# Incremental Redundancy Hybrid ARQ with LDPC and Raptor Codes

Emina Soljanin, Nedeljko Varnica, and Philip Whiting

**Abstract**

Two incremental redundancy hybrid ARQ (IR-HARQ) schemes are proposed, analyzed, and compared: one is based on LDPC code ensembles with random transmission assignments, the other is based on recently introduced Raptor codes. A number of important issues, such as rate and power control, Raptor code design, and error rate performance after each transmission on time varying binary-input, symmetric-output channels are addressed by analyzing performance of LDPC and Raptor codes on parallel channels. The spectrum properties of LDPC code ensembles that are necessary for this analysis are derived. A set of rules for incrementing redundancy and setting the signal power at each transmission in order to maximize the throughput are derived for both schemes. The theoretical results obtained for random code ensembles are tested on several practical code examples by simulation. Both theoretical and simulation results show that both LDPC and Raptor codes are suitable for HARQ schemes. Which codes would make a better choice depends mainly on the width of the operating range of the HARQ scheme, prior knowledge of that range, and other design parameters and constraints dictated by standards.

**Index Terms**

Hybrid ARQ, rateless codes, incremental redundancy.

This work was supported in part by DIMACS.

E. Soljanin and P. Whiting are with Bell Labs, Murray Hill NJ, Email: {emina,pawhiting}@lucent.com.

N. Varnica is with Harvard University, Cambridge MA, Email: varnica@deas.harvard.edu.

## I. INTRODUCTION

In conventional *a*utomatic *r*epeat re*q*uest (ARQ) schemes, frame errors are examined at the receiving end by an error detecting (usually cyclic redundancy check (CRC)) code. If a frame passes the CRC, the receiving end sends an acknowledgement (ACK) of successful transmission to the receiver. If a frame does not pass the CRC, the receiving end sends a negative acknowledgement (NAK), requesting retransmission. User data and its CRC bits may be additionally protected by an error correcting code which increases the probability of successful transmission. Such ARQ schemes which combine the ARQ principle with error control coding are known as *h*ybrid ARQ (HARQ) schemes.

The standard measure of ARQ protocol efficiency is *throughput*, defined as the average number of user data bits accepted at the receiving end in the time required for transmission of a single bit. Therefore the level of redundancy of the error correcting code employed in an HARQ scheme has two opposing effects on the scheme efficiency, namely, with increased redundancy the probability of successful transmission increases but the percentage of user data in the frame decreases. Usually, a fixed rate code which is well suited to the channel characteristics and throughput requirements is selected.

In applications with fluctuating channel conditions within a range of signal-to-noise ratios (SNRs), such as mobile and satellite packet data transmission, the so called *incremental redundancy* (IR) HARQ schemes exhibit higher throughput efficiency by adapting their error correcting code redundancy to different channel conditions. An IR-HARQ protocol operates as illustrated by the example in Figure 1. At

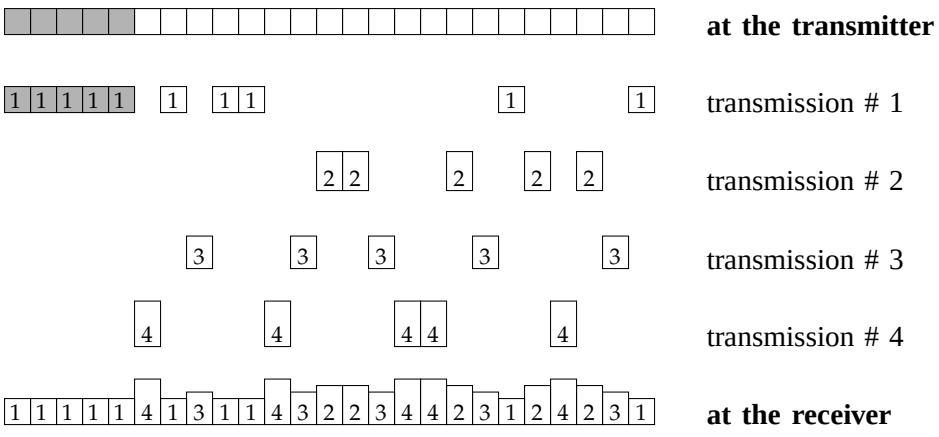



Fig. 1. Incremental redundancy HARQ protocol.

the transmitter, the information and CRC bits are encoded by a systematic “mother” code. Initially, only

the systematic part of the codeword and a selected number of parity bits are transmitted. The selected parity bits together with the systematic bits form a codeword of a punctured mother code. Decoding of this code is performed at the receiving end. If a retransmission is requested, the transmitter sends additional parity bits possibly under different channel conditions or at different power. Decoding is again attempted at the receiving end, where the new parity bits are combined with those previously received. The procedure is repeated after each subsequent retransmission request until all the parity bits of the mother code are transmitted.

A historic overview of hybrid ARQ schemes up to 1998, can be found in [2]. Recent interest in the schemes comes from the quest for reliable and efficient transmission under fluctuating conditions in wireless networks. An information-theoretic analysis of some HARQ protocols, concerning throughput and average delay for block-fading, Gaussian, collision channels have been reported in [1], [24]. Another line of recent work on HARQ is concerned with the mother code and its puncturing since the throughput in these schemes is strongly affected by the power of the mother code used in the system and the family of codes obtained by puncturing [23], [12], [8], [29].

The HARQ scheme of the third generation wireless standards is based on powerful turbo codes. There are two crucial questions in this application of HARQ: 1) how to evaluate the error rate performance after each transmission (which is equivalent to evaluating performance of punctured codes on time varying channels [14]), and 2) how to choose the signal power and the number of bits for transmission $j$ after a failed transmission $j-1$. In [26], both questions were successfully addressed by analyzing performance of IR-HARQ schemes averaged over certain ensembles of turbo codes and all possible transmission assignments (or puncturing patterns) of the mother code bits. A number of related practical methods for efficient link error prediction based on convex metrics are proposed in [11].

Recently, various issues concerning possible use of LDPC codes for HARQ have been examined in terms of belief propagation (BP) decoding performance. A density evolution analysis and puncturing patterns for long LDPC codes were considered in [8]. Practical regular and irregular LDPC code constructions under BP decoding for HARQ were studied in [12], [29]. However, LDPC code performance limits in HARQ schemes under maximum-likelihood (ML) decoding received little attention. On the other hand, new decoding algorithms [5] and improved decoding algorithms (relative to BP) for LDPC codes (see e.g. [6], [19], [27] and the references therein) are becoming an increasingly important research topic making the ultimate ML performance limits increasingly relevant. We here investigate the ML limits for LDPC based HARQ schemes. Even more importantly, we use this analysis to address the practical questions mentioned above, concerning link error prediction and code rate selection.

Throughout the paper we suppose that the channel is a Binary Input Symmetric Channel (BISC). Input is taken from one of two discrete symbols and the channel is additive noise (discrete or continuous). Furthermore we assume that the channel is known only at the receiver and that the goal is to maximize the throughput. Consequently, we organize an IR-HARQ protocol as follows: Initially the transmitter sends only as many codeword symbols as necessary to ensure a high probability of successful ML decoding over a high SNR channel. If the decoding fails, the receiver sends a NACK and the channel information to the transmitter. Taking into account the channel information of the past transmission(s), the transmitter sends only as many additional codeword symbols as necessary to insure a high probability of successful ML decoding assuming a high SNR channel during the current transmission.

In addition to LDPC codes, another family of codes seem to be a natural candidate for use in HARQ schemes. This is the class of Fountain Codes, originally designed for reliable transmission of data over an erasure channel with unknown erasure probability. The first class of efficient Fountain Codes were LT-codes [15]. The codewords of an LT code are generated based on the $k$ information symbols by the means of a probability distribution on the numbers $1, \ldots, k$. Each codeword symbol is obtained independently, by first sampling this distribution to obtain a number $d$, and then adding the values of $d$ randomly chosen information symbols. Raptor codes are a modified version of LT codes in which the information sequence of $k$ symbols is pre-coded by a high rate, block code, (*e.g.*, LDPC code), and then the $n$ resulting symbols are used to generate the Raptor codeword symbols in the same manner as for LT codes, [25]. Both, LT and Raptor codes were originally designed for erasure channels, but performance of Raptor codes on arbitrary symmetric channels have been studied in [4]. For a more general description of Fountain codes, we refer the reader to [15], [25], and [4].

In [4], the following scenario for use of Raptor codes over a symmetric channel was considered: the receiver collects outputs from the channel whose statistical characteristics do not change in time (*e.g.*, AWGN channel with a constant SNR), until the cumulative reliability of the collected bits reaches a certain value determining the overhead of the code. Once reception is complete the receiver attempts to recover the input bits by BP decoding. The main concern in [4] is to design Raptor Codes that achieve a reception overhead arbitrarily close to zero, while maintaining the reliability and efficiency of the decoding algorithm. Although this problem has been solved for the erasure channel [25], it is not yet fully understood for general symmetric channels. Nevertheless, significant progress has been made, and in particular, it has also been shown that there are no universal Raptor Codes whose performance comes arbitrarily close to the capacity regardless of the noise of the channel [4].

The ability of Raptor codes to produce, for a given set of $k$ information symbols, as many codeword

symbols as needed for their successful decoding is what makes these codes of interest for use in HARQ schemes. In this paper, we first study the spectra of Raptor codes and the ML decoding error rates for HARQ schemes based on Raptor codes. As in the case of LDPC codes, we assume that the channel is known only at the receiver and the goal is to maximize the throughput. With that in mind, we organize an IR-HARQ scheme based on Raptor codes in a very similar fashion as in the HARQ scheme with LDPC codes. Taking into account the channel information of the past transmission(s), the transmitter generates and then sends only as many codeword symbols as necessary to insure a high probability of successful ML decoding assuming a high SNR channel during the current transmission. Consequently, the central question is to determine the minimum number of symbols which should be generated at each transmission and the minimum power at which they should be transmitted to ensure a low error rate. This question is answered in this paper.

We also note that the study of performance of Raptor codes on arbitrary symmetric channels reported in [4], addressed a number of fundamental issues such as design of optimal probability distribution. These issues, although not a main concern of this paper, are of utmost importance for performance of HARQ and naturally connected with questions we attempt to answer. Consequently, some of them will also be addressed here to a certain extent.

The remainder of the paper is organized as follows. In Section II we begin with a spectrum analysis of the LDPC code ensembles which we use in the HARQ schemes. In Section III we analyze ML decoding of LDPC codes for HARQ and describe an IR-HARQ protocol with random transmission assignments for this HARQ scheme. In this section we also provide results for belief-propagation (BP) decoding of the same codes. In Sections IV and V, we focus on Raptor codes – in Section IV we give an ML analysis and propose an IR-HARQ protocol and in Section V we provide several results on BP decoding of Raptor codes for HARQ. In Section VI we give a comparison between HARQ schemes employing LDPC and Raptor codes. The concluding remarks are given in Section VII.

## II. The Spectrum of Regular LDPC Code Ensembles

We begin with several results regarding the spectrum of regular LDPC codes. The results given in this section are used as a foundation for both LDPC and Raptor code ensemble analysis.

We study ensembles of regular binary LDPC code whose $k \times n$ parity check matrices have $r$ as the sum of each row and $c$ as the sum of each column where

$$0 < \zeta = \frac{c}{r} = \frac{k}{n} < 1.$$

The code rate of such codes is $R \geq 1 - \zeta$.

Generally, for a binary linear code $\mathcal{C}$ we denote the weight enumerator by $A_h$ (*i.e.*, the number of codewords of weight $h$ in this code is $A_h$). For a code ensemble $[\mathcal{C}](n)$, the average number of codewords of normalized weight $\theta = h/n$ is denoted by $\overline{A}_\theta^{[\mathcal{C}](n)}$. To analyze the performance of HARQ schemes based on LDPC codes, we are interested in the asymptotic behavior of left tail of the ensemble spectrum, namely

$$\sum_{h=1}^{\lceil n\theta_0 \rceil} \overline{A}_h^{[\mathcal{C}](n)},$$

where $0 < \theta_0 \leq 1$, and in the quantity known as the ensemble *noise threshold* [9], which we here define as follows:

$$c_0^{[\mathcal{C}]} = \limsup_{n\to\infty} \max_{\lceil n\theta_0 \rceil < h \leq n} \frac{\log \overline{A}_h^{[\mathcal{C}](n)}}{h}.$$

We next show how these two quantities can be bounded. Our derivations are based on the results of [13] and on certain results from the theory of large deviations. Only the main steps are presented here; details will be given in the Appendix.

### *A. The Left Tail of the Ensemble Spectrum*

We first derive upper bounds on the number of code words of small weight in the ensemble. Let $\rho$ be the unique positive root of the following equation:

$$\frac{(1+\rho)^{r-1} + (1-\rho)^{r-1}}{(1+\rho)^r + (1-\rho)^r} = 1 - \theta, \quad 0 < \theta < 1. \tag{1}$$

Note that $rho \to 0$ as $\theta \to 0$. Then the following holds for sufficiently large $n$:

*Theorem 1:* There is a constant $C$ independent of $\theta$ and $n_0$ so that for $n > n_0$,

$$\overline{A}_\theta^{[\mathcal{C}](n)} \leq C \left[ \frac{(1+\rho)^r + (1-\rho)^r}{2\rho^{\theta r}} \right]^{n\zeta} \left[ (1-\theta)^{(1-\theta)} \theta^\theta \right]^{n(\zeta r - 1)}$$

*Proof:* See Appendix I. ■

Note that for all sufficiently small $\theta$ and $c \geq 2$, we can use the above upper bound to obtain

$$\overline{A}_\theta^{[\mathcal{C}](n)} \leq C \left[ \frac{\theta^{\zeta\theta r}}{\rho^{\zeta\theta r} \theta^\theta} \right]^n .$$

Using an estimate for $\rho$ (see Appendix I) for sufficiently small $\theta$, we find there is an $\varepsilon > 0$ so that the RHS of the above inequality is upper-bounded by

$$C \left[ \theta^{(c/2-1)} \cdot ((r-1)(1+\varepsilon))^{c/2} \right]^{n\theta}. \tag{2}$$

Consequently,

$$\overline{A}_{\theta}^{[\mathcal{C}](n)} \leq C\left[\theta^{(c/2-1)} \cdot ((r-1)(1+\varepsilon))^{c/2}\right]^{n\theta}$$

or, equivalently,

$$\overline{A}_{h}^{[\mathcal{C}](n)} \leq C\left[\left(\frac{ha}{n}\right)^{c/2-1}\right]^{h},$$

where $a = [(r-1)(1+\varepsilon)]^{c/(c-2)}$.

We next investigate the left tail of the spectrum

$$\sum_{h=1}^{\lceil n\theta_0 \rceil} \overline{A}_{h}^{[\mathcal{C}](n)} \leq C \sum_{h=1}^{\lceil n\theta_0 \rceil}\left[\left(\frac{ha}{n}\right)^{c/2-1}\right]^{h},$$

and show that it converges to 0 as $n \to \infty$ for a suitable choice of $\theta_0$. Note that we must choose $c \geq 3$ and that we may show the result for $c = 3$ only as the individual terms decrease monotonically as $c$ is increased for a given $(ha)/n$. By considering $x \log x$, we observe that the sequence $[(ha)/n]^h$ decreases as $h$ increases provided $(ha)/n < e^{-1}$. Thus

$$\sum_{h=1}^{\lceil n\theta_0 \rceil}\left[\left(\frac{ha}{n}\right)^{c/2-1}\right]^{h} < (a/n)^{\frac{1}{2}} + (2a)/n + n\theta_0\left((3a)/n\right)^{3/2},$$

and consequently

$$\sum_{h=1}^{\lceil n\theta_0 \rceil} \overline{A}_{h}^{[\mathcal{C}](n)} = O(n^{-\frac{1}{2}}).$$

### *B. The Ensemble Noise Threshold*

The noise threshold $c_0^{[\mathcal{C}](n)}$ for a fixed $n$ is

$$c_0^{[\mathcal{C}](n)} = \max_{\lceil n\theta_0 \rceil < h \leq n} \frac{\log \overline{A}_{h}^{[\mathcal{C}](n)}}{h}.$$

We can also equivalently write

$$c_0^{[\mathcal{C}](n)} = \sup_{\theta_0 < \theta \leq 1} \frac{\mathfrak{a}_\theta}{\theta}, \tag{3}$$

where

$$\mathfrak{a}_\theta \triangleq \log \overline{A}_\theta / n. \tag{4}$$

Now, by applying the result of Thm. 1, we obtain

$$\frac{\mathfrak{a}_\theta}{\theta} \leq \frac{(1-r\zeta)H(\theta)}{\theta} + \frac{\zeta}{\theta}\log\frac{\{(1+\rho)^r + (1-\rho)^r\}}{2\rho^{r\theta}}, \tag{5}$$

where $H(\theta) = -(\theta \log \theta + (1-\theta)\log(1-\theta))$ is the binary entropy function.

The RHS of (5) has a unique maximum in $(0, 1/2)$ [28]. Therefore, we can obtain an upper bound on $c_0^{[\mathcal{C}]}$ by differentiation with respect to $\theta$ of the RHS of (5). Recall that there is a dependency between $\rho$ and $\theta$ expressed by (53). We can find the minimizing $\theta^*$ numerically. For instance, in the case of $r = 5$, $c = 3$, we find that $\theta^* = 0.3189$ and $c_0^{[\mathcal{C}]} \leq 0.6966$. We will come back to this bound later in Section III-D.

## III. IR-HARQ Schemes Based on Punctured LDPC Codes

Recall that we are mainly considering the scenario when the channel is known only at the receiver and the goal is to maximize the throughput. Therefore, in an IR-HARQ schemes based on LDPC codes, the idea is to, at each transmission, transmit only as many codeword symbols as necessary to insure a high probability of successful ML decoding on an ideal channel taking into account the information about the overhead and the channel state information during the past transmissions. We first analyze the ML performance of IR-HARQ schemes averaged over certain ensembles of LDPC codes and all possible transmission assignments (or puncturing patterns) of the mother code bits. We then test our results on HARQ schemes based on practical finite-length LDPC codes with rate compatible random puncturing.

### *A. The ML Decoding Analysis for LDPC Codes over Parallel Channels*

We first consider a binary input memoryless channel with output alphabet $\mathcal{Y}$ and transition probabilities $W(y|0)$ and $W(y|1)$, $y \in \mathcal{Y}$. When a codeword $\boldsymbol{x} \in \mathcal{C} \subseteq \{0,1\}^n$ has been transmitted, the probability that the ML detector finds codeword $\boldsymbol{x'}$ at Hamming distance $h$ from $\boldsymbol{x}$ more likely can be bounded as follows:

$$P_e(\boldsymbol{x}, \boldsymbol{x'}) \leq \gamma^h, \tag{6}$$

where $\gamma$ is the *Bhattacharyya noise parameter* defined as

$$\gamma = \sum_{y \in \mathcal{Y}} \sqrt{W(y|x=0)W(y|x=1)} \tag{7}$$

if $\mathcal{Y}$ is discrete and as

$$\gamma = \int_{\mathcal{Y}} \sqrt{W(y|x=0)W(y|x=1)}\, dy$$

if $\mathcal{Y}$ is a measurable subset of $\mathcal{R}$.

Generally, for an $(n,k)$ binary linear code $\mathcal{C}$ with the weight enumerator $A_h$, we have the well known *union-Bhattacharyya bound* on the ML decoder word error probability

$$P_W^{\mathcal{C}} \le \sum_{h=1}^{n} A_h \gamma^h.$$

Recall that, for a code ensemble $[\mathcal{C}](n)$, the average number of codewords of weight $h$ in $\mathcal{C}^{(n)}$ is denoted by $\overline{A}_h^{[\mathcal{C}](n)}$. The bound on the ML decoder word error probability averaged over the ensemble is obtained by averaging the (additive) union bound:

$$\overline{P}_W^{[\mathcal{C}](n)} \le \sum_{h=1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \gamma^h. \tag{8}$$

Now, from the results of Section II, we know that there is $\theta^*$, such that $0 < \theta^* < 1$, and

$$\sum_{h=1}^{\lceil n\theta^* \rceil} \overline{A}_h^{[\mathcal{C}](n)} = O(n^{-\frac{1}{2}})$$

and, for sufficiently large $n$,

$$\overline{A}_h^{[\mathcal{C}](n)} \le_n \exp\bigl(h c_0^{[\mathcal{C}]}\bigr), \qquad \forall h \;\; n\theta^* < h \le n. \tag{9}$$

Therefore, for sufficiently large $n$, we have

$$\begin{aligned} \overline{P}_W^{[\mathcal{C}](n)} &\le \sum_{h=1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \gamma^h \\ &\le \sum_{h=1}^{\lceil n\theta^* \rceil} \overline{A}_h^{[\mathcal{C}](n)} + \sum_{h=\lceil n\theta^* \rceil + 1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \gamma^h \\ &\le O(n^{-\frac{1}{2}}) + \sum_{h=\lceil n\theta^* \rceil + 1}^{n} \exp[h(c_0^{[\mathcal{C}]} + \log\gamma)]. \end{aligned} \tag{10}$$

Thereby, when

$$\gamma < \exp(-c_0^{[\mathcal{C}]}), \tag{11}$$

we have

$$\overline{P}_W^{[\mathcal{C}](n)} \le O(n^{-\frac{1}{2}}).$$

We now assume that the channel varies during the transmission of a single codeword, namely, channel transition probabilities at time $i$ are $W_i(b|0)$ and $W_i(b|1)$, $b \in \mathcal{Y}$. When codeword $\boldsymbol{x} \in \{0,1\}^n$ has been transmitted, the probability that the ML detector finds codeword $\boldsymbol{x'} \in \{0,1\}^n$ more likely can be bounded as follows:

$$P_e(\boldsymbol{x}, \boldsymbol{x'}) \le \sum_{\boldsymbol{y} \in \mathcal{Y}^n} \sqrt{W^n(\boldsymbol{y}|\boldsymbol{x}) W^n(\boldsymbol{y}|\boldsymbol{x'})},$$

where we denote

$$W^n(\boldsymbol{y}|\boldsymbol{x}) = \prod_{i=1}^{n} W_i(y_i|x_i).$$

It is easy to see that

$$\begin{aligned} P_e(\boldsymbol{x}, \boldsymbol{x'}) &\leq \sum_{\boldsymbol{y} \in \mathcal{Y}^n} \sqrt{W^n(\boldsymbol{y}|\boldsymbol{x}) W^n(\boldsymbol{y}|\boldsymbol{x'})} \\ &= \prod_{i=1}^{n} \Big( \sum_{b \in \mathcal{Y}} \sqrt{W_i(b|x_i) W_i(b|x'_i)} \Big). \end{aligned} \tag{12}$$

Note that when $x_i = x'_i$, the corresponding factor $\sum_{b \in \mathcal{Y}} \sqrt{W_i(b|x_i) W_i(b|x'_i)}$ in the product (12) equals 1 and can be omitted. When $x_i \neq x'_i$, the corresponding factor $\sum_{b \in \mathcal{Y}} \sqrt{W_i(b|x_i) W_i(b|x'_i)}$ equals to the Bhattacharyya noise parameter $\gamma_i$ of the channel at time $i$:

$$\gamma_i = \sum_{b \in \mathcal{Y}} \sqrt{W_i(b|0) W_i(b|1)}$$

Therefore, the bound (12) can be written as

$$P_e(\boldsymbol{x}, \boldsymbol{x'}) \leq \prod_{i:\, x_i \neq x'_i} \gamma_i. \tag{13}$$

Note that when all $\gamma_i$ have the same value $\gamma$ (time-invariant channel case), the above bound reduces to the well known $\gamma^h$ bound (6), where $h$ is the Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{x'}$.

We now assume that the codewords of the mother code are transmitted in $m$ transmissions, and the decoding is performed after the last transmission has been received. This will help us to later analyze an IR-HARQ protocol with at most $m$ transmissions. Let $\mathcal{I} = \{1, \ldots, n\}$ denote the set indexing the bit positions in a codeword. For the $m$ transmissions, set $\mathcal{I}$ is partitioned in $m$ subsets $\mathcal{I}(j)$, for $1 \leq j \leq m$. During the $j$-th transmission, only bits at positions $i$ where $i \in \mathcal{I}(j)$ are transmitted. We assume that the channel is slowly time-varying, namely that $W_i(y|0)$ and $W_i(y|1)$ remain constant for all bits at positions $i$ taking part in the same transmission. Consequently, the Bhattacharyya noise parameter for transmission $j$ depends only on $j$:

$$\gamma_i = \gamma(j) \quad \text{for all } i \in \mathcal{I}(j).$$

Let $h_j = d_H(\boldsymbol{x}, \boldsymbol{x'}, \mathcal{I}(j))$ denote the Hamming distance between sequences $\boldsymbol{x}$ and $\boldsymbol{x'}$ over the index set $\mathcal{I}(j)$. The bound (13) can be written as

$$P_e(\boldsymbol{x}, \boldsymbol{x'}) \leq \prod_{j=1}^{m} \gamma(j)^{h_j}, \qquad h_j = d_H(\boldsymbol{x}, \boldsymbol{x'}, \mathcal{I}(j)).$$

In the case of only two transmissions, we have

$$P_e(\boldsymbol{x},\boldsymbol{x'}) \leq \gamma(1)^{d_H(\boldsymbol{x},\boldsymbol{x'},\mathcal{I}(1))} \cdot \gamma(2)^{d_H(\boldsymbol{x},\boldsymbol{x'},\mathcal{I}(2))} = \gamma(1)^{h_1}\gamma(2)^{h-h_1},$$

where $h$ is the Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{x'}$.

Let $A_{h_1 \ldots h_m}$ denote the number of codewords with weight $h_j$ over the index set $\mathcal{I}(j)$, for $1 \leq j \leq m$. The union bound on the ML decoder word error probability is given by

$$P_W \leq \sum_{h_1=1}^{|\mathcal{I}(1)|} \cdots \sum_{h_m=1}^{|\mathcal{I}(m)|} A_{h_1 \ldots h_m} \prod_{j=1}^{m} \gamma(j)^{h_j}. \tag{14}$$

Further direct analysis of this expression seems formidable, even in the case of only two transmissions for which we have

$$\begin{aligned} P_W &\leq \sum_{h_1=1}^{|\mathcal{I}(1)|} \sum_{h_2=1}^{|\mathcal{I}(2)|} A_{h_1 h_2} \gamma(1)^{h_1}\gamma(2)^{h_2} \\ &= \sum_{h=1}^{n} \sum_{h_1=1}^{|\mathcal{I}(1)|} A_{h_1\, h-h_1} \gamma(1)^{h_1}\gamma(2)^{h-h_2}. \end{aligned}$$

We thus resort to finding the expected performance over all possible transmission assignments where a bit of a mother code is assigned to transmission $j$ with probability $\alpha_j$, $\alpha_j > 0$, $\sum_j \alpha_j = 1$. The expected (and asymptotic as $n \to \infty$) number of bits assigned to transmission $j$ equals to $\alpha_j n$. Such scheme can actually be implemented as follows:

1) For each bit position $i$, $i = 1, 2, \ldots, n$, generate a number $\theta_i$ independently and uniformly at random over $[0, 1)$.
2) Compute $m$ numbers $\lambda_j$ as follows:

$$\lambda_j = 1 - \sum_{i=1}^{j} \alpha_i \text{ for } 1 \leq j \leq m.$$

   Note that $0 = \lambda_m < \lambda_{m-1} < \cdots < \lambda_2 < \lambda_1 < 1$.
3) Make the transmission assignment for each bit $i$, $i = 1, 2, \ldots, n$, as follows:
   a) if $\theta_i \geq \lambda_1$, assign bit $i$ to transmission 1, otherwise
   b) if $\lambda_j \leq \theta_i < \lambda_{j-1}$, for some $j$ s.t. $2 \leq j \leq m$, assign bit $i$ to transmission $j$.

We are interested in the expected performance of the mother code under this probabilistic model. If each bit of a codeword with Hamming weight $h$ is randomly assigned to transmission $j$ with probability $\alpha_j$, then the probability that the sub-word corresponding to the $j$-th transmission has weight $h_j$ for $1 \leq j \leq m$ is given by

$$\binom{h}{h_1}\binom{h-h_1}{h_2} \ldots \binom{h-h_1-\cdots-h_{m-1}}{h_m} \alpha_1^{h_1}\alpha_2^{h_2} \ldots \alpha_m^{h_m}. \tag{15}$$

Therefore, for a given codeword with Hamming weight $h$, the expected value of $A_{h_1,\ldots,h_m}$ is given by

$$\overline{A}_{h_1,\ldots,h_m} = A_h \binom{h}{h_1}\binom{h-h_1}{h_2}\cdots\binom{h-h_1-\cdots-h_{m-1}}{h_m}\alpha_1^{h_1}\alpha_2^{h_2}\ldots\alpha_m^{h_m},$$

and consequently, the expected value of the union bound (14) is

$$\begin{aligned}\overline{P}_W &\le \sum_{h_i\ge 0;\sum h_i\le n} \overline{A}_{h_1,\ldots,h_m}\gamma(1)^{h_1}\gamma(2)^{h_2}\ldots\gamma(m)^{h_m}\\ &= \sum_h A_h\Big\{\sum_{\sum h_i=h}\binom{h}{h_1}\binom{h-h_1}{h_2}\cdots\binom{h-h_1-\cdots-h_{m-1}}{h_m}\prod_{j=1}^{m}\big(\gamma(j)\alpha_j\big)^{h_j}\Big\}\\ &= \sum_h A_h\Big(\sum_{j=1}^{m}\gamma(j)\alpha_j\Big)^h.\end{aligned}$$

We define the average Bhattacharyya noise parameter seen by the mother code as

$$\overline{\gamma} = \sum_{j=1}^{m}\gamma(j)\alpha_j. \tag{16}$$

Then, we have

$$\overline{P}_W^{[\mathcal{C}]} \le \sum_{h=1}^{n}\overline{A}_h^{[\mathcal{C}](n)}\overline{\gamma}^h. \tag{17}$$

Therefore, when

$$\overline{\gamma} < \exp(-c_0^{[\mathcal{C}]}), \tag{18}$$

we have

$$\overline{P}_W^{[\mathcal{C}](n)} \le O(n^{-\frac{1}{2}}).$$

### *B. An IR-HARQ Protocol*

We consider an IR-HARQ scheme with at most $m$ transmissions where a bit is assigned to transmission $j$ with probability $\alpha_j$. Transmission $j$ takes place if transmission $j-1$ fails. The rates $\alpha_j$ may be predetermined (*e.g.,* specified by a standard) or determined based on current network conditions. In both cases, we are interested in evaluating performance after $j$ transmissions, $1 \le j \le m$. In the latter case, we are interested in determining the parameters $\alpha_j$ to achieve some required performance[1].

To ensure that the upper bound (8) on the probability of error of the ML decoder approaches 0 on a channel with the Bhattacharyya noise parameter $\gamma$, as $n \to \infty$, it is sufficient and necessary that the

[1]The random transmission assignment (which is based on the parameters $\alpha_j$) for this IR-HARQ protocol can be implemented by an "on-the-fly" dynamic version of the algorithm described in [26].

condition (11) holds. Therefore, in HARQ schemes, the mother code is chosen so that this condition is satisfied for the worst probable channel realization.

We now assume that the decoding after transmission $j-1$ failed. On the average, $n\alpha_j$ bits will participate in the $j$-th transmission, and the remaining $(1-\alpha_1-\cdots-\alpha_j)\cdot n$ bits of the mother code will not be transmitted. We assume that they are transmitted over a really bad channel, *i.e.*, a channel with $\gamma(j+1)=1$, and compute $\overline{\gamma}(j)$, the average Bhattacharyya noise parameter after the $j$-th transmission, as

$$\overline{\gamma}(j)=\alpha_1\cdot\gamma(1)+\cdots+\alpha_j\cdot\gamma(j)+(1-\alpha_1-\cdots-\alpha_j)\cdot 1.$$

Our goal is to guarantee $\lim_{n\to\infty}\overline{P}_W^{[\mathcal{C}](n)}=0$, and this can be done by choosing $\alpha_j$ or $\gamma(j)$ or both so that

$$\overline{\gamma}(j)<\exp(-c_0^{[\mathcal{C}]}). \tag{19}$$

Condition (19) can be written in a form which clearly shows the tradeoff between the rate of the $j$-th transmission code and the signal power:

$$\alpha_j(1-\gamma(j))>1-\exp(-c_0^{[\mathcal{C}]})-\sum_{i=1}^{j-1}\alpha(i)(1-\gamma(i)). \tag{20}$$

To satisfy the above lower bound on the product of $\alpha_j$ and $1-\gamma(j)$, the transmitter can either increase the code redundancy $\alpha_j$ or increase the signal power which results in a decrease of $\gamma(j)$ and increase of $1-\gamma(j)$. An increase in redundancy results in the lower throughput of the user while an increase in the power results in a higher interference level experienced by other users in the network. Since $\gamma(j)$ is positive, there is a minimum redundancy requirement:

$$\alpha_j>1-\exp(-c_0^{[\mathcal{C}]})-\sum_{i=1}^{j-1}\alpha(i)(1-\gamma(i)). \tag{21}$$

Note that this condition ensures that the probability of error of the ML decoding is bounded by $O(n^{-1/2})$ for high SNR. In the case of predetermined $\alpha_j$ (as it is sometimes in practice), the required signal power is specified by

$$\gamma(j)<\frac{\exp\left(-c_0^{[\mathcal{C}]}\right)-(1-\alpha_j)+\sum_{i=1}^{j-1}\alpha(i)(1-\gamma(i))}{\alpha_j}. \tag{22}$$

In this protocol, equations (20), (21), and (22) constitute $j$-th transmission rules after transmission $j-1$ fails.

### *C. Upper Bounds on Throughput for BP Decoding of LDPC Codes in High SNR Region*

We now turn to belief-propagation (BP) decoding. We first examine the maximum throughputs that can be supported by randomly punctured LDPC codes ensembles decoded using BP. To do so, we study the code performance over an ideal channel *i.e.*, very high SNR channel. The following results are described in [16],[20], [22] (see also [10]). In random puncturing, the bits which have not been transmitted can be considered as erasures. For ensembles of very long LDPC codes, successful decoding is obtained provided the rate of erasures is below the *iterative decoding threshold* $p$. This latter quantity is defined for single parameter families of channels with parameter $\theta$ as follows.

*Definition 1:* Let $P_e^{\infty}(\ell)$ be the expected fraction of incorrect messages passed in iteration $\ell$ under the condition that the graph does not contain any cycles of length $2\ell$ or less. Then the iterative decoding threshold is defined to be

$$\theta^* := \limsup_{\theta_0} \{\theta_0 > 0 : P_e^{\infty}(\ell) \to 0, \ell \to \infty, \quad \forall \theta < \theta_0\}$$

$\theta^*$ can be determined as the largest $p \in [0,1]$ for which

$$x = p\lambda(1 - \rho(1 - x)) \tag{23}$$

has no other root than 0 for $x \in [0, p]$. Here $\lambda(x) \doteq \sum_i \lambda_i x^{i-1}, \rho(x) \doteq \sum_j \rho_j x^{j-1}$ are the generator polynomials for the degree distributions of the variable and check nodes respectively. That is, $\lambda_i$ denotes the fraction of edges connected to symbol nodes of degree $i$ and $\rho_j$ denotes the fraction of edges connected to check nodes of degree $j$.

For example consider a regular $(3, 5)$ LDPC code so that the variable and check node edge distribution polynomials are $\lambda(x) = x^2, \rho(x) = x^4$. The rate of this code is $R_{(3,5)} = 0.4$. By optimizing for $x \in (0, 1]$ we find that the largest $p$ for which

$$x = p(1 - (1 - x)^4)^2 \tag{24}$$

has no root other than 0 is $p_{(3,5)} = 0.5175702$ which is the iterative decoding threshold in this case. It follows that a punctured version of this code ensemble can attain a maximum throughput of $T_{(3,5)} = 0.4/(1.0 - 0.5175702) = 0.82914$ over an ideal channel. For regular $(3, 15)$ and $(3, 30)$ codes we similarly find that $T_{(3,15)} = 0.8/(1.0 - 0.167518) = 0.96098$ and $T_{(3,30)} = 0.9/(1.0 - 0.082835) = 0.98128472$. Thus we may expect high rate LDPC mother codes to provide high throughputs when the channel SNR is high, but we see that very high throughputs are not achievable when the LDPC mother code rate is low. This agrees with the results presented in [12] and is confirmed with our simulation results presented next.

### *D. LDPC Code Examples*

We consider the IR-HARQ schemes on an additive white Gaussian noise channel (AWGN) with BPSK signalling. In Figures 2 and 3 we plot the average throughput for a range of SNRs. (SNR is defined as $\mathrm{SNR} = 10\log_{10}\frac{1}{\sigma^2}$, where $\sigma$ is the noise standard deviation.) The puncturing rates were chosen to be

$$R_p = 1,\ 0.975,\ 0.95,\ 0.925,\ \ldots,\ R\ . \tag{25}$$

In other words, after sending the first $k = Rn$ bits, in the subsequent transmission (if it is necessary, *i.e.*, if a codeword is not achieved after $50$ decoding iterations) we send additional $(1 - 0.975)n$ randomly selected parity bits, and decoding is attempted again. This procedure is repeated until an acknowledgement (ACK) is received or until all $n$ symbols are sent.

First, in Figure 2, we evaluate the performance of the punctured regular-(3,5) codes with block lengths $n = 384$ and $n = 3840$. (These block lengths are typically specified by wireless standards.) The code rates of these mother codes are $R = \zeta = 0.4$. Then, in Figure 3 we plot the performance of two punctured codes with higher mother code rates. (For comparison we also include the plots from Figure 2 in Figure 3.) The parity check matrices of all mother codes were chosen randomly from the (expurgated) ensembles consisting of the codes satisfying the column-sum and the row-sum constraints (*e.g.*, $c = 3$ and $r = 5$ for regular-(3,5) codes) and the additional constraint that the girth of the corresponding code graphs is at least $6$.

For comparison, in Figures 2 and 3 we also plot the BPSK capacity of the AWGN channel and the performance of one optimized irregular LDPC code with the code rate $R = 0.5$. The irregular mother code was designed based on the optimized edge degree polynomials from [21], given by $\lambda(x) = \sum_i \lambda_i x^{i-1} = 0.21991x + 0.23328x^2 + 0.02058x^3 + 0.08543x^5 + 0.06540x^6 + 0.04767x^7 + 0.01912x^8 + 0.08064x^{18} + 0.22798x^{19}$ and $\rho(x) = \sum_i \rho_i x^{i-1} = 0.64854x^7 + 0.34747x^8 + 0.00399x^9$. Its block length was set to $n = 10000$. From Figure 2, we observe that the two regular-(3,5) codes with different block lengths have almost identical performance except in the close neighborhood of the point for which the throughput equals the mother code rate $R = 0.4$. Naturally, the performance of the optimized irregular mother code is better than the performances of the regular mother codes. This performance is within $1$dB of the capacity for the range of throughputs $0.5 - 0.75$. As the throughput is further increased above $0.8$ (i.e., as the average puncturing rate further increases) the performance of the irregular code quickly deteriorates. This performance curve saturates roughly at the rate $0.9$. Very similar behavior is observed for the regular codes shown in Figures 2 and 3. Note that the saturation of the regular-(3,5) code performance curves happens at the rate $0.8$. We next demonstrate on this code example how to use the results of Section II

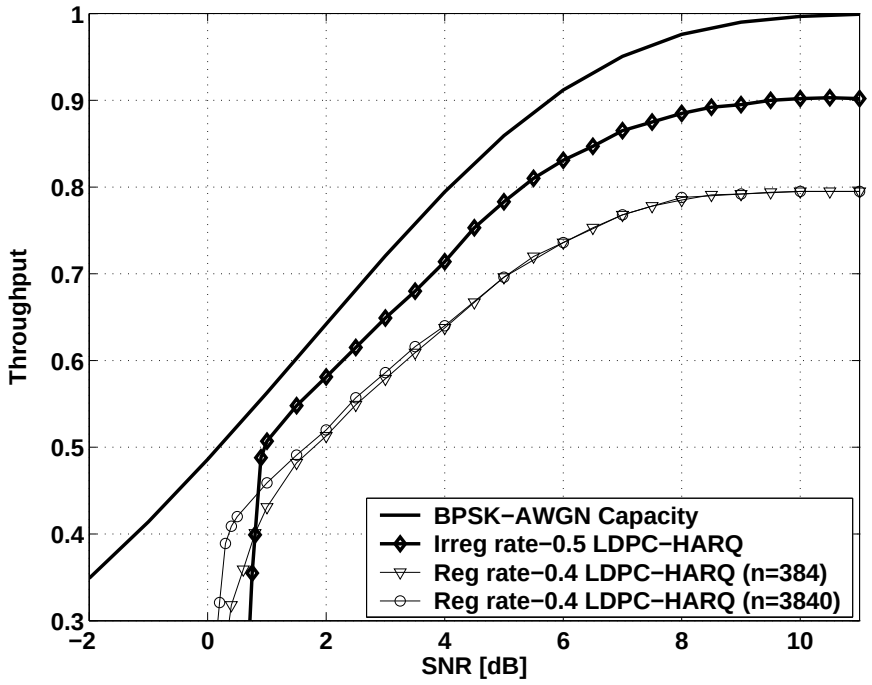



Fig. 2. Average throughput versus SNR for IR-HARQ scheme with LDPC codes on AWGN channel with BPSK signalling. Shown are performances of two regular-(3,5) mother codes with block lengths $n = 384$ and $n = 3840$, one optimized irregular mother code (with block length $n = 10000$) and the Shannon limit.

to estimate the point at which the code "breaks down".

An upper bound to the noise threshold $c_0^{[\mathcal{C}]}$ for the regular-(3,5) ensemble was computed in Section II to be $0.6966$. Since the minimal redundancy requirement for the first transmission is $\alpha_1 > 1-\exp(-c_0^{[\mathcal{C}]})$, we can compute a conservative estimate of this quantity based on the upper bound on $c_0^{[\mathcal{C}]}$. We obtain $\alpha_1 = 0.514$ and the corresponding rate $r_p = \frac{r}{\alpha_1} < 0.7973$. Although this result gives only the necessary condition on the minimal $\alpha_1$, our simulations show that it predicts the saturation point very well. Indeed, looking at Figure 2, we see that the performance curve saturates at exactly this rate.

Another way to estimate the saturation point is to use directly the results of Section III-C. Recall that the upper bound on the throughput for regular-(3,5) code was evaluated to be $T_{(3,5)} = 0.82914$. Naturally, this bound is not tight for the finite-length codes presented in Figure 2 as the bound is achievable only with very long codes when a sufficiently large number of decoding iterations is allowed.

In Figure 4, we demonstrate the word error rate (WER) performance of the two regular mother codes studied in Figure 2. We compare the performances of the punctured codes with rates equaling $0.65$ and

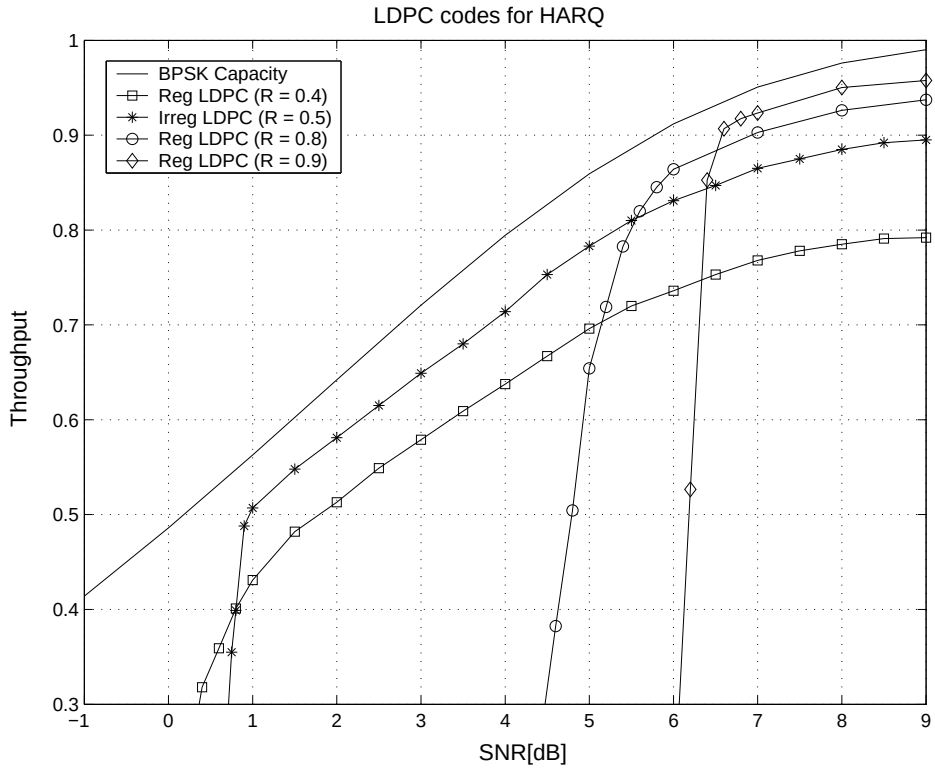



Fig. 3. Average throughput versus SNR for IR-HARQ scheme with LDPC codes on AWGN channel with BPSK signalling. Shown are performances of three regular mother codes (regular-(3,5), regular-(3,15) and regular-(3,30) code), one optimized irregular code and the Shannon limit.

$0.81$. (These codes were obtained from the two regular mother codes after random puncturing.) It is not surprising that the slope of the word error rate curve in the "waterfall region" decreases as the block length is decreased from $n = 3840$ to $n = 384$. It is, however, interesting that from these plots we can clearly observe that puncturing is not effective when the puncturing rates are very high. That is, for the rate $0.81$ the performance of both codes is very poor and even at high SNRs the WERs below $0.04$ can not be achieved. Finally, we observe from Figure 3 that one solution that allows higher throughputs is to use higher rate mother LDPC codes. They, however, have a quite narrow operation region of SNRs in which they are very effective, see Figure 3. In some applications, it would be more useful to have codes that are effective at a wide operating range of SNRs. We next analyze IR-HARQ schemes based on Raptor codes and show that they indeed have this property.

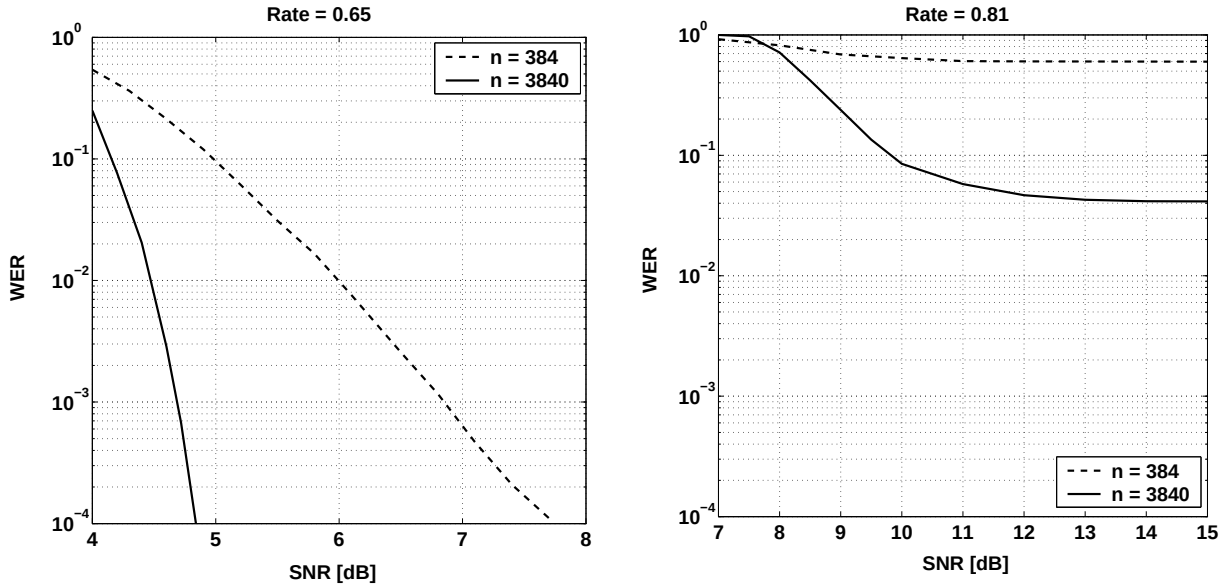



Fig. 4. Word error rates of randomly punctured regular LDPC mother codes with block lengths $n = 384$ and $n = 3840$. The number of decoding iterations was set to $50$.

## IV. HARQ Schemes Based on Raptor Codes

Recall that to obtain a Raptor codeword, the information sequence of $k$ symbols is pre-coded by a high rate block code. Here LDPC codes will be used for pre-coding. The Raptor codeword symbols are then obtained based on the $n$ resulting symbols by the means of a probability distribution $\Omega$ on the numbers $1, \ldots, n$. The probability generating function of this distribution is

$$\Omega(x) = \sum_{d=1}^{n} \Omega_d x^d. \tag{26}$$

Each codeword symbol is obtained independently, by first sampling this distribution to obtain a number $d$, and then adding the values of $d$ randomly chosen information symbols. Note that $\Omega$ represents the degree distribution of the codeword symbols, and thus can be used to determine the degree distribution of the corresponding bipartite varible/check graph used for BP decoding [25], [4].

In an IR-HARQ schemes based on Raptor codes, the idea is to, at each transmission, generate and then transmit only as many codeword symbols as necessary to insure a high probability of successful ML decoding on an ideal channel taking into account the information about the overhead and the channel state information during the past transmissions. Thus, we first analyze the ML performance of HARQ schemes based on Raptor codes.

### *A. The ML Decoding Analysis for Raptor Codes over Parallel Channels*

When a codeword $\boldsymbol{x}$ of length-$N$ Raptor code has been transmitted over the channel with the Bhattacharyya noise parameter $\gamma$, the probability that the ML detector finds codeword $\boldsymbol{x'}$ at Hamming distance $w$ from $\boldsymbol{x}$ more likely can be bounded as

$$P_e(\boldsymbol{x}, \boldsymbol{x'}) \leq \gamma^w. \tag{27}$$

If an $(n, k)$ binary LDPC code ensemble $[\mathcal{C}](n)$ with the weight enumerator $A_h$ is used as the precode in the Raptor scheme with the degree distribution $\Omega$, then the number of Raptor codewords of weight $w$ is given by

$$\sum_{h=1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \binom{N}{w} p(h/n)^w \big(1 - p(h/n)\big)^{N-w},$$

where $p(h/n)$ denotes the probability of 1 in the Raptor codeword when the input LDPC codeword has normalized weight $h$. It is easy to see the following:

$$\begin{aligned} p(\beta) &= \sum_d \Omega_d \sum_{j=1,\, j \text{ odd}}^{d} \binom{d}{j} \beta^j (1-\beta)^{d-j} \\ &= \frac{1}{2} \sum_d \Omega_d [\beta + (1-\beta)]^d - \frac{1}{2} \sum_d \Omega_d [-\beta + (1-\beta)]^d \\ &= \frac{1}{2} - \frac{1}{2} \sum_d \Omega_d (1-2\beta)^d \end{aligned}$$

and

$$1 - p(\beta) = \frac{1}{2} + \frac{1}{2} \sum_d \Omega_d (1-2\beta)^d.$$

The Union-Bhattacharyya bound on the ML decoder word error probability for Raptor code ensembles can therefore be expressed as

$$\begin{aligned} \overline{P}_W^{[\mathcal{C}](n)} &\leq \sum_{w=1}^{N} \sum_{h=1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \binom{N}{w} p(h/n)^d \big(1 - p(h/n)\big)^{N-w} \gamma^w \\ &= \sum_{h=1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \sum_{w=1}^{N} \binom{N}{w} p(h/n)^d \big(1 - p(h/n)\big)^{n-d} \gamma^w \\ &= \sum_{h=1}^{n} \exp(n\theta \mathfrak{a}_\theta) \big[1 - p(\theta)(1-\gamma)\big]^N. \end{aligned}$$

Note that $\gamma < p(h/n)\cdot\gamma + 1 - p(h/n) < 1$. Therefore, the above expression can be bounded in a manner of (10), as follows

$$\begin{aligned}
\overline{P}_W^{[\mathcal{C}](n)} &\le \sum_{h=1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \gamma^h \\
&\le \sum_{h=1}^{\lceil n\theta^* \rceil} \overline{A}_h^{[\mathcal{C}](n)} + \sum_{h=\lceil n\theta^* \rceil+1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \big[p(h/n)\cdot\gamma + 1 - p(h/n)\big]^N \qquad (28)\\
&\le O(n^{-\frac{1}{2}}) + \sum_{h=\lceil n\theta^* \rceil+1}^{n} \overline{A}_h^{[\mathcal{C}](n)} \big[p(h/n)\cdot\gamma + 1 - p(h/n)\big]^N \\
&= O(n^{-\frac{1}{2}}) + \sum_{\theta\in\mathcal{T}, \theta>\theta^*} \exp(n\theta \mathfrak{a}_\theta) \cdot \big[1 - p(\theta)(1-\gamma)\big]^N, \qquad (29)
\end{aligned}$$

where $\mathfrak{a}$ is the spectrum of the LDPC code as defined by equation (4) and $\mathcal{T} = \{\frac{1}{n}, \cdots, \frac{n-1}{n}, 1\}$. It is interesting to compare the expression (28) with the corresponding expression (10) for the LDPC codes without the LT coding, which can be obtained from (28) merely by substituting $\gamma^h$ in the place of $\big[p(h/n)\cdot\gamma + 1 - p(h/n)\big]^N$. Since $\gamma < \big[p(h/n)\cdot\gamma + 1 - p(h/n)\big]$, the LT code has the effect of making the channel noisier according to the original weight of the LDPC codeword.

In the time-varying case, when a codeword $\boldsymbol{x}$ of length–$(N_1 + N_2)$ Raptor code has been transmitted over the channel with the Bhattacharyya noise parameter $\gamma_1$ during the first $N_1$ symbol intervals and the channel with the Bhattacharyya noise parameter $\gamma_2$ during the following $N_2$ symbol intervals, the probability that the ML detector finds codeword $\boldsymbol{x'}$ at Hamming distance $w_1$ from $\boldsymbol{x}$ over the first $N_1$ bits and Hamming distance $w_2$ from $\boldsymbol{x}$ over the second $N_2$ bits more likely can be bounded as

$$P_e(\boldsymbol{x}, \boldsymbol{x'}) \le \gamma_1^{w_1} \gamma_2^{w_2}.$$

If an $(n, k)$ binary LDPC code $\mathcal{C}$ with the weight enumerator $A_h$ is used as the precode in the raptor scheme with the degree distribution $\Omega$, then the number of Raptor codewords of weight $w$ is given by

$$B_{w_1 w_2} = \sum_{h=1}^{n} A_h \binom{N_1}{w_1} p(h/n)^{w_1} \big(1 - p(h/n)\big)^{N_1 - w_1} \binom{N_2}{w_2} p(h/n)^{w_1} \big(1 - p(h/n)\big)^{N_2 - w_2},$$

where $p(h/n)$ denotes the probability of 1 in the Raptor codeword when the input LDPC codeword has normalized weight $h$. The Union-Bhattacharyya bound on the ML decoder word error probability for Raptor codes can therefore be expressed as

$$\begin{aligned}
\overline{P}_W^{[\mathcal{C}](n)} &\le B_{w_1 w_2} \gamma_1^{w_1} \gamma_2^{w_2} \\
&= \sum_{\theta\in\mathcal{T}} \exp(n\theta \mathfrak{a}_\theta) \big[1 - p(\theta)(1-\gamma_1)\big]^{N_1} \big[1 - p(\theta)(1-\gamma_2)\big]^{N_2}
\end{aligned}$$

Similarly, when a codeword $\boldsymbol{x}$ of length–$(N_1+N_2+\cdots+N_m)$ Raptor code has been transmitted over the channel with the Bhattacharyya noise parameter $\gamma_1$ during the first $N_1$ symbol intervals, the channel with the Bhattacharyya noise parameter $\gamma_2$ during the following $N_2$ symbol intervals, and so on, the channel with the Bhattacharyya noise parameter $\gamma_m$ during the last $N_m$ symbol intervals, then the ML decoder word error probability can be bounded as

$$\overline{P}_W^{[\mathcal{C}](n)} \leq \sum_{\theta\in\mathcal{T}} \exp(n\theta\mathfrak{a}_\theta)\big[1-p(\theta)(1-\gamma_1)\big]^{N_1}\big[1-p(\theta)(1-\gamma_2)\big]^{N_2}\ldots\big[1-p(\theta)(1-\gamma_m)\big]^{N_m} \qquad (30)$$

*B. An IR-HARQ Protocol*

In Section IV-A, we derived the following bound (see (29)):

$$\overline{P}_W^{[\mathcal{C}](n)} \leq O(n^{-\frac{1}{2}}) + \sum_{\theta\in\mathcal{T},\theta>\theta^*} \exp(n\theta\mathfrak{a}_\theta)\cdot\big[1-p(\theta)(1-\gamma)\big]^N,$$

We will use the inequality $(1-x)\leq e^{-x}$ to bound $\big[1-p(\theta)(1-\gamma)\big]^N$, which is tight in the low SNR region ($\gamma$ close to 1). Taking into account the definition of the noise threshold (3), we obtain

$$\begin{aligned}\overline{P}_W^{[\mathcal{C}](n)} \leq& O(n^{-\frac{1}{2}}) + \sum_{\theta\in\mathcal{T},\theta>\theta^*} \exp(n\theta\mathfrak{a}_\theta)\cdot\big[1-p(\theta)(1-\gamma)\big]^N\\ \leq& O(n^{-\frac{1}{2}}) + \sum_{\theta\in\mathcal{T},\theta>\theta^*} \exp(n\mathfrak{a}_\theta)\cdot\exp[-Np(\theta)(1-\gamma)]\\ \leq& O(n^{-\frac{1}{2}}) + \sum_{\theta\in\mathcal{T},\theta>\theta^*} \exp\Big[n\theta\Big(c_0-\frac{p(\theta)}{\theta}(1-\gamma)\frac{1}{R_l}\Big)\Big]\end{aligned}$$

Therefore, when the rate of the Raptor code satisfies

$$R_l < \frac{(1-\gamma)}{c_0}\cdot\pi_\Omega,$$

where

$$\pi_\Omega \doteq \min_\theta \frac{p(\theta)}{\theta}$$

we have

$$\overline{P}_W^{[\mathcal{C}](n)} \leq O(n^{-\frac{1}{2}}).$$

By using the same bounding techniques in the time-varying case (see (30)), when a codeword $\boldsymbol{x}$ of length–$(N_1+N_2+\cdots+N_m)$ Raptor code has been transmitted over the channel with the Bhattacharyya noise parameter $\gamma_1$ during the first $N_1$ symbol intervals, the channel with the Bhattacharyya noise

parameter $\gamma_2$ during the following $N_2$ symbol intervals, and so on, the channel with the Bhattacharyya noise parameter $\gamma_m$ during the last $N_m$ symbol intervals, we obtain the following result:

$$\overline{P}_W^{[\mathcal{C}](n)} \leq O(n^{-\frac{1}{2}}) + \exp\Big\{n\theta\Big[c_0 - \frac{p(\theta)}{\theta}\Big(\frac{1-\gamma_1}{R_{l1}} + \frac{1-\gamma_2}{R_{l2}} + \cdots + \frac{1-\gamma_m}{R_{lm}}\Big)\Big]\Big\},$$

where $R_{lj} = n/N_j$. Therefore, when

$$\frac{c_0}{\pi_\Omega} < \frac{1-\gamma_1}{R_{l1}} + \frac{1-\gamma_2}{R_{l2}} + \cdots + \frac{1-\gamma_m}{R_{lm}}, \tag{31}$$

we have

$$\overline{P}_W^{[\mathcal{C}](n)} \leq O(n^{-\frac{1}{2}}).$$

Condition (31) can be written in a form which clearly shows the tradeoff between the rate of the $j$-th transmission code and the signal power:

$$R_{lj}^{-1}(1-\gamma(j)) > \frac{c_0}{\pi_\Omega} - \sum_{i=1}^{j-1} R_{li}^{-1}(1-\gamma(i)). \tag{32}$$

To satisfy the above lower bound on the product of $R_{lj}^{-1}$ and $1-\gamma(j)$, the transmitter can either increase the code redundancy $R_{lj}^{-1}$ or increase the signal power which results in a decrease of $\gamma(j)$ and increase of $1-\gamma(j)$. An increase in redundancy results in the lower throughput of the user while an increase in the power results in a higher interference level experienced by other users in the network. Since $\gamma(j)$ is positive, there is a minimum redundancy requirement:

$$R_{lj}^{-1} > \frac{c_0}{\pi_\Omega} - \sum_{i=1}^{j-1} R_{li}^{-1}(1-\gamma(i)). \tag{33}$$

Note that this condition ensures that the probability of error of the ML decoding is bounded by $O(n^{-1/2})$ for high SNR. In the case of predetermined $\alpha_j$ (as it is sometimes in the practice), the required signal power is specified by

$$\gamma(j) < \frac{-\frac{c_0}{\pi_\Omega} + R_{lj}^{-1} + \sum_{i=1}^{j-1} R_{li}^{-1}(1-\gamma(i))}{R_{lj}^{-1}}. \tag{34}$$

Equations (32), (33), and (34) constitute $j$-th transmission rules after transmission $j-1$ fails. It is interesting to compare them with their counterparts for LDPC codes given by equations (20), (21), and (22).

## V. Throughput of Belief Propagation Decoded Raptor codes in the High SNR Region

### A. Ensemble bounds on the Iterative Decoding Threshold

We turn to the question of designing a Raptor code for Hybrid ARQ. A design must specify the parity check degree polynomial $\Omega$ as well as the inner code. As our simulation results will show subsequently, schemes based on Raptor codes have superior performance at low SNR over conventional systematic punctured LDPC codes. In fact the throughput of punctured LDPC codes falls off rapidly as the SNR falls to the point where the channel capacity corresponds to the rate of the mother code. Finally results in [4] show that no universal $\Omega$ can be found which is capacity achieving over a range of SNRs.

Given the superior performance at low SNR, we will concentrate on the high SNR performance of Raptor codes. In this case puncturing an LDPC code performs better than sending random parity check bits, as in Raptor codes as far as hybrid ARQ throughput is concerned. In fact the performance over such channels may be approximated by the performance over an ideal channel. Consideration of transmission over an ideal channel is also important because lower bounds for ensemble code performance are determined for Raptor codes and LDPC codes once throughput is given for the ideal channel. We begin by discussing this ensemble lower bound.

The lower bound on ensemble performance of infinite length graph based codes is due to Khandekar [10] and provides a limit on the *iterative decoding threshold* see definition 1 (It is well defined in cases where worse channels can be obtained by *physical degradation* of the channel with a smaller parameter value.)

We turn to the bound itself which applies to any physically degradable BISC:

*Theorem 2 (Khandekar):* Suppose the Binary Erasure Channel with erasure probability $p$ is within the iterative decoding threshold for an ensemble of codes. Then so is any other BISC with Bhattacharya parameter $\mathbb{E}\left[e^{-\frac{Z}{2}}\right] = \gamma \leq p$.

The above bound can be used to determine a lower bound on the iterative decoding threshold for Raptor codes over a Binary Input Channel with AWGN noise. To do so first consider the Raptor codes being used over an ideal channel. Take its outer code to be an ensemble of length $n$ regular LDPC codes with rate $R_L$ and with an iterative decoding threshold $p_0$ for the binary erasure channel.

*Definition 2:* Define $\kappa_\Omega(p_0)$ to be the *Raptor threshold rate*. This is the smallest fraction of LT symbols per LDPC symbol needed to determine all but a fraction $p_0$ of the LDPC symbols in the limit as $n \to \infty$. Now suppose that the same Raptor code is used over a BIAWGN channel with Bhattacharya noise $\gamma$. Since the fraction of parity check symbols must be inflated by $1/(1-p)$ for a BEC with parameter $p$,

Theorem 2 implies that we will be within the iterative decoding threshold for this channel provided we transmit at least

$$\kappa_{\Omega}^{\gamma} = \frac{\kappa_{\Omega}(p_0)}{(1-\gamma)} \tag{35}$$

LT parity check symbols per LDPC symbol. The rate of the Raptor code in bits per channel therefore exceeds

$$R_{Raptor} = \frac{R_L}{\kappa_{\Omega}^{\gamma}} = \frac{R_L\,(1-\gamma)}{\kappa_{\Omega}(p_0)} \tag{36}$$

which depends only on the Raptor threshold rate and the Bhattacharya noise of the channel.

(36) may be taken as an approximate lower bound to the throughput which can be achieved by using Hybrid ARQ if the channel is fixed to be BIAWGN with Bhattacharya noise $\gamma$. It may be an overestimate for finite length codes as they typically have worse performance than their corresponding infinite length ensembles. This is balanced by the fact that the codeword is transmitted piecemeal with an attempt at decoding at each stage in Hybrid ARQ. This obviously gives better throughput performance than one shot decoding of the complete codeword.

As we mentioned earlier we thus see that this lower bound is determined via the performance of the Raptor code over an ideal channel. It should be noted that Etesami and Shokrollahi, [4], have obtained a corresponding upper bound for the performance of Raptor codes (and other graph based codes). This too leads to a performance bound in connection with a further BEC. Its erasure probability is given as $1 - \mathbb{E}[\tanh(Z)/2]$ where $Z$ is the distribution of the Log Likelihood Ratio between 0 and 1 over the channel given that 0 was transmitted. This bound coincides with the lower bound for an ideal channel. Furthermore this bound is also determined once $\kappa_{\Omega}(p_0)$ is given.

We now turn to obtaining an upper bound, over the ideal channel, for the throughput for the set of design choices $(p_0, \Omega)$ where $p_0$ is the iterative decoding threshold for the BEC for ensembles of the outer code (not necessarily LDPC) and $\Omega$ is the degree polynomial for the LT parity checks.

### *B. Linear Programming Bounds*

To fix things we will consider Raptor codes with a regular LDPC inner code. Suppose the variable and check node edge distribution polynomials of the LDPC code are $\lambda(x), \omega(x)$. For ensembles of graph based codes, recall that the iterative decoding threshold $p_0$ for the BEC can be determined as the largest $p$ for which (23) has no other root than $x = 0$ in $[0, p]$ as. A punctured version of an LDPC code ensemble can thus attain a maximum throughput

$$T_{\text{Punc LDPC}} := \text{Information bits per bit sent} = \frac{R_L}{(1.0 - p_0)}$$

over an ideal channel.

For Raptor codes the fraction of erased bits $x_0$ remaining after the first round of iterative decoding depends on the choice of degree polynomial $\Omega$. In this case the edge distribution of the check nodes is given by $\omega(x) = \Omega'(x)$ and the data (LDPC code bits) nodes are Poisson $\mathcal{P}(\alpha)$ where $\alpha$ is the average number of bits in a random parity check. Hence $\lambda(x) = e^{\alpha(x-1)}$. $x_0$ is determined as the largest root in $(0, 1)$ of

$$x = e^{-\kappa\Omega'(1-x)} \quad . \tag{37}$$

and $\kappa$ is the number of parity checks per LDPC code bit generated. In this case the throughput is

$$T_{\text{Raptor}} = \frac{R_L}{\kappa}.$$

For Raptor codes we can thus upper bound the throughput performance over an ideal channel for a given underlying LDPC code by minimising $\kappa_\Omega(p_0)$ over all possible choices of $\Omega$. It is actually more convenient to maximise $1/\kappa_\Omega$ as we may then obtain a bound using a linear program. (Other linear programming constructions are described in [4]). For convenience we write $\kappa$ for $\kappa_\Omega$.

As we have just discussed it is necessary for the Raptor ensemble to be BP decodable that,

$$x \geq e^{-\kappa\Omega'(1-x)}, x \in [p_0, 1] \tag{38}$$

so that all roots are in $(0, p_0)$. Rewriting this constraint in terms of $1/\kappa$, we may form the objective,

$$\max_{\Omega} \min_{x} -\frac{\Omega'(1-x)}{\log x}, x \in [p_0, 1] \tag{39}$$

we also have the constraints $\Omega_d \geq 0$ and $\sum_d \Omega_d = 1$. Note that (39) is linear in the coefficients and we obtain a finite linear program by working with polynomials of maximum length $D$ and discretising the objective finely over the given interval. The problem is made an LP by using the standard construction,

$$\begin{aligned} & \max \quad v \\ \textit{subject to} & \\ v &\leq -\frac{\Omega'(1-x_k)}{\log x_k}, k = 1, \cdots, K \\ 1 &= \sum_{d=1}^{D} \Omega_d \\ \Omega_d &\geq 0 \end{aligned}$$

where $x_k$ are the chosen constraint points, $x_1 = p_0, \cdots, x_K = 1$.

Practical Raptor codes have further constraints which make the bound tighter. For example a certain fraction of single degree nodes are needed in order to start BP decoding. However this tightens the bound. Indeed the information rate over an ideal channel is reduced as there will be a consequent fraction of single node repeats which are entirely redundant.

Table I are the throughput bounds for 3 Raptor codes using regular LDPC codes as outer codes. Bounds for ensembles of other codes such as irregular LDPC codes and Turbo codes may also be obtained. Fixing $\Omega_1 = 0.01$ tightens the bound to be $T_{\text{Raptor}} = 0.586$ for ensembles of $(3, 5)$ codes. In figure V-B we

| Code Ensemble | Raptor Throughput Bound |
|---|---|
| (3,5) | 0.607 |
| (3,15) | 0.8699 |
| (3,30) | 0.935 |

TABLE I

THROUGHPUT LINEAR PROGRAMMING BOUNDS FOR 3 REGULAR LDPC CODES

present a graph of the throughput bound divided by the code rate of the outer code as a function of the iterative decoding threshold $p$. As the figure shows the throughput for the Raptor code does not exceed that which would be achieved by puncturing the underlying code. This can never be the case in fact. Indeed suppose we transmit $n(1-p)$ Raptor parity check symbols over an ideal channel. Then we cannot possibly determine more symbols than this under belief propagation decoding (since each Raptor symbol can provide only at most one additional outer code symbol).

In fact for every $p > 0$ we will on the average decode a smaller fraction of symbols than this and figure V-B shows the smallest possible gap in performance. This widens with increasing $p$ so that an efficient Raptor design at high SNR must choose $p$ to be low (a high rate code which corrects a small number of erasures). We are then left to see how such designs will perform when the SNR is low.

This picture changes if we replace BP decoding with say joint ML decoding of the Raptor code (including the underlying LDPC precode) . In this case capacity can be approached using choices of $\Omega$ which would restrict throughput if employed with BP decoding.

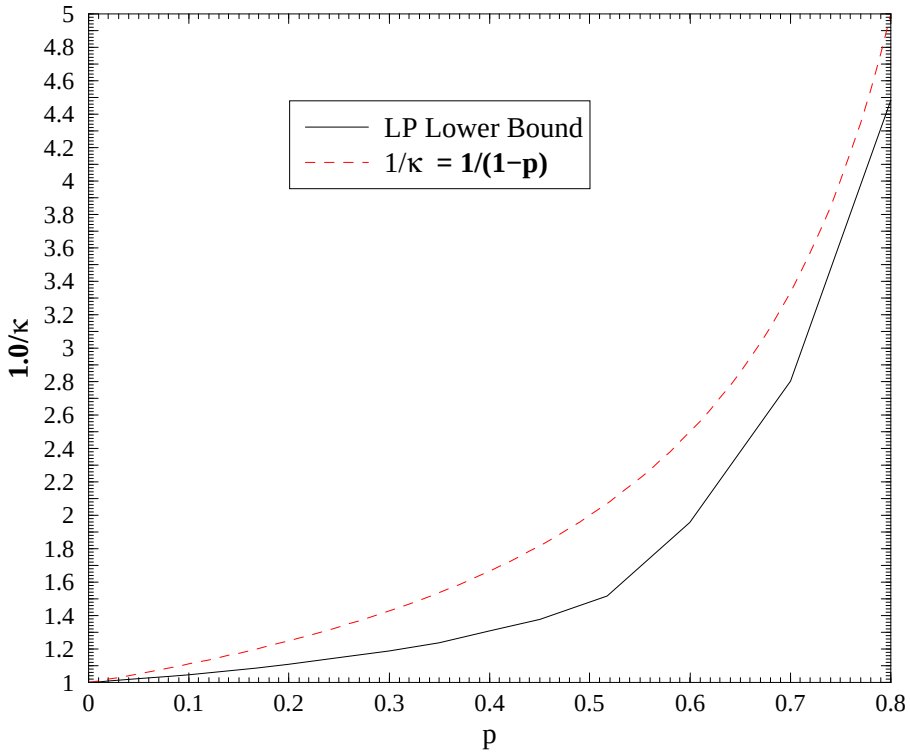



Fig. 5. LP Bound for Raptor Codes vs Iterative Decoding Threshold $p$

### *C. Raptor Code Examples*

In this section we present simulation results for IR-HARQ based on Raptor codes decoded using BP. In Figure 6 we show the results for three Raptor codes with the same LT degree distribution $\Omega(x) = 0.05x + 0.5x^2 + 0.05x^3 + 0.25x^4 + 0.05x^6 + 0.1x^8$ and three different regular LDPC precodes (with $\lambda(x) = x^2$ and $\rho(x) = x^4$, $\rho(x) = x^{14}$ and $\rho(x) = x^{29}$). The degree distribution polynomial $\Omega(x)$ was chosen in an ad-hoc manner – the choice was based on the results presented in [4]. We should note here that similar results are obtained when the degree distribution polynomial $\Omega(x)$ is derived using the linear programming optimization procedure for high SNRs presented in Section V-B.

First, we observe from Figure 6 that we benefit from using high rate LDPC precodes in Raptor coding schemes. In other words, as we increase the rate of the precode (from 0.4 to 0.8 and then to 0.9) higher throughputs are achievable at all SNRs of interest. (For high SNRs, this can also be concluded from Figure V-B.) Our results show that, among regular LDPC codes, the regular-(3,30) code achieves the satisfactory results and that increasing the LDPC precode rate above 0.9 results in negligible gains or no gains. We also note that the performance curve corresponding to the Raptor code with the regular-(3,30)

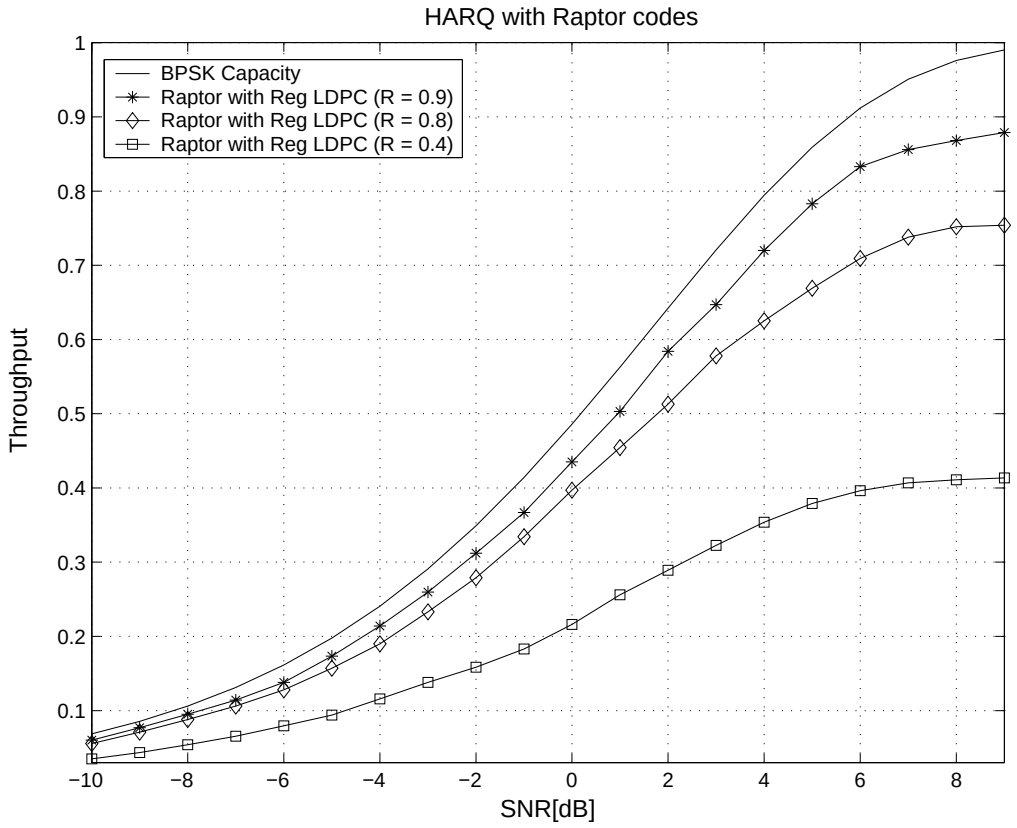



Fig. 6. Average throughput versus SNR for IR-HARQ scheme with Raptor codes on AWGN channel with BPSK signalling.

LDPC precode approaches the capacity to within 1dB for a wide range of SNRs.

As predicted by the analysis in Section V-B the curves saturate at high SNRs. Again, the predictions are accurate for very long block codes under assumption that the number of BP decoding iterations is sufficiently large. For finite length codes, these bounds can be used in estimating the throughput limits, but they are not tight. For example, the bound on the throughput for the regular-(3,15) LDPC precode from Section V (see Table I) is $T = 0.8699$. The simulation from Figure 6 shows the Raptor code curve saturates at the throughput roughly equaling $T = 0.75$.

## VI. Comparison Between HARQ Schemes Based on LDPC and Raptor Codes

In Section IV we discussed the theoretical results obtained for the two different schemes. We now turn to the comparison between the simulation results for IR-HARQ schemes based on LDPC and Raptor codes. In Figure 7 we plot the performance of HARQ with several different punctured LDPC codes

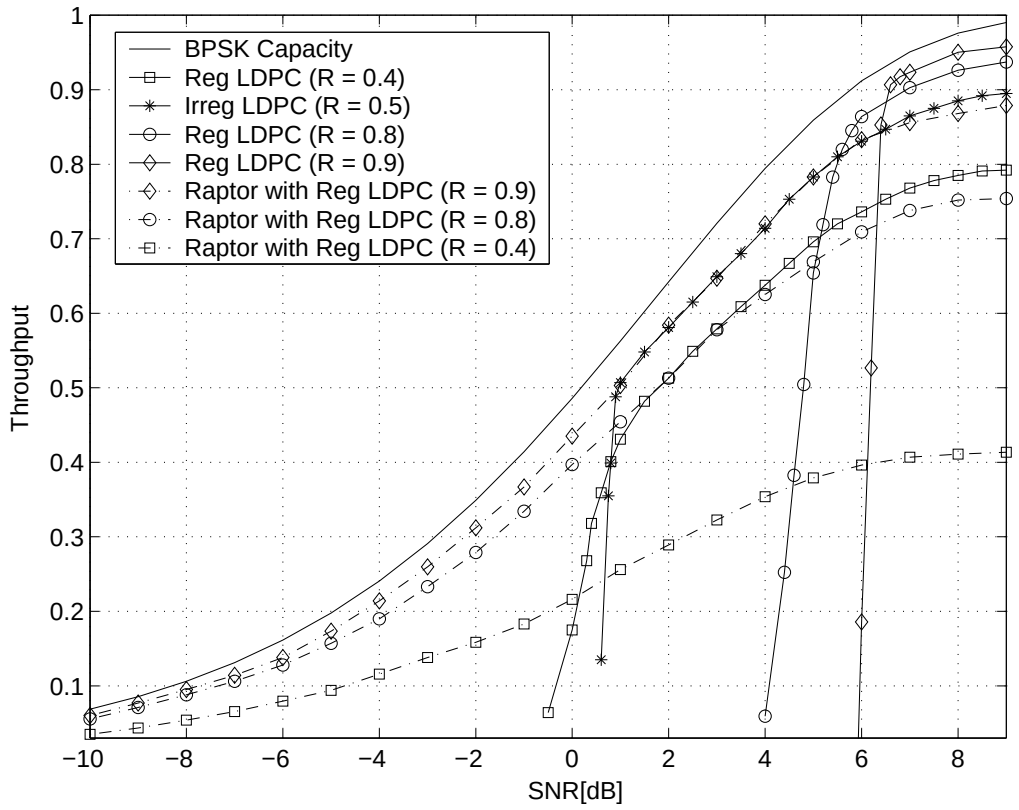



Fig. 7. Average throughput versus SNR for IR-HARQ schemes with LDPC and Raptor codes.

and Raptor codes. The performances of punctured LDPC codes with three different regular mother codes with $\lambda(x) = x^2$ and rates: $R = 0.4$, $0.5$ and $0.8$ are shown. (For comparison, in the same figure, we plot the BPSK capacity and the performance of the punctured LDPC code with the irregular mother code given in Figure 2). Also shown are three Raptor codes with the same three regular LDPC codes now used as precodes. The LT degree distribution polynomial $\Omega(x)$ in Raptor codes is given by $\Omega(x) = 0.05x + 0.5x^2 + 0.05x^3 + 0.25x^4 + 0.05x^6 + 0.1x^8$. We can observe from Figure 7 that Raptor codes have an obvious advantage at low SNRs. In fact, Raptor codes can be used for signalling at extremely low SNRs and still perform very near the capacity, which is generally difficult to achieve with standard punctured LDPC and turbo codes. For example, when the precode is a regular-$(3, 30)$ LDPC code, the Raptor code simulation shown in Figure 7 demonstrates that the throughput $T = 0.1$ bits is achieved at SNR about $0.65$dB away from the Shannon limit. Moreover, on the range of throughputs $T = 0 - 0.75$ the gap to the capacity for this Raptor code is less than $1$dB. Therefore, Raptor codes provide a much

broader dynamic range of rates (or SNRs) for HARQ than punctured LDPC codes, and in this respect are more robust than LDPC codes. On the other hand, using LT inner coding instead of puncturing on LDPC codes results in a performance loss in the high-SNR region as we have seen in Section V-B. This is also obvious from Figure 7. In particular, we can observe from this figure that if operating range of SNRs is guaranteed to be very high (say the SNR is always greater than 7dB) than it is more beneficial to use punctured LDPC codes with high rate mother codes than Raptor codes. However, if the information about SNR is not available or not reliable it is more advisable to use Raptor coding schemes in IR-HARQ.

Our final comment is on the difference between the encoding/decoding complexities of these schemes. Although the encoding and decoding complexities of Raptor codes are higher than the corresponding complexities of the underlying LDPC codes (and generally higher than the complexities of punctured LDPC codes) they have the property that we only need to encode as many parity bits as we need to send in the initial transmission or in subsequent re-transmission(s). On the other hand, for punctured codes we need to encode all parity bits, even though we may send only a small fraction of them[2].

## VII. Conclusion

We analyzed and compared IR-HARQ schemes based on two different families of codes: LDPC codes and Raptor codes. Our theoretical and simulation results suggest that both classes of codes are suitable for IR-HARQ.

The error rate performance results after each transmission on time varying binary-input, symmetric-output channels were given by analyzing both LDPC and Raptor codes on parallel channels. This analysis is based on the results on the spectra of ensembles of regular LDPC codes and Raptor codes and their performance bounds under the maximum-likelihood decoding assumption. Based on these results we proposed IR-HARQ protocols with a set of rules for incrementing redundancy and allocating the signal power at each transmission in order to maximize the throughput for both HARQ schemes. We also provided several results regarding belief-propagation decoding of LDPC and Raptor codes for HARQ in high SNR regions. Finally, we compared the simulation results for the HARQ schemes based on LDPC and Raptor codes under the belief-propagation decoding scenario.

Which codes are better to use depends whether the operating range of SNRs is available and (if available) on which part of the SNR axis this region lies. The presented results suggest that if the operating SNR region is not known, or if the operating region is very broad, it is beneficial to use Raptor

[2]An alternative approach that provides lower complexity than puncturing of LDPC bits is to use extending of LDPC codes [12].

codes. Even when the operating region is known, if this region covers relatively low SNRs Raptor codes provide near-capacity performance which is difficult to achieve with punctured LDPC or turbo codes at these SNRs. For instance, we have shown by simulations that Raptor codes with a carefully chosen degree distribution polynomial $\Omega(x)$ and a regular-(3,30) LDPC code used as a precode approach the capacity to within $0.65$dB at low SNRs. Moreover, these codes can operate near the capacity for the range of throughputs 0–0.75. On the other hand, the price one needs to pay for using Raptor codes instead of punctured LDPC codes is a higher encoding and decoding complexity.

This implies that appropriately optimized punctured LDPC codes may be more suitable when the operating region is known and is in medium-to-high SNRs. This is especially true in the very high SNR region (high throughput region) since in this region puncturing of LDPC codes is more effective than LT coding of LDPC encoded symbols. Moreover, the highest throughputs are achieved by high rate mother LDPC codes. Our results showed that these mother codes guarantee near-capacity performance (to within less than 1dB) at very high SNRs but that they have a quite narrow operating region of SNRs in which they are very effective.

## APPENDIX I
## THE LEFT TAIL OF THE SPECTRUM OF REGULAR LDPC CODE ENSEMBLES

Let $\Lambda_{k,n}$ denote the set of binary $k \times n$ matrices, and $\Lambda_{k,n}^{\mathbf{c},\mathbf{r}}$ denote the set of binary $k \times n$ parity-check matrices whose column weights are given by vector $\mathbf{c} = (c_1, \ldots, c_n)$ and row weights by $\mathbf{r} = (r_1, \ldots, r_k)$. If $c_i = c, \ \forall\, i$, and $r_i = r, \ \forall\, i$, the code ensemble with parity check matrices $\Lambda_{k,n}^{c,r}$ is referred to as *regular ensemble*; otherwise, the ensemble is referred to as *irregular*. We will deal only with the former case and assume that $r \geq 2$. We define the parameter $\zeta$ as

$$0 < \zeta = \frac{c}{r} = \frac{k}{n} < 1$$

for regular code ensembles, and denote the set of the corresponding parity check matrices by $\Lambda_n^{\zeta,r}$.

Counting the number of codewords of weight $w$ and the form

$$\mathbf{1}^w\mathbf{0}^{n-w} = \underbrace{11\ldots1}_{w \text{ times}}\,\underbrace{00\ldots0}_{n-w \text{ times}}$$

in the ensemble is equivalent to counting the number of matrices in $\Lambda_n^{\zeta,r}$ whose row sum over the first $w$ columns is even. Furthermore, a permutation of the columns of such a matrix ensures that the same permutation of $\mathbf{1}^w\mathbf{0}^{n-w}$ is then a codeword. Therefore, the average number of weight $w$ codewords in

the ensemble is at most $\binom{n}{w}$ times greater of the number of matrices in $\Lambda_n^{\zeta,r}$ whose row sum over the first $w$ columns is even.

For $n\theta = w = 1, 2, \ldots, n-1$, define $\Lambda_{n,\theta}^{\zeta,r} \subset \Lambda_n^{\zeta,r}$ as

$$\Lambda_{n,\theta}^{\zeta,r} = \Big\{ \Lambda \in \Lambda_n^{\zeta,r} : \sum_{j=1}^{w} \Lambda_{ij} \in \{0, 2, 4, \ldots\} \Big\}.$$

By the definition of an ensemble,

$$P_{n,\theta}^{\zeta,r} = \frac{\mid \Lambda_{n,\theta}^{\zeta,r} \mid}{\mid \Lambda_n^{\zeta,r} \mid} \tag{40}$$

is the probability of such a matrix. By constructing an upper bound on $P_{n,\theta}^{\zeta,r}$, we will obtain an upper bound on the spectrum of the code itself.

To enumerate $\Lambda_{n,\theta}^{\zeta,r}$ for $r$ even, we further define $L_{n,\theta}^{\zeta,r} \subset \Lambda_n^{\zeta,r}$ to be the set of binary matrices with the first $m_0$ rows having sum 0, the next $m_2$ rows having sum 2, and so on, the last $m_r$ rows having sum $r$. Thus $L_{n,\theta}^{\zeta,r}$ contains all possibilities for the first $w$ columns of a matrix in $\Lambda_{n,\theta}^{\zeta,r}$ given the row sums in increasing order. Similarly, we define $R_{n,\theta}^{\zeta,r}$ to be the set of corresponding matrices complementing $L_{n,\theta}^{\zeta,r}$ to form $\Lambda_{n,\theta}^{\zeta,r}$, with the first $m_0$ rows summing to $r$, the next $m_2$ rows summing to $r-2$ and so on. We have

$$\mid \Lambda_{n,\theta}^{\zeta,r} \mid = \sum \binom{\zeta n}{m_0 \; m_2 \; \ldots \; m_r} \mid L_{n,\theta}^{\zeta,r} \mid\mid R_{n,\theta}^{\zeta,r} \mid \tag{41}$$

where the sum is over all feasible combinations of the row sums *i.e.*, $m_0 \; m_2 \; \ldots \; m_r$ satisfying

$$\sum_j m_{2j} = \zeta n = m \quad \text{and} \quad \sum_j 2j m_{2j} = \zeta r \theta n = wc. \tag{42}$$

A similar result holds for $r$ odd, with (42) being over even arguments; so that, the final term is for $2j = r-1$ instead of $2j = r$.

To find bounds on $\mid \Lambda_{n,\theta}^{\zeta,r} \mid$, $\mid L_{n,\theta}^{\zeta,r} \mid$, and $\mid R_{n,\theta}^{\zeta,r} \mid$, we will use the following result on the number of zero-one matrices with prescribed column and row-weight. See [13] and references therein.

*Lemma 1:* The number $\mathcal{N}_{\mathbf{c},\mathbf{r}}$ of zero-one matrices with row weight distributions $\mathbf{r}$ and column weight distributions $\mathbf{c}$ can be bounded as follows:

$$\mathcal{N}_{\mathbf{c},\mathbf{r}} \leq \frac{S!}{\prod_i r_i! \prod_j c_j!}, \tag{43}$$

$S = \sum_i r_i = \sum_j c_j = nc = mr$.

Theorem 3 of [13] provides an asymptotic *lower bound* for $\mid \Lambda_n^{\zeta,r} \mid$:

$$\mid \Lambda_n^{\zeta,r} \mid \geq C_1 \frac{(nr\zeta)!}{(r!)^{n\zeta} \left((\zeta r)!\right)^n} \tag{44}$$

for sufficiently large $n > n_0$, which is of course independent of $\theta$.

We now establish the following theorem:

*Theorem 3:* For fixed $r, c \in \mathbb{N}$, $r$ even, there is a constant $C_2$, and $n_0$ both independent of $\theta$ such that

$$P_{n,\theta}^{r,\zeta} \leq C_2 \frac{1}{\binom{nr\zeta}{n\theta r\zeta}} \sum_{\mathbf{m}} \binom{\zeta n}{m_0 \ \cdots \ m_r} \binom{r}{2}^{m_2} \cdots \binom{r}{r-2}^{m_{r-2}} \tag{45}$$

whenever $n > n_0$. The sum is taken with values constrained as

$$m_0 + m_2 + \cdots + m_r = \zeta n$$

$$2m_2 + 4m_4 + \cdots + rm_r = \zeta\theta rn \tag{46}$$

*Proof:* We first apply Lemma 1 to upper bound $\mid L_{n,\theta}^{\zeta,r} \mid$ and $\mid R_{n,\theta}^{\zeta,r} \mid$. Then use (44) to lower bound $\mid \Lambda_n^{\zeta,r} \mid$ for sufficiently large $n_0$ and all $n > n_0$. The result follows on substituting into (41) and using the definition of $P_{n,\theta}^{r,\zeta}$ given in (40). ■

Again a similar result holds for $r$ odd with the changes indicated above.

We introduce next a simple method for evaluating the sum in (45) based on a set of results from large deviation theory. (We have also used this approach to compute the spectrum of trapping sets and simplify the proofs of [18] for stopping set enumeration [17]). Let

$$p_j \doteq 2^{-r} \binom{r}{j}, \tag{47}$$

hence $\boldsymbol{p} = \{p_j\}_{j=0}^{r}$ represents a probability vector. Multiplying both the numerator and denominator of the expression in (45) by $2^{r\zeta n}$, we obtain

$$P_{n,\theta}^{r,\zeta} \leq C_2 \frac{2^{r\zeta n}}{\binom{nr\zeta}{n\theta r\zeta}} \sum \binom{\zeta n}{m_0 \ldots m_r} p_0^{m_0} p_1^{m_1} \ldots p_r^{m_r}, \tag{48}$$

where the constraints (46) hold. The expression above can be bounded and its log-asymptotics can be assessed in terms of *Sanov's theorem* [3, p. 292], stated below.

*Theorem 4:* Let $\{X_1, \ldots, X_n\}$ be i.i.d random variables with probability mass function $Q(x)$ over a bounded set of $K$ elements. Let $\mathcal{F} \subset \mathcal{P}$ be a set of probability distributions. Then

$$Q^n(\mathcal{F}) = Q^n(\mathcal{F} \cap \mathcal{P}) \leq (n+1)^K \, 2^{-nD(P^*||Q)}, \tag{49}$$

where

$$P^* = \arg \min_{P \in \mathcal{F}} D(P||Q).$$

Furthermore, if $\mathcal{F}$ is the closure of its interior, then

$$\frac{1}{n} \log Q^n(\mathcal{F}) \to -D(P^*||Q).$$

Therefore, the problem of estimating the probability in (12) reduces to finding a probability mass function $q_i$ that minimizes $\sum\, q_i\, \log\,(q_i/p_i)$, such that

$$\sum_i\, q_i = 1 \quad \text{and} \quad \sum_i\, i q_i = \theta r, \tag{50}$$

with probabilities $p_i$ defined in (47). By using the Lagrangian multiplier method, with the multiplier function

$$\sum_i\, q_i \log \frac{q_i}{p_i} + \mu_1 \sum_i\, q_i + \mu_2 \sum_i\, i\, q_i + \mu_3 \sum_i\, q_{2i+1}, \tag{51}$$

one can show that the unique [3]optimizing distribution for both $r$ even and $r$ odd is of the form

$$q_i^* = \frac{2\binom{r}{i}\rho^i}{(1+\rho)^r + (1-\rho)^r}, \quad \text{for even values of } \; i, \tag{52}$$

and zero for odd values of $i$, where $\rho$ is the unique positive root of the equation

$$\frac{(1+\rho)^{r-1} + (1-\rho)^{r-1}}{(1+\rho)^r + (1-\rho)^r} = 1 - \theta. \tag{53}$$

It follows that

$$D(\boldsymbol{q}^* || \, \boldsymbol{p}) = \log \frac{2\rho^{\theta r}}{(1+\rho)^r + (1-\rho)^r} + \log G. \tag{54}$$

In the upper bound for $P_{n,\theta}^{r,\zeta}$ there remains the factor $\binom{nr\zeta}{n\theta r\zeta}^{-1}$ which we may upper bound using Stirling's formula (see for example [7, p. 530]):

$$\binom{nr\zeta}{n\theta r\zeta} > e^{n\zeta r h(\theta)} \frac{1}{\sqrt{8nr\zeta\theta(1-\theta)}}. \tag{55}$$

There is a corresponding upper bound for the remaining term in the spectrum,

$$\binom{n}{n\theta} < e^{nh(\theta)} \frac{1}{\sqrt{n2\pi\theta(1-\theta)}} \tag{56}$$

Using Theorem 3 together with (45), (49), (54), (55), (56), we obtain the following upper bound on the spectrum:

*Theorem 5:* There is a constant $C_3$ independent of $1 > \theta > 0$ and $n_0$ so that for $n > n_0$

$$\overline{A}_\theta^{[\mathcal{C}](n)} \leq C_3 \left[ \frac{(1+\rho)^r + (1-\rho)^r}{2\rho^{\theta r}} \right]^{n\zeta} \left[ (1-\theta)^{(1-\theta)} \theta^\theta \right]^{n(\zeta r - 1)}, \tag{57}$$

where $\rho$ is the unique positive root of (53).

[3]Uniqueness follows from the strict convexity of the relative entropy function with respect to the first argument, $q$

In order to apply the above result to bounding the left tail of the spectrum, we must investigate the behavior of $\rho$ near 0, which we examine using (53). As $\theta$ approaches 0, so does $\rho$ with

$$\rho^2 = \frac{\theta}{r-1} + O(\theta^2).$$

Since $\binom{r}{2}\rho^2 = r\theta/2 + O(\theta^2)$,

$$\log\left[\frac{1}{2}\left((1+\rho)^r + (1-\rho)^r\right)\right]^{n\zeta}[1-\theta]^{n(\zeta r-1)(1-\theta)} = n\theta\left\{\frac{\zeta r}{2} - (1-\theta)(\zeta r - 1) + O(\theta^2)\right\} < 0$$

for all sufficiently small $\theta$ and $c \geq 2$. We thus have that

$$\overline{A}_\theta^{[\mathcal{C}](n)} \leq C_3\left[\frac{\theta^{\zeta\theta r}}{\rho^{\zeta\theta r}\theta^\theta}\right]^n$$

Using our estimate for $\rho$ for sufficiently small $\theta$ there is an $\varepsilon > 0$ so that the RHS is upper bounded by

$$C_3\left[\frac{\theta^{\zeta r}\left((r-1)(1+\varepsilon)\right)^{\frac{\zeta r}{2}}}{\theta\theta^{r\zeta/2}}\right]^{n\theta} = C_3\left[\theta^{(c/2-1)}\cdot\left((r-1)(1+\varepsilon)\right)^{c/2}\right]^{n\theta}. \tag{58}$$

Thus the tail of the spectrum for some $\theta_0 > 0$ is upper bounded by

$$\sum_{j=1}^{\lceil n\theta_0\rceil}\overline{A}_\theta^{[\mathcal{C}](n)} < C_3\sum_{j=1}^{\lceil n\theta_0\rceil}\left[\left(\frac{ja}{n}\right)^{c/2-1}\right]^j,$$

where $a = [(r-1)(1+\varepsilon)]^{c/(c-2)}$ We now show that this converges to 0 as $n\to\infty$ for suitable choice of $\theta_0$. We must choose $c \geq 3$ and note that we may show the result for $c = 3$ only as the individual terms decrease monotonically as $c$ is increased provided $(ja)/n < 1$. Also by considering $x\log x$ we observe that the sequence $((ja)/n)^j$ decreases as $j$ increases provided $(ja)/n < e^{-1}$. Thus

$$\sum_{j=1}^{\lceil n\theta_0\rceil}\overline{A}_\theta^{[\mathcal{C}](n)} < \sum_{j=1}^{\lceil n\theta_0\rceil}\left[\left(\frac{ja}{n}\right)^{c/2-1}\right]^j < (a/n)^{\frac{1}{2}} + (2a)/n + n\theta_0\left((3a)/n\right)^{3/2}$$

and so converges to 0 at least as fast as $O(n^{-\frac{1}{2}})$.

## REFERENCES


[1] G. Caire and D. Tuninetti. The throughput of Hybird-ARQ protocols for the Gaussion collision channel. *IEEE Trans. Inform. Theory*, 47:1971–1988, July 2001.

[2] D. J. Costello, J. Hagenauer Jr., H. Imai, and S. B. Wicker. Applications of error-control coding. *IEEE Trans. Inform. Theory*, 44:2531–2560, 1998.

[3] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley, John & Sons, Inc.

[4] O. Etesami and A. Shokrollahi. Raptor codes on symmetric channels. *preprint*, 2005.

[5] J. Feldman. *Decoding Error-Correcting Codes via Linear Programming*. PhD thesis, California Istitute of Technology, 2003.

[6] M.P.C. Fossorier. Iterative reliability based decoding of low-density parity check codes. *IEEE Journal on Selected Areas in Communications*, 19:908–917, May 2001.

[7] R. Gallager. *Information Theory and Reliable Communication*. John Wiley, London, 1968.

[8] J. Ha, J. Kim, and S.W. McLaughlin. Rate-compatible puncturing of low-density parity-check codes. *IEEE Trans. Inform. Theory*, 50:2824–2836, November 2004.

[9] H. Jin and R.J. McEliece. Coding theorems for turbo code ensembles. *IEEE Trans. Inform. Theory*, 48:1451–1461, June 2002.

[10] A. Khandekar. *Graph Based Codes and Iterative Decoding*. PhD thesis, Massachuestts Institute of Technology, Cambridge MA, 2003.

[11] J. Kim, A. Ashikhmin, A. van Wijngaarden, E. Soljanin, and N. Gopalakrishnan. On efficient link error prediction based on convex metrics. In *2004 IEEE 60th Vehicular Technology Conference, (VTC2004-Fall)*, volume 6, pages 4190 – 4194, 26-29 Sept. 2004.

[12] J. Li and K. Narayanan. Rate-compatible low-density parity-check codes for capacity-approaching ARQ scheme in packet data communications. In *Int. Conf. on Comm., Internet, and Info. Tech. (CIIT)*, Nov. 2002.

[13] S. Litsyn and V. Shevelev. On Ensmebles of Low Density Parity-Check Codes. *IEEE Trans. Inform. Theory*, 48:887–908, April 2002.

[14] R. Liu, P. Spasojević, and E. Soljanin. Reliable channel regions for good binary codes transmitted over parallel channels. *IEEE Trans. Inform. Theory*, submitted for publication, Oct. 2004.

[15] M. Luby. LT codes. In *Proc. of the 43rd Annual IEEE Symp. on the Foundations of Comp. Science (STOC)*, 2002.

[16] M. Shokorollahi M Luby, M. Mitzenmacher and D. Spielman. Efficient erasure correcting codes. *IEEE Transactions Information Theory*, 47(2):569–584, 2001.

[17] O. Milenkovic, E. Soljanin, and P. Whiting. On average throughput benefits for network coding. *submitted to 43rd Annual Allerton Conference*, Monticello, IL, Oct. 2005.

[18] A. Orlitsky, K. Viswanathan, and J. Zhang. Stopping setdistribution of ldpc code ensembles. *IEEE Trans. Inform. Theory*.

[19] H. Pishro-Nik and F. Fekri. On decoding of low-density parity-check codes over the binary erasure channel. *IEEE Tran. Inform. Theory*, 50:439–454, March 2004.

[20] T. Richardson, A. Shokrollahi, and R. Urbanke. Design of capacity approaching irregular low-density parity check codes. *IEEE Trans. Inform. Theory*, 47(2):619–637, 2001.

[21] T. Richardson, A. Shokrollahi, and R. Urbanke. Design of capacity-approaching low-density parity-check codes. *IEEE Trans. Inform. Theory*, 47:619–637, February 2001.

[22] T. Richardson and R. Urbanke. The capacity of low density parity-check codes under message passing decoding. *IEEE Transactions Information Theory*, 47(2):599–618, 2001.

[23] D.N. Rowitch and L.B. Milstein. On the performance of hybrid FEC/ARQ systems using rate compatible punctured turbo (RCPT) codes. *IEEE Trans. Commun.*, 48:948–959, June 2000.

[24] S. Sesia, G. Caire, and G. Vivier. Incremental redundancy Hybrid ARQ schemes based on low-density parity-check codes. *IEEE Trans. Commun.*, submitted for publication.

[25] A. Shokrollahi. Raptor codes. *preprint*, 2002.

[26] E. Soljanin, R. Liu, and P. Spasojević. Hybrid ARQ with random transmission assignments. In P. Gupta, G. Kramer, and A. Wijngarden, editors, *Advances in Network Information Theory*, volume 66, pages 321–334. DIMACS Series in Discrete Mathematics and Thepretical Computer Science, American Mathematical Society, August 2004.

[27] N. Varnica, M. Fossorier, and A. Kavčić. Augmented belief-propagation decoding of low-density parity-check codes. Submitted to IEEE Transactions on Communications.

[28] N. Varnica, E. Soljanin, and P. Whiting. LDPC codes for HARQ. In *Proc. 2005 IEEE Internat. Symp. Inform. Theory*, Adelaide, 4-9, Sept. 2005.

[29] M.R. Yazdani and A.H. Banihashemi. On construction of rate-compatible low-density parity-check codes. *IEEE Commun. Lett.*, 8:159–161, March 2004.