Complexity versus Performance of Capacity-Achieving Irregular Repeat-Accumulate Codes on the Binary Erasure Channel[*]

Igal Sason
Department of Electrical Engineering
Technion – Israel Institute of Technology
Haifa 32000, Israel
E-mail: Sason@ee.technion.ac.il

Rüdiger Urbanke
Department of Communications and Computer Science
EPFL – Swiss Federal Institute of Technology
Lausanne, CH–1015, Switzerland
E-mail: Rudiger.Urbanke@epfl.ch

April 22, 2004

Abstract

We derive upper and lower bounds on the encoding and decoding complexity of two capacity-achieving ensembles of irregular repeat-accumulate (IRA1 and IRA2) codes on the binary erasure channel (BEC). These bounds are expressed in terms of the gap between the channel capacity and the rate of a typical code from this ensemble for which reliable communications is achievable under message-passing iterative (MPI) decoding. The complexity of the ensemble of IRA1 codes grows like the negative logarithm of the gap to capacity. On the other hand, the complexity of the ensemble of IRA2 codes with any choice of the degree distribution grows at least like the inverse square root of the gap to capacity, and at most like the inverse of the gap to capacity.

Index Terms – Channel capacity, complexity, density evolution, erasure channel, irregular repeat-accumulate (IRA) codes, low-density parity-check (LDPC) codes, message-passing iterative (MPI) decoding.

1 Introduction

In recent years, there has been an exciting development in constructing low-complexity error-correction codes which closely approach the capacity of many standard communication channels. These codes are usually defined on sparse graphs and decoded by a message-passing iterative (MPI) algorithm. In spite of the sub-optimality of the decoding algorithm, it is well known that there exist ensembles of codes which closely approach the capacity of memoryless binary-input output-symmetric (MBIOS) channels with feasible complexity.

[*] The paper will appear in the *IEEE Trans. on Information Theory*, vol. 50, no. 6, June 2004. It was submitted on April 12, 2003, and revised on January 12, 2004. The paper was presented in part at the *Third International Symposium on Turbo Codes & Related Topics*, Brest, France, September 1–5, 2003.

In [3, 5], Khandekar and McEliece have suggested to study the encoding and decoding complexity of ensembles of codes whose transmission takes place over an MBIOS channel. They were especially interested to explore the growth rate of the complexity under MPI decoding when the gap between the channel capacity and the achievable rate of these codes vanishes. They conjectured that if the achievable rate under MPI decoding is a fraction $1-\varepsilon$ of the channel capacity, then for a wide class of channels, the encoding complexity scales like $\ln \frac{1}{\varepsilon}$ and the decoding complexity scales like $\frac{1}{\varepsilon} \ln \frac{1}{\varepsilon}$. However, there is one exception: for low-density parity-check (LDPC) codes whose transmission takes place over a binary erasure channel (BEC), the decoding complexity under the MPI algorithm behaves like $\ln \frac{1}{\varepsilon}$ (same as encoding complexity) [6, 8]. This is true since for a BEC, the MPI decoding algorithm can be modified so that each edge is only used *once* (due to the absolute reliability of information which is not erased by the BEC). For a general MBIOS channel however, one has to consider the average number of iterations which are required for successful decoding; under MPI decoding, this number was conjectured to scale like $\frac{1}{\varepsilon}$. It was stated in [3] and proved in [4] that the encoding and decoding complexity of the ensemble of *right-regular* systematic repeat-accumulate codes behave like $\frac{1}{\varepsilon}$, which yields a significantly larger complexity as compared to the logarithmic behavior of the complexity of LDPC codes on the BEC [6, 8]. Khandekar and McEliece have conjectured (see Conjecture 1 in [3]) that for the ensemble of systematic IRA codes (which are named here IRA1 codes), there is a choice of degree distributions for which the complexity on the BEC scales like $\ln \frac{1}{\varepsilon}$ (i.e., the same logarithmic behavior as for the complexity of LDPC codes). In this paper we prove their conjecture, and also derive a probabilistic lower bound on the complexity of the ensemble of IRA1 codes. We prove in this paper that with high probability (as the block length of the codes goes to infinity), the encoding and decoding complexity of the IRA1 ensemble under MPI decoding behaves like $O\left(\ln \frac{1}{\varepsilon}\right)$. For a second ensemble which we consider in this paper (called the IRA2 ensemble), we show that for a certain choice of the degree distribution, the complexity on the BEC behaves like $O\left(\frac{1}{\varepsilon}\right)$, but it cannot be reduced by *any* degree distribution below $O\left(\frac{1}{\sqrt{\varepsilon}}\right)$ (the latter statement is true with high probability, as the block length goes to infinity.) This indicates that although for a certain pair of degree distributions the ensemble of systematic IRA codes achieves under MPI decoding a complexity which scales like $\ln \frac{1}{\varepsilon}$, there are some other ensembles of IRA codes, for which this logarithmic behavior of the complexity cannot be achieved by any degree distribution. These results are summarized in Table 1.

Complexity (χ)	General Ensembles	Right-Regular Ensembles
IRA1 Codes	$\chi = O\left(\ln \frac{1}{\varepsilon}\right)$	$\chi \leq O\left(\frac{1}{\varepsilon}\right)$
IRA2 codes	$O\left(\frac{1}{\sqrt{\varepsilon}}\right) \leq \chi \leq O\left(\frac{1}{\varepsilon}\right)$	$O\left(\frac{1}{\sqrt{\varepsilon}}\right) \leq \chi \leq O\left(\frac{1}{\varepsilon}\right)$
LDPC Codes	$\chi = O\left(\ln \frac{1}{\varepsilon}\right)$	$\chi = O\left(\ln \frac{1}{\varepsilon}\right)$

Table 1: Bounds on the encoding and the decoding complexity (χ) of general and right-regular ensembles of IRA and LDPC codes. The bounds refer to MPI decoding on the BEC. The bounds on the growth rate of the complexity are depicted as the gap ε between the channel capacity and the achievable rate of these codes vanishes.

Throughout the paper, we use interchangably the terms 'rate' and 'design rate' for an ensemble of LDPC or IRA codes; the latter term forms a lower bound on the actual rate of codes in the ensemble. Therefore, if the design rate of an ensemble is at least $1-\varepsilon$ of the channel capacity, then clearly the same is also true for the rate of a code from this ensemble.

The paper is organized as follows: Section 2 provides the main results, Section 3 presents the two ensembles of IRA codes which achieve the capacity of the BEC under MPI decoding and whose encoding/ decoding complexity is considered in this paper, Section 4 proves the theorems in this paper, and Section 5 provides numerical results for the upper and lower bounds on the complexity of ensembles of IRA codes. Section 6 concludes our discussion, and an appendix provides supplementary mathematical details about the proof in Section 4.2.

2 Main Results

Definition 1. Let $\{\mathcal{C}_m\}$ be a sequence of binary linear codes of rate R_m, and assume that for every m, the codewords of the code $\mathcal{C}_m$ are transmitted with equal probability over a BEC whose capacity is C. This sequence is said to *achieve a fraction* $1-\varepsilon$ *of the channel capacity with vanishing bit erasure probability* if $\lim_{m\to\infty} R_m = (1-\varepsilon)C$, and if there exists a decoding algorithm under which the average bit erasure probability of the code $\mathcal{C}_m$ tends to zero in the limit where $m \to \infty$.

Definition 2. Let $\mathcal{C}$ be an ensemble of LDPC or IRA codes whose degree distributions $\lambda(\cdot)$ and $\rho(\cdot)$ can be chosen arbitrarily, subject to possibly some constraints. The *encoding and the decoding complexity* are defined to be the average number of operations per information bit which are required for encoding and decoding in order to achieve a fraction $1-\varepsilon$ of the channel capacity with vanishing bit erasure probability. The encoding and the decoding complexity are with respect to *the best ensemble* (i.e., for the optimized pair of degree distributions), and refer to the average complexity over this ensemble (as the block length of the codes tends to infinity, the complexity of a typical code from this ensemble concentrates to the average complexity). We denote the encoding and the decoding complexity by $\chi_E(\varepsilon, \mathcal{C})$ and $\chi_D(\varepsilon, \mathcal{C})$, respectively.

Theorem 1. Consider the ensemble of IRA1 codes which are decoded on a BEC under MPI decoding. Then in the limit where the block length goes to infinity

$$\chi_E(\varepsilon, \text{IRA1}), \;\; \chi_D(\varepsilon, \text{IRA1}) > \frac{K_1 + K_2 \ln\left(\frac{1}{\varepsilon}\right)}{1-\varepsilon} \tag{1}$$

where

$$K_1 = \frac{p}{1-p} \, \frac{\ln\left(\frac{p}{1-p}\right)}{\ln\left(\frac{1}{1-p}\right)}, \quad K_2 = \frac{p}{1-p} \, \frac{1}{\ln\left(\frac{1}{1-p}\right)} \tag{2}$$

and p designates the bit-erasure probability of the BEC.

Theorem 2. In the limit where the block length of the ensemble of IRA1 codes goes to infinity, the encoding and decoding complexity under MPI decoding satisfy

$$\chi_E(\varepsilon, \text{IRA1}), \;\; \chi_D(\varepsilon, \text{IRA1}) = O\left(\ln \frac{1}{\varepsilon}\right). \tag{3}$$

More specifically, under MPI decoding

$$\chi_E(\varepsilon, \text{IRA1}), \;\; \chi_D(\varepsilon, \text{IRA1}) \leq \frac{K_3 + K_4 \ln\left(\frac{1}{\varepsilon}\right)}{1-\varepsilon} \tag{4}$$

where K_3 and K_4 are constants which only depend on the erasure probability (p) of the BEC.[1]

Theorem 3. Consider the ensemble of IRA2 codes which are decoded on a BEC under MPI decoding. Then in the limit where the block length goes to infinity

$$O\left(\frac{1}{\sqrt{\varepsilon}}\right) \leq \chi_E(\varepsilon, \text{IRA2}), \chi_D(\varepsilon, \text{IRA2}) \leq O\left(\frac{1}{\varepsilon}\right). \tag{5}$$

[1] The constants K_3 and K_4 are explicitly determined in the proof of Theorem 2 in Section 4. Numerical values of these constants and their comparison with the constants in Eq. (2) is shown later in Section 5.

3 Ensembles of IRA Codes

We introduce here two ensembles of irregular repeat-accumulate (IRA) codes, and assume that their transmission takes place over a BEC. We present the density evolution equations of these ensembles under MPI decoding. The IRA1 ensemble was presented in [2] and is reviewed here only briefly. On the other hand, the IRA2 ensemble is new, and is presented here in detail.

Using standard notations, an ensemble of IRA codes is characterized by its block length n, the interleaver which separates between the outer and inner codes, and the polynomials $\lambda(x) = \sum_{i=1}^{\infty} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{i=1}^{\infty} \rho_i x^{i-1}$, where λ_i (ρ_i) is equal to the probability that a randomly chosen edge (among the edges that connect the variable nodes and the check nodes) is connected to a variable (check) node of degree i. The structure of IRA codes is depicted in Fig. 1. Let

$$L(x) = \sum_{i=1}^{\infty} L_i x^i \ , \qquad R(x) = \sum_{i=1}^{\infty} R_i x^i$$

where L_i and R_i designate the probability that an information node or a check node has degree i (see Fig. 1). It is easy to show that

$$L(x) = \frac{\int_0^x \lambda(t) \, \mathrm{d}t}{\int_0^1 \lambda(t) \, \mathrm{d}t} \ , \qquad R(x) = \frac{\int_0^x \rho(t) \, \mathrm{d}t}{\int_0^1 \rho(t) \, \mathrm{d}t} \ . \tag{6}$$

Throughout the analysis in this paper which refers to the asymptotic case where $n \to \infty$, we consider a random interleaver which is chosen uniformly among all interleavers of length n.

3.1 IRA1 Codes (Systematic IRA Codes)

The ensemble of systematic IRA codes was introduced in [2] and [4]. It is easy to show that the rate of the ensemble of IRA1 codes is

$$R_{\text{IRA1}} = \frac{1}{1 + \frac{\int_0^1 \rho(x) \, \mathrm{d}x}{\int_0^1 \lambda(x) \, \mathrm{d}x}} \ . \tag{7}$$

The schedule of the messages under MPI decoding in [2] involves doing a forward/ backward recursion on the "accumulate" portion of the graph, and a single update on the "repeat" portion of the graph. Though the authors of [2] did not describe this subtlety, it is implicit in their derivation. Based on the density evolution equations of the ensemble of IRA1 codes, a fixed point of the the bit erasure probability under MPI decoding satisfies the equation [2]

$$x = p \, \lambda \left(1 - \left(\frac{1-p}{1 - p \, R(1-x)} \right)^2 \rho(1-x) \right) . \tag{8}$$

If Eq. (8) has no solution in the interval $(0, p]$, then the bit erasure probability under MPI decoding must converge to zero as the number of iterations grows (under the assumption that the block length of these codes tends to infinity).

3.2 IRA2 Codes

We consider here an ensemble of IRA codes where every information bit of these interleaved serially concatenated codes is repeated by the outer code a number of times which varies between 2 and

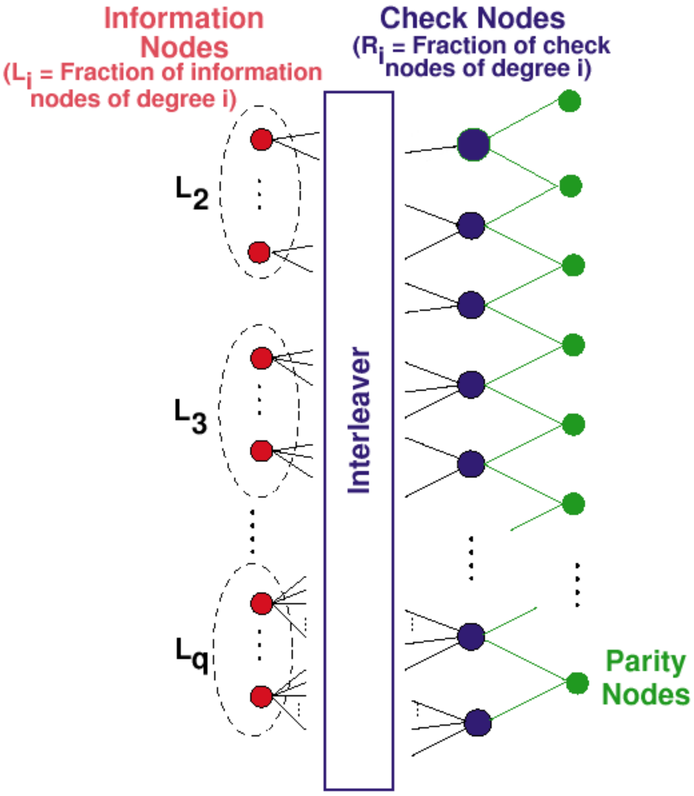
Information Nodes
(L_i = Fraction of information nodes of degree i)
Check Nodes
(R_i = Fraction of check nodes of degree i)
L_2
L_3
L_q
Interleaver
Parity Nodes

Figure 1: The Tanner graph of IRA1 codes. L_i and R_i designate the probability that an information node or a check node have degree i with respect to the edges that connect information nodes with check nodes (if the degree of a check node is i, then $i+2$ edges emanate from this check node, due to the two additional edges which connect this check node with two parity nodes). For the IRA2 ensemble, there is only one edge between every check node and the information nodes (so basically $R_1 = 1$ and $R_i = 0$ for $i \geq 2$), and part of the information bits and parity bits are punctured (with possibly different puncturing rates, r_s and r_p, respectively). Fig. 1 was reproduced from [2] with the appropriate modifications.

a certain maximal number (q), subject to an arbitrary probability distribution. The inner code is a differential encoder, and the interleaver separating between these two component codes is uniform. Finally, the information (systematic) bits and the parity bits are randomly punctured, with possibly different puncturing rates (designated by r_s and r_p, respectively). Referring to Fig. 1, the IRA2 codes are decoded by an MPI decoding algorithm, where the scheduling of the messages which are transmitted through the edges of the Tanner graph is as follows: the messages are transmitted through the edges emanating from the parity nodes to the check nodes, and then they are transmitted through the edges emanating from the check nodes to the information nodes (where every check node is connected by an edge to a single information node, since the inner code of the IRA2 codes is a differential encoder). The messages are then transmitted back through the edges emanating from the information nodes to the check nodes, and finally they are transmitted back through the edges emanating from the check nodes to the parity nodes. Since we consider the BEC which is error-free, we assume that the message-passing decoding algorithm uses every edge only once: after passing a message through an edge in the graph (which is of absolute certainty for the BEC), this edge is removed from the graph.

We note that the ensemble of regular RA codes [1] is a particular case of the IRA2 ensemble for the specific case of an outer code which repeats the information bits a constant number of times (q) and by setting: $r_s = 1$, $r_p = 0$ (i.e., in the case where all the information bits are punctured and all the parity bits are transmitted). It can be easily verified that the rate of the IRA2 ensemble is

$$R_{\mathrm{IRA2}} = \frac{1}{1 - r_s + \frac{1 - r_p}{\int_0^1 \lambda(x)\,\mathrm{d}x}} \,. \tag{9}$$

We introduce now the density evolution equations for the IRA2 ensemble under MPI decoding. Let p be the erasure probability of the BEC. We will iterate the probability of erasure along the edges of the graph during the course of the algorithm. Referring to the l^{th} iteration of the decoding algorithm, let x_l be the probability of erasure on an edge from a parity node to a check node, let u_l be the probability of erasure on an edge from a check node to an information node, let v_l be the probability of erasure on an edge from an information node to a check node, and let w_l be the probability of erasure on an edge from a check node to a parity node. Then in the asymptotic case where the block length tends to infinity, and the messages are statistically independent, we obtain the following equations from the Tanner graph of the IRA2 ensemble

$$\begin{array}{lcl} u_l & = & 1 - (1 - x_l)^2 \\ v_l & = & p_1\,\lambda(u_l) \\ w_l & = & 1 - (1 - x_l)(1 - v_l) \\ x_{l+1} & = & p_2\,w_l \end{array} \tag{10}$$

where

$$p_1 = 1 - (1 - p)(1 - r_s), \quad p_2 = 1 - (1 - p)(1 - r_p) \tag{11}$$

are the effective probabilities of erasure of the information bits and the parity bits, respectively, caused either by the BEC or the puncturing of the code. Clearly, we have the two trivial extreme cases in (11): if the code is not punctured, then $p_{1,2} = p$, and on the other hand, if all the bits are punctured (i.e., $r_s = r_p = 1$) then $p_{1,2} = 1$.

Based on the density evolution equations in (10), it follows that

$$x_{l+1} = f(x_l, p_1, p_2) \quad l = 0, 1, 2, \ldots \tag{12}$$

where the initial value is $x_0 = p_2$, and

$$f(x, p_1, p_2) = p_2\,\Big(1 - (1 - x)\,\Big(1 - p_1\,\lambda\big(1 - (1 - x)^2\big)\Big)\Big). \tag{13}$$

By calculating the first derivative of the right side of (13) w.r.t. x at zero, it follows immediately that the stability condition for the IRA2 ensemble under MPI decoding is

$$\big(1 + 2p_1\lambda'(0)\big)\;p_2 < 1. \tag{14}$$

From the recursive equation (12), then for a given polynomial $\lambda(\cdot)$, the resulting threshold on the BEC is the supremum over the values of p for which $f(x, p_1, p_2) < x$, $\forall x : 0 < x \leq p_2$.

The substitution $x = 1 - \sqrt{1 - u}$ transforms the above inequality to

$$\lambda(u) < \frac{1}{p_1}\left(\frac{1}{p_2} - 1\right)\left(\frac{1}{\sqrt{1 - u}} - 1\right) \;,\; \forall u : 0 < u \leq 1 - (1 - p_2)^2 \tag{15}$$

or equivalently

$$\sum_{i=2}^{\infty} \lambda_i u^{i-1} < \frac{1}{p_1}\left(\frac{1}{p_2} - 1\right) \sum_{i=1}^{\infty} \left\{\frac{1}{4^i}\binom{2i}{i} u^i\right\} \;,\; \forall u : 0 < u \leq 1 - (1 - p_2)^2. \tag{16}$$

4 Proofs of the Theorems

4.1 Proof of Theorem 1

We derive here a lower bound on the encoding and decoding complexity of IRA1 codes where the transmission takes place over a BEC with an erasure probability p, and the codes are iteratively decoded with an MPI decoding algorithm. Based on Eq. (8), in order to achieve vanishing bit erasure probability as the number of iterations tends to infinity, we require that

$$p\,\lambda\left(1-\left(\frac{1-p}{1-p\,R(1-x)}\right)^2\rho(1-x)\right)<x \qquad \forall\, 0<x\le p. \tag{17}$$

By dividing both sides of Eq. (17) by p, taking the inverse of $\lambda(\cdot)$ from both sides of the inequality (since $\lambda(\cdot)$ is a monotonic increasing function, then also $\lambda^{-1}(\cdot)$ is monotonic increasing), and finally integrating from $x=0$ to $x=p$, we obtain that

$$p-\int_0^p\left(\frac{1-p}{1-p\,R(1-x)}\right)^2\rho(1-x)\,\mathrm{d}x<\int_0^p\lambda^{-1}\left(\frac{x}{p}\right)\,\mathrm{d}x. \tag{18}$$

Since $\lambda(0)=0$ and $\lambda(1)=1$, the substitution $x=p\lambda(u)$ and integration by parts give

$$\begin{aligned}\int_0^p\lambda^{-1}\left(\frac{x}{p}\right)\mathrm{d}x &= p\int_0^1 u\,\lambda'(u)\,\mathrm{d}u\\ &= p\left(u\lambda(u)\Big|_{u=0}^{1}-\int_0^1\lambda(u)\,\mathrm{d}u\right)\\ &= p\left(1-\int_0^1\lambda(u)\,\mathrm{d}u\right).\end{aligned}$$

The substitution of the latter equality in the right-hand side of Eq. (18) gives

$$\int_0^1\lambda(u)\,\mathrm{d}u<\frac{(1-p)^2}{p}\int_0^p\frac{\rho(1-x)}{\big(1-p\,R(1-x)\big)^2}\,\mathrm{d}x\,. \tag{19}$$

Based on Eq. (6), it follows that

$$\rho(1-x)=-\int_0^1\rho(t)\,\mathrm{d}t\cdot\frac{\mathrm{d}}{\mathrm{d}x}\Big[R(1-x)\Big]\,, \tag{20}$$

and from the substitution of Eq. (20) in the right-hand side of Eq. (19), one obtains that

$$\begin{aligned}\int_0^p\frac{\rho(1-x)}{\big(1-p\,R(1-x)\big)^2}\,\mathrm{d}x &= -\int_0^1\rho(x)\,\mathrm{d}x\cdot\int_0^p\frac{1}{\big(1-p\,R(1-x)\big)^2}\cdot\frac{\mathrm{d}}{\mathrm{d}x}\Big[R(1-x)\Big]\,\mathrm{d}x\\ &= \int_0^1\rho(x)\,\mathrm{d}x\cdot\int_{R(1-p)}^1\frac{\mathrm{d}u}{(1-pu)^2}\qquad(\text{since } R(1)=1)\\ &= \frac{1}{1-p}\,\frac{1-R(1-p)}{1-\;p\,R(1-p)}\cdot\int_0^1\rho(x)\,\mathrm{d}x\,.\end{aligned} \tag{21}$$

The substitution of Eq.(21) in the right-hand side of Eq. (19) gives

$$\int_0^1\lambda(u)\,\mathrm{d}u<\frac{1-p}{p}\,\frac{1-R(1-p)}{1-\;p\,R(1-p)}\cdot\int_0^1\rho(x)\,\mathrm{d}x\,. \tag{22}$$

The rate of the ensemble of IRA1 codes is given in Eq. (7), so from Eqs. (7) and (22)

$$R_{\text{IRA1}} < \frac{1}{\frac{1}{1-p} + \frac{p\,R(1-p)}{1-R(1-p)}} \,. \tag{23}$$

If a fraction $1-\varepsilon$ of the capacity is achieved with vanishing bit erasure probability under MPI decoding, then

$$R_{\text{IRA1}} = (1-\varepsilon)(1-p) \tag{24}$$

which yields from Eq. (23) that

$$R(1-p) < \frac{\varepsilon}{p(1-p)} \,. \tag{25}$$

From Jensen's inequality,

$$R(1-p) = \sum_i R_i (1-p)^i \geq (1-p)^{a_{\text{R}}} \qquad a_{\text{R}} \triangleq \sum_i i R_i$$

which yields from Eq. (25) that for an arbitrary ensemble of IRA1 codes (i.e., for any choice of their degree distributions)

$$a_{\text{R}} > \frac{\ln\left(\frac{p(1-p)}{\varepsilon}\right)}{\ln\left(\frac{1}{1-p}\right)} \,. \tag{26}$$

The encoding of IRA1 codes is equivalent to the following two steps: first, sets of information bits are repeated and interleaved, and then the resulting bits are differentially encoded. The number of operations which are required for encoding IRA1 codes is therefore equal to the number of edges in the Tanner graph which represents the code (see Fig. 1). Since the MPI decoder can be modified for a BEC so that every edge in the graph is only used once, then the number of operations which are required for decoding IRA1 codes is equal to the number of edges in the Tanner graph. Therefore, the encoding and decoding complexity of IRA1 codes on a BEC are the same, and their common value is equal to the average number of edges in the graph normalized per information bit.

The average number of edges in the graph when normalized per check node is $a_{\text{R}} + 2$ (see Fig. 1), so the average number of edges normalized per information bit is equal to $\left(\frac{1-R_{\text{IRA1}}}{R_{\text{IRA1}}}\right) \cdot (a_{\text{R}} + 2)$. The substitution of Eqs. (24) and (26) in the latter result finally gives

$$\begin{aligned}
\chi_E(\varepsilon, \text{IRA1}),\ \ \chi_D(\varepsilon, \text{IRA1}) &= \left(\frac{1-R_{\text{IRA1}}}{R_{\text{IRA1}}}\right) \cdot (a_{\text{R}} + 2) \\
&> \frac{1-(1-p)(1-\varepsilon)}{(1-p)(1-\varepsilon)} \left(\frac{\ln\left(\frac{p(1-p)}{\varepsilon}\right)}{\ln\left(\frac{1}{1-p}\right)} + 2 \right) \\
&> \frac{p}{(1-p)(1-\varepsilon)} \cdot \frac{\ln\left(\frac{p}{\varepsilon(1-p)}\right)}{\ln\left(\frac{1}{1-p}\right)} \\
&= \frac{K_1 + K_2 \ln\left(\frac{1}{\varepsilon}\right)}{1-\varepsilon}
\end{aligned}$$

which proves the lower bound in Eq. (1) with the coefficients K_1 and K_2 in Eq. (2). We note that the concept of the derivation of the lower bound on a_{R} in Eq. (26) is similar to the derivation of Shokrollahi for LDPC codes [8] (except for the modifications which are required to adapt the proof to IRA1 codes; these modifications stem from the difference between Eqs. (7) and (8) and their parallels for LDPC codes).

4.2 Proof of Theorem 2

The concept of the beginning of this proof is similar to the proof in Section 3.4.2 of [4]. However, [4] refers to the right-regular ensemble of IRA1 codes whose encoding and decoding complexity on the BEC behave like $O\left(\frac{1}{\varepsilon}\right)$ (see Section 3.6 in [4]), and here we analyze the ensemble of IRA1 codes with another pair of degree distributions. For the latter choice of degree distributions, we prove that the encoding and decoding complexity of the IRA1 ensemble behave like $O\left(\ln \frac{1}{\varepsilon}\right)$. For the derivation of the upper bound on the complexity of the IRA1 ensemble, we choose the right degree distribution of the *edges* which connect between check nodes and information nodes in the Tanner graph (see Fig. 1) to be

$$\rho(x) = e^{\alpha(x-1)} \quad \alpha > 0. \tag{27}$$

The recursive equation (8) refers to the bit erasure probability of the ensemble of IRA1 codes which are transmitted on a BEC and are iteratively decoded by an MPI decoding algorithm. In order to achieve vanishing bit erasure probability as the number of iterations tends to infinity, we require that the condition in Eq. (17) will be fulfilled. The latter condition is automatically fulfilled for $x \in (p, 1)$, so without any loss of generality, one can extend the validity of (17) for $x \in (0, 1)$. Based on Eqs. (6) and (27), the right degree distribution of the *check nodes* in the graph is

$$R(x) = \frac{e^{\alpha(x-1)} - e^{-\alpha}}{1 - e^{-\alpha}} \quad \alpha > 0. \tag{28}$$

Let us denote by $f_p(x)$ the argument of $\lambda(\cdot)$ in the left-hand side of Eq. (17). Based on Eqs. (17), (27) and (28)

$$f_p(x) = 1 - \left(\frac{1-p}{1 - p\left(\frac{e^{-\alpha x} - e^{-\alpha}}{1 - e^{-\alpha}}\right)}\right)^2 e^{-\alpha x} \tag{29}$$

and Eq. (17) gets the form

$$p\,\lambda\left(f_p(x)\right) < x \qquad \forall\, x \in (0, 1). \tag{30}$$

In general, we would like to expand $f_p^{-1}(x)$ in a power series and to choose $\lambda(x)$ to be a suitably truncated version of this power series. For simplifying the analysis in the continuation, we define an auxiliary function $h_p(x)$ as

$$h_p(x) = 1 - \left(\frac{1-p}{1 - p\big(1 - z(x)\big)}\right)^2 \big(1 - z(x)\big) \qquad z(x) = 1 - \frac{e^{-\alpha x} - e^{-\alpha}}{1 - e^{-\alpha}}\,. \tag{31}$$

Since $\frac{e^{-\alpha x} - e^{-\alpha}}{1 - e^{-\alpha}} < e^{-\alpha x}$ for $\alpha > 0$ and $x > 0$, then it follows that $f_p(x) < h_p(x)$ for $x \in (0, 1)$, so the requirement in Eq. (30) is replaced by the stronger requirement

$$p\,\lambda\left(h_p(x)\right) < x \qquad \forall\, x \in (0, 1). \tag{32}$$

Lemma 1. For every $\alpha > 0$, the function $g_p(x) \triangleq h_p^{-1}(x)$ has a power series expansion with non-negative coefficients around $x = 0$.

Proof. See Appendix A.1. □

Let $g_p(x) = \sum_{i=1}^{\infty} g_{p,i} x^i$, and let us choose the left degree distribution of the IRA1 ensemble to be

$$\lambda(x) = \frac{1}{p}\left(\sum_{i=1}^{N-1} g_{p,i} x^i + \mu x^N\right). \tag{33}$$

where based on Lemma 1, the coefficients $g_{p,i}$ for $i \geq 1$ are positive. The parameters N and μ in Eq. (33) are uniquely determined so that

$$\sum_{i=1}^{N-1} g_{p,i} + \mu = p, \qquad 0 < \mu < g_{p,N}. \tag{34}$$

For the choice of $\lambda(\cdot)$ in Eq. (33) we obtain from Lemma 1 that

$$p\lambda(x) < g_p(x) = h_p^{-1}(x) < f_p^{-1}(x)$$

where the last inequality follows because $f_p(x) < h_p(x)$ for $x \in (0, 1)$. This implies that the condition in Eq. (30) is fulfilled, so as the number of iterations tends to infinity, the IRA1 ensemble achieves vanishing bit erasure probability under MPI decoding.

Based on Eqs. (7), (27) and (33), the rate of the considered ensemble of IRA1 codes is

$$R_{\text{IRA1}} = \frac{1}{1 + \frac{p(1-e^{-\alpha})}{\alpha} \left(\sum_{i=1}^{N-1} \frac{g_{p,i}}{i+1} + \frac{\mu}{N+1} \right)^{-1}} \,. \tag{35}$$

Since

$$\begin{aligned}
\sum_{i=1}^{N-1} \frac{g_{p,i}}{i+1} + \frac{\mu}{N+1} &\overset{\text{(a)}}{>} \sum_{i=1}^{N-1} \frac{g_{p,i}}{i+1} \\
&= \sum_{i=1}^{\infty} \frac{g_{p,i}}{i+1} - \sum_{i=N}^{\infty} \frac{g_{p,i}}{i+1} \\
&= \int_0^1 g_p(x)\, \mathrm{d}x - \sum_{i=N}^{\infty} \frac{g_{p,i}}{i+1} \\
&\overset{\text{(b)}}{\geq} \int_0^1 g_p(x)\, \mathrm{d}x - \frac{1}{N+1} \sum_{i=N}^{\infty} g_{p,i} \\
&\overset{\text{(c)}}{\geq} \int_0^1 g_p(x)\, \mathrm{d}x - \frac{g_p(1)}{N+1} \\
&\overset{\text{(d)}}{=} \int_0^1 g_p(x)\, \mathrm{d}x - \frac{1}{N+1}
\end{aligned}$$

where inequality (a) follows from Eq. (34), inequalities (b) and (c) follow from Lemma 1, and equality (d) follows from Eq. (31) and since $g_p(\cdot)$ is the inverse function of $h_p(\cdot)$, and on the other hand

$$\begin{aligned}
\sum_{i=1}^{N-1} \frac{g_{p,i}}{i+1} + \frac{\mu}{N+1} &\overset{\text{(a)}}{<} \sum_{i=1}^{N} \frac{g_{p,i}}{i+1} \\
&\overset{\text{(b)}}{<} \sum_{i=1}^{\infty} \frac{g_{p,i}}{i+1} \\
&= \int_0^1 g_p(x)\, \mathrm{d}x
\end{aligned}$$

where inequalities (a) and (b) follow from the same reasoning as above, then we obtain from Eq. (35) and the latter two chains of inequalities that

$$\frac{1}{1 + \frac{p(1-e^{-\alpha})}{\alpha} \left(\int_0^1 g_p(x)\, \mathrm{d}x - \frac{1}{N+1} \right)^{-1}} < R_{\text{IRA1}} < \frac{1}{1 + \frac{p(1-e^{-\alpha})}{\alpha} \left(\int_0^1 g_p(x)\, \mathrm{d}x \right)^{-1}} \,. \tag{36}$$

For an arbitrary positive value of α, since the function $g_p(\cdot)$ is the inverse of the function $h_p(\cdot)$ in Eq. (31) (and vice versa), these functions are monotonic increasing in the interval $[0,1]$, and $h_p(0) = 0$ and $h_p(1) = 1$, then for $\alpha > 0$

$$\begin{aligned}\int_0^1 g_p(x)\,\mathrm{d}x &= 1 - \int_0^1 h_p(x)\,\mathrm{d}x \\ &= \int_0^1 \left(\frac{1-p}{1-p\left(\frac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}}\right)}\right)^2 \frac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}}\,\mathrm{d}x\end{aligned}$$

and the substitution $u = \dfrac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}}$ gives the equality

$$\int_0^1 g_p(x)\,\mathrm{d}x = \frac{(1-p)^2(1-e^{-\alpha})}{\alpha} \int_0^1 \frac{u}{(1-pu)^2}\,\frac{1}{e^{-\alpha}+u(1-e^{-\alpha})}\,\mathrm{d}u. \tag{37}$$

Lemma 2. The parameter N in the left-hand side of Eq. (36) grows at least exponentially in α, and in particular

$$N > \ln\left(\frac{p}{x}\right)\cdot\left(e^{\alpha x}-1\right) \qquad \forall\, x \in (0,p). \tag{38}$$

Proof. See Appendix A.2. □

It is now easy to show that the ensemble of IRA1 codes with the degree distributions in Eqs. (27) and (33) achieves the capacity of the BEC with vanishing bit erasure probability in the limit where $\alpha \to \infty$ and the block length tends to infinity. To show this, we first observe that based on Lemma 2, N grows at least exponentially in α as $\alpha \to \infty$, so we obtain from Eqs. (36) and (37) that

$$\begin{aligned}\lim_{\alpha\to\infty} R_{\text{IRA1}} &= \lim_{\alpha\to\infty} \frac{1}{1+\frac{p(1-e^{-\alpha})}{\alpha}\left(\int_0^1 g_p(x)\,\mathrm{d}x\right)^{-1}} \\ &= \lim_{\alpha\to\infty} \frac{1}{1+\frac{p}{(1-p)^2}\left(\int_0^1 \frac{u}{(1-pu)^2}\,\frac{1}{e^{-\alpha}+u(1-e^{-\alpha})}\,\mathrm{d}u\right)^{-1}} \\ &= \frac{1}{1+\frac{p}{(1-p)^2}\left(\int_0^1 \frac{\mathrm{d}u}{(1-pu)^2}\right)^{-1}} \\ &= 1-p.\end{aligned}$$

For achieving a fraction $1-\varepsilon$ of the channel capacity with vanishing bit erasure probability under MPI decoding, we need that the ensemble rate of the IRA1 codes will be at least $(1-\varepsilon)(1-p)$. From the left-hand side of Eq. (36) and the latter requirement, it follows that it is sufficient to require that the lower bound on the rate of the IRA1 ensemble is at least $(1-\varepsilon)(1-p)$, which gives the inequality

$$\frac{\alpha}{p(1-e^{-\alpha})}\left(\int_0^1 g_p(x)\,\mathrm{d}x - \frac{1}{N+1}\right) \geq \left(\frac{1}{(1-\varepsilon)(1-p)}-1\right)^{-1}.$$

Since $\frac{1}{1-\varepsilon} > 1+\varepsilon$ for $0 < \varepsilon < 1$, then the latter inequality can be replaced by the stronger requirement

$$\frac{\alpha}{p(1-e^{-\alpha})}\left(\int_0^1 g_p(x)\,\mathrm{d}x - \frac{1}{N+1}\right) > \frac{1-p}{p+\varepsilon}. \tag{39}$$

In order to proceed in our analysis, we need the following lemma.

Lemma 3. For any $\alpha > \max\Bigl(\ln 2,\ \ln\left(\frac{1}{1-p}\right)\Bigr)$

$$\frac{\alpha}{1-e^{-\alpha}}\ \int_0^1 g_p(x)\,\mathrm{d}x > 1-p-8\left(\frac{1-p}{1+p}\right)^2\ \alpha e^{-\alpha}\ . \tag{40}$$

Proof. See Appendix A.3. □

From Eq. (40), it follows that the requirement in Eq. (39) can be strengthened to

$$\frac{1-p}{p}-\frac{8}{p}\left(\frac{1-p}{1+p}\right)^2\ \alpha e^{-\alpha}-\frac{\alpha}{p(1-e^{-\alpha})}\ \frac{1}{N+1} > \frac{1-p}{p+\varepsilon}$$

which can be further strengthened to the requirement

$$\frac{8(1-p)}{(1+p)^2}\cdot\alpha e^{-\alpha}+\frac{2\alpha}{1-p}\ \frac{1}{N+1} < \frac{\varepsilon}{p+1} \tag{41}$$

since $\frac{1}{1-e^{-\alpha}} < 2$ for $\alpha > \ln 2$, and also $\frac{\varepsilon}{p+1} < \frac{\varepsilon}{\varepsilon+p}$ for $0<\varepsilon<1$.

Based on Eq. (38), if we substitute $x = p-\eta$ where $0<\eta<p$, then we obtain a lower bound on N

$$\begin{aligned} N &> \ln\left(\tfrac{p}{p-\eta}\right)\cdot\left(e^{\alpha(p-\eta)}-1\right) \\ &> e^{\alpha(p-\eta)}\ \left(1-2^{-(p-\eta)}\right)\cdot\ln\left(\tfrac{p}{p-\eta}\right) \end{aligned} \tag{42}$$

where the latter inequality is valid for $\alpha > \ln 2$. From Eq. (42), we replace the condition in (41) by the stronger condition

$$\frac{8(1-p)}{(1+p)^2}\cdot\alpha e^{-\alpha}+\frac{2\alpha}{1-p}\ \frac{e^{-\alpha(p-\eta)}}{\ln\left(\frac{p}{p-\eta}\right)\ \left(1-2^{-(p-\eta)}\right)} < \frac{\varepsilon}{p+1}. \tag{43}$$

Let η be in the interval $(0,\frac{p}{2})$. It can be easily verified that for $\alpha>0$, the second term in the left-hand side of Eq. (43) is bigger than the first term, and since both terms are positive for $\alpha>0$, then we can replace the requirement in (43) by the stronger condition

$$\alpha\ e^{-\alpha(p-\eta)} < \frac{\varepsilon}{c} \tag{44}$$

where c is equal to

$$c \triangleq \frac{4(1+p)}{(1-p)\ \ln\left(\frac{p}{p-\eta}\right)}\ \frac{1}{1-2^{-(p-\eta)}}. \tag{45}$$

Let $\alpha_0 = \alpha_0(\eta)$ be the minimal positive number so that $\alpha < e^{\alpha\eta}$ for $\alpha > \alpha_0$. It can be easily verified that since $\eta < \frac{1}{2}$ then $\frac{1}{2\eta}\ln\left(\frac{1}{\eta}\right) < \alpha_0 < \frac{2}{\eta}\ln\left(\frac{1}{\eta}\right)$.[2] It follows that if $\alpha > \frac{2}{\eta}\ln\left(\frac{1}{\eta}\right)$, then the requirement in Eq. (44) can be replaced by the stronger condition $e^{-\alpha(p-2\eta)} < \frac{\varepsilon}{c}$ which is valid for $\alpha > \dfrac{\ln\left(\frac{c}{\varepsilon}\right)}{p-2\eta}$.

[2] For $\alpha = \frac{1}{2\eta}\ln\left(\frac{1}{\eta}\right)$ and $\alpha = \frac{2}{\eta}\ln\left(\frac{1}{\eta}\right)$, we obtain that $e^{\alpha\eta} = \frac{1}{\sqrt{\eta}}$ and $\frac{1}{\eta^2}$, respectively. The lower bound on α_0 follows since $\frac{\sqrt{\eta}}{2} < \ln 2 < \ln\left(\frac{1}{\eta}\right)$ for $0<\eta<\frac{1}{2}$, and the upper bound on α_0 follows since $2\eta\ln\left(\frac{1}{\eta}\right) \le \frac{2}{e} < 1$.

To conclude, the analysis above enables to choose α to be

$$\alpha = \max\left(\frac{\ln\left(\frac{c}{\varepsilon}\right)}{p-2\eta}\ ,\ \frac{2}{\eta}\ln\left(\frac{1}{\eta}\right)\ ,\ \ln 2\ ,\ \ln\left(\frac{1}{1-p}\right)\right) \tag{46}$$

where η is chosen arbitrarily in the interval $(0, \frac{p}{2})$, and c is defined in Eq. (45). Then, the encoding and the decoding complexity of the IRA1 ensemble are

$$\left(\frac{1-R_{\text{IRA1}}}{R_{\text{IRA1}}}\right)\left(\frac{1}{\int_0^1 \rho_\alpha(x)\,\mathrm{d}x}+2\right) \leq \frac{p+\varepsilon(1-p)}{(1-p)(1-\varepsilon)}\left(\frac{\alpha}{1-e^{-\alpha}}+2\right) \tag{47}$$

where the latter inequality follows from Eq. (27) and since $R_{\text{IRA1}} \geq (1-p)(1-\varepsilon)$. Based on Appendix A.4, it finally follows that if a fraction $1-\varepsilon$ of the capacity of the BEC is achieved with vanishing bit erasure probability (where $0<\varepsilon<1$) under MPI decoding, then $\chi_E(\varepsilon, \text{IRA1})$ and $\chi_D(\varepsilon, \text{IRA1})$ are both upper bounded by the right-hand side of Eq. (4) with K_3 and K_4 in Appendix A.4.

4.3 Proof of Theorem 3

We start here with the derivation of a lower bound on the encoding and decoding complexity of the IRA2 ensemble. By integrating both sides of Eq. (15) from $u=0$ to $u=1-(1-p_2)^2$, we have

$$\sum_{i=2}^{\infty}\frac{\lambda_i}{i}\left[1-(1-p_2)^2\right]^i < \frac{p_2(1-p_2)}{p_1}$$

and the division of both side of this inequality by $\sum_{j=2}^{\infty}\frac{\lambda_j}{j}$ gives

$$\sum_{i=2}^{\infty}L_i\left[1-(1-p_2)^2\right]^i < \frac{p_2(1-p_2)}{p_1}\cdot\frac{1}{\sum_{j=2}^{\infty}\frac{\lambda_j}{j}}\ , \tag{48}$$

where $L_i = \frac{\frac{\lambda_i}{i}}{\sum_{j=2}^{\infty}\frac{\lambda_j}{j}}$ designates the probability that a left node (i.e., an information node) in the Tanner graph of the IRA2 ensemble has degree i (see Fig. 1). Based on Jensen's inequality

$$\xi^{\sum_i iL_i} \leq \sum_i L_i \xi^i \quad \forall\ \xi \in (0,1)$$

and since $\sum_{i=2}^{\infty} iL_i = \frac{1}{\sum_{i=2}^{\infty}\frac{\lambda_i}{i}}$, then it follows from Eq. (48) that

$$\left[1-(1-p_2)^2\right]^x < \frac{p_2(1-p_2)x}{p_1}\ , \tag{49}$$

where

$$x \triangleq \frac{1}{\sum_{i=2}^{\infty} \frac{\lambda_i}{i}} \,. \tag{50}$$

Suppose that the IRA2 ensemble achieves a fraction $1-\varepsilon$ of the capacity of the BEC under MPI decoding. From Eqs. (9), (11) and (50), it follows that

$$1-\varepsilon = \frac{R_{\text{IRA2}}}{C} = \frac{1}{1-p_1+(1-p_2)x} \tag{51}$$

where $C = 1-p$ is the capacity of the BEC. Let $p_1 = f(\varepsilon, p)$, then it follows from Eq. (11) that $p \leq f(\varepsilon,p) \leq 1$. From Eq. (51), we obtain that $1-p_2 = \frac{1}{x}\left(f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}\right)$, and Eq. (49) transforms to

$$\left[1-\left(\frac{f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}}{x}\right)^2\right]^x < \left(1+\frac{\varepsilon}{(1-\varepsilon)f(\varepsilon,p)}\right)\left[1-\frac{1}{x}\left(f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}\right)\right] \,. \tag{52}$$

We wish now to determine the behavior of the solution x in Eq. (52) for small values of ε (i.e., for $\varepsilon \rightarrow 0$, which corresponds to capacity-approaching IRA2 ensembles on the BEC). Now we take the natural logarithms from both sides of Eq. (52) and substitute $x = \frac{1}{c\varepsilon^b}\left(f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}\right)$ where b is a real number and $c > 0$ (since c is an arbitrary positive number and $p \leq f(\varepsilon,p) \leq 1$, then $x = O\left(\frac{1}{\varepsilon^b}\right)$). From the power series expansion

$$\ln(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \ldots \qquad 0 \leq x < 1$$

one obtains that in the limit where $\varepsilon \rightarrow 0$

$$\begin{aligned}
& x \ln\left(1-\left(\frac{f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}}{x}\right)^2\right) - \ln\left(1+\frac{\varepsilon}{(1-\varepsilon)f(\varepsilon,p)}\right) - \ln\left(1-\frac{1}{x}\left(f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}\right)\right) \\
= & \left(\frac{f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}}{c\varepsilon^b}\right) \ln(1-c^2\varepsilon^{2b}) - \ln\left(1+\frac{\varepsilon}{(1-\varepsilon)f(\varepsilon,p)}\right) - \ln(1-c\varepsilon^b) \\
= & \left(\frac{f(\varepsilon,p)+\frac{\varepsilon}{1-\varepsilon}}{c\varepsilon^b}\right)\left[-c^2\varepsilon^{2b} - \frac{c^4\varepsilon^{4b}}{2} - \frac{c^6\varepsilon^{6b}}{3} - \ldots\right] - \\
& \left[\frac{\varepsilon}{(1-\varepsilon)f(\varepsilon,p)} - \frac{1}{2}\left(\frac{\varepsilon}{(1-\varepsilon)f(\varepsilon,p)}\right)^2 + \frac{1}{3}\left(\frac{\varepsilon}{(1-\varepsilon)f(\varepsilon,p)}\right)^3 - \ldots\right] - \left[-c\varepsilon^b - \frac{c^2\varepsilon^{2b}}{2} - \frac{c^3\varepsilon^{3b}}{3} - \ldots\right] \\
= & c\varepsilon^b\left(1-f(\varepsilon,p)-\frac{\varepsilon}{1-\varepsilon}\right) - \frac{\varepsilon}{(1-\varepsilon)f(\varepsilon,p)} + \frac{c^2\varepsilon^{2b}}{2} + \frac{c^3\varepsilon^{3b}}{3}\left(1-\frac{3}{2}f(\varepsilon,p)-\frac{3}{2}\frac{\varepsilon}{1-\varepsilon}\right) + \ldots \,.
\end{aligned}$$

Since $p \leq f(\varepsilon,p) \leq 1$ (where $0 < p < 1$) and $c > 0$, we obtain that if $b < \frac{1}{2}$, then for small values of ε, the above expression is dominated by $c\varepsilon^b\big(1-f(\varepsilon,p)\big) + \frac{c^2\varepsilon^{2b}}{2}$ which is positive. This implies that if $b < \frac{1}{2}$, any solution of the form $x = O\left(\frac{1}{\varepsilon^b}\right)$ does not satisfy Eq. (52). Since on the BEC, the encoding/ decoding complexity of IRA2 ensembles with MPI decoding is linearly proportional to the average number of edges per information bit in their Tanner graphs (i.e., it is linearly proportional to x), then it follows that the encoding and decoding complexity of capacity-approaching IRA2 ensembles cannot be reduced below $O\left(\frac{1}{\sqrt{\varepsilon}}\right)$ for *any choice of their degree distribution.*

The upper bound on the complexity is derived by choosing the degree distribution to be

$$\lambda(x) = K \sum_{i=1}^{q-1} \binom{2i}{i} \left(\frac{\alpha}{4}\right)^i x^i \tag{53}$$

where q denotes the maximal number of the repetitions of the information bits of codes from the ensemble of IRA2 codes, $0 < \alpha < 1$, and K is a scaling factor so that $\sum_{i=2}^{q} \lambda_i = 1$. We note that the degree distribution in Eq. (53) satisfies the condition in Eq. (16) which ensures vanishing bit erasure probability under MPI decoding, as the number of iterations tends to infinity. The puncturing rates of the information bits and of the parity bits, and the parameters α and q in Eq. (53) are chosen to achieve a fraction $1 - \varepsilon$ of the channel capacity with vanishing bit erasure probability under MPI decoding. Then, it can be proved that this choice of a degree distribution enables the IRA2 ensemble to achieve capacity, and the encoding/ decoding complexity with MPI decoding scales like $O\left(\frac{1}{\varepsilon}\right)$. The upper bound on the complexity of the IRA2 ensemble is of secondary importance, since we proved in Section 4.2 that the encoding and decoding complexity of the IRA1 ensemble is superior as it behaves like $O\left(\ln \frac{1}{\varepsilon}\right)$. We wish to emphasize in this section that for the ensemble of IRA2 codes which also achieves the capacity of the BEC with MPI decoding, the complexity behaves at least like the inverse square root of the gap to capacity (and not like the negative logarithm of the gap to capacity, as is the case with the ensemble of IRA1 codes).

5 Numerical Results

In this section, we present numerical results for the upper and lower bounds on the complexity of IRA1 (i.e., systematic IRA) codes whose transmission takes place over a BEC and the codes are iteratively decoded with the MPI decoding algorithm (see Theorems 1 and 2 in Section 2).

The left plot of Fig. 2 shows the coefficients K_3 and K_4 of the upper bound (4) on the complexity of IRA1 codes. Though these coefficients can be made in general to be independent of the gap ε to capacity (see Eq. (A.6) in Appendix A.4), we show in the left plot of Fig. 2 the tighter version of K_3 in (A.7) which corresponds to the case of vanishing gap between the channel capacity and the achievable rate (i.e., K_3 refers to the case where $\varepsilon \rightarrow 0$). The left plot of Fig. 2 refers to Eqs. (A.6) and (A.7) where we determine η in Eq. (A.6) to be $\eta = \frac{p^3}{2}$, and p designates the bit-erasure probability of the BEC. In the left plot of Fig. 2, the latter choice for η appears to suggest a good tradeoff between the coefficients K_3 and K_4 in the upper bound (4). We note that in the first extreme case where we let η tend to zero, the positive logarithmic coefficient K_4 in (4) is minimized, but the coefficient K_3 in this upper bound tends to infinity (so this upper bound on the complexity tends to infinity if $\eta \rightarrow 0$). On the other hand, in the second extreme case where we choose η to be close to $\frac{p}{2}$ (since η in Eq. (A.6) should be in the interval $(0, \frac{p}{2})$), then the coefficient K_4 in the upper bound (4) tends to infinity and K_3 is minimized, so also in this case, the upper bound (4) tends to infinity. For values of ε which are close to zero (i.e., for capacity-approaching ensembles of IRA1 codes under MPI decoding), the choice $\eta = \frac{p^3}{2}$ in (A.7) yields a reasonable balance between the two coefficients in (4). The right plot in Fig. 2 shows the ratio $\frac{K_4}{K_2}$ where K_2 and K_4 are the coefficients of the logarithms in the lower and upper bounds on the complexity of the IRA1 ensemble, respectively (see Eqs. (1), (2), (4), and (A.6)). The coefficients K_2 and K_4 dominate the behavior of these bounds in the limit where the IRA1 ensemble achieves the capacity of the BEC (i.e., if $\varepsilon \rightarrow 0$). The right plot corresponds to the same case where $\eta = \frac{p^3}{2}$ in Eq. (A.6). It is shown in the right plot that the ratio $\frac{K_4}{K_2}$ gets moderate values unless p is close to unity (referring to the catastrophic case where the probability of bit-erasure of the BEC is very high, and hence the capacity of the BEC is approximately zero).

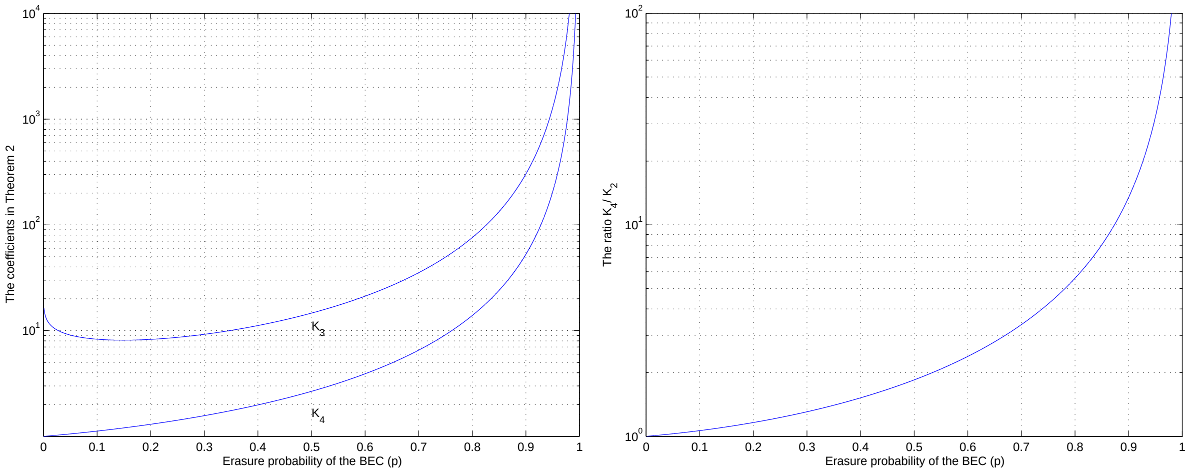

Figure 2: Numerical results for the coefficients of the bounds in Theorems 1 and 2 which correspond to IRA1 (i.e., systematic IRA) codes.

6 Discussion

- The encoding and the decoding complexity of systematic IRA codes scales like $O\left(\ln \frac{1}{\varepsilon}\right)$. This is in contrast to the complexity of the ensemble of IRA2 codes which for every choice of the degree distribution, it grows at least like the inverse square root of the gap to capacity, and at most like the inverse of the gap to capacity. The former result proves Conjecture 1 in [3], and the latter finding shows the existence of capacity-achieving ensembles of IRA codes whose complexity under MPI decoding is worse than a logarithmic behavior in ε (for any choice of the degree distribution.)

- On the BEC, a right-regular ensemble of LDPC codes yields asymptotically (in the limit where the block length tends to infinity) the optimal choice under MPI decoding with respect to the tradeoff between performance and complexity (see [6, 7, 8]). However, right-regular ensembles of systematic IRA codes may not be optimal, since their provable encoding and decoding complexity behave like $O\left(\frac{1}{\varepsilon}\right)$ (see Sections 3.4.2 and 3.6 in [4]), whereas this complexity behaves like $O\left(\ln \frac{1}{\varepsilon}\right)$ for the general IRA1 ensemble with the pair of degree distributions introduced in the proof of Theorem 2 (see Section 4.2).

- The probabilistic lower bound in Theorem 1 is similar to the information-theoretic bound which was presented in [7, Theorem 1]. In [7], Sason and Urbanke considered the question of how sparse can parity-check matrices of binary linear codes be, as a function of their gap (in rate) to capacity (where this gap depends on the channel and the decoding algorithm). If the code is represented by a standard Tanner graph *without state nodes*, the decoding complexity under MPI decoding is strongly linked to the density of the corresponding parity-check matrix (or alternatively, to the normalized number of edges in the graph per information bit). Consider a sequence of binary linear codes whose transmission takes place over a memoryless symmetric channel, and assume that it achieves a fraction $1 - \varepsilon$ of the channel capacity with vanishing bit error probability. By information-theoretic tools, it was proved in [7, Theorem 1] that for every such sequence of codes and for every sequence of parity-check matrices which represent these codes, the asymptotic density of these parity-check matrices grows at least like $\frac{K_1 + K_2 \ln \frac{1}{\varepsilon}}{1-\varepsilon}$ where the coefficients K_1 and K_2 only depend on the channel (this information-theoretic bound is valid under ML decoding, and hence, it is valid under every sub-optimal decoding algorithm). The information nodes and the parity nodes of systematic IRA codes can be clearly viewed as the variable nodes in the representation of this ensemble by a bipartite graph (see Fig. 1). It then follows from the proof in Section 4.1 that the density evolution equation (8) for systematic IRA codes does not yield any inherent degradation in the tradeoff between performance and complexity as compared to the information-theoretic lower bound in [7, Theorem 1] (since the coefficients K_1 and K_2 in Section 4.1 coincide in both cases).

- A recent work of Pfister, Sason and Urbanke [9] presents two sequences of ensembles of non-systematic IRA codes which asymptotically (as the block length tends to infinity) achieve capacity on the BEC *with bounded complexity.* The new bounded complexity result is achieved by allowing a sufficient number of state nodes in the Tanner graph representing the codes. This observation indicates the significance of state nodes in a Tanner graph which can considerably reduce the complexity of capacity-achieving ensembles of codes on graphs under MPI decoding.

Acknowledgment

The authors wish to thank Aamod Khandekar for providing them his Ph.D. dissertation [4], and the anonymous reviewers for their comments on an earlier version of this paper. The authors thank the associate editor Simon Litsyn for handling their paper.

Appendix A
Proofs of Lemmas 1–3 in Section 4.2

A.1 Proof of Lemma 1

Based on Eq. (31), it is sufficient to show that the inverse of the function

$$y(z) = 1 - \left(\frac{1-p}{1-p(1-z)}\right)^2 (1-z)$$

has a power series expansion with non-negative coefficients around $y = 0$, and the inverse of the function

$$z(x) = 1 - \frac{e^{-\alpha x} - e^{-\alpha}}{1 - e^{-\alpha}} \tag{A.1}$$

has a power series expansion with non-negative coefficients around $z = 0$. The former statement was proved in Appendix B of [4] (see Theorem B.2 in pp. 94–96), and the latter statement follows from Eq. (A.1) since

$$\begin{aligned} x &= -\frac{1}{\alpha}\,\ln\bigl(1 - z(1-e^{-\alpha})\bigr) \\ &= \sum_{n=1}^{\infty} \frac{(1-e^{-\alpha})^n\, z^n}{n\alpha} \end{aligned}$$

so for $\alpha > 0$, the latter power series expansion has positive coefficients around $z = 0$. It follows therefore that the power series expansion of

$$g_p(x) = z^{-1}\bigl(y^{-1}(x)\bigr)$$

has non-negative coefficients around $x = 0$. Since it was shown in [4] that the coefficients of the power series of the inverse of $y(\cdot)$ are positive around $y = 0$ (except of the free coefficient of this power series expansion which is zero), then the coefficients of the power series expansion of the function $g_p(x)$ around $x = 0$ are also positive (except of the free coefficient of the power series expansion of $g_p(\cdot)$ which is zero).

A.2 Proof of Lemma 2

For $x \in (0,1)$

$$\begin{aligned} g_p(x) &= \sum_{i=1}^{\infty} g_{p,i} x^i \\ &> \sum_{i=1}^{N} g_{p,i} x^i \\ &\geq \sum_{i=1}^{N} g_{p,i}\, x^N > p x^N \end{aligned}$$

where the last transition follows from Eq. (34), so $N > \frac{\ln\left(\frac{p}{g_p(x)}\right)}{\ln\left(\frac{1}{x}\right)}$. Substituting $h_p(x)$ for x in the latter inequality gives

$$N > \frac{\ln\left(\frac{p}{x}\right)}{\ln\left(\frac{1}{h_p(x)}\right)}\,. \tag{A.2}$$

Since $\alpha > 0$ and $x \in (0,1)$, then $\frac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}} < 1$. From Eq. (31) and the latter inequality, it follows that $h_p(x) > 1 - \frac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}}$, and for $\alpha > 0$ and $x \in (0,1)$

$$\begin{aligned}
\ln\left(\tfrac{1}{h_p(x)}\right) &< -\ln\left(1 - \tfrac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}}\right) \\
&= \sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}}\right)^n \\
&< \sum_{n=1}^{\infty} \left(\frac{e^{-\alpha x}-e^{-\alpha}}{1-e^{-\alpha}}\right)^n \\
&= \tfrac{1-e^{-\alpha(1-x)}}{e^{\alpha x}-1} \\
&< \tfrac{1}{e^{\alpha x}-1}.
\end{aligned}$$

Eq. (38) follows from Eq. (A.2) and the latter result, so if we choose $x \in (0,p)$, then we obtain that N grows faster than a positive constant times $e^{\alpha x}$.

A.3 Proof of Lemma 3

Based on Eq. (37)

$$\begin{aligned}
\frac{\alpha}{1-e^{-\alpha}} \int_0^1 g_p(x)\,\mathrm{d}x &= (1-p)^2 \int_0^1 \frac{1}{(1-pu)^2}\,\frac{u}{e^{-\alpha}+u(1-e^{-\alpha})}\,\mathrm{d}u \\
&= (1-p)^2 \int_0^1 \frac{1}{(1-pu)^2}\left(1 - \frac{e^{-\alpha}(1-u)}{e^{-\alpha}+u(1-e^{-\alpha})}\right)\mathrm{d}u \\
&= (1-p)^2 \int_0^1 \frac{\mathrm{d}u}{(1-pu)^2} - (1-p)^2 e^{-\alpha} \int_0^1 \frac{1-u}{e^{-\alpha}+u(1-e^{-\alpha})}\,\frac{\mathrm{d}u}{(1-pu)^2} \\
&= 1-p-(1-p)^2 e^{-\alpha} \int_0^1 \frac{1-u}{e^{-\alpha}+u(1-e^{-\alpha})}\,\frac{\mathrm{d}u}{(1-pu)^2}
\end{aligned} \tag{A.3}$$

Straightforward calculation shows that

$$\int_0^1 \frac{1-u}{e^{-\alpha}+u(1-e^{-\alpha})}\,\frac{\mathrm{d}u}{(1-pu)^2} = \frac{\alpha - 1 + (1-p)e^{-\alpha} + \ln\left(\frac{1}{1-p}\right)}{\left(1-(1-p)e^{-\alpha}\right)^2}$$

so for $\alpha > \max\left(\ln 2, \ln\left(\frac{1}{1-p}\right)\right)$ we obtain that

$$\begin{aligned}
\int_0^1 \frac{1-u}{e^{-\alpha}+u(1-e^{-\alpha})}\,\frac{\mathrm{d}u}{(1-pu)^2} &< \frac{\alpha + \ln\left(\frac{1}{1-p}\right)}{\left(1-(1-p)e^{-\alpha}\right)^2} \\
&< \frac{\alpha + \ln\left(\frac{1}{1-p}\right)}{\left(1-\frac{1-p}{2}\right)^2} \\
&< \frac{8\alpha}{(1+p)^2}\,.
\end{aligned}$$

Eq. (40) follows from Eq. (A.3) and the latter result.

A.4 Derivation of the coefficients K_3 and K_4 in Eq. (4)

From Eq. (46), it follows that

$$\ln\left(\frac{c}{\varepsilon}\right) < \alpha < \frac{\ln\left(\frac{c}{\varepsilon}\right)}{p-2\eta} + m \tag{A.4}$$

where m is defined to be

$$m \triangleq \max\left(\frac{2}{\eta}\ln\left(\frac{1}{\eta}\right), \ln\left(\frac{1}{1-p}\right), \ln 2\right) \tag{A.5}$$

and the upper bound on α in Eq. (A.4) follows from Eq. (46) since the maximal value of some positive numbers is smaller than their sum (we note that from Eq. (45), it follows that $c > 1$ and since $0 < \varepsilon < 1$, then α in (46) is expressed as a maximum of positive numbers).

If a fraction $1-\varepsilon$ of the capacity of a BEC (whose erasure probability is p) is achieved for the IRA1 ensemble with vanishing bit erasure probability under MPI decoding, then from Eq. (47)

$$\begin{aligned}
\chi_E(\varepsilon, \text{IRA1}), \chi_D(\varepsilon, \text{IRA1}) &= \frac{p+\varepsilon(1-p)}{(1-p)(1-\varepsilon)}\left(\frac{\alpha}{1-e^{-\alpha}}+2\right)\\
&< \frac{p+\varepsilon(1-p)}{(1-p)(1-\varepsilon)}\left(\frac{\frac{1}{p-2\eta}\ln\left(\frac{c}{\varepsilon}\right)+m}{1-\frac{\varepsilon}{c}}+2\right)\\
&= \frac{p+\varepsilon(1-p)}{(1-p)(1-\varepsilon)}\left(\frac{\ln\left(\frac{c}{\varepsilon}\right)}{p-2\eta}+m+\frac{1}{p-2\eta}\,\frac{1}{1-\frac{\varepsilon}{c}}\,\frac{\varepsilon}{c}\ln\left(\frac{c}{\varepsilon}\right)+\frac{m\varepsilon}{c-\varepsilon}+2\right)\\
&\overset{\text{(a)}}{\leq} \frac{p+\varepsilon(1-p)}{(1-p)(1-\varepsilon)}\left(\frac{\ln\left(\frac{c}{\varepsilon}\right)}{p-2\eta}+m+\frac{1}{p-2\eta}\,\frac{1}{e}\,\frac{1}{1-\frac{\varepsilon}{c}}+\frac{m\varepsilon}{c-\varepsilon}+2\right)\\
&\overset{\text{(b)}}{<} \frac{p+\varepsilon(1-p)}{(1-p)(1-\varepsilon)}\left(\frac{\ln\left(\frac{c}{\varepsilon}\right)}{p-2\eta}+m+\frac{\frac{1}{p-2\eta}\,\frac{c}{e}+m}{c-1}+2\right)\\
&\overset{\text{(c)}}{\leq} \frac{p\ln\left(\frac{c}{\varepsilon}\right)+(1-p)(\varepsilon\ln c+\frac{1}{e})}{(p-2\eta)(1-p)(1-\varepsilon)}+\\
&\qquad \frac{p+\varepsilon(1-p)}{(1-p)(1-\varepsilon)}\left(m+\frac{\frac{c}{e(p-2\eta)}+m}{c-1}+2\right).
\end{aligned}$$

We note that inequalities (a) and (c) are based on the inequality $x\ln(\frac{1}{x}) \leq \frac{1}{e}$ for $0 < x < 1$ (equality is achieved for $x = \frac{1}{e}$). Inequality (b) follows from Eq. (45) which yields that $c > \frac{4}{\ln 2}$ (and therefore $c > 1$). Based on the calculations above, it is possible to choose K_3 and K_4 in Eq. (4) to be independent of ε, e.g.,

$$K_3 = \frac{\ln c}{1-p}\,\frac{p}{p-2\eta}+\frac{\ln c+\frac{1}{e}}{p-2\eta}+\frac{1}{1-p}\left(\frac{mc}{c-1}+\frac{1}{e(p-2\eta)}\frac{c}{c-1}+2\right), \quad K_4 = \frac{1}{1-p}\frac{p}{p-2\eta} \tag{A.6}$$

where $\eta \in (0, \frac{p}{2})$ is arbitrary, and c and m are defined in Eqs. (45) and (A.5), respectively. From the calculations above, it is also clear that in the limit where the gap to capacity vanishes (i.e.,

$\varepsilon \to 0$), one can improve K_3 in (A.6) by reducing its value to

$$K_3 = \frac{\ln c}{1-p} \, \frac{p}{p-2\eta} + \frac{2p}{1-p}. \tag{A.7}$$

References

[1] D. Divsalar, H. Jin and R. J. McEliece, "Coding theorems for turbo-like codes," *Proceedings of the 36th Allerton Conference on Communications, Control and Computing*, Allerton, Illinois, pp. 201–210, September 1998.

[2] H. Jin, A. Khandekar and R. J. McEliece, "Irregular repeat-accumulate codes," *Proceedings of the Second International Symposium on Turbo Codes and Related Topics*, pp. 1–8, Brest, France, September 2000. [Online]. Available: http://www.systems.caltech.edu/EE/Faculty/rjm.

[3] A. Khandekar and R. J. McEliece, "On the complexity of reliable communication on the erasure channel," *Proceedings 2001 IEEE International Symposium on Information Theory (ISIT2001)*, p. 1, Washington, D.C., USA, June 2001.

[4] A. Khandekar, *Graph-based codes and iterative decoding*, Ph.D. dissertation, California Institute of Technology, Pasadena, California, USA, June 2002. [Online]. Available: http://etd.caltech.edu/etd/available/etd-06202002-170522/

[5] R. J. McEliece, "Achieving the Shannon limit: A progress report," plenary talk given at the *38th Annual Allerton Conference on Communication, Control and Computing*, Allerton, Illinois, USA, October 5, 2000. [Online]. Available: http://www.systems.caltech.edu/EE/Faculty/rjm.

[6] P. Oswald and A. Shokrollahi, "Capacity achieving sequences for the erasure channel," *IEEE Trans. on Information Theory*, vol. 48, no. 12, pp. 3017–3028, December 2002.

[7] I. Sason and R. Urbanke, "Parity-check density versus performance of binary linear block codes over memoryless symmetric channels," *IEEE Trans. on Information Theory*, vol. 49, no. 7, pp. 1611–1635, July 2003.

[8] A. Shokrollahi, "New sequences of time erasure codes approaching channel capacity," *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lectures Notes in Computer Science 1719, Springer Verlag, pp. 65–76, 1999.

[9] H. Pfister, I. Sason and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity," *Proceedings of the 2004 IEEE International Symposium on Information Theory*, Chicago, Illinois, USA, June 27–July 2, 2004.