)^{-1/\alpha}\frac{N-1}{N} = e^{-1+\gamma}\lim_{\alpha\to 0}(1-\alpha)^{-1/\alpha} = e^{\gamma}, \tag{B-7}$$

where in both cases, we have used the relationship $\lim_{\alpha\to 0}(1-\alpha)^{-c/\alpha} = e^c$, where c is a constant with respect to α. From (B-6) and (B-7), we conclude that

$$\lim_{\alpha\to 0}\frac{(1-\epsilon)^{-1/\alpha}}{N} = e^{\gamma}.$$

Also note the following.
$\lim_{\alpha\to 0}\frac{(1-\epsilon)^{-1}}{N^\alpha} = \lim_{\alpha\to 0}\left(\frac{(1-\epsilon)^{-1/\alpha}}{N}\right)^\alpha = \lim_{\alpha\to 0}(e^\gamma)^\alpha = 1$. Therefore

$$\lim_{\alpha\to 0}\frac{1}{N^\alpha} = 1-\epsilon.$$

This completes the proof for GC sequences.

For GR sequences, starting from (B-3) and setting $\beta = 1$, we have

$$\frac{R^{-1/\alpha}}{N} < \frac{1}{N}\left(\frac{N^{\alpha+1} - L(\alpha,N)}{(N-1)L(\alpha,N)}\right)^{1/\alpha}.$$

With a similar argument to the one that led to (B-3), and using (A-1), (A-2), and (13), we can see that

$$\frac{R^{-1/\alpha}}{N} \geq \frac{1}{N}\left(\frac{(N-1)^{\alpha+1} - U(\alpha)}{(N-2)U(\alpha)}\right)^{1/\alpha}.$$

Putting the bounds together, replacing the values of $L(\alpha, N)$ and $U(\alpha)$ from Appendix A, and taking the limit of both bounds as α tends to zero, we can see that both limits have the same value equal to e^γ. We thus have

$$\lim_{\alpha\to 0}\frac{R^{-1/\alpha}}{N} = e^{\gamma}.$$

Also note that $\lim_{\alpha\to 0}\frac{R^{-1}}{N^\alpha} = \lim_{\alpha\to 0}\left(\frac{R^{-1/\alpha}}{N}\right)^\alpha = \lim_{\alpha\to 0}(e^\gamma)^\alpha = 1$. Therefore

$$\lim_{\alpha\to 0}\frac{1}{N^\alpha} = R.$$

This completes the proof for GR sequences. ■

Proposition 2: Consider GC and GR ensemble sequences for which the values of N are computed based on the equation pairs (9), (10), and (12), (13), respectively. If function $f(N)$ is also chosen such that $\lim_{\alpha\to 0} f(N)^\alpha = M$, where for GC ensembles $1 < M < 1/(1-\epsilon)$, and for GR ensembles $1 < M < 1/R$, we have

$$\lim_{\alpha\to 0} L(\alpha, f(N)) - \frac{f(N)}{N\alpha}(\alpha+1)(U(\alpha) - (1-\epsilon)f(N)^\alpha) = \lim_{\alpha\to 0} U(\alpha) - \frac{f(N)}{N\alpha}(\alpha+1)(L(\alpha, f(N)) - (1-\epsilon)f(N)^\alpha) = 1$$

where ϵ should be interpreted as ϵ_n for GR sequences.

Proof: We only state the proof for GC ensembles. The proof for GR ensembles is similar. From the proposition assumption, we have $\lim_{\alpha\to 0} f(N)^\alpha = M < 1/(1-\epsilon)$. From Proposition 1, we have $\lim_{\alpha\to 0} N^\alpha = \frac{1}{1-\epsilon}$. By dividing the sides of these two equalities, we obtain

$$\lim_{\alpha\to 0}\frac{f(N)^\alpha}{N^\alpha} = \lim_{\alpha\to 0}\left(\frac{f(N)}{N}\right)^\alpha = M(1-\epsilon)$$

where $M(1-\epsilon) < 1$. Now based on the definition of the limit

$$\forall\eta > 0,\ \exists\delta > 0,\ \text{such that if } |\alpha| < \delta,\ \text{then}: \\ M(1-\epsilon) - \eta < \left(\frac{f(N)}{N}\right)^\alpha < M(1-\epsilon) + \eta.$$

Bearing in mind that $0 < M(1-\epsilon) < 1$, we choose η such that $p = M(1-\epsilon) + \eta < 1$, and $q = M(1-\epsilon) - \eta > 0$. We thus have

$$0 < q < \left(\frac{f(N)}{N}\right)^\alpha < p < 1, \\ \text{and} \\ \frac{q^{1/\alpha}}{\alpha} < \frac{f(N)}{\alpha N} < \frac{p^{1/\alpha}}{\alpha}.$$

Taking the limits of all terms as $\alpha \to 0$, we have

$$\lim_{\alpha\to 0}\frac{q^{1/\alpha}}{\alpha} \leq \lim_{\alpha\to 0}\frac{f(N)}{\alpha N} \leq \lim_{\alpha\to 0}\frac{p^{1/\alpha}}{\alpha}.$$

Since constants p and q are smaller than 1, and using an argument similar to the one in the proof of Lemma 2 ($\lim_{\alpha\to 0} H(\alpha) = 0$), the limits of the upper and the lower bounds are zero, and thus

$$\lim_{\alpha\to 0}\frac{f(N)}{\alpha N} = 0. \tag{B-8}$$

Using the assumption $\lim_{\alpha\to 0} f(N)^\alpha = M$, it can be simply shown that

$$\lim_{\alpha\to 0}(\alpha+1)(L(\alpha, f(N)) - (1-\epsilon)f(N)^\alpha) = 1 - (1-\epsilon)M.$$

Using (B-8), we obtain

$$\lim_{\alpha\to 0}\frac{f(N)}{\alpha N}(\alpha+1)(L(\alpha, f(N)) - (1-\epsilon)f(N)^\alpha) = 0.$$

Therefore

$$\lim_{\alpha\to 0} U(\alpha) - \frac{f(N)}{\alpha N}(\alpha+1)(L(\alpha, f(N)) - (1-\epsilon)f(N)^\alpha) = 1.$$

It can be similarly proven that

$$\lim_{\alpha\to 0} L(\alpha, f(N)) - \frac{f(N)}{\alpha N}(\alpha+1)(U(\alpha) - (1-\epsilon)f(N)^\alpha) = 1.$$

This completes the proof of the proposition. ■

Proposition 3: If function $f(N)$ satisfies $\lim_{\alpha\to 0}\frac{f(N)}{N}=K$, where $K>0$, then for GC ensembles

$$\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{L(\alpha,f(N))}{f(N)^\alpha}-(1-\epsilon)\right)=\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{U(\alpha)}{f(N)^\alpha}-(1-\epsilon)\right)=(1-\epsilon)\ln(1/K)$$

and for GR ensembles

$$\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{L(\alpha,f(N))}{f(N)^\alpha}-R\right)=\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{U(\alpha)}{f(N)^\alpha}-R\right)=R\ln(1/K).$$

Proof: We first consider GC sequences. From $\lim_{\alpha\to 0}\frac{f(N)}{N}=K$, or equivalently $\lim_{\alpha\to 0}\frac{N}{f(N)}=\frac{1}{K}$, we have

$$\forall\eta>0,\exists\delta>0:|\alpha|<\delta\Rightarrow\left|\frac{N}{f(N)}-\frac{1}{K}\right|<\eta.$$

Therefore, for $|\alpha|<\delta$,

$$(1/K-\eta)/N<1/f(N)<(1/K+\eta)/N.$$

We now take all terms to the power of α, and multiply them by $L(\alpha,f(N))$, to obtain

$$(1/K-\eta)^\alpha(L(\alpha,f(N))/N^\alpha)<L(\alpha,f(N))/f(N)^\alpha<(1/K+\eta)^\alpha(L(\alpha,f(N))/N^\alpha).$$

By slightly modifying the lower bound, we obtain

$$(1/K-\eta)^\alpha(U(\alpha)/N^\alpha)(L(\alpha,f(N))/U(\alpha))<L(\alpha,f(N))/f(N)^\alpha<(1/K+\eta)^\alpha(L(\alpha,f(N))/N^\alpha).$$

From (B-5), we have $\frac{L(\alpha,N)}{N^\alpha}<1-\epsilon\le\frac{U(\alpha)}{(N-1)^\alpha}$. This is equivalent to $1-\epsilon\le\frac{U(\alpha)}{(N-1)^\alpha}$ and $\frac{L(\alpha,f(N))}{N^\alpha}<(1-\epsilon)e^{\alpha(\frac{1}{2N}-\frac{1}{2f(N)})}$. We therefore conclude that

$$(L(\alpha,f(N))/U(\alpha))\,(1/K-\eta)^\alpha(1-\epsilon)\left(\frac{N-1}{N}\right)^\alpha<L(\alpha,f(N))/f(N)^\alpha<(1/K+\eta)^\alpha\,(1-\epsilon)e^{\alpha(\frac{1}{2N}-\frac{1}{2f(N)})},$$

or equivalently

$$e^{\alpha(1-1/(2f(N)))}(1-\alpha)e^{\alpha\ln(1/K-\eta)}(1-\epsilon)e^{\alpha\ln((N-1)/N)}<L(\alpha,f(N))/f(N)^\alpha<e^{\alpha\ln(1/K+\eta)}(1-\epsilon)e^{\alpha(\frac{1}{2N}-\frac{1}{2f(N)})}.$$

Subtracting $1-\epsilon$, and dividing all terms by α, we obtain

$$\frac{e^{\alpha(1-1/(2f(N)))}(1-\alpha)e^{\alpha\ln(1/k-\eta)}e^{\alpha\ln((N-1)/N)}-1}{\alpha}\times(1-\epsilon)<\frac{1}{\alpha}\left(\frac{L(\alpha,f(N))}{f(N)^\alpha}-(1-\epsilon)\right)<\frac{e^{\alpha\ln(1/K+\eta)}e^{\alpha(\frac{1}{2N}-\frac{1}{2f(N)})}-1}{\alpha}(1-\epsilon).$$

and thus

$$\frac{e^{\alpha(1-1/(2f(N)))+\alpha\ln(1/K-\eta)+\alpha\ln((N-1)/N)}(1-\alpha)-1}{\alpha}\times(1-\epsilon)<\frac{1}{\alpha}\left(\frac{L(\alpha,f(N))}{f(N)^\alpha}-(1-\epsilon)\right)<\frac{e^{\alpha\ln(1/K+\eta)+\alpha(\frac{1}{2N}-\frac{1}{2f(N)})}-1}{\alpha}(1-\epsilon).$$

It is a straight forward exercise to see that the limit of both the upper and the lower bounds is $(1-\epsilon)\ln(1/K)$ as α tends to zero. This implies that

$$\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{L(\alpha,f(N))}{f(N)^\alpha}-(1-\epsilon)\right)=(1-\epsilon)\ln(1/K).$$

Similarly, one can see that

$$\lim_{\alpha\to 0}\frac{1}{\alpha}\left(\frac{U(\alpha)}{f(N)^\alpha}-(1-\epsilon)\right)=(1-\epsilon)\ln(1/K).$$

This completes the proof for GC sequences.

The approach for GR sequences is similar and thus omitted. ■

Proposition 4: If function $f(N)$ satisfies $\lim_{\alpha\to 0}\frac{f(N)}{N}=K$, where $K>0$, then for GC ensembles, $\lim_{\alpha\to 0}\frac{(1-\epsilon)^{-1/\alpha}}{f(N)}=e^\gamma/K$, and for GR ensembles, $\lim_{\alpha\to 0}\frac{R^{-1/\alpha}}{f(N)}=e^\gamma/K$, where γ is the Euler constant.

Proof: For GR ensembles, we have

$$\lim_{\alpha\to 0}\frac{R^{-1/\alpha}}{f(N)}=\lim_{\alpha\to 0}\frac{R^{-1/\alpha}}{N}\frac{N}{f(N)}=\lim_{\alpha\to 0}\frac{R^{-1/\alpha}}{N}\lim_{\alpha\to 0}\frac{N}{f(N)}=\frac{e^\gamma}{K},$$

where the last equality follows from Proposition 1 and the assumption of Proposition 4.

The proof for GC ensembles is similar. ■

Proposition 5: For GC and GR ensemble sequences, if $\lim_{\alpha\to 0}\frac{f(N)}{N}=K>0$, then $\lim_{\alpha\to 0}f(N)^\alpha=1/(1-\epsilon)$ and $\lim_{\alpha\to 0}f(N)^\alpha=1/R$, for GC and GR ensemble sequences, respectively.

Proof: The proof follows from Proposition 1, i.e., for GC and GR ensembles, we have $\lim_{\alpha\to 0}\frac{1}{N^\alpha}=1-\epsilon$ and $\lim_{\alpha\to 0}\frac{1}{N^\alpha}=R$, respectively, and that by the assumption, we have $\lim_{\alpha\to 0}\frac{f(N)^\alpha}{N^\alpha}=\lim_{\alpha\to 0}\left(\frac{f(N)}{N}\right)^\alpha=1$. ■

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their helpful comments which improved the presentation of this paper.

REFERENCES

[1] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 596–584, Feb. 2001.

[2] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, “Finite-length analysis of low-density parity-check codes on the binary erasure channel,” *IEEE Trans. Inf. Theory*, vol. 48, pp. 1570–1579, Jun. 2002.

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

[4] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. Spielman, and V. Stemann, “Practical loss-resilient codes,” in *Proc. 29th Ann. ACM Symp. Theory Comput.*, 1997, pp. 150–159.

[5] A. Shokrollahi, “Capacity-achieving sequences,” in *Codes, Systems, and Graphical Models (IMA Volumes in Mathematics and Its Applications)*, B. Marcus and J. Rosenthal, Eds. New York: Springer-Verlag, 2000, vol. 123, pp. 153–166.

[6] A. Shokrollahi, M. Fossorier, H. Imai, S. Lin, and A. Poli, Eds., “New sequences of linear time erasure codes approaching the channel capacity,” in *Proc. 13th Int. Symp. Appl. Algebra, Algebraic Algorithms, and Error Correcting Codes*, 1999, vol. 1719, Lecture Notes in Computer Science, pp. 65–76.

[7] P. Oswald and A. Shokrollahi, “Capacity-achieving sequences for the erasure channel,” *IEEE Trans. Inf. Theory*, vol. 48, pp. 3017–3028, Dec. 2002.

[8] I. Sason and R. Urbanke, “Parity-check density versus performance of binary linear block codes over memoryless symmetric channels,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 1611–1635, Jul. 2003.

[9] I. Sason and R. Urbanke, “Complexity versus performance of capacity-achieving irregular repeat-accumulate codes on the binary erasure channel,” *IEEE Trans. Inf. Theory*, vol. 50, pp. 1247–1256, Jun. 2004.

[10] H. D. Pfister, I. Sason, and R. Urbanke, “Capacity-achieving ensembles for the binary erasure channel with bounded complexity,” *IEEE Trans. Inf. Theory*, vol. 51, pp. 2352–2379, Jul. 2005.

[11] H. D. Pfister and I. Sason, “Accumulate-repeat-accumulate codes: Capacity-achieving ensembles of systematic codes for the erasure channel with bounded complexity,” *IEEE Trans. Inf. Theory*, vol. 53, pp. 2088–2115, Jun. 2007.

[12] M. Lu, “On convergence speed of capacity-achieving sequences for erasure channel,” *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1793–1794, Apr. 2008.

[13] A. Ashikhmin, G. Kramer, and S. ten Brink, “Extrinsic Information Transfer Functions: Model and erasure channel properties,” *IEEE Trans. Inf. Theory*, vol. 50, pp. 2657–2673, Nov. 2004.

[14] E. Paolini, M. Chiani, and M. Fossorier, “Pseudo-binomial degree distributions from derivative matching,” in *Proc. 5th Int. Symp. Turbo Codes and Related Topics*, Lausanne, Switzerland, Sep. 2008, pp. 168–173.

[15] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[16] H. Saeedi and A. H. Banihashemi, “Systematic design of LDPC codes for binary erasure channels,” *IEEE Trans. Commun.*, vol. 58, no. 1, pp. 118–127, Jan. 2010.

[17] H. Saeedi and A. H. Banihashemi, “Deterministic design of LDPC codes for binary erasure channels,” in *Proc. IEEE Globcom*, Washington, DC, USA, Nov. 26–30, 2007.

[18] I. Sason and G. Wiechman, “Bounds on the number of iterations for turbo-like ensembles over the binary erasure channel,” *IEEE Trans. Inf. Theory*, vol. 55, pp. 2602–2617, Jun. 2009.

Hamid Saeedi (S’01–M’08) received the B.Sc. and M.Sc. degrees from Sharif University of Technology, Tehran, Iran, in 1999 and 2001, respectively, and the Ph.D. degree from Carleton University, Ottawa, ON, Canada, in 2007, all in electrical engineering.

In 2008–2009, he was a postdoctoral fellow with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst. In 2010, he joined the Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran, where he is now an Assistant Professor. He is also affiliated with the Advanced Communications Research Institute (ACRI), Sharif University of Technology, Tehran. His research interests include coding and information theory, wireless communications, and signal processing for broadband communications.

Dr. Saeedi is the recipient of some awards including Carleton University Senate Medal for Outstanding Academic Achievement, a Natural Sciences and Engineering Council of Canada (NSERC) Industrial Research and Development Fellowship, and an Ontario Graduate Scholarship.

Amir H. Banihashemi (S’90–A’98–M’03–SM’04) received the B.A.Sc. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 1988, and the M.A.Sc. degree in communications engineering from the University of Tehran, Tehran, Iran, in 1991, with the highest academic rank in both classes.

From 1991 to 1994, he was with the Electrical Engineering Research Center and the Department of Electrical and Computer Engineering, Isfahan University of Technology. During 1994–1997, he was with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, working toward the Ph.D. degree. He held two Ontario Graduate Scholarships for international students during this period. In 1997, he joined the Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada, where he worked as a Natural Sciences and Engineering Research Council of Canada (NSERC) Postdoctoral Fellow. He joined the Faculty of Engineering at Carleton University in 1998, where at present he is a Professor with the Department of Systems and Computer Engineering. His research interests include coding and information theory, digital and wireless communications, theory and implementation of communications algorithms and compressive sensing and sampling. He has published more than 120 papers in refereed journals and conferences.

Dr. Banihashemi served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS from 2003 to 2009. He is a member of the Board of Directors for the Canadian Society of Information Theory and the Director of Broadband Communications and Wireless Systems (BCWS) Centre at Carleton University. He has been involved in many international conferences as chair, member of technical program committee and member of organizing committee. These include Co-Chair for Communication Theory Symposium of Globecom’07, TPC Co-Chair of Information Theory Workshop (ITW) 2007, member of organizing committee for International Symposium on Information Theory (ISIT) 2008, and Co-Chair of Canadian Workshop on Information Theory (CWIT) 2009. He is a recipient of Carleton’s Research Achievement Award in 2006, and was awarded one of NSERC’s 100 2008 Discovery Accelerator Supplements (DAS).