Bounds on Achievable Rates of LDPC Codes Used Over the Binary Erasure Channel [*†]

Ohad Barak, David Burshtein and Meir Feder

School of Electrical Engineering

Tel-Aviv University

Tel-Aviv 69978, Israel

Abstract

We derive upper bounds on the maximum achievable rate of low-density parity-check (LDPC) codes used over the binary erasure channel (BEC) under Gallager's decoding algorithm, given their right-degree distribution. We demonstrate the bounds on the ensemble of right-regular LDPC codes and compare them with an explicit left-degree distribution constructed from the given right-degree.

Index Terms - Low-density parity-check (LDPC) codes, Binary erasure channel (BEC), Iterative decoding.

I Introduction

Low-density parity-check (LDPC) codes were invented by Gallager in 1963 [1], but were relatively ignored for three decades. Their revival started when they were rediscovered in the mid 90's, and since then they have attracted a great deal of interest. The binary erasure channel (BEC),

[*]To be published, IEEE Transactions on Information Theory, vol. 50, no. 10, October 2004 (submitted July 2002, revised July 2004)

[†]This research was supported by the Israel Science Foundation, grant No. 22/01-1.

presented by Elias [2] already in 1955, has lately become increasingly popular, as it may be used to model communication via packet-loss networks, such as the Internet. Luby *et. al.* [3] suggested an iterative algorithm for decoding LDPC codes over the BEC and showed that the proposed scheme can approach channel capacity arbitrarily close. This algorithm is Gallager's soft decoding algorithm [1] when applied to the BEC.

Throughout the paper we shall consider irregular LDPC codes with left, right edge-degree distribution polynomials

$$\lambda(x) = \sum_{i=l_{min}}^{l_{max}} \lambda_i x^{i-1} \qquad , \qquad \rho(x) = \sum_{i=r_{min}}^{r_{max}} \rho_i x^{i-1}$$

respectively, where λ_i (ρ_i) is the fraction of edges in the bipartite graph that have left (right) degree i. The same code profile may alternatively be described in terms of node-degree distribution (the degree distribution from the *node* perspective). The left, right node-degree distribution polynomials are

$$\tilde{\lambda}(x) = \sum_{i=l_{min}}^{l_{max}} \tilde{\lambda}_i x^{i} \qquad , \qquad \tilde{\rho}(x) = \sum_{i=r_{min}}^{r_{max}} \tilde{\rho}_i x^{i}$$

respectively, where $\tilde{\lambda}_i$ ($\tilde{\rho}_i$) is the fraction of left (right) nodes in the bipartite graph that have degree i.

We denote the number of left (variable) nodes by n and the number of right (check) nodes by $n-k$. The designed rate of the code is

$$R \triangleq \frac{k}{n} = 1 - \frac{\int \rho}{\int \lambda} \tag{1}$$

where $\int \lambda \triangleq \int_0^1 \lambda(x)dx = \sum_i \frac{\lambda_i}{i}$, and $\int \rho \triangleq \int_0^1 \rho(x)dx = \sum_i \frac{\rho_i}{i}$.

We shall also consider a BEC with the input X taking values from $\{0,1\}$ and the output Y taking values from $\{0,\varepsilon,1\}$. Let the loss fraction (probability of erasure) be δ, thus $P\{Y=\varepsilon \,|\, X=0\} = P\{Y=\varepsilon \mid X=1\} = \delta$ and $P\{Y=X\} = 1-\delta$.

The LDPC code is transmitted over the BEC, and is iteratively decoded using Gallager's soft-decoding message-passing algorithm, also named belief-propagation (which for the BEC assumes a particularly simple form described, for instance, in [4, 3]). It has been shown [3] that the belief-propagation decoding scheme can correct a δ fraction of erasures (losses) in the channel if and

only if

$$\delta\lambda(1-\rho(1-x)) < x \qquad \forall \qquad x \in (0,1] \ . \tag{2}$$

This inequality shall henceforth be called the *successful decoding condition*.

The paper is organized as follows. In Section II we derive a measure for how close the rate of an LDPC code is to the capacity of the worst BEC over which the code is successfully decodable, given some right-degree distribution. In Section III we use this measure to derive the zero-order bound on the maximal fraction of errors δ that can be corrected by a rate R LDPC, with a given $\rho(x)$. This bound has already been shown before [5, Theorem 1]. In Section IV we derive the first-order bound which always improves the zero-order bound. In Section V we derive the second-order bound, which is sometimes better than the first-order bound. In Section VI we demonstrate the bounds on the ensemble of right-regular codes, and compare them to the achievable rate of an actual code sequence. Section VII concludes the paper.

II How close is the code rate to capacity?

In this section we show the relation between the fulfillment of the successful decoding condition and a limit on the code rate. We start with the following lemma:

Lemma 1 *For any LDPC code characterized by degree distributions $\lambda(x)$ and $\rho(x)$ and rate $R = 1 - \frac{\int\rho}{\int\lambda}$, given a BEC with erasure probability δ, and having the function $f(x)$ defined such that*

$$f(x) = \frac{1-\rho^{-1}(1-x)}{\delta} - \lambda(x). \tag{3}$$

Then:

$$\frac{1}{1-C} - \frac{1}{1-R} = a_r \int_0^1 f(x)dx \tag{4}$$

where $\rho^{-1}(\cdot)$ is the inverse function of $\rho(\cdot)$, $a_r \triangleq 1/\int\rho$ is the average degree of right (check) nodes and $C \triangleq 1-\delta$ is the capacity of the channel.

Proof: Note that since $\lambda(x)$ and $\rho(x)$ are both polynomials with non-negative coefficients that sum to one (and they are not constant), they are strictly monotonically increasing functions of

x for $0 \leq x \leq 1$. Hence they are both invertible over the above range [3]. In addition, they both equal to 0 for $x = 0$, and to 1 for $x = 1$.

We define $z \stackrel{\Delta}{=} \rho^{-1}(1-x)$ or, equivalently, $\rho(z) = 1 - x$. Thus $\frac{d\rho(z)}{dz} = -\frac{dx}{dz}$. We get

$$\begin{aligned} \int_0^1 1 - \rho^{-1}(1-x)dx &= 1 + \int_1^0 z\frac{d\rho(z)}{dz}dz \\ &= 1 + [z\rho(z)]_1^0 - \int_1^0 \rho(z)dz \\ &= \int \rho \ . \end{aligned} \tag{5}$$

Integrating (3) over $[0, 1]$ and substituting (5) and (1) results in

$$\int_0^1 f(x)dx = \frac{\int \rho}{\delta} - \int \lambda = \int \rho \left[\frac{1}{1-C} - \frac{1}{1-R}\right] \tag{6}$$

thus proving the lemma. □

Implication: From this lemma we can derive a measure of how close the rate of the code is to the capacity of the worst BEC for which the code is successfully decodable. This measure is in terms of the average degree of check (right) nodes a_r and of the function $f(x)$ we have defined here. Note that defining a new variable $x \stackrel{\Delta}{=} 1 - \rho(1-\hat{x})$ and substituting it into the successful decoding condition, $\lambda(1-\rho(1-\hat{x})) < \frac{\hat{x}}{\delta}$, yields

$$\lambda(x) < \frac{1 - \rho^{-1}(1-x)}{\delta} \qquad \forall \qquad 0 < x \leq 1 \ . \tag{7}$$

First we see from (7) that for a successfully decodable code, $f(x)$ is positive over the range $[0, 1]$, verifying that the rate must be less than the capacity. But in addition, any upper bound on $\int_0^1 f(x)dx$ provides an upper bound on the maximal fraction of errors that can be corrected, and we see that the closer the non-negative integral $\int_0^1 f(x)dx$ is to zero, the closer the rate R is to the capacity C.

Consider the following design problem. We wish to design a code so as to maximize its rate R subject to the requirement that it should be successfully decodable for a BEC with erasure probability δ. Thus, given the right-degree distribution $\rho(x)$, it is desired to find a left-degree distribution $\lambda(x)$ so that the integral of $f(x)$ over the range $[0, 1]$ is minimized, subject to (7). The smaller this integral is, the higher the achievable code rate is. In the sequel we shall see that these constraints on $\lambda(x)$ limit the maximum achievable rate away from the channel capacity even farther than has been stated thus far.

III The zero-order bound

Theorem 1 ***(The zero-order bound) [5, Theorem 1]*** *The rate of an LDPC code with a fixed right edge-degree distribution $\rho(\cdot)$, which is successfully decodable under iterative decoding over a BEC with an erasure probability δ, never exceeds the following upper bounds:*

1. *The simple bound*

$$R \leq 1 - \frac{\delta}{1-(1-\delta)^{a_r}} \tag{8}$$

2. *The tighter bound*

$$R \leq 1 - \frac{\delta}{1-\tilde{\rho}(1-\delta)} \tag{9}$$

where $\tilde{\rho}(\cdot)$ is the corresponding right node-degree distribution.

In general, the idea behind the zero-order bound is based on the fact that the expression $\frac{1}{\delta}(1-\rho^{-1}(1-x))$ is greater than 1 for some interval near $x=1$, while $\lambda(x) \leq 1$. Hence calculating the area of this specific part that exceeds 1 renders a value by which $\frac{1}{1-R}$ is bounded away from $\frac{1}{1-C}$. In Figure 1 we illustrate this value by the painted region. The complete proof of these bounds is deferred to Appendix A.

We note that Burshtein *et. al.* [6] presented an upper-bound on the achievable rate of LDPC codes over a *general* binary-input symmetric-output channel under maximum likelihood (ML) decoding. Let $X \in \{0,1\}$ denote the channel input, let Y denote the channel output, and let $\phi(y) \triangleq P(Y=y \mid X=1) = P(Y=-y \mid X=0)$. They defined a *crossover probability* ϵ of the channel (the probability of estimation error in optimal decoding)

$$\epsilon \triangleq \frac{1}{2}\int_{-\infty}^{\infty} \min(\phi(y), \phi(-y))dy \ ,$$

and proved that for a right-regular code with right node-degree $d = D+1$, the rate is bounded as follows

$$R \leq 1 - \frac{1-C}{h(\epsilon_d)}$$

where $\epsilon_d = \frac{1}{2}(1-(1-2\epsilon)^d)$ and $h(\cdot)$ is the binary entropy function. Applying this bound to the specific case of BEC with loss-fraction δ, we substitute $\delta/2$ for the crossover probability ϵ

and thus have $\epsilon_d = \frac{1}{2}(1-(1-\delta)^d)$, hence setting $\tilde{\rho}(x) = x^d$ in the *zero-order bound* (9) yields $R \leq 1 - \frac{1-C}{2\epsilon_d}$. Recalling that $h(x) \geq 2x$ in $[0, \frac{1}{2}]$, the zero-order bound is tighter than the one stated in [6] . This is not surprising as it considers iterative decoding and not ML decoding and as it only considers the special case of transmitting over a BEC. Recently, it has been shown in [7] that the zero-order bound also applies to ML decoding over the BEC and is valid for *every* particular code with the given (right) profile. This result does not necessarily apply to the new bounds we present in Section IV and in Section V.

IV The first-order bound

The zero-order bound is actually not new. Shokrollahi proved a completely equivalent inequality [5, Theorem 1]. Our approach differs however from the one given in that paper, and it enables us to tighten the bound. We start by asserting a few auxiliary lemmas.

Lemma 2 *Let $\rho(\cdot)$ be a right degree distribution, let $\rho^{-1}(\cdot)$ be its inverse function, and let*

$$y(x) \triangleq \frac{1-\rho^{-1}(1-x)}{\delta} \ . \tag{10}$$

Then both $y(x)$ and $\frac{dy}{dx}$ are monotonically increasing.

Proof: Defining $\hat{y} \triangleq \delta y$, we write

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

and differentiate it with respect to x

$$1 = \frac{d\hat{y}}{dx} \cdot \sum_{i \geq 2} (i-1)\rho_i (1-\hat{y})^{i-2}.$$

Recalling that ρ_i are all non-negative and that they sum to 1 (therefore at least one of them is strictly positive) we conclude that $\frac{dy}{dx}$ is strictly positive over the range $(0,1)$. Differentiating the expression once again, we obtain

$$0 = \frac{d^2\hat{y}}{dx^2} \cdot \sum_{i \geq 2} (i-1)\rho_i (1-\hat{y})^{i-2} - \left(\frac{d\hat{y}}{dx}\right)^2 \cdot \sum_{i \geq 3} (i-1)(i-2)\rho_i (1-\hat{y})^{i-3}.$$

Having proved that $\frac{d\hat{y}}{dx}$ is strictly positive, we conclude that $\frac{d^2y}{dx^2}$ is also strictly positive over $(0,1)$. □

Lemma 3 *Let $y(x)$ be defined as in Lemma 2 with $0 < \delta < 1$. Suppose that $\left.\frac{dy}{dx}\right|_{x=0} < 1$. Then there exists exactly one tangent to y that passes through the point $(1,1)$, and this tangent touches $y(x)$ within the range $(0,1)$.*

Proof: We recall that $y(0) = 0$ and that $y(1) > 1$. Given that it is convex $\cup$ (Lemma 2) and that its slope is less than 1 at $x = 0$ it is easy to see that there exists a unique tangent to $y(x)$ that passes through $(1,1)$, and that the tangent point lies within the relevant interval $(0,1)$. □

Notes pertaining to finding the tangent point in Lemma 3 can be found in Appendix B.

Lemma 2 and Lemma 3 allow us to state a tighter bound on the achievable rate:

Theorem 2 ***(The first-order bound)*** *For any LDPC code successfully decodable under iterative decoding over a BEC with erasure probability δ, if the first derivative of $y(x)$ (as defined in Lemma 2) at $x = 0$ is less than 1, then the code rate R is bounded as follows.*

1. *The simple bound*
$$R \leq 1 - \frac{\delta}{1 - (1 - \delta y_a)^{a_r} + \delta a_r \frac{(1-y_a)(1-x_a)}{2}} \ . \tag{11}$$
2. *The tighter bound*
$$R \leq 1 - \frac{\delta}{1 - \tilde{\rho}(1 - \delta y_a) + \delta a_r \frac{(1-y_a)(1-x_a)}{2}} \tag{12}$$

where (x_a, y_a) is the tangent point defined in Lemma 3, and a_r is the average right degree $1/\int \rho$.

Proof: We denote by $a(x)$ the tangent line defined in Lemma 3.

$$a(x) = \frac{1 - y_a}{1 - x_a} x + \frac{y_a - x_a}{1 - x_a} \ .$$

We recall that $\lambda(x)$ is convex $\cup$ for $x \in (0,1)$. In addition, $\lambda(1) = 1$ and $\lambda(x_a) < y_a$. We conclude that $\lambda(x) < a(x)$ for $x \in [x_a, 1)$.

Recalling (3), we obtain

$$f(x) \geq \frac{1-\rho^{-1}(1-x)}{\delta} - a(x) \qquad \forall \qquad x_a \leq x \leq 1 \ .$$

Thus we have

$$\begin{aligned} \int_0^1 f(x)dx &\geq \int_{x_a}^1 \left[\frac{1-\rho^{-1}(1-x)}{\delta} - \frac{(1-y_a)x + (y_a - x_a)}{1-x_a} \right] dx \\ &\stackrel{(a)}{=} (1-x_a)y_a + \tilde{\rho}(\rho^{-1}(1-x_a)) \frac{\int \rho}{\delta} - \frac{(1-x_a)(1+y_a)}{2} \\ &= \frac{1}{\delta}\tilde{\rho}(1-\delta y_a) \int \rho - \frac{1}{2}(1-x_a)(1-y_a) \end{aligned}$$

where (a) follows by (20) in Appendix A.

The tighter bound (12) now follows from Lemma 1 after rewriting (4) as

$$R = 1 - \frac{1}{\frac{1}{\delta} - a_r \int_0^1 f(x)dx} \ , \tag{13}$$

whereas the simple bound (11) then follows from (21) in Appendix A. □

Note that the above expressions hold for *any* (x_a, y_a) on the curve $y(x)$. Thus it is easy to see that the zero-order bound is a special case of the first-order bound, when $y_a = 1$. However, (x_a, y_a) is chosen to be the above mentioned *tangent point* in order to obtain the *tightest* bound on R. It is easy to see that this bound necessarily improves on the zero-order bound.

The painted area in Figure 2 denotes the difference in our bound to $\int_0^1 f(x)dx$ between the zero-order and the first-order bounds.

Note: In the last theorem, we excluded the case in which the first derivative of $y(x)$ is at least 1. In this case, simply choosing $\lambda(x) = x$ meets the condition for successful decoding (7). As this choice maximizes $\int \lambda$ given the fixed right-degree distribution $\rho(x)$, this yields the highest code rate possible, which renders in this case $R = 1 - \frac{\int \rho}{\int \lambda} = 1 - 2\int \rho$. From a design point of view this is not an interesting case, and the consequent code will tolerate a higher erasure probability than the considered one δ. Practically, it means that $\rho(x)$ has been chosen ineffectively as it is not suited to the relatively low value of δ, hence it could have been chosen such that the achievable rate would have been higher and closer to the capacity. This can also be seen as follows. It is easy to verify that $\left.\frac{dy}{dx}\right|_{x=0} = \frac{1}{\delta \cdot \rho'(1)}$. On the other hand, the stability condition [8], which is a

necessary condition for successful iterative decoding states that $\lambda'(0)\rho'(1) < \frac{1}{\delta}$ should hold. It is also known [8] that for any sequence of capacity-achieving degree distributions over the BEC, the stability condition becomes tight. Thus as $\lambda'(0) < 1$ for these capacity-achieving ensembles, $\frac{dy}{dx}\Big|_{x=0} \to \lambda'(0) < 1$.

V The second-order bound

Before stating the *second-order bound*, we need the following lemma.

Lemma 4 *Let $\lambda(x), \rho(x)$ be the degree distributions of an LDPC code used over a BEC. Let $a \stackrel{\Delta}{=} \frac{d}{dx} y(x)\Big|_{x=0}$ (where $y(x)$ is defined above). Suppose that $a < 1$ and that the code is successfully decodable for a BEC with erasure-probability δ. Let $b(x) \stackrel{\Delta}{=} ax + (1-a)x^2$. Then*

$$\lambda(x) \leq b(x) \qquad \forall \qquad x \in [0,1] \ .$$

Proof: We prove the lemma by contradiction. Let us assume that the statement of the lemma does not hold. Thus there exists some point $x_0 \in (0,1)$ such that

$$\lambda(x_0) > b(x_0) \ .$$

We recall that $\lambda(0) = b(0) = 0$ and that $\lambda(1) = b(1) = 1$. Hence there exist $x_1 \in (0, x_0)$ and $x_2 \in (x_0, 1)$ such that

$$\lambda'(x_1) > b'(x_1) \qquad , \qquad \lambda'(x_2) < b'(x_2) \ . \tag{14}$$

The derivative of the parabola $b(x)$ is the straight line

$$b'(x) = a + 2(1-a)x \ .$$

As $\lambda'(0) \leq a$ (the stability condition, [5, 8]), we have that

$$\lambda'(0) \leq b'(0) \ . \tag{15}$$

Recalling that all the derivatives of $\lambda(x)$ are positive, monotonically increasing and convex $\cup$ in $(0,1]$, the following must hold

$$\lambda'(x_1) \stackrel{(a)}{=} \lambda'(\alpha x_2)$$

$$\begin{aligned} &\overset{(b)}{\leq} && \alpha\lambda'(x_2) + (1-\alpha)\lambda'(0) \\ &\overset{(c)}{\leq} && \alpha b'(x_2) + (1-\alpha)b'(0) \\ &\overset{(d)}{=} && b'(\alpha x_2) = b'(x_1) \end{aligned}$$

where in (a) we defined $\alpha \triangleq \frac{x_1}{x_2} < 1$, (b) follows by the convexity of $\lambda'(x)$, (c) follows (14) and (15), and (d) holds as b'(x) is a straight line. This is impossible as it contradicts (14). □

Theorem 3 ***(The second-order bound)*** *Consider an LDPC code with left, right degree distribution $\lambda(x)$, $\rho(x)$, respectively, successfully decodable under iterative decoding over a BEC with erasure probability δ. Let $b(x)$ be the parabola defined in Lemma 4, and let x_b be the minimum value of $\hat{x}_b$ such that $b(x) \leq y(x) \ \forall \ x \in [\hat{x}_b, 1]$, where $y(x)$ is defined in Lemma 2. Let $a(x)$ be the tangent line defined in Lemma 3. We define $c(x)$ to be the convex envelope of $a(x)$ in the interval $[x_a, 1]$, and the parabola $b(x)$ in the interval $[x_b, 1]$. Suppose further that $\frac{dy}{dx}\Big|_{x=0} < 1$. Then*

$$R \leq 1 - \frac{\delta}{1 - \delta a_r \int_\alpha^1 f_b(x)} \tag{16}$$

where $f_b(x) \triangleq y(x) - c(x)$, $\alpha \triangleq \min(x_a, x_b)$ and a_r denotes the average right degree $1/\int \rho$.

Note: The existence of an interval $[x_b, 1]$ in which $b(x) \leq y(x)$ is guaranteed as $b(1) < y(1)$. The proof of the theorem follows from (13), recalling that $\lambda(x)$ is a convex function that satisfies both $\lambda(x) \leq b(x)$ and $\lambda(x) \leq a(x)$, and using the definition of a convex envelope (e.g. [9, p. 125]).

The painted area in Figure 3 denotes the difference in our bound to $\int_0^1 f(x)dx$ between the first-order and the second-order bounds.

It is not guaranteed that the second-order bound improves on the first-order bound. This depends on whether the parabola $b(x)$ is in some interval below $a(x)$. Otherwise, $c(x) = a(x)$ and the two bounds coincide. As we demonstrate in the next section, both cases are possible.

VI Examples: right-regular codes

We examined the behavior of these bounds with right-regular codes, and compared them to the rate achieved by some specific code profiles. The code profile we consider is a variant of the 'right-regular sequence' introduced in [5, 10].

For a given right-degree $d = D + 1$ (i.e., right generator polynomial $\rho(x) = x^D$) and erasure probability δ we set the left generator polynomial to

$$\lambda(x) = \sum_{i \leq I} a_i x^i + b x^{I+1} \tag{17}$$

where a_i are the first I Taylor coefficients of the function $\frac{1}{\delta}(1-(1-x)^{1/D})$ (which are all positive), I is the highest integer such that $\sum_{i=1}^{I} a_i \leq 1$ and b is set such that $\lambda(1) = 1$. The rate R can then be calculated by $R = 1 - \frac{\int \rho}{\int \lambda}$.

Since (2) can be written as $\lambda(x) < \frac{1}{\delta}(1 - \rho^{-1}(1-x)) \quad \forall x \in (0, 1]$, it can easily be seen that the above sequence meets this requirement by definition. It has been shown that the designed rate of this sequence approaches the capacity $1 - \delta$ for $D \to \infty$.

Figure 4 shows the maximum achievable rate of right-regular codes according to each of the bounds versus the right degree, for two values of the fraction-loss. The upper-bounds are also compared with the rate achieved by the code sequence defined in (17). The code sequence in (17) produced higher rates than the code sequence in [5].

The figure demonstrates that while all bounds approach the channel capacity $C = 1 - \delta$ for $D \to \infty$, the first-order bound is below the zero-order bound for all right degrees. We can also see that the second-order bound improves on the first-order bound only for small values of D (for larger values of D, where the second-order bound does not improve, we omitted it from the figure). One may figure out that the improvement of our new bounds on the previously known bound (the zero-order bound) is substantial for low right degrees, exactly where achievable rates are farthest from channel capacity, and that they are very close to the achievable rate of the code sequence defined in (17).

VII Conclusion

We derived improved upper bounds on the rate of LDPC codes used over the BEC under iterative decoding, for which reliable communication is achievable, given their right-degree distribution.

While our novel bounds are not provably tight, they are practically tight. This was demonstrated for several right-regular degree profiles, by showing that they are close to the rate of some

actual left-degree profile.

Appendices

A Proof of Theorem 1

The *node-perspective* left, right degree-distribution is the set $\{\tilde{\lambda}_i\}$, $\{\tilde{\rho}_i\}$, respectively, where

$$\tilde{\lambda}_i = \frac{\lambda_i/i}{\int \lambda} \quad ; \quad \tilde{\rho}_i = \frac{\rho_i/i}{\int \rho} \ , \tag{18}$$

or by means of the polynomials

$$\tilde{\lambda}(x) = \frac{\int_0^x \lambda(\hat{x})d\hat{x}}{\int \lambda} \quad ; \quad \tilde{\rho}(x) = \frac{\int_0^x \rho(\hat{x})d\hat{x}}{\int \rho}. \tag{19}$$

Claim: For any $0 < \alpha < 1$ and $\beta = \frac{1-\rho^{-1}(1-\alpha)}{\delta}$

$$\int_\alpha^1 \left[\frac{1-\rho^{-1}(1-x)}{\delta}\right] dx = (1-\alpha)\beta + \tilde{\rho}(\rho^{-1}(1-\alpha)) \cdot \frac{\int \rho}{\delta} \tag{20}$$

Proof: Let $z(x) = \rho^{-1}(1-x)$, thus $z(1) = 0$ and $\frac{dx}{dz} = -\frac{d\rho(z)}{dz}$. We obtain

$$\begin{aligned}
\int_\alpha^1 1-\rho^{-1}(1-x)dx &= 1-\alpha+\int_{\rho^{-1}(1-\alpha)}^0 z\frac{d\rho(z)}{dz}dz \\
&= 1-\alpha+z\rho(z)|_{\rho^{-1}(1-\alpha)}^0 + \int_0^{\rho^{-1}(1-\alpha)} \rho(z)dz \\
&\overset{(a)}{=} (1-\alpha)(1-\rho^{-1}(1-\alpha)) + \tilde{\rho}(\rho^{-1}(1-\alpha)) \cdot \int \rho
\end{aligned}$$

where in (a) we utilize (19). □

We now prove the zero-order bound, starting with the tighter one (9) then proceeding to (8).

Proof: *(of Theorem 1)* We start with (3) and note that $\lambda(x) \leq 1$. Thus

$$f(x) \geq \frac{1-\rho^{-1}(1-x)}{\delta} - 1$$

in which the right hand side is non-negative for $x \geq 1-\rho(1-\delta)$. As $f(x)$ is non-negative over the whole range $[0,1]$, we have

$$\begin{aligned}
\int_0^1 f(x)dx &\geq \int_{1-\rho(1-\delta)}^1 \left[\frac{1-\rho^{-1}(1-x)}{\delta} - 1\right] dx \\
&\overset{(a)}{=} \frac{1}{\delta}\left[\rho(1-\delta)(1-(1-\delta)) + \tilde{\rho}(1-\delta)\int \rho\right] - \rho(1-\delta) \\
&= \frac{1}{\delta}\tilde{\rho}(1-\delta) \cdot \int \rho
\end{aligned}$$

where (a) follows by (20). Now (9) follows by (4)

To prove the weaker bound (8) we recall [5] that since $\tilde{\rho}_i$ form a probability distribution, we have

$$\tilde{\rho}(x) = \sum_i \tilde{\rho}_i x^i \geq x^{\sum_i i\tilde{\rho}_i} = x^{1/\int \rho} = x^{a_r}, \tag{21}$$

which leads to the desired bound. □

B Finding the Tangent Point of Lemma 3

In this appendix we show how the tangent point in Theorem 2 can be found by solving a polynomial equation. Presenting (10) as $x = 1 - \rho(1 - \delta y)$, the tangent point (x_a, y_a) is determined by the two equations

$$\begin{aligned} x_a &= 1 - \rho(1 - \delta y_a) \\ \tfrac{1-x_a}{1-y_a} &= \delta\rho'(1 - \delta y_a) \end{aligned}$$

which, by substituting $u = 1 - \delta y_a$, can be presented as

$$\rho(u) = (\delta - 1 + u) \cdot \rho'(u) \tag{22}$$

and

$$\begin{aligned} x_a &= 1 - \rho(u) \\ y_a &= \tfrac{1-u}{\delta} \end{aligned} \tag{23}$$

In order to calculate the tangent point (x_a, y_a) one first solves (22), which is a polynomial equation in u, and finds the unique solution over $(1-\delta, 1)$. The existence of this unique solution has already been proved in Lemma 3. The tangent point is then calculated using (23).

In the particular case of a right-regular code discussed in Section VI, where $\rho(x) = x^D$ and $D + 1$ is the right-degree, there exists a closed-form solution to the tangent point, namely:

$$\begin{aligned} x_a &= 1 - \left(\tfrac{(1-\delta)D}{D-1}\right)^D \\ y_a &= \tfrac{1}{\delta}\left(1 - \tfrac{(1-\delta)D}{D-1}\right) \end{aligned}$$

Acknowledgment

The authors would like to thank Simon Litsyn and Avner Dor for some fruitful discussions. They would also like to thank Igal Sason for his constructive comments.

References

[1] R. G. Gallager, *Low Density Parity Check Codes*, M.I.T. Press, Cambridge, Massachusetts, 1963.

[2] P. Elias, "Coding for two noisy channels," in *Information Theory, Third London Symposium*, London, England, 1955, Butterworth's Scientific Publications.

[3] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 569–584, Feb. 2001.

[4] A. Shokrollahi, "Capacity-achieving sequences," in *IMA volumes in Mathematics and its Applications*, B. Marcus and J. Rosenthal, Eds., 2000, vol. 123, pp. 153–166.

[5] M. A. Shokrollahi, "New sequences of linear time erasure codes approaching the channel capacity," in *Proceedings of AAECC-13*. 1999, vol. 1719, pp. 65–76, Lecture Notes in Computer Science.

[6] D. Burshtein, M. Krivelevich, S. Litsyn, and G. Miller, "Upper bounds on the rate of LDPC codes," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2437–2449, Sept. 2002.

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

[8] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Transactions on Information Theory*, pp. 619–637, Feb. 2001.

[9] M. S. Bazaraa, H. D. Sherali, and C. M. Shetty, *Nonlinear Programming, Theory and Applications*, Wiley, second edition, 1993.

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

List of Figures

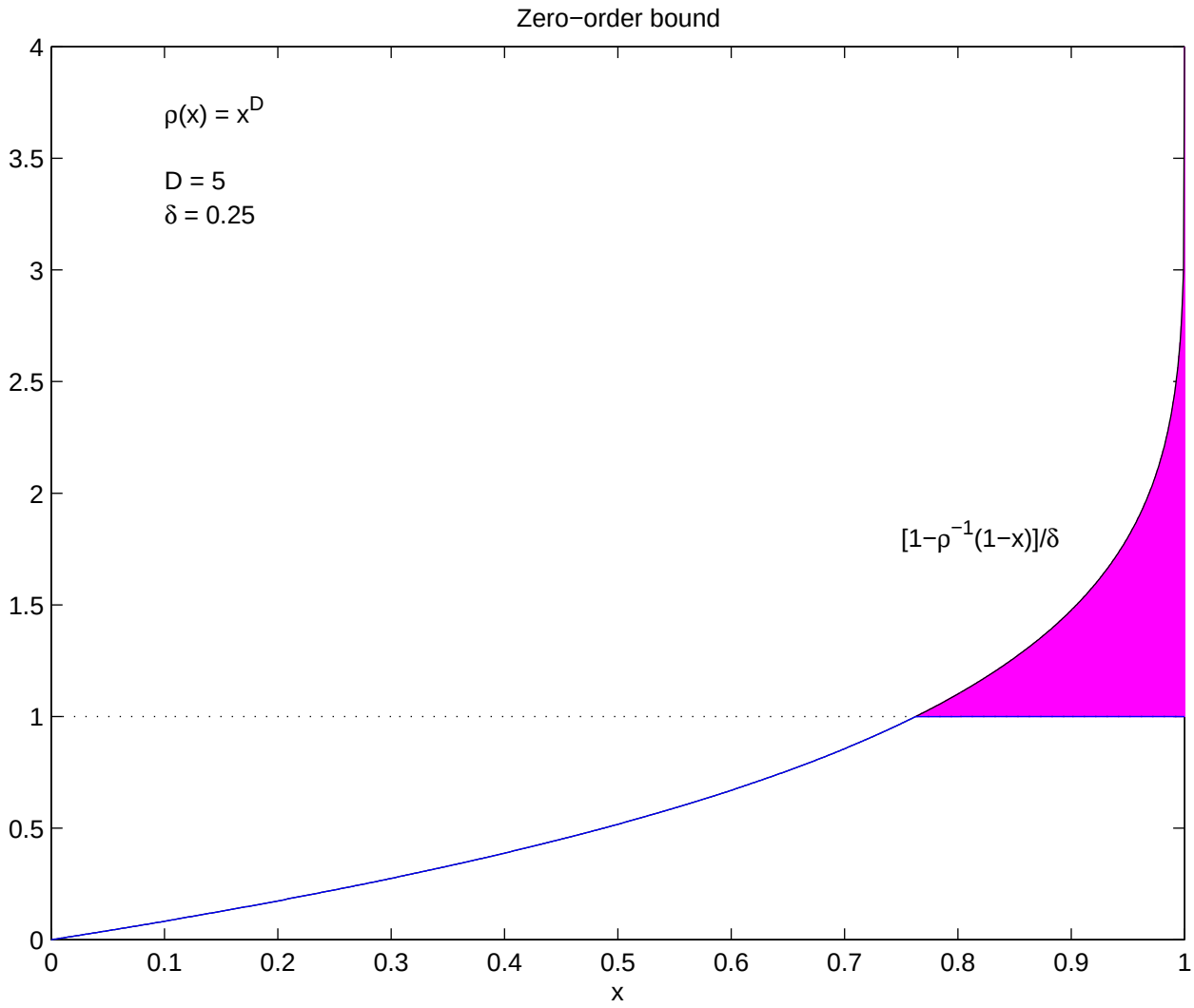

Figure 1: Zero-order bound

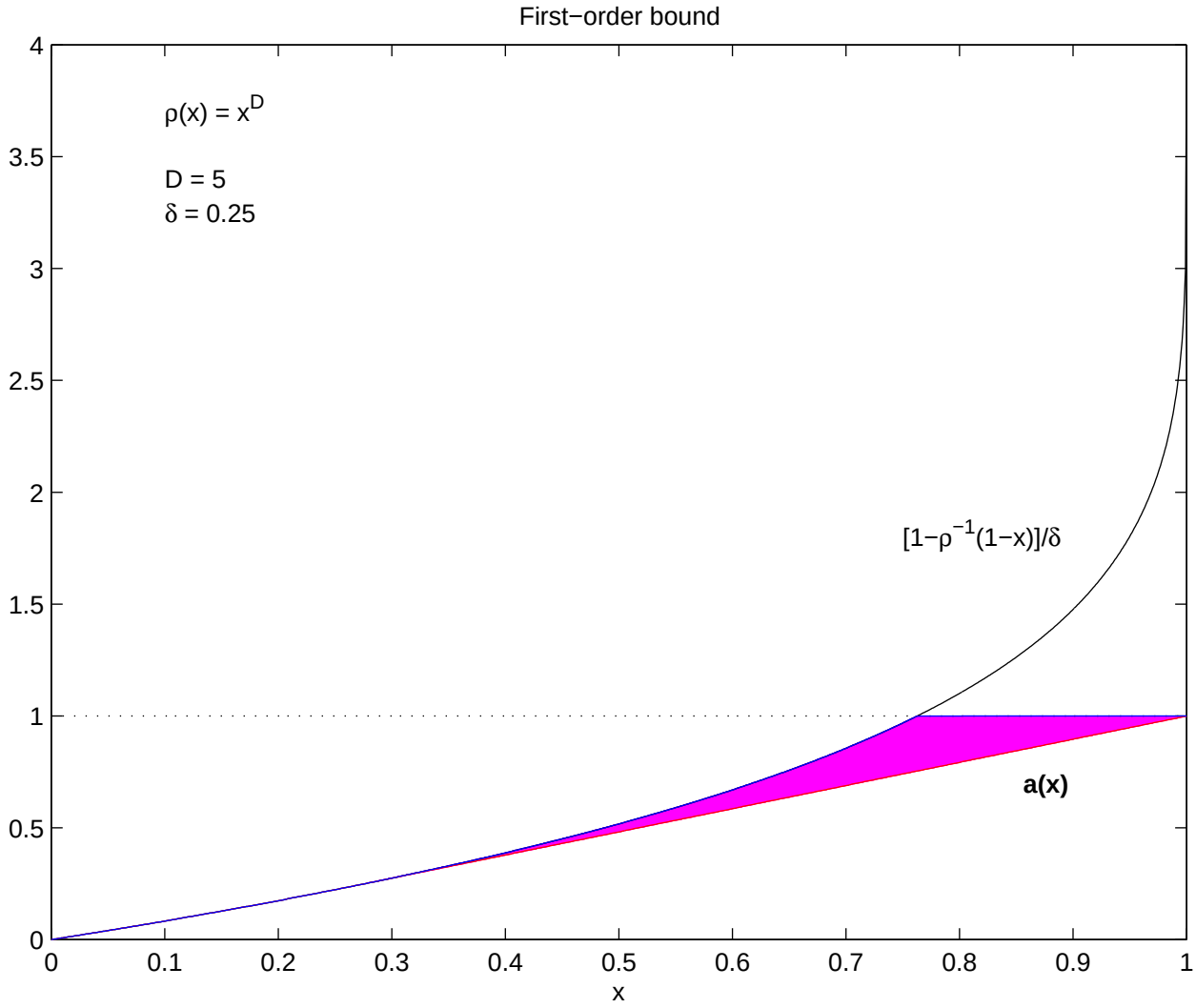

Figure 2: First-order bound

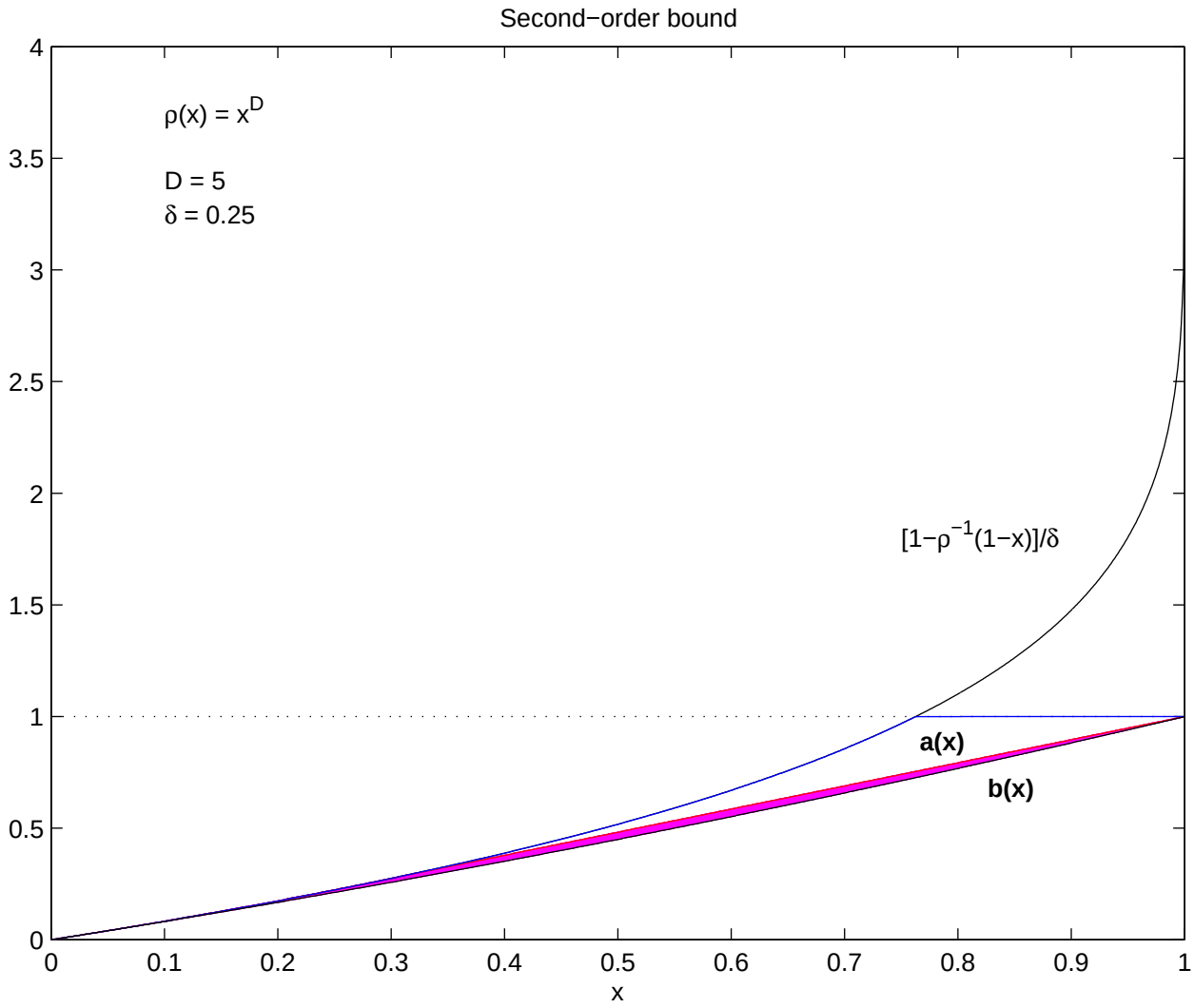

Figure 3: Second-order bound

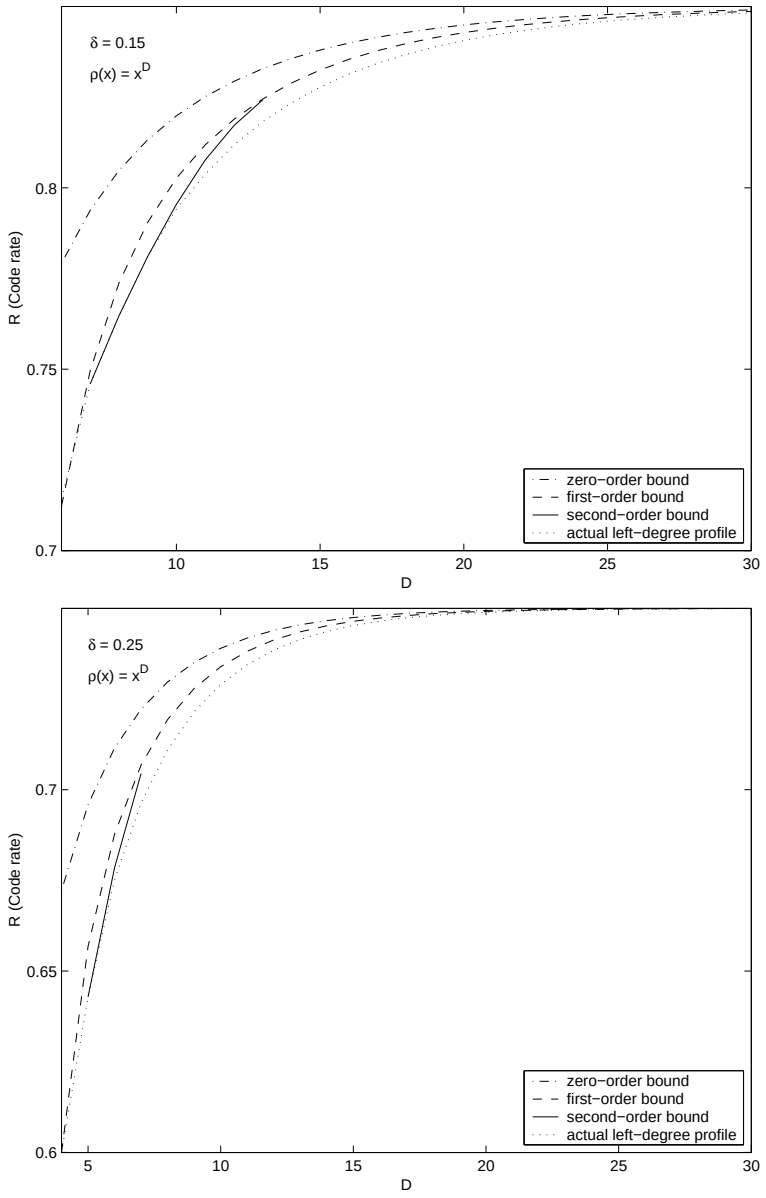

Figure 4: Bounds on LDPC codes that are right-regular, for two values of loss-fraction δ, compared to the rates achieved by the code profiles defined in (17).