The Throughput of an LDPC-Based Incremental-Redundancy Scheme over Block-Fading Channels

Stefania Sesia, and Giuseppe Caire [1]
Eurecom Institute,
Sophia Antipolis, France.
{sesia, caire}@eurecom.fr

I. Introduction and Background

INcremental-Redundancy (INR) is a form of hybrid ARQ where the receiver asks the transmitter for additional parity bits when decoding is not successful. This technique is particularly useful in time-selective fading channels, since it implements variable-rate adaptive transmission with a very simple feedback binary channel, where the feedback messages are positive or negative acknowledgments (ACK and NACK, respectively).

An information-theoretic analysis of the achievable throughput and delay of INR over block-fading channels, assuming random Gaussian code ensembles, is provided in [5]. In this work, we provide results for random binary codes and for Low-Density Parity-Check (LDPC) binary linear codes.

In the channel model under consideration, time is divided into *slots* of duration T and (approximate) bandwidth W. Under the assumption that $WT \gg 1$, the number of complex independent dimensions per slot available for transmission is $L \approx WT$. The channel in slot s is defined by

$$\mathbf{y}_s = c_s \, \mathbf{x}_s + \nu_s \tag{1}$$

where $\mathbf{x}_s, \mathbf{y}_s$ and ν_s denote the transmitted, received and noise signal sequences in slot s, given by

$$\begin{aligned} \mathbf{x}_s &= (x_{s,1}, x_{s,2}, \ldots, x_{s,L}) \\ \mathbf{y}_s &= (y_{s,1}, y_{s,2}, \ldots, y_{s,L}) \\ \nu_s &= (\nu_{s,1}, \nu_{s,2}, \ldots, \nu_{s,L}) \end{aligned} \tag{2}$$

and c_s is the (scalar) channel fading coefficient. The noise is zero-mean complex Gaussian with i.i.d components with variance N_0. The energy per symbol is constant and given by $E = \left[|x_{s,l}|^2\right]$. The fading is frequency non-selective and constant over each slot (block-fading). Moreover, we assume that the fading is normalized so that $E[|c_s|^2] = 1$ and it is i.i.d. over different blocks (this model applies, for example, to narrowband transmission with slow frequency-hopping). We denote by $\gamma = E/N_0$, $\alpha_s = |c_s|^2$ and $\beta_s = \alpha_s \gamma$ the average SNR, the fading power gain and the instantaneous SNR on slot s, respectively.

The transmitter encodes information messages of b bits, by using a channel code with codebook $\mathcal{C} \in \mathbb{C}^{LM}$ of length LM where M is a given integer. The codewords are divided in M subblocks of length L. Each subblock is sent over one slot. Let $\mathcal{C}_m$ denote the punctured code of length Lm obtained from $\mathcal{C}$ by deleting the last $M - m$ subblocks. As in [5], the system works according to the following INR protocol. In order to transmit a given codeword, the transmitter sends the first L symbols on slot s_1. The receiver decodes the code $\mathcal{C}_1$, by processing the corresponding received signal $\mathbf{y}_{s_1}$. If decoding is successful, an ACK is sent on a delay-free error-free feedback channel, the transmission of the current codeword is stopped and the transmission of the next codeword will start in the next slot (say, s_2). If a decoding error is revealed, then a NACK is sent and the next subblock of the current codeword is sent on the next slot s_2. In this case, the receiver decodes $\mathcal{C}_2$ by processing the received signal $\{\mathbf{y}_{s_1}, \mathbf{y}_{s_2}\}$ and the same ACK/NACK procedure is repeated, until either successful decoding occurs, or all M subblocks of the current codeword are transmitted without succesful decoding. For simplicity, and without loss of generality as far as the throughput is concerned, we may assume that in the latter case the information message is lost. Let $R = \frac{b}{LM}$ denote the rate of code $\mathcal{C}$ and let $r = \frac{b}{L}$. If succesful decoding occurs after m subblocks, the effective coding rate for the current codeword is $\frac{r}{m}$ bit/symbol. Let $J(\beta_s)$ denote the mutual information (per input symbol) on slot s, for a given (fixed) input distribution $Q(x)$. Following [5], we have that there exist codes $\mathcal{C}$ such that, for sufficiently large L, the probability of decoding error after m slots (conditioned on the fading realization) vanishes if

$$I_m \stackrel{\Delta}{=} \sum_{i=1}^{m} J(\beta_{s_i}) > r \tag{3}$$

On the contrary, for all codes $\mathcal{C}_m$ of length mL the (conditional) probability of decoding error tends to 1 if $I_m < r$. Finally, the (conditional) probability of an undetected decoding error, assuming typical set decoding, vanishes for sufficiently large L. In the following, the probability $\Pr(I_m \leq r)$ will be referred to as the *information outage probability* at step m.

II. Throughput Analysis

We analyse the average throughput of the INR protocol described above in the limit of large L. The throughput, expressed in bits per second per Hertz is given by

$$\eta = \lim_{t \to \infty} \frac{b(t)}{Lt} \tag{4}$$

where t counts the number of slots and $b(t)$ the number of information bits successfully decoded up to slot t. The event $\mathcal{E} = \{$The user stops transmitting the current codeword$\}$ is recognized to be a *recurrent event* ([4, 8, 5]). A random *reward* $\mathcal{R}$ is associated to the occurrence of the recurrent event: $\mathcal{R} = r$ bit/symbol if transmission stops because successful decoding and $\mathcal{R} = 0$ bit/symbol if it stops because at step M it is not possible to successfully decode. As an application of the Renewal Theorem we obtain

$$\eta = \frac{\mathrm{E}[\mathcal{R}]}{\mathrm{E}[\tau]} \tag{5}$$

[1] This work was supported by Motorola Lab, Paris.

where τ is the inter-renewal time expressed in number of slots, i.e., it is the time between two consecutive occurrences of the recurrent event.

We define the event $\mathcal{A}_m = \{I_m > r\}$ and the probability $q(m)$ of successful decoding with m transmitted slots. We have

$$\begin{aligned} q(m) &\triangleq \Pr\left(\overline{\mathcal{A}}_1, \overline{\mathcal{A}}_2, \ldots, \overline{\mathcal{A}}_{m-1}, \mathcal{A}_m\right) \\ &= p(m-1) - p(m) \end{aligned} \tag{6}$$

where we define

$$p(m) \triangleq \Pr\left(\overline{\mathcal{A}}_1, \overline{\mathcal{A}}_2, \ldots, \overline{\mathcal{A}}_m\right) = 1 - \sum_{i=1}^{m} q(m) \tag{7}$$

Hence, from (5) it is immediate to obtain

$$\eta = R\,M\,\frac{1-p(M)}{1+\sum_{m=1}^{M-1} p(m)} \tag{8}$$

Random Binary Codes. We apply the above throughput analysis to random binary codes, i.e., when the input distribution $Q(x)$ puts uniform probability on the binary antipodal alphabet $\{-\sqrt{E}, \sqrt{E}\}$. We have to compute the probability

$$p(m) = \Pr(I_1 \le r, \ldots, I_m \le r) \tag{9}$$

Since $I_m = \sum_{i=1}^{m} J(\beta_i)$ is a non-decreasing sequence with probability 1, then

$$p(m) = \Pr\left(\sum_{i=1}^{m} J(\beta_i) \le r\right) \tag{10}$$

On slot i, the conditional mutual information function $J(\beta_i)$ is given by

$$J(\beta_i) = 1 - \int_{-\infty}^{\infty} \log_2\left(1 + e^{4\sqrt{\beta_i}\left(z-\sqrt{\beta_i}\right)}\right) \frac{e^{-z^2}}{\sqrt{\pi}} \mathrm{d}z \tag{11}$$

Since the β_i's are i.i.d. random variables, the cumulative distribution function (cdf) (10) is obtained from the m-fold convolution of the probability density function (pdf) of $J(\beta_i)$, given by

$$f(x) = \frac{1}{\gamma} f_\alpha\left(J^{-1}(x)/\gamma\right)\left(\frac{\mathrm{d}J^{-1}(x)}{\mathrm{d}x}\right) \tag{12}$$

where $f_\alpha(x)$ is the fading gain pdf. In order to reduce the computation complexity for large m, we can use the Gaussian Approximation (GA) or the Chernoff bound. Using the GA, we have

$$p(m) \approx 1 - \mathrm{Q}\left(\frac{r - m\mu}{\sqrt{m}\sigma}\right) \tag{13}$$

where μ and σ^2 are the mean and the variance of $J(\beta_i)$. Using the Chernoff bound, we have

$$p(m) \le \min_{\lambda} e^{\lambda r}[\Phi(\lambda)]^m \tag{14}$$

where $\Phi(\lambda) = \mathrm{E}\left[e^{-\lambda J(\beta_i)}\right]$ is the moment-generating function of $J(\beta_i)$.

In all our numerical examples we assumed Rayleigh fading, i.e., $f_\alpha(x) = e^{-x}$. Figs. 1 and 2 show the probabilities $p(m)$ for different values of m as a function of the coding rate R, for $\gamma = 0$dB and 10dB, respectively. For large SNR ($\gamma = 10$dB), $p(m)$ shows a "step" behavior while for small SNR ($\gamma = 0$dB) it is a smooth function of R. Figs. 3 and 4 show the throughput vs. R evaluated via convolution, GA and Chernoff bound for $\gamma = 10$ and 0dB, respectively. The Chernoff bound yields a loose lower bound for small SNR, while the accuracy of the GA improves for small SNR. The (almost) piecewise linear behavior of the throughput as a function of R for large SNR is explained by the step behavior of the probabilities $p(m)$. For example, for $R \in [0.1, 0.2]$ bit/symbol we have $\eta \approx \frac{RM}{1+p(1)+p(2)}$. In particular, since $p(1) = 1$ and $p(2) \approx 0$ for $R = 0.1$ and $p(1) = p(2) \approx 1$ for $R = 0.2$, the throughput takes on the values 1/2 and 2/3, respectively. For $R \in (0.1, 0.2)$, $p(2)$ increases slowly with R, so that $\hat{\eta} = RM/(2+\epsilon(R))$ with $\epsilon(R) \ll 1$. Therefore, η is an almost linear function of R in this interval. This effect is less obvious for larger values of R.

LDPC codes. *Low Density Parity Check* [6] are a class of very powerful random like binary codes suited to iterative decoding via the belief propagation (BP) algorithm. Their bit-error rate (BER) performance under BP, in the limit of large block length, can be obtained via the *Density Evolution* (DE) method [7]. These codes exhibit a threshold phenomenon: as the block length tends to infinity, an arbitrarily small BER can be achieved if the noise level is smaller than a certain threshold [7]. Otherwise, the BER is bounded away from zero for any number of decoder iterations.

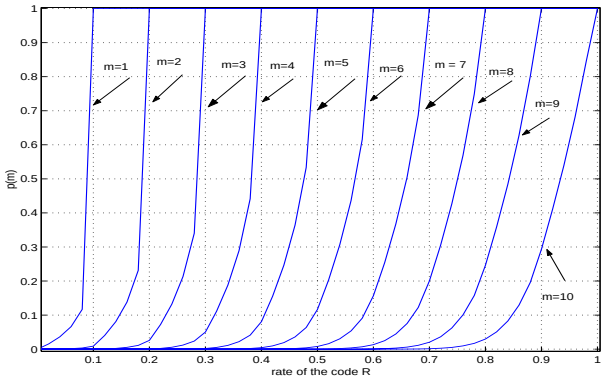

Fig. 1: $p(m)$ for $\gamma = 10$dB.

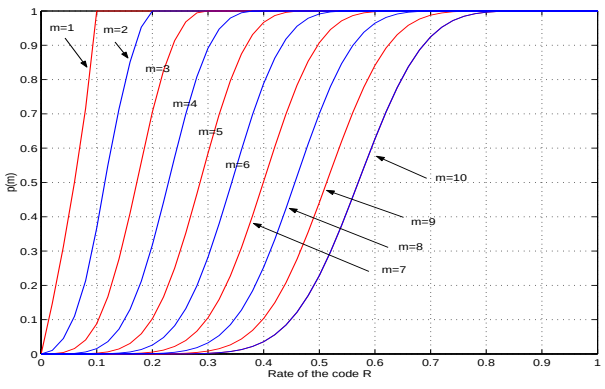

Fig. 2: $p(m)$ for $\gamma = 0$dB.

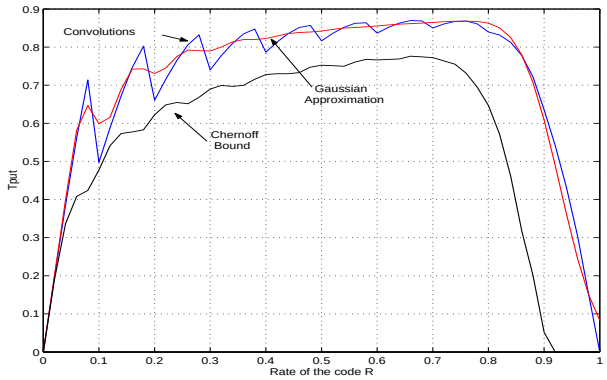

Fig. 3: η for $\gamma = 10$dB.

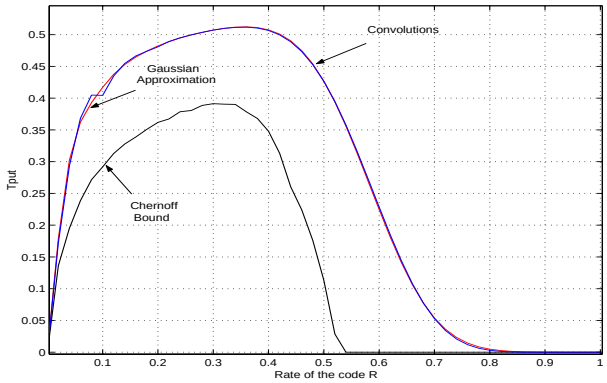

Fig. 4: η for $\gamma = 0$dB.

In our analysis, we assume that decoding is successful with high probability if, after m received slots, the BER under BP decoding tends to zero with the number of decoder iterations, while we have decoding failure if the BER is bounded away from zero. We assume that this behavior can be detected by the decoder, so that decoding failure is always revealed. Hence, we can use the same throughput formula with the new definition of $p(m)$ as

$$p(m) = \Pr\left(\lim_{l\to\infty} \mathrm{BER}^{(l)}(m) > 0\right) \tag{15}$$

where $\mathrm{BER}^{(l)}(m)$ is the BER at BP decoder iteration l with m received slots.

We assume that the reader is familiar with BP decoding and the DE method (see for the details [7]). Consider the LDPC ensemble defined by the left and right degree sequences $\lambda(x)$ and $\rho(x)$. Denote by v the messages sent from bitnodes to checknodes, and by u the messages sent from checknodes to bitnodes. Let u_0 denote the channel observation message, in the form of the log-likelihood ratio for the symbol associated to the given bitnode, given the channel output. Assuming, without, loss of generality that the all-zero codeword is transmitted, u_0 is real Gaussian with mean $4\beta_m$ and variance $8\beta_m$ if the symbol corresponding to the bitnode is transmitted on the m-th slot. In order to simplify the DE, we use the following Gaussian Approximation: we assume that all messages are Gaussian distributed, and we enforce the *symmetry condition* [7, 3] that must be satisfied by the true distribution of the messages propagated by the BP. The symmetry condition applied to a Gaussian distribution implies that, at each iteration, the variance of the messages is equal to twice the conditional mean. Therefore, tracking the evolution of the message distribution along the BP iterations is equivalent to tracking the evolution of the message mean. However, following [1], we choose to express the one-parameter evolution by using mutual information.

We define a random variable P that governs the distribution of the variable node belonging to the m-th block, so that P is uniformly distributed over $m = 1, \ldots, M$. Let X denote the bitnode variable and Y denote all the information available at the bitnode at a given iteration. Then, the mutual information between the output of the bitnode and the symbol X is given by

$$I(X, Y \,|\, P) \;=\; \sum_{m=1}^{M} \frac{1}{M}\, I(X, Y \,|\, P = m) \tag{16}$$

From the Gaussian Approximation, it follows that

$$I(X; Y | P = m) = J((d-1)\mu + \gamma\alpha_m)$$

for a bitnode of degree d transmitted on slot m, where μ denotes the mean divided by 4 of the messages u coming from the checknodes. Hence, the mutual information of a message passed along a random edge from a bitnode to a checknode at iteration l is given by

$$I^l_{out,v} = \frac{1}{M} \sum_{m=1}^{M} F_\lambda\left(I^{l-1}_{out,c}, \gamma\alpha_m\right) \tag{17}$$

where we define

$$F_\lambda(x, a) \stackrel{\Delta}{=} \sum_i \lambda_i J\left((i-1)J^{-1}(x) + a\right)$$

and where $I^{l-1}_{out,c}$ is the mutual information of messages passed along a random edge from a checknode to a bitnode at iteration $l-1$.

In order to find the mutual information transfer function relationship for the checknodes, we use the reciprocal channel approximation [2]. With this approximation, a checknode can be replaced by a bitnode provided that its input mutual information I_{in} is transformed into $1 - I_{in}$ and its output mutual information I_{out} is transformed into $1 - I_{out}$. Hence, the mutual information transfer of a checknode of degree d is approximated by

$$I^l_{out,c} = 1 - J\Big((d-1)\; J^{-1}\left(1 - I^l_{out,v}\right)\Big) \tag{18}$$

Therefore, the mutual information of a message passed along a random edge from a checknode to a bitnode at iteration l is given by

$$I^l_{out,c} = 1 - F_\rho\left(1 - I^l_{out,v}, 0\right) \tag{19}$$

By putting together equations (17) and (19), we obtain the one-dimensional recursion

$$I^l_{out,v} \;=\; \frac{1}{M} \sum_{m=1}^{M} F_\lambda\left(1 - F_\rho\left(1 - I^{l-1}_{out,v}, 0\right), \gamma\alpha_m\right) \tag{20}$$

with initial condition $I^0_{out,v} = 0$.

The trajectories (and hence the fixed points) of the above recursion are functions of the fading coefficients α_m. The condition of vanishing BER is approximated by the condition that (20) has a unique fixed point in $I_{out,v} = 1$. This holds if and only if

$$\Psi(z, \alpha_1, \ldots, \alpha_M) > z, \quad \forall\, z \in [0, 1) \tag{21}$$

where we define the iteration mapping function

$$\Psi(z, \alpha_1, \ldots, \alpha_M) \triangleq \frac{1}{M} \sum_{m=1}^{M} F_\lambda(1 - F_\rho(1 - z, 0), \gamma\alpha_m)$$

Finally, we evaluate by Monte Carlo simulation the probabilities $p(m)$ as

$$p(m) = \Pr\left(\Psi\left(z, \alpha_1, \ldots, \alpha_m, \underbrace{0, \ldots, 0}_{M-m} \right) > z, \quad \forall\, z \in [0, 1) \right)$$

where $\alpha_1, \ldots, \alpha_m$ are i.i.d., distributed according to the fading pdf $f_\alpha(x)$.

Figs. 5 and 6 show the comparison between the throughput obtained using random binary codes and the LDPC codes. The results for LDPC codes have been obtained by considering irregular codes where for each value of R we use the degree distribution optimized for that R and for the binary-input AWGN channel, [7]. We observe that the LDPC codes yield throughput very close to binary random codes, and therefore are good candidate component codes for INR schemes. Fig. 7 shows the details for the interval $R = (0.1, 0.3)$b/s/Hz. We notice that by choosing carefully the basic coding rate, it is possible to increase the throughput considerably. For example, by using $R = 0.12$ instead of $R = 0.1$ the throughput increases from 0.5 to 0.59.

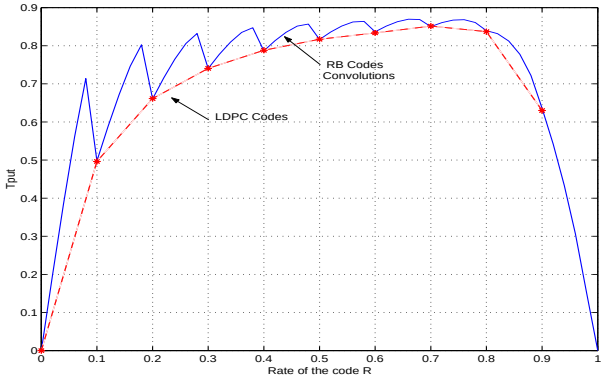

Fig. 5: Throughput of LDPC codes and binary random codes for $\gamma = 10$dB.

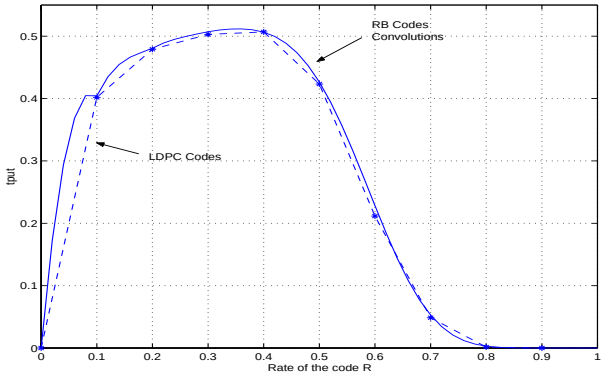

Fig. 6: Throughput of LDPC codes and binary random codes for $\gamma = 0$dB.

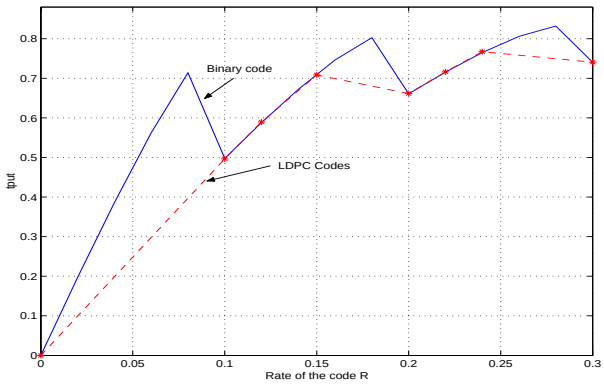

Fig. 7: Throughput of LDPC codes for $\gamma = 10$dB in the range $R = (0.1, 0.3)$ bit/symbol.

References

[1] S. T. Brink, "Convergenge Behavior of Iteratively Decoded Parallel Concatenated Codes", *IEEE Trans. on Communications*, 2001.

[2] S. Y. Chung, "On the Construction of Some Capacity-Approaching Coding Scheme", *PhD thesis, Massachussetts Institute of Technology*, 2000.

[3] S. Y Chung, T. J. Richardson, and R. L Urbanke, "Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Aproximation", *IEEE Trans. on Information Theory*, 2001.

[4] W. Feller, "An Introduction of Probability Theory and Its Applications", *John Wiley and Sons*, 1968.

[5] Caire G. and D. Tuninetti, "The Throughput of Hybrid-ARQ Protocols for the Gaussian Collision Channel", *IEEE Trans. on Information Theory*, 2001.

[6] R. G. Gallager, "Low-Density Parity-Check Codes", *PhD thesis, Cambrige, MA: MIT Press*, 1963.

[7] T. J. Richardson and R. L Urbanke, "The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding", *IEEE Trans on Information Theory*, 2001.

[8] M. Zorzi and R. R. Rao, "On the Use of Renewal Theory in the Analysis of ARQ Protocols", *IEEE Trans. on Communications*, 1996.