Error Exponents of Low-Density Parity-Check Codes on the Binary Erasure Channel

Thierry Mora
Laboratoire de Physique Théorique et Modèles Statistiques, Bât. 100
Université Paris-Sud and CNRS
F–91405 Orsay, France.
Email: mora@lptms.u-psud.fr

Olivier Rivoire
Laboratory of Living Matter
The Rockefeller University
1230 York Avenue, Box 34
New York, NY–10021, USA
Email: orivoire@rockefeller.edu

Abstract — **We introduce a thermodynamic (large deviation) formalism for computing error exponents in error-correcting codes. Within this framework, we apply the heuristic cavity method from statistical mechanics to derive the average and typical error exponents of low-density parity-check (LDPC) codes on the binary erasure channel (BEC) under maximum-likelihood decoding.**

I. Introduction

Assessing the performance of error-correcting codes is a founding topics of information theory. Amongst the simplest codes are the binary *block codes*, where a source generates with equal probability one of 2^L *codewords*, each a sequence of N bits. As a codeword is transmitted through a *discrete memoryless channel*, a noise ξ alters independently each bit with some probability. The *binary erasure channel* (BEC), for instance, erases a bit with a prescribed probability $p \in [0,1]$. Given the received message, the decoding task consists in inferring the most likely original codeword. The probability of error $\mathbb{P}_\xi(\text{error}|\mathcal{C}_N)$ then provides a simple characterization of the performance of a code $\mathcal{C}_N$.

The properties of error-correcting codes are conveniently studied through *ensembles* of codes C_N, consisting for instance of the set of all block codes with length N and *rate* $R = L/N$. Shannon showed that, in the limit $N \to \infty$, a typical code in such an ensemble has a vanishing probability of error if (and only if) $R < R_c(p)$, where $R_c(p)$ corresponds to the *channel capacity*. This capacity is simply $R_c(p) = 1 - p$ for the BEC. We are here interested in refining the description of the error probability beyond the channel capacity. *Error exponents* give the exponential rate of decay of $\mathbb{P}_\xi(\text{error}|\mathcal{C}_N)$ with N, for $\mathcal{C}_N \in C_N$, and offer the most appealing generalization. Of particular interest is the so-called *reliability function*, which gives the lowest achievable exponents as a function of the rate R [2]. However, despite significant efforts to estimate error exponents, resulting in the establishment of a number of bounds, exact expressions are scarce and restricted to a few extreme cases.

In this note, we put forward a *thermodynamic* (or *large deviation*) formalism [13] for evaluating error exponents in error-correcting codes. This formalism coherently encompasses two types of exponents: if $C = \{C_N\}_{N\geq 1}$ denotes a sequence of ensembles of codes, we can indeed define, depending on the procedure for choosing the codes $\mathcal{C}_N$ in the ensembles C_N, an *average* and a *typical* error exponents as

$$E_{\text{av}} = -\lim_{N\to\infty} \frac{1}{N} \log \mathbb{E}_{\mathcal{C}_N} \left[\mathbb{P}_\xi(\text{error}|\mathcal{C}_N)\right], \quad (1)$$

$$E_{\text{typ}} = -\lim_{N\to\infty} \frac{1}{N} \mathbb{E}_{\mathcal{C}_N} \left[\log \mathbb{P}_\xi(\text{error}|\mathcal{C}_N)\right], \quad (2)$$

where $\mathbb{E}_{\mathcal{C}_N}$ denotes the expectation value when $\mathcal{C}_N$ is drawn uniformly from the ensemble C_N (log is base 2 throughout). Although the typical error exponent is the most interesting from the practical point of view, the average error exponent is usually simpler to estimate theoretically.

We analyze in the thermodynamic formalism one of the most promising family of block codes, the low-density parity-check (LDPC) codes [5]. The codewords of these codes correspond to the kernel of a sparse $M \times N$ *parity-check matrix* A, with $M = N - L$. Different choices for A lead to different ensemble of codes C_N, the simplest example being regular ensembles[1] defined with A having ℓ 1's per column and k per line, and zeros otherwise (in which case $R = 1 - \ell/k$). LDPC codes have been shown to formally map to physical models of disordered systems on random graphs [7], and we shall exploit this analogy to apply the (non-rigorous) cavity method [12] recently proposed in this context[2] (see also [14] for a related approach).

II. Thermodynamic formalism

Given a received word, consisting of a codeword from a code $\mathcal{C}_N$ altered by a noise ξ on the BEC, let $\mathcal{N}_N(\xi, \mathcal{C}_N)$ be the number of codewords from which it could come from (this quantity is independent of the initial codeword with LDPC codes). By definition, decoding is achievable if and only if $\mathcal{N}_N(\xi, \mathcal{C}_N) = 1$. For random codes, the geometry of the space of codewords indicates that, at least in

[1] In this paper we restrict to regular codes, even though our method can be generalized to any irregular ensemble [11].

[2] While the exponential scaling of the error probability is guaranteed when the ensemble of codes comprises all block codes, the average error probability of LDPC codes is known to be polynomial in N [5]. Following Gallager, we shall ignore the few atypical codes responsible for this behavior, and consider the average error exponent associated with an expurgated ensemble where they have been excluded [5].

1-4244-0067-8/06/$20.00 ©2006 IEEE.

the vicinity of the channel capacity, an error most probably involves an exponential number of potential codewords (see e.g. [1]). In such situations, we characterize $\mathcal{N}_N(\xi, \mathcal{C}_N)$ by an *entropy*, defined as

$$S_N(\xi, \mathcal{C}_N) = \log \mathcal{N}_N(\xi, \mathcal{C}_N). \tag{3}$$

In the limit $N \to \infty$, for sequences of codes $\mathcal{C} = \{\mathcal{C}_N\}_N$ taken from the sequence of ensembles $C = \{C_N\}_N$, the entropy density $s = S_N/N$ concentrates to a well defined value $\bar{s}$, and the channel coding theorem takes the following form: there exists p_c, such that $\bar{s} = 0$ for $p < p_c$, and $\bar{s} > 0$ for $p > p_c$ [4]. More generally, we postulate that, for a typical sequence of codes $\mathcal{C}^0 = \{\mathcal{C}^0_N\}_N$, the entropy S_N satisfies a *large deviation principle* [3], i.e.,

$$\mathbb{P}_\xi[S_N(\xi, \mathcal{C}^0_N)/N = s] \asymp 2^{-NL_0(s)}, \tag{4}$$

with $a_N \asymp b_N$ meaning that $\log a_N / \log b_N \to 1$. The typical value $\bar{s}$ corresponds here to the minimum of the *rate function* L_0, with $L_0(\bar{s}) = 0$. In cases where L_0 is strictly convex, the typical error exponent is obtained as

$$\begin{aligned} E_{\rm typ} &= -\lim_{N\to\infty} \frac{1}{N} \log \sum_{s \geq 1/N} \mathbb{P}_\xi[S_N(\xi, \mathcal{C}^0_N)/N = s] \\ &= L_0(s = 0). \end{aligned} \tag{5}$$

A simpler quantity to compute than $L_0(s)$ is $L_1(s)$, the rate function for the large deviations of $S_N(\xi, \mathcal{C}_N)$ with respect to both the noise ξ and the codes $\mathcal{C}_N$,

$$\mathbb{P}_{\xi, \mathcal{C}_N}[S_N(\xi, \mathcal{C}_N)/N = s] \asymp 2^{-NL_1(s)}. \tag{6}$$

In the so-called *thermodynamic formalism* [13], $L_1(s)$ is associated with a *potential* $\phi(x)$ defined through the relation

$$2^{N\phi(x)} = \mathbb{E}_{\xi, \mathcal{C}_N}[2^{xS_N(\xi, \mathcal{C}_N)}] \asymp \int \mathrm{d}s \; 2^{N[xs - L_1(s)]}. \tag{7}$$

Under the assumption that it is convex, the rate function $L_1(s)$ is derived from the knowledge of $\phi(x)$ by Legendre transformation:

$$L_1(s) = \max_x \left[xs - \phi(x)\right]. \tag{8}$$

The average exponent, obtained from $E_{\rm av} = L_1(s = 0)$, may differ from the typical exponent $E_{\rm typ}$. Typical codes $\mathcal{C}^0_N$ can however also be described within a thermodynamic formalism, provided an extra "temperature" y is introduced, together with a generalized potential $\psi(x, y)$ satisfying

$$2^{N\psi(x,y)} = \mathbb{E}_{\mathcal{C}_N}\left[\left(\mathbb{E}_\xi[2^{xS_N(\xi, \mathcal{C}_N)}]\right)^y\right]. \tag{9}$$

The average case is here recovered for $y = 1$, with $\psi(x, y = 1) = \phi(x)$. Typical error exponents are associated with $y = 0$ (see [11] for details and exceptions), with

$$E_{\rm typ} = L_0(s = 0) = -\partial_y \psi(x^*, y = 0), \tag{10}$$

where x^* selects for $s = \frac{1}{y}\partial_x \psi(x^*, y)\Big|_{y=0} = 0$.

III. Cavity method

Disordered systems constructed out of random ensembles, of which LDPC codes are particular examples, have been the subject of intensive studies in statistical mechanics. One of the most elaborate analytical tool developed in this context is the *cavity method* [10], which allows to extract the typical properties of models defined on random graphs. While yielding virtually equivalent predictions than the similar *replica method*, this method has both more sound probabilistic foundations, and an attractive relation to message-passing algorithms, such as *belief propagation* (BP). The cavity method has also been recently extended to deal with large deviations [12], making it perfectly suited to the evaluation of error exponents.

As far as typical codes and typical noise are concerned, the cavity method is equivalent to a BP *density evolution* analysis. Belief propagation, also known as the "peeling decoder" in the context of the BEC [8], consists in propagating messages between *bits* (the N letters of a word) and *checks* (the M linear equations encoded in the parity-check matrix A that each codeword must satisfy). The messages can take three different values: $*$ (erasure) or 0 or 1. Initially, each bit sends its value 0 or 1, or $*$ if erased, to each of the parity checks it is involved in. Check-to-bit and bit-to-check messages are then sent alternatively. If a check a receives non-erasure messages from all its bits but i, it sends to i the sum (modulo 2) of these messages; otherwise, the check a sends $*$ to i. If an erased bit i receives at least one non-erasure message from any of its checks but a, it sends it to a (if more than one, they are necessarily identical); otherwise, the bit i sends its value, 0 or 1, or $*$ if erased, to a. The algorithm stops after convergence of the iterations.

The (typical) cavity method, or BP density evolution, analyzes the outcome of this procedure in the limit where the codeword length N is infinite. It introduces η, the probability that a bit sends an erasure message to a check, and ζ the probability that a check sends an erasure message to a bit, both taken after BP has reached convergence. The *cavity equations* satisfied by these two probabilities,

$$\zeta = 1 - (1 - \eta)^{k-1}, \qquad \eta = p\zeta^{\ell - 1}, \tag{11}$$

characterize the fixed point of the BP density evolution (see Fig. 1).

Once BP has converged, bits receiving at least one non-erasure message are fixed to their correct value, as are the non-erased bits. When eliminated, along with the checks receiving no more than one erasure message, they leave the so-called *core*. The dimensions $M_c \times N_c$ of the associated residual matrix are, with high probability:

$$\begin{aligned} N_c &= p\zeta^\ell N + o(N), \\ M_c &= \frac{\ell}{k}[1 - (1 - \eta)^k - k\eta(1 - \eta)^{k-1}]N + o(N). \end{aligned} \tag{12}$$

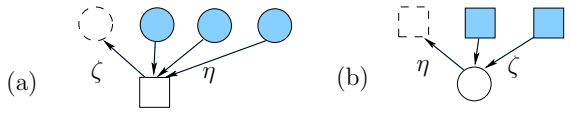

Figure 1: Illustration of the cavity equations (11), with $k = 4$ and $\ell = 3$. (a): a check node (square) sends an erasure message to a bit node (dashed circle) if at least one of its other variables sends an erasure message. (b): a bit node (circle) sends an erasure message to a check node (dashed square) if it has been erased and if all its other checks send an erasure message.

For $p < p_d(\ell, k)$, the only solution to (11) is $\zeta = 0, \eta = 0$, meaning that BP is able to decode the whole word with high probability. For $p > p_d$ however, BP gets stuck at some $\zeta > 0$, $\eta > 0$. In this case, it can be proved that the residual matrix has full-rank with high probability [9]. Therefore, the problem has exactly $2^{N_c - M_c}$ solutions if $N_c > M_c$, and one solution (the original codeword) otherwise. In this approach, the critical noise $p_c(\ell, k)$ is obtained from the condition $N_c = M_c$, and $\bar{s}$ is given by $\max(0, \bar{s}_{\rm cav})$, with $\bar{s}_{\rm cav} = \lim_{N\to\infty}(N_c - M_c)/N$.

The large deviation cavity method is built on the same ideas but incorporates a biased measure over the noise and code ensemble, as prescribed by Eq. (9). When we consider the value of a bit-to-check message as a function of its $(\ell-1)(k-1)$ "grandparents", we also evaluate the "entropy shift" ΔS associated with the addition of the bit and its $\ell - 1$ checks, i.e. the difference between the numbers of columns and lines contributed by the bit and its checks to the residual matrix. Then the message is sent with a probability proportional to

$$\left(\mathbb{E}_\xi 2^{x\Delta S}\right)^y . \tag{13}$$

For regular LDPC codes, we thus obtain for the potential

$$\psi(x,y) = \log Z_\ell - \frac{\ell(k-1)}{k} \log\left[(1-\eta)^k + (1-(1-\eta)^k)2^{-xy}\right] \tag{14}$$

with

$$Z_\ell = (\zeta 2^{-xy} + 1 - \zeta)^\ell - (\zeta 2^{-xy})^\ell + \zeta^\ell (p2^x + 1 - p)^y 2^{-\ell xy} \tag{15}$$

and

$$\begin{aligned} \eta &= \zeta^{\ell-1}(p2^x)^y 2^{-(\ell-1)xy} Z_{\ell-1}^{-1}, \\ \zeta &= 1 - (1-\eta)^{k-1}. \end{aligned} \tag{16}$$

Note that the entropy conjugated with x is not the "real" entropy s, but $s_{\rm cav} = (N_c - M_c)/N$. When $x = 0$, the fixed point of the usual density evolution equations (11) is recovered, with $(1/y)\partial_x \psi(x = 0, y)$ giving back $\bar{s}_{\rm cav}$, the typical value.

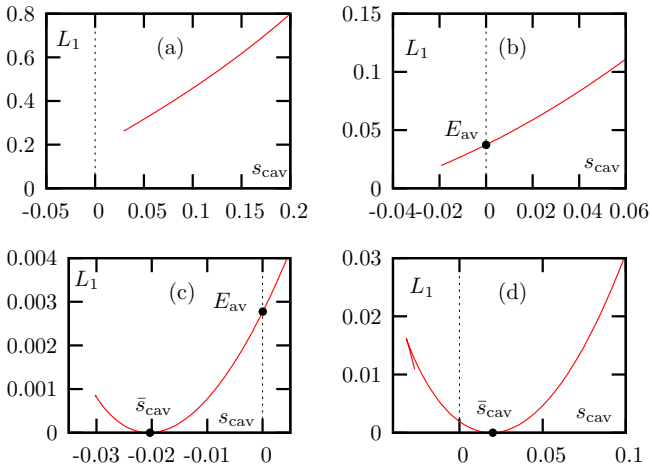

Figure 2: Average entropic rate function $L_1(s)$ as a function of the entropy density $s_{\rm cav}$, for the regular LDPC code $\ell = 3$, $k = 6$ on the BEC with increasing values of p. The real entropy is actually $s = \max(0, s_{\rm cav})$. (a): $p < p_{\rm 1rsb}$, no solution with $s = 0$; (b): $p_{\rm 1rsb} < p < p_d$, a solution with $s = 0$, but $\bar{s}$ is not defined; (c): $p_d < p < p_c$, $\bar{s} = 0$; (d): $p > p_c$, $\bar{s} > 0$ indicates that decoding typically fails.

IV. LDPC codes

We first discuss average error exponents. The calculation of the average rate function $L_1(s)$ reveals four distinct regimes when the noise level p is varied, as illustrated and explained in Fig. 2. In particular, we find that the rate function $L_1(s)$ is no longer defined for $s = 0$ when p is too small ($p < p_{\rm 1rsb}$), which points to the inadequacy of our method in this low-noise regime.

Indeed, by retaining $s = 0$ as criterion for correct decoding, we assumed that an error implicates an exponential number of codewords. An error may however also be caused by the presence of one (or a few) isolated codeword(s). Estimating this probability requires an alternative, "energetic", scheme, as opposed to the "entropic" scheme discussed so far[3]. Equations for the energetic average and typical error exponents can also be obtained from the large deviation cavity method [11], but their solutions are confined to a restricted interval $p > p_{\rm rs}$, indicating again that the lowest noise levels are not appropriately described. The entropic and energetic exponents are found to cross at p_e, which corresponds to the so-called *critical rate* [1, 6]. We conjecture that the entropic exponent, as given by the above equations, is exact in the range $[p_e, p_c]$, while the energetic exponent (not presented here), which applies for $[p_{\rm rs}, p_e]$, is only approximate.

[3]The energetic version of the cavity method is also referred to as "replica symmetric" in the physics literature, while the entropic version is known as "one-step replica symmetry breaking".

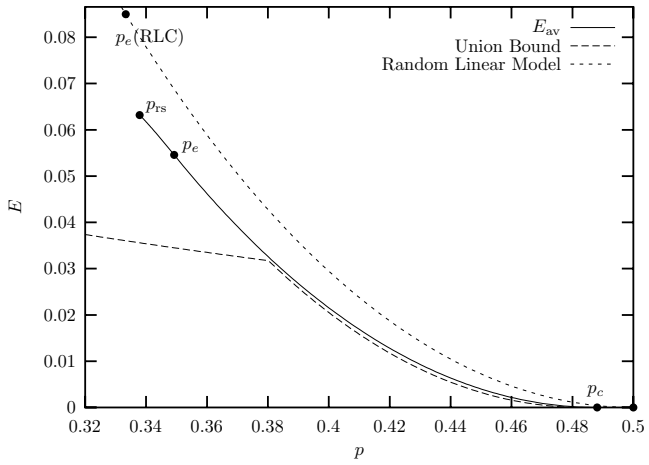

Figure 3: Average error exponent as a function of the noise level p of the BEC for the regular LDPC code ensemble with $k = 6$ and $\ell = 3$. Gallager's union bound and the random linear code limit (19) are also plotted for comparison.

(k, ℓ)	$(4, 3)$	$(6, 3)$
$p_{\rm 1rsb}$	0.3252629709	0.2668568754
$p_{\rm rs}$	0.5465748811	0.3378374641
p_e	0.6068720166	0.3491884902
p_d	0.6474256494	0.4294398144
p_c	0.7460097025	0.4881508842

Table 1: Thresholds $p_{\rm 1rsb}$, $p_{\rm rs}$, p_e, p_d and p_c (see text and Fig. 2) for two regular ensembles of LDPC codes.

Fig. 3 shows our predictions for the average exponent of the $\ell = 3$, $k = 6$ regular LDPC codes, with the two regimes represented; the same general picture holds for other regular or irregular ensembles (see also Table 1).

V. The Random Linear Code limit

This limit is obtained from regular codes with $k, \ell \to \infty$ and $R = 1 - \ell/k$ fixed, where the potential simplifies to:

$$\psi(x, y) = y \log(p2^x + 1 - p) + (R - 1)xy. \tag{17}$$

The trivial dependence of $\psi(x, y)$ with y implies that the two error exponents $E_{\rm av}$ and $E_{\rm typ}$, as obtained from the entropic scheme, are identical. They are equal to the *volume bound* [2] $D(1 - R||p)$, where $D(x||y) = x \log(x/y) + (1 - x) \log((1 - x)/(1 - y))$ denotes the *Kullback-Leibler divergence*.

The intersection of the entropic and energetic average error exponents yields the threshold

$$p_e = \frac{1 - R}{1 + R}, \tag{18}$$

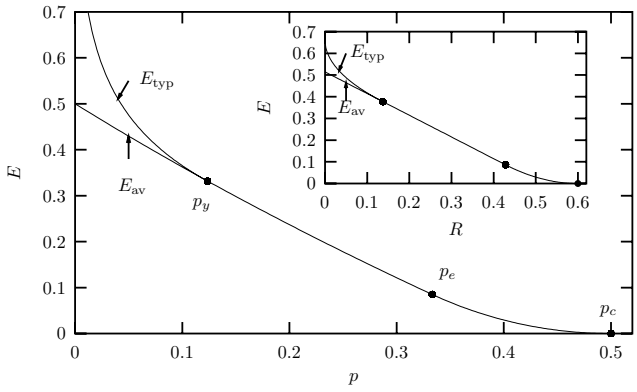

Figure 4: Average and typical error exponents of random linear codes on the BEC as a function of p, with $R = 1/2$ fixed. Inset: the same exponents as a function of R, with $p = 0.4$ fixed.

and we obtain for the average error exponent in the infinite connectivity limit:

$$E_{\rm av}({\rm RLC}) = \begin{cases} 1 - R - \log(1 + p) & \text{if } p < p_e, \\ D(1 - R||p) & \text{if } p_e < p < p_c. \end{cases} \tag{19}$$

It coincides with the average error exponent of the *random linear code* (RLC) ensemble, where the $M \times N$ parity-check matrix is chosen at random with uniform probability among all possible parity-check matrices. Assuming that the inversion of the limits $N \to \infty$ and $k, \ell \to \infty$ is justified, we interpret this result as a validation of our approach (note that here, $p_{\rm rs} = 0$).

The analysis of the typical error exponent in the energetic regime leads us to introduce an additional threshold,

$$p_y = \frac{\delta_{GV}(R)}{1 - \delta_{GV}(R)}, \tag{20}$$

where $\delta_{GV}(R)$, the minimal reduced distance of a typical linear code [1], is given by the smallest solution of $-\delta \log \delta - (1 - \delta) \log(1 - \delta) = 1 - R$. Below p_y, physical arguments [11] indicates that the typical error exponent must differ from the average one, with:

$$E_{\rm typ}({\rm RLC}) = \begin{cases} -\delta_{GV}(R) \log p & \text{if } p < p_y, \\ E_{\rm av}({\rm RLC}) & \text{if } p > p_y. \end{cases} \tag{21}$$

We are not aware of any previous report of this expression in the literature, but the fact that it matches the *union bound* suggests that it is exact. Fig. 4 presents the error exponents as a function of p for a fixed value of the rate $R = 1/2$.

The two thresholds p_e and p_y are presumably generic features of block codes, and are also found with random codes on the binary symmetric channel [1].

VI. Discussion

Despite being one of the earliest and most basic topics in information theory, error exponents still retain today a number of unsolved issues. We advocated here a novel, thermodynamical, formulation of this problem. Using the cavity method from statistical mechanics, we worked out in this framework expressions for the average and typical error exponents of LDPC codes on the BEC. Our method provides an alternative to the replica method, applied to the BSC in [14], with the advantage of being based on explicit probabilistic assumptions. Our approach helps clarify the nature of the phase diagram, while the extension to the BEC allows for an analytical treatment.

While non rigorous, the cavity method aims at providing exact formulæ. Accordingly, our expressions are consistent with the various rigorous studies reported in the literature. The quest for rigorous proofs of formulæ obtained from the cavity method is currently an active fields of mathematics [15]. Remarkably, predictions from the cavity method on the maximum-likelihood threshold p_c [4] could be turned into rigorous theorems [9]. This may inspire alternative derivations of our results.

Perhaps not too surprisingly, the entropic range $p_e < p < p_c$ where we conjecture our results to be exact also coincides with the limited interval for which the related problem of determining the reliability function of block codes has been solved so far. Extending our method to $p < p_e$, where we could obtain only approximate results (except in the infinite connectivity limit), remains a challenging open problem.

Using the same approach, we also analyzed the case of the binary symmetric channel, obtaining comparable results [11]. A more interesting extension would be to iterative decoding, such as BP. Although arguably quite academic, studying maximum-likelihood decoding, as we did, is nevertheless certainly an essential preliminary step.

Acknowledgments

It is a pleasure to thank Stefano Ciliberti, Marc Mézard and Lenka Zdeborová for their critical reading. The work of T.M. was supported in part by the EC through the network MTR 2002-00319 'STIPCO' and the FP6 IST consortium 'EVERGROW'. O.R. is a fellow of the Human Frontier Science Program.

References

[1] A. Barg and G. D. Forney Jr., "Random codes : minimum distances and error exponents," *IEEE Trans. Inform. Theory*, 48:2568–2573, 2002.

[2] E. R. Berlekamp, "The performance of block codes," *Notices of the AMS*, pages 17–22, January 2002.

[3] F. den Hollander, *Large deviations*, Fields Institute Monographs 14. American Mathematical Society, Providence RI, 2000.

[4] S. Franz, M. Leone, A. Montanari, and F. Ricci-Tersenghi, "The dynamic phase transition for decoding algorithms," *Phys. Rev. E*, 66:046120, 2002.

[5] R. G. Gallager, "Low-density parity check codes," *IRE Trans. Inf. Theory*, IT-8:21, 1962.

[6] R. G. Gallager, *Information theory and reliable communication*, John Wiley and Sons, New York, 1968.

[7] Y. Kabashima and D. Saad, "Statistical mechanics of low-density parity-check codes," *J. Phys. A: Math. Gen*, 37:R1–R43, 2004.

[8] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol. 47, 569–584, Feb. 2001.

[9] C. Measson, A. Montanari, T. Richardson, and R. Urbanke, "Life above threshold: from list decoding to area theorem and MSE," In *Proc. ITW*, San Antonio, USA, October 2004.

[10] M. Mézard and G. Parisi. "The Bethe lattice spin glass revisited," *Eur. Phys. J. B*, 20:217, 2001.

[11] T. Mora and O. Rivoire, 2006. In preparation.

[12] O. Rivoire. "The cavity method for large deviations," *J. Stat. Mech.*, P07004, 2005.

[13] D. Ruelle. *Thermodynamic formalism*, Cambridge Math. Library, 2nd Ed, 2004.

[14] N. S. Skantzos, J. van Mourik, D. Saad, and Y. Kabashima, "Average and reliability error exponents in low-density parity-check codes," *J. Phys. A*, 36:11131–11141, 2003.

[15] M. Talagrand, *Spin glasses : a challenge for mathematicians. Cavity and mean field models*, Springer-Verlag, New-York, 2003.