Statistical mechanics of error exponents for error-correcting codes

Thierry Mora
Laboratoire de Physique Théorique et Modèles Statistiques, Bât. 100, Université Paris-Sud, F–91405 Orsay, France

Olivier Rivoire
Laboratory of Living Matter, The Rockefeller University, 1230 York Avenue, Box 34, New York, New York 10021, USA
(Received 27 June 2006; published 15 November 2006)

Error exponents characterize the exponential decay, when increasing message length, of the probability of error of many error-correcting codes. To tackle the long-standing problem of computing them exactly, we introduce a general, thermodynamic, formalism that we illustrate with maximum-likelihood decoding of low-density parity-check codes on the binary erasure channel and the binary symmetric channel. In this formalism, we apply the cavity method for large deviations to derive expressions for both the average and typical error exponents, which differ by the procedure used to select the codes from specified ensembles. When decreasing the noise intensity, we find that two phase transitions take place, at two different levels: a glass to ferromagnetic transition in the space of codewords and a paramagnetic to glass transition in the space of codes.

DOI: 10.1103/PhysRevE.74.056110 PACS number(s): 89.90+n, 89.70+c, 05.50+q

I. INTRODUCTION

Communicating information requires a physical channel whose inherent noise impairs the transmitted signals. Reliability can be improved by adding redundancy to the messages, thus allowing the receiver to correct the effects of the noise. This procedure has the drawbacks of increasing the cost of generating and sending the messages and of decreasing the speed of transmission. At first sight, better accuracy seems achievable only at the expense of lesser efficiency. Remarkably, Shannon showed that, in the limit of infinite-length messages, error-free communication is possible using only limited redundancy [1]. His proof of principle has triggered many efforts to construct actual error-correcting schemes that would approach the theoretical bounds. A renewal of interest in the subject has taken place during the last ten years, as new error-correcting codes were finally discovered [2], or rediscovered [3], which showed practical performances close to Shannon’s bounds.

In this paper, we analyze a major family of such codes, the low-density parity-check (LDPC) codes, also known as Gallager codes, from the name of their inventor [4]. Our focus is on the characterization of rare decoding errors, in situations where most realizations of the noise are accurately corrected. Error-free communication, as guaranteed by Shannon’s theorem, indeed results from a law of large number for concisely and nontechnically expressed as large deviation functions [11]. A thermodynamic formalism is introduced where error exponents are expressed as large deviation functions [12], which we compute by means of the extension of the cavity method [14] proposed in [15]. This approach offers an alternative to the related replica method employed in [10] and allows us to address both average and typical error exponents. We thus obtain an interesting phase diagram, with two very distinct phase transitions occurring when the intensity of the noise in the channels is varied.

A brief summary of our results can be found in [16]. We present in what follows a much more detailed account of our approach. In a first part, we define LDPC codes, recall their mapping to some models of spin glasses and optimization problems, and give a general overview of our thermodynamic (large deviation) formalism. The two subsequent parts apply this framework to the analysis of LDPC codes over the BEC and BSC, respectively. We sum up our results in a conclusion where we also point out some open questions. Most of the technical calculations are relegated to the Appendixes, which also contain a detailed discussion of the limiting case of random linear codes.
II. ERROR-CORRECTING CODES AND THE LARGE DEVIATION FORMALISM

A. Error-correcting codes

Error-correcting codes are based on the idea that adding sufficient redundancy to the messages can allow the receiver to reconstruct them, even if they have been partially corrupted by the noisy channel [17]. A schematic view of how these codes operate is presented in Fig. 1. Given a message composed of $L$ bits, an encoding map $\{0,1\}^L \rightarrow \{0,1\}^N$ first introduces redundancy by converting the $L$ bits of the message into a longer sequence of $N$ bits, called a codeword. The ratio $R = L/N$ defines the rate of the code and should ideally be as large as possible to reduce communication costs, yet small enough to allow for corrections. Corrections are implemented downstream by decoding a mapping $\{0,1\}^N \rightarrow \{0,1\}^L$ whose purpose is to reconstruct the original message from the received corrupted codeword. Decoding is composed of two steps: first, the most probable codeword is inferred, and second, it is converted into its corresponding message.

In this scheme, messages and codewords are related by the one-to-one encoding map, and translating messages into codewords or conversely is relatively straightforward. The computationally most demanding part is concentrated on inferring the most probable codeword sent, given the corrupted codeword received. In what follows, we shall focus exclusively on this problem, which requires manipulating only codewords.

B. Communication channels

Formally, a noisy channel is characterized by a transition probability $Q(\mathbf{y}|\mathbf{x})$ giving the probability for its output to be $\mathbf{y}$ given that its input was $\mathbf{x}$. For the sake of simplicity, we confine ourselves to memoryless channels where the noise affects each bit independently of the others—i.e., $Q(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{N} Q(y_i|x_i)$ with $Q(y_i|x_i)$ independent of $i$.

We shall consider more specifically two examples of memoryless channels. The first one is the binary erasure channel where a bit is erased with probability $p$—that is, $Q^*(|x) = p$ and $Q(x|x) = 1 - p$ where $*$ represents an erased bit (see Fig. 2). The second is the binary symmetric channel where a bit is flipped with probability $p$—that is, $\mathcal{Q}(0|1) = Q(1|0) = p$ and $\mathcal{Q}(0|0) = \mathcal{Q}(1|1) = 1 - p$ (see Fig. 2).

C. LDPC codes and code ensembles

Shannon first formalized the problem of error correction and determined the lowest achievable rate $R$ allowing error-free correction [1]. He found a general expression for this limit, called the channel capacity, which depends only on the nature of the channel and takes the form $C_{\text{BEC}}(p) = 1 - p$ and $C_{\text{BSC}}(p) = 1 - p \ln p - (1 - p) \ln(1 - p)$ for the BEC and BSC, respectively. Shannon’s proof for the existence of codes achieving the channel capacity was nonconstructive and his analysis restricted to the limit of infinitely long messages, $L \to \infty$. Among the various families of codes proposed to practically perform error correction, one of the most promising is the family of low-density parity-check codes [4].

A LDPC code is defined by a sparse matrix $A$ where “sparse” means that $A$ is mostly composed of 0’s, with otherwise a few 1’s. The parity-check matrix $A$ has size $M \times N$ with $M = N - L$ and is associated with a generator matrix $G$ of size $L \times N$ such that $GA=0$ (see, e.g., [3] for explicit constructions); the encoding map is taken to be the linear map $x = Gm$ and the rate of the code is $R = L/N = 1 - M/N$. By construction, an $N$-bit codeword $x$ satisfies the $M$ parity-check equations $A x = 0$, or, in other words, the set of codewords is the kernel of $A$. The parity-check matrix $A$ is usually represented graphically by a factor graph, as in Fig. 3: the columns of $A$ are associated with check nodes labeled with $a \in \{1, \ldots, M\}$ and represented by squares, and the lines of $A$ are associated with variable nodes labeled with $i \in \{1, \ldots, N\}$ and represented by circles. A nonzero element of the matrix $A$ such as $A_{ia}=1$ appears as a link between the variable node $i$ and the check node $a$.

A particularly powerful approach for analyzing error-correcting codes is the probabilistic method where, instead of considering a single code, one studies an ensemble of codes. With LDPC codes, code ensembles correspond to sets of matrices or, equivalently, sets of factor graphs. A popular choice is to consider the ensemble of factor graphs with given connectivities $c_k$ and $\nu_\ell$, which is the set of factor graphs having $c_k M$ check nodes with connectivity $k$ and $\nu_\ell N$ variable nodes with connectivity $\ell$, where $\sum_k c_k = \sum_\ell \nu_\ell = 1$. A convenient representation is by means of the generating function $D(z)$, which is the probability generating function of the number of links in a factor graph:

\[
D(z) = \sum_{k=0}^{\infty} D_k z^k = \sum_{\ell=0}^{\infty} D_\ell z^\ell,
\]

where

\[
D_k = \frac{1}{M^{(k)}} \sum_{\ell=0}^{\infty} D_\ell \left( \frac{\nu_\ell}{M} \right)^k
\]

\[
D_\ell = \frac{1}{N^{(\ell)}} \sum_{k=0}^{\infty} D_k \left( \frac{c_k}{N} \right)^\ell
\]

where $M^{(k)}$ and $N^{(\ell)}$ are the numbers of factor graphs having $k$ check nodes and $\ell$ variable nodes, respectively.

FIG. 1. Error correction scheme. A message $m$ composed of $L$ bits, $m \in \{0,1\}^L$, is first encoded in a codeword of longer size $N$ with $R = L/N < 1$, defining the rate of the code. The noise $\xi$ of the channel corrupts the transmitted codeword which becomes $y$ (see Fig. 2 for examples of channels). This output is generically not a codeword, and the correction consists in inferring the most probable codeword to which it comes from. Finally, the inferred codeword $x'$ is converted back into its corresponding message $m'$. The communication is successful if $m' = m$.

FIG. 2. Communication channels. On the left the BEC (binary erasure channel) erases a bit with probability $p$ and leaves it unchanged with probability $1-p$. On the right the BSC (binary symmetric channel) flips a bit with probability $p$ and leaves it unchanged with probability $1-p$. 

\[056110-2\]
functions \( c(x) = \sum_i c_i x^i \) and \( v_i = \sum_j v_{ij} x^j \); these notations allow one, for instance, to write the mean connectivities as \( \langle k \rangle = c'(1) \) and \( \langle \ell \rangle = v'(1) \). Due to their simplicity, particular attention will be devoted to regular codes, whose check nodes have all same degree \( k \) and variable nodes same degree \( \ell \), corresponding to \( c_{\ell k} = \delta_{\ell,k} \) and \( v_{\ell k} = \delta_{\ell,\ell'} \) or, equivalently, \( c(x) = x^k \) and \( v(x) = x^\ell \).

The mathematical fact underlying the probabilistic method is the phenomenon of measure concentration which occurs in the limit where \( N \to \infty \) and \( M \to \infty \) with fixed ratio \( \alpha = M/N \); in this limit, many properties are shared by almost all elements of the ensemble (i.e., all but a subset of measure zero). As a consequence, by studying average properties over an ensemble, one actually has access to properties of typical elements of this ensemble. This fact is one of the building blocks of random graph theory [19] and is also central to the physics of disordered systems where it is known as the self-averaging property [20].

While the factor graph representation makes obvious the connection between LDPC codes and random graph theory, it will also turn particularly fruitful to exploit the close ties of LDPC codes with both optimization problems [21] and spin-glass systems [20]. LDPC codes are indeed intimately related to a class of combinatorial optimization problems known as XORSAT problems, where, given a sparse matrix \( A \) and a vector \( \tau \), one is to find solutions \( \sigma \) to the equation \( A\sigma = \tau \). Although algorithmically relatively simple (Gauss method provides an answer in a time polynomial in the size of the matrix), XORSAT problems share many common features with notably more difficult, NP-complete [21], problems such as \( K \)-SAT. A recent physical approach to XORSAT problems makes use of their formal equivalence with a class of spin-glass systems known as \( c \)-spin models [14, 25] from spin-glass theory to analyze LDPC codes. We note that alternative, sometimes equivalent, physical approaches have previously been applied to LDPC codes; we refer the reader to [26] for a review of the subject.

The distinctive feature of XORSAT at the root of its computational simplicity is the presence of an underlying group symmetry that relates all solutions. In the context of LDPC codes, it corresponds to the fact that the set of codewords is the kernel of the parity-check matrix \( A \); we shall refer to the XORSAT problem \( A\sigma = 0 \) whose solutions define the set of codewords as the encoding constraint satisfaction problem (CSP) of the LDPC code with check matrix \( A \). The group symmetry has a number of interesting consequences which will crucially simplify the analysis.

Most of the interest in LDPC codes stems from the possibility to decode them using efficient, iterative algorithms (described in Sec. III A 3). Unless otherwise stated, we shall, however, be here concerned with the theoretically simpler, yet computationally much more demanding, maximum-likelihood decoding procedure. It consists in systematically decoding a received message to the most probable codeword (a task that iterative algorithms are in some cases unable to perform, as recalled in Sec. III A 3).

Finally, it is interesting to note that in the limit where \( \langle k \rangle, \langle \ell \rangle \to \infty \) with fixed ratio, LDPC codes define the random linear model (RLM) whose typical elements have been shown by Shannon to achieve the channel capacity. This particular limit, where many quantities can be computed by invoking only elementary combinatorial arguments, is discussed in detail in Appendix B.

### D. Typical properties and phase transitions

The performance of a particular code over a given channel is measured by its error probability—i.e., the probability that it fails to correctly decode a corrupted codeword. More precisely, if \( d(y) \) denotes the inferred codeword when \( x \) is sent and \( y \) received, one defines the block error probability for \( x \) as

\[
P_B^N(x) = \sum_y Q(y|x) \delta_{d(y) \neq x}
\]

and the average block error probability as

\[
P_B^N = E_x[P_B^N(x)],
\]

where \( E_x \) denotes the expectation (average) over the set of codewords. With LDPC codes, this average is trivial since, due to the group symmetry, all codewords are equivalent, and \( P_B^N(x) \) is independent of \( x \).

The concentration phenomenon alluded to above means here that \( P_B^N \to p_B \) with \( N \to \infty \) within a given code ensemble defined by generating functions \( c(x) \) and \( v(x) \). As the level of the noise \( p \) is increased, a phase transition is generically observed: a critical value \( p_c \) exists above which error-free correction is no longer possible (\( p = 0 \) for \( p < p_c \) and \( p = 1 \) for \( p > p_c \)). The formalism to be presented in the next sections will yield in particular the value of \( p_c \) for given code ensembles and channels. Obviously, the presence of this phase transition indicates that, when using a channel with noise level \( p \), one should choose a code from an ensemble for which \( p < p_c \). The phase transition is, however, occurring only in the limit of infinite codewords (thermodynamic limit) whereas practical coding inevitably deals with finite \( N \). This leads to the fact that the block error probability is not exactly zero, even in the regime \( p < p_c \).

For a given code of finite but large block-length \( N \), error can thus be caused by rare, atypical, realizations of the noise. Similarly, when picking a code at random from a code ensemble of finite size, one can observe properties differing from the typical properties predicted by the law of large numbers. We show in what follows how these two atypical features induced by finite-size effects can be analyzed in a common framework.
TABLE I. The analogy with spin glasses or, more generally, the statistical physics of disordered system with quenched disorder.

<table>
<thead>
<tr>
<th>Disorder</th>
<th>Spin glass</th>
<th>Average</th>
<th>Typical</th>
<th>Multistep, step 1</th>
<th>Multistep, step 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurations</td>
<td>Couplings $J_{ij}$</td>
<td>Noise+codes $(\xi, C)$</td>
<td>Typical codes $C^0$</td>
<td>Codes $C$ at $y$</td>
<td>Codes $C$</td>
</tr>
<tr>
<td>Observable</td>
<td>$E=\sum_{i} J_{ij} \sigma_i \sigma_j$</td>
<td>$S_N(\xi, C)$</td>
<td>$S_N(\xi, C^0)$</td>
<td>$S_N(\xi, C)$</td>
<td>$L_C(s)$</td>
</tr>
<tr>
<td>Entropy</td>
<td>$s(x=E/N)$</td>
<td>$L_0(s=N/N)$</td>
<td>$L(s=N/N)$</td>
<td>$L(\phi, x)$</td>
<td>$y=\partial C L$</td>
</tr>
<tr>
<td>Temperature$^{-1}$</td>
<td>$\beta=-\beta_0 x$</td>
<td>$x=\beta_0 L_0$</td>
<td>$x=\beta_0 L_0$</td>
<td>$\phi_0=x=x-L_0$</td>
<td>$\phi=x-L_0$</td>
</tr>
<tr>
<td>Potential</td>
<td>$\beta f=+\beta x$</td>
<td>$\phi_1=x-L_1$</td>
<td>$\phi_0=x-L_1$</td>
<td>$\phi_0=x-L_0$</td>
<td>$\psi=y \phi-L_0$</td>
</tr>
</tbody>
</table>

E. Large deviations

At this stage, it is useful to make explicit the three different levels of statistics involved in the analysis of error-correcting codes: (i) statistics over the codes $C$ in a defined code ensemble $C$, (ii) statistics over the set of transmitted codewords $x$ of a particular code, and (iii) statistics over the noise $\xi$ of the channel, with a specified $p$. For given $C, x$, and $\xi$, a fourth level of statistics is involved in the decoding process, over the possible codewords $y \in \{0,1\}^N$ from which the received corrupted codeword originates. The group structure of the set of codewords of LDPC codes makes level (ii) trivial since all codewords are in fact equivalent (isomorphic). We will consequently ignore it and address only levels (i) and (iii).

The problem of evaluating the probability that, due to finite-size effects, a property differs from the typical case belongs to large deviation theory [13]. To give here a general presentation of the concepts and methods to be used, we assume that the success of the decoding is measured by a function $S_N(\xi, C)$ extensive in $N$ and such that $S_N(\xi, C)=0$ if the code $C$ correctly decodes a message subject to noise $\xi$ and $S_N(\xi, C)>0$ otherwise; in the next sections, we will show explicitly how such an observable can be defined with LDPC codes, for both the BAC and BSC channels. In terms of $S_N$, the decoding phase transition takes the following form: in the limit $N \to \infty$, the distribution of the noise $S_N/N$ concentrates around a typical value $s_{typ}(p)$ which verifies $s_{typ}(p) \leq 0$ if $p=p_c$ and $s_{typ}(p)>0$ if $p > p_c$, where $p$ denotes as before the level of noise of the channel (see Fig. 2 for examples).

For typical codes in their ensemble, denoted $C^0$, we describe large deviations of $S_N$ with respect to the noise $\xi$ by a rate function $L_0(s)$ such that the probability to observe $S_N(\xi, C^0)/N=s$ satisfies

$$\Pr_N[\xi; S_N(\xi, C^0)/N = s] \approx e^{-NL_0(s)}. \tag{3}$$

Here the symbol $a_N \approx b_N$ refers to an exponential equivalence, $\ln a_N/\ln b_N \to 1$ as $N \to \infty$. Viewed as a function of the noise level $p$, the rate function $E_{typ}(p)=L_0(s=0)$ is known in the coding literature as the typical error exponent [5]. The exponential decay with $N$ of atypical properties is quite generic when dealing with large deviations, but this scaling is not necessarily ensured, as discussed in more detail in Appendix A. In the thermodynamic formalism that we shall adopt, rate functions are computed by introducing a potential $\Phi_c(x)$ defined by

$$\Phi_c(x) = \ln(E[\xi e^{S_N(\xi, C)}]). \tag{4}$$

In the limit $N \to \infty$ limit, the density $\Phi_c(x)/N$ tends to a typical value $\phi_0(x)$, which is related to the rate function $L_0(s)$ by

$$e^{N\phi_0(x)} \approx \int ds \ e^{N[x-L_0(s)]}. \tag{5}$$

Equivalently, by taking the saddle point,

$$\phi_0(x) = x - L_0(s), \quad x = \partial_0 L_0(s). \tag{6}$$

The rate function $L_0(s)$ can thus be reconstructed from $\phi_0(x)$ by inverting the Legendre transformation,

$$L_0(s) = s x - \phi_0(x), \quad s = \partial_0 \phi_0(x). \tag{7}$$

The analogy with the usual thermodynamics is summarized in Table I.

From a theoretical perspective, it is simpler to make an average over the codes and compute the rate function $L_1(s)$ defined as

$$\Pr_N[\xi, C; S_N(\xi, C)/N = s] \approx e^{-NL_1(s)}. \tag{8}$$

This procedure yields the so-called average error exponent $E_{av}=L_1(s=0)$. In the thermodynamical formalism, $L_1(s)$ is conjugated to the potential $\phi_1(x)$ satisfying

$$e^{N\phi_1(x)} = E_1(\xi, C) e^{S_N(\xi, C)} = \int ds \ e^{N[x-L_1(s)]}. \tag{9}$$

The two rate functions $L_0(s)$ and $L_1(s)$ may differ, meaning that the average exponent can be associated with atypical codes. Such atypical codes correspond themselves to large deviations of the potential $\Phi_c(x)$. For fixed values of $x$, we define a rate function $L(\phi, x)$ as

$$\Pr_N[C; \Phi_c(x)/N = \phi] \approx e^{-NL(\phi, x)}. \tag{10}$$

In a thermodynamic formalism, $L(\phi, x)$ is again associated with a potential $\psi(x,y)$ defined by
TABLE II. Analogy with the replica approach of spin glasses. The replica-symmetric method describes that the typical partition function $Z_0$ of a disordered system is given by $Z_0 \sim \exp\left[\sum_{ij} J_{ij} \sigma_i \sigma_j \right]$ with $n \to 0$ or, more precisely, if $\lambda N = \ln Z_0$, the typical value of $\lambda = \lambda_0 N$ is $\lambda_0 = \lim_{x \to 0} \lim_{N \to \infty} (1/N) \ln \exp(e^{\lambda x})$. This is mathematically justified by the G"artner-Ellis theorem which moreover provides a rigorous basis for the interpretation of nonzero values of $n$ in terms of large deviations, as discussed in the text. According to this theorem, if the function $\phi(x) = \lim_{N \to \infty} (1/N) \ln \exp(e^{\lambda_0 x})$ exists and is regular enough (see, e.g., [13] for a rigorous presentation), then a large deviation principle holds for $\lambda$ with a rate function being the Legendre transform of $\phi(x)$; if we assume the functions differentiable, $L(\lambda) = \lambda x - \phi(x)$ with $\lambda = \partial_\lambda \phi(x)$. As a corollary of this theorem, the typical value $\lambda_0$, which by definition satisfies $L(\lambda_0) = 0$ and $x = \partial_\lambda L(\lambda_0) = 0$, is given by $\lambda_0 = \partial_\lambda \phi(x=0) = \lim_{x \to 0} \phi(x)/x$ for $x = 0$, as predicted by the replica method. Note also that $n = 1$, with $Z_1 = \exp[Z_0]$, corresponds to the so-called annealed approximation.

<table>
<thead>
<tr>
<th>Replica (symmetric) theory of spin glasses</th>
<th>Multistep large deviations for LDPC codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hamiltonian $H_0[\sigma] = \sum_{i,j} J_{ij} \sigma_i \sigma_j$</td>
<td>$S_N(\xi, C)$</td>
</tr>
<tr>
<td>Disorder ${J_{ij}}$</td>
<td>Codes $C$</td>
</tr>
<tr>
<td>Configurations ${\sigma_i}$</td>
<td>Noise $\xi$</td>
</tr>
<tr>
<td>Number of replicas $n$</td>
<td>Temperature $-1$ $y$</td>
</tr>
<tr>
<td>Physical temperature $-1$ $\beta$</td>
<td>Temperature $-1$ $x$</td>
</tr>
<tr>
<td>Annealed approximation $n \to 1$</td>
<td>Average codes $y = 1$</td>
</tr>
<tr>
<td>Quenched computation $n \to 0$</td>
<td>Typical codes $y \to 0$</td>
</tr>
</tbody>
</table>

\[ e^{N\Phi(x,y)} = E_\xi\left[ e^{S_N(\xi,C)} \frac{\partial}{\partial \xi} \Phi(\phi_\xi, \xi) \right] = E_\xi\left[ e^{\Phi(\phi_\xi)} \right] = \int d\phi e^{N[y \phi - \beta \Phi(\phi_\xi)]}, \]

(11)

We refer to this hierarchical embedding of large deviations as a *multistep large deviation* structure [15], a term meant to reflect the formal equivalence with the multistep replica symmetry breaking scenario developed for spin glasses [20] (see Table II). In the limit $N \to \infty$ where the integral is dominated by its saddle point we obtain the Legendre transformation

\[ \psi(x,y) = y \phi - \mathcal{L}(\phi, x), \quad y = \partial_\phi \mathcal{L}(\phi, x). \]  

(12)

Within this extended framework, we recover the average case by taking $y = 1$. Indeed, from the definitions (9) of $\phi_1(x)$ and (11) of $\psi(x, y)$ it follows that

\[ e^{N\psi(x,1)} = E_\xi\left[ e^{S_N(\xi,C)} \frac{\partial}{\partial \xi} \Phi(\phi_\xi, \xi) \right] = E_\xi\left[ e^{S_N(\xi,C)} \right] = e^{N\phi_1(x)}, \]

(13)

that is,

\[ \psi(x, y = 1) = \phi_1(x). \]

(14)

This average case differs in general from the typical case which corresponds to $y = 0$. Indeed, by definition [see Eq. (10)], typical codes are associated with the potential $\phi_0$ minimizing $\mathcal{L}(\phi, x)$, with $\mathcal{L}(\phi_0, x) = 0$, yielding $y = \partial_\phi \mathcal{L}_x = 0$. Note that the potential $\phi_0$ is related to $\psi(x, y)$ by $\phi_0(x) = \lim_{x \to 0} (1/y) \phi(x, y)$, which can also be viewed as a corollary of G"artner-Ellis theorem [13], best known in statistical physics as the replica trick [20] (see Table II). In the language of the replica method, the average case ($y = 1$) and the typical case ($y = 0$) are, respectively, referred to as the annealed and quenched computations.

The previous discussion assumed that the potentials were analytical functions of their parameters $x$ and $y$, but this may not be the case, and we will find that phase transitions can occur when these temperatures are varied. In such cases, taking naively the limit $y \to 0$ leads to erroneous results. We will discuss how to overcome such difficulties when encountering them.

### III. LDPC Codes over the BEC

We now proceed to illustrate our formalism with LDPC codes over the binary erasure channel. We start with deriving the typical phase diagram by means of the cavity method, a slightly different approach than the replica method originally used in [27]. This sets the stage for the analysis of error exponents that follows.

#### A. Typical phase diagram

1. **Formulation**

Consider a LDPC code $C$ with parity-check matrix $A$; its encoding CSP (the constraint satisfaction problem whose SAT assignments define the codewords) has cost function

\[ H(\sigma) = \sum_{i=1}^{M} E_a(\sigma), \quad \text{with } E_a(\sigma) = \sum_{i=1}^{N} A_{ai} \sigma_i \mod 2. \]  

(15)

Since $E_a(\sigma) \in \{0,1\}$, the cost function $H(\sigma)$ counts the number of constraints violated by the assignment $\sigma = \{\sigma_i\}_{i=1}^{N}$ (where $\sigma_i \in \{0,1\}$). When a codeword $\sigma^*$, satisfying $H(\sigma^*) = 0$, goes through a BEC, each of its bits $\sigma_i$ has probability $p$ to be erased. A given realization of the noise can be characterized by a vector $\xi = (\xi_1, \ldots, \xi_N)$ with $\xi_i \equiv 1$ implying that the bit $\sigma_i^*$ is lost and $\xi_i \equiv 0$ that it is unaffected. If we denote by $E$ the set of indices $i$ for which $\xi_i^* = 1$ (erased bits), the decoding task consists in reconstructing $\{\sigma_i^*\}_{i \in E}$ and knowledge of the encoding CSP $H_C$. This decoding problem defines a new constraint satisfaction problem, the *decoding CSP*, obtained from the encoding CSP by fixing the values of the noncorrupted bits. More explicitly, the decoding CSP has cost function $H^*_{E_0}[\sigma^0] = \sum_{i \in E_0} A_{ai} \sigma_i^*$ where $\sigma^0 = \{\sigma_i^*\}_{i \in E}$ and

\[ E_{a_i}^{\mathcal{E}_0}[\sigma^0] = \sum_{i \in E} A_{ai} \sigma_i + \sum_{i \in E} A_{ai} \sigma_i^* \mod 2. \]  

(16)

Decoding is possible if and only if $\{\sigma_i^*\}_{i \in E}$ is the only SAT assignment of the decoding CSP.

If $N(\xi, C)$ denotes the number of solutions of the decoding CSP, $S_N(\xi, C)$ can be taken as $S_N(\xi, C) = \ln N(\xi, C)$. This entropy fulfills the desired properties: namely, $S_N(\xi, C) \leq 0$ if decoding is successful, and $S_N(\xi, C) > 0$ otherwise.
The particularity of LDPC codes compared to other error-correcting codes is that the decoding CSP (both are XORSAT problems). As a consequence, the $\mathbb{Z}_2$ symmetry of the group of codewords is always preserved, at variance with what happens in other CSP’s where fixing variables breaks a symmetry. The BEC is also particular compared with other channels, since the set $\mathcal{E}$ of corrupted bits is known to the receiver (this will not be the case with the BSC, where identifying the corrupted bits is part of the decoding problem). This entails that bits can only be fixed to their correct value.

2. Cavity approach

Before considering large deviations, it is instructive to recall the typical results—i.e., the values taken by $S_p(\xi, C^0)$ when $C^0$ is a typical code from a given ensemble specified by $c(x)$ and $v(x)$, and $\xi$ a typical realization of the noise from the probability distribution specified by $p$. We resort here to the cavity method at zero temperature [14], whose validity is based on the treelike structure of the factor graphs associated with typical LDPC codes. The essentially equivalent replica method has been used in the past: in [28], $S_p(\xi, C)$ is thus obtained by first computing a free energy with the replica method and then taking the zero-temperature limit to obtain $S_p(\xi, C)$, viewed as the entropy of the zero-energy ground states.

The approach we follow here, which corresponds to a particular implementation of the entropic cavity method presented in [29], has several advantages over the replica approach: it involves neither a zero- replica limit nor a zero-temperature limit, it emphasizes the specificities of LDPC codes associated with the underlying $\mathbb{Z}_2$ symmetry, and it naturally connects to the algorithmic analysis of single codes. In the common language of the replica and cavity methods, the calculation to be done is coined one-step replica symmetry breaking (1RSB) and the entropy $s=S_p/N$ is referred to as a complexity. This is reflected in what follows by the fact that we strictly restrict to SAT assignments and assume that all constraints are satisfied (the reweighting parameter $\mu$, as denoted in [25], is here infinite, $\mu=\infty$). This 1RSB approach is known to exactly describe XORSAT problems [23,24].

Let $P_i(\sigma_i)$ be the probability, taken over the set of solutions of the decoding CSP, that the bit $i$ assumes the value $\sigma_i \in \{0,1\}$. Due to the preservation of the $\mathbb{Z}_2$ symmetry, no bit can be nontrivially biased: either it is fixed to 0 or 1, corresponding to $P_i=\delta_{i0}$ and $P_i=\delta_{i1}$, respectively, or it is completely free, corresponding to $P_i=(\delta_{i0}+\delta_{i1})/2$, where we denote $\delta_{i0}(\sigma)=\delta_{i\sigma}$. In technical terms, the evanescent fields that are generically required to compute entropies in CSP [29] have here a trivial distribution, thus explaining that they can be safely ignored, as was done in [28].

Let $\nu$ be the probability, taken over the $N$ nodes of a typical factor graph, that a bit $i$ is free—i.e., that $P_i=(\delta_{i0}+\delta_{i1})/2$. Since a free node has equal probability to be 0 or 1, its contribution to the entropy is $\ln 2$ and the mean entropic contribution per node is $\nu \ln 2$. This value is, however, only an upper bound (known as the annealed, or first moment, bound) on the entropy density $s=S_p/N$ that we wish to calculate. In fact, it holds only if the bits are independent: indeed, two bits may both be free but, by fixing one, the second may be constrained to a unique value, in which case the joint entropic contribution of the two nodes is $\ln 2$ and not $2 \ln 2$. The correct expression is given by the Bethe formula, which can be heuristically derived as follows. First, we sum the entropic contributions $\Delta S_{\sigma_0\sigma_1}$ of each node $\sigma$, including the corrections due to its adjacent parity checks $\square \in \sigma$. Second, we note that each parity check $\square$ is involved in $k_{\square}$ terms, with $k_{\square}$ being the connectivity of $\square$. To count it only once, we therefore subtract $(k_{\square}-1)$ times the entropic contribution $\Delta S_{\square}$ of each parity check $\square$. This leads to

$$s = \frac{1}{N} \left( \sum_\square \Delta S_{\sigma_0\sigma_1} - \sum_\square (k_{\square} - 1) \Delta S_{\square} \right)$$

$$= \langle \Delta S_{\sigma_0\sigma_1} \rangle - \langle \ell \rangle \sum_k c_k (k-1) \langle \Delta S_{\square}^{(k)} \rangle,$$  \hspace{1cm} (17)

where $\langle \Delta S_{\sigma_0\sigma_1} \rangle$ represents the average of $\Delta S_{\sigma_0\sigma_1}$ over the nodes $\sigma$ and $\langle \Delta S_{\square}^{(k)} \rangle$ the average of $\Delta S_{\square}$ over the parity checks $\square$ with connectivity $k_{\square}=k$; the factor $\langle \ell \rangle / \langle k \rangle$ accounts for the ratio of the number $M$ of parity checks over the number $N$ of nodes.

To compute $\Delta S_{\sigma_0\sigma_1}^0$, we need to know whether the bits of the nodes adjacent to $\sigma$ are fixed or not, in the absence of the “cavity node” $\sigma$. As the cavity node is connected to its neighbors through parity checks [see Fig. 4(a)], we can decompose the computation in two steps. First, we observe that a given neighboring parity check constrains the value of the cavity node if and only if all the other nodes to which it is connected have themselves their bit fixed in the absence of the cavity node. Denoting by $\zeta$ the probability of this event and by $\eta$ the probability for a node to be free in the absence of one of its adjacent parity check, we thus have

$$\zeta = \sum_k \frac{k c_k}{\langle k \rangle} [1 \cdot (1-\eta)^{k-1}] = 1 - \frac{c'(1-\eta)}{\langle k \rangle},$$  \hspace{1cm} (18)

where $k c_k/\langle k \rangle$ is the probability for a parity check be connected to $k-1$ nodes in addition to the cavity node [see Fig. 4(a)] and $1-(1-\eta)^{k-1}$ is the probability that at least one of these $k-1$ nodes is free in the absence of the parity check. Next, we observe that the probability for the cavity node to
The cavity method is related to a particular decoding algorithm known as belief propagation (BP). Its principle is the following: starting from a configuration where only the noncorrupted bits are fixed to their values, one goes through each node of the factor graph, checks if its immediate neighboring environment constrains it to a unique value, fixes it to this value if it is the case, and iterates the whole procedure until convergence. At the end, some bits may still not be fixed, which certainly occurs if the decoding CSP has not a unique solution, but if all the bits end up fixed, one is ensured to have correctly decoded. Similar message-passing algorithms can be defined with different channels. They are responsible for the practical interest of LDPC codes as they provide algorithmically efficient decoding (yet suboptimal, as discussed below). With the BEC, these algorithms are particularly easy to analyze thanks to the fact that one can never be fooled by fixing bits to an incorrect value. To perform the analysis of the possible outcomes of the belief propagation algorithm, we can assume without loss of generality that the transmitted message is (0, …, 0) (the $Z_2$ symmetry implies that all codewords are equivalent). We thus start with $\sigma_j = *$ if $i \in \mathcal{E}$ and $\sigma_j = 0$ otherwise. Cavity fields are attributed to each oriented link of the factor graphs and are updated with the following rules, where $t$ indexes iteration steps:

$$h_{i \rightarrow a}^{(t+1)} = \begin{cases} 0 & \text{if } \sigma_t = 0 \text{ or if } u_{b \rightarrow i}^{(t)} = 1 \text{ for some } b \in i - a, \\ * & \text{otherwise}, \end{cases}$$

$$u_{i \rightarrow a}^{(t+1)} = \begin{cases} 1 & \text{if } h_{j \rightarrow a}^{(t)} = 0 \text{ for all } j \in a - i, \\ * & \text{otherwise}. \end{cases}$$

Here, $u_{i \rightarrow a}^{(t)} = 1$ (*) means that the parity check $a$ is constraining (is not constraining) $i$, $h_{i \rightarrow a}^{(t)} = 0$ (*) means that $\sigma_i$ is fixed (not determined) to its correct value 0 without taking
into account the constraints due to $a$. The algorithm is analyzed statistically by introducing

$$\eta^{(t)} = \frac{1}{\langle \ell \rangle N} \sum_{(i,a)} \delta(h_{i,a}^{(t)}), \quad \zeta^{(t)} = \frac{1}{\langle k \rangle M} \sum_{(i,a)} \delta(u_{i,a}^{(t)}) - 1.$$

(26)

As suggested by our notations, the evolution for these quantities exactly mimics the derivation of the formulas for the cavity fields, yielding

$$\eta^{(t+1)} = -\frac{\langle \zeta^{(t)} \rangle}{\langle \ell \rangle}, \quad \zeta^{(t+1)} = 1 - \frac{1}{\langle k \rangle} \eta^{(t)}.$$

(27)

The fixed point is given by Eq. (24). When $p < p_d$, the algorithm converges towards the unique, ferromagnetic, fixed point $\eta^{(s)}=\xi^{(s)}=0$ and decoding is successfully achieved. When $p_d < p < p_c$, a paramagnetic fixed point appears in addition to the ferromagnetic fixed point and the iteration leads to this second paramagnetic fixed point. The belief propagation algorithm thus fails to decode above the dynamical threshold $p_d$, before reaching the static threshold $p_c$, below which no algorithm can possibly be successful (in this sense, BP is suboptimal).

### B. Average error exponents

1. **Entropic (1RSB) large deviations**

The previous section recalled the properties of typical codes subject to typical noise. With finite codewords, $N < \infty$, failure to decode may also be due to atypical noise with unusually destructive effects. This is the purpose of our large deviation approach to investigate such events. We first focus on the simplest case: namely, the computation of the average error exponent where both the codes $C$ and the noise $\xi$ are treated on the same footing (see Sec. II E). Our procedure to deal with the statistics over atypical factor graphs is an application of the cavity method for large deviations proposed in [15]. For the sake of simplicity, we restrain ourselves here to regular codes, where nodes and check nodes have both fixed connectivity, $\ell$ and $k$, respectively, and defer the generalization to irregular codes to Appendix D.

As explained in Sec. II E, the thermodynamic formalism assigns a Boltzmann weight $e^{aS_C(C,\xi)}$ to each “configuration” $(C,\xi)$. The parameter $x$ plays the role of an inverse temperature or, in other words, is a Lagrange multiplier enforcing the value of $S_N$. Taking the infinite-temperature limit $x=0$ (no constraint on the value of $S_N$) will thus lead us back to the typical case discussed above.

The cavity equations are as before derived by considering the effect of the addition of a node. As adding a new node, along with its adjacent parity checks, inevitably increases the degrees of the other nodes, strictly restraining to regular graphs is not possible and we must work in a larger framework. Accordingly, we consider ensembles where the degree of parity checks is fixed to $k$, but where the degree of nodes has a distribution $\{v_L\}$ (meaning that degree $L$ has probability $v_L$, independently for each node). We will describe the regular ensemble by taking $v_L = \delta_{v_L}$ in the final formulas. Adding a new node with $\ell$ parity checks brings us from an ensemble characterized by $v_L$ to an ensemble characterized by $v'_L$, with

$$v'_L = \left(1 - \frac{\ell(k-1)}{N}\right) v_L + \frac{\ell}{N} v_{L-1} = v_L + \frac{\ell}{N} \delta v_L,$$

(28)

where $\delta v_L = v_{L-1} - v_L$, since $\ell(k-1)$ nodes have their degree increased by 1. Let denote by $L(s,\{v_L\})$ the rate function for the probability to observe $S_N/N = s$ in an ensemble characterized by $\{v_L\}$—that is,

$$P_N(s = S(N+1)/N)v_{\{v_L\}} = e^{-N L(s,\{v_L\})}.$$

(29)

We introduce $P_{N+1}(s = S(N+1)/N)v_{\{v_L\}} = e^{-N L(s,\{v_L\})}$, the probability distribution of the entropy contribution caused by the addition of the new nodes along with its $\ell$ adjacent parity checks. The passage from $N$ nodes to $N+1$ nodes can then be described by

$$P_{N+1}(s = S(N+1)/N)v_{\{v_L\}} = e^{-N L(s,\{v_L\})} = \sum_{\ell} v_{\ell} \int d\Delta S_{\{v_L\}} e^{-N L(s,\{v_L\})} P_{N+1}(s = S(N+1)/N)v_{\{v_L\}}.$$ 

(30)

Expanding for large $N$, one gets

$$\phi(x) = xs - L(s,\{v_L\})$$

$$= \ln \sum_{\ell} v_{\ell} \int d\Delta S_{\{v_L\}} e^{x\Delta S + \phi(\ell-1)},$$

(31)

with

$$\phi(x) = \sum_{\ell} \delta v_L \frac{\partial L(s,\{v_L\})}{\partial v_L}.$$ 

(32)

The parameter $\phi(x)$ is determined by noting that the addition of a new parity check changes the node degree distribution in the same way as in Eq. (28), with $v''_L = v_L + (k/N) \delta v_L$, yielding
Finally, we obtain a self-consistent equation for the addition of a new cavity node: if the new node is free, which occurs with probability $1 - \eta$, then there is an entropic reduction $-\ln 2$ per nonconstraining adjacent parity check and therefore a weight $2^{x_d}$. Otherwise, if the new node is free, which occurs with probability $p_d z_d$, the entropy shift is $(\ln 2)(1 - \ell)$, giving a weight $2^{x_d(1-\ell)}$. Taking $v_d = \delta_d$, Eq. (31) therefore reads

$$e^{-NL[\ln(v_d)]} \geq \int d\Delta S [\Delta S] e^{-NL[\ln \{\ln(\Delta S)\}/N]} ,$$

(33)

where $P_{\square}(\Delta S)$ is the probability of the entropy reduction caused by the addition of a new parity check. Expanding here also for large $N$ leads to an equation for $z$:

$$z = -\frac{1}{k} \ln \left( \int d\Delta S [\Delta S] e^{\eta \Delta S} \right).$$

(34)

Following the same line of reasoning as in the typical case, the two distributions $P_{\square}(\Delta S)$ and $P_{\square}$ can be expressed by means of cavity fields $\eta$ and $\xi$. First consider the addition of a node: If the bit of the new node is fixed, either because it was not erased or because one of its adjacent parity checks constrains it, there is an entropic reduction $-\ln 2$ per nonconstraining adjacent parity check and thus a weight $2^{x_d}$. Otherwise, if the new node is free, which occurs with probability $p_d z_d$, the entropy shift is $(\ln 2)(1 - \ell)$, giving a weight $2^{x_d(1-\ell)}$. Taking $v_d = \delta_d$, Eq. (31) therefore reads

$$\phi_d(x) = \ln[\xi^{2^{\eta}} + (1 - \xi)\frac{x}{\eta}] - p_d(\xi^{2^{\eta}} + p_d \xi^{2^{x_d(1-\ell)}}) + \ell (k - 1)z ,$$

(35)

with

$$\xi = 1 - (1 - \eta)^{k-1} .$$

(36)

Similarly, a new parity check removes a degree of freedom if and only if one of its adjacent node is free, which happens with probability $1 - (1 - \eta)^k$, yielding

$$z = -\frac{1}{k} \ln[1 - (1 - \eta)^k] + [1 - (1 - \eta)^k]2^{-x_d} .$$

(37)

Finally, we obtain a self-consistent equation for $\eta$ by considering the addition of a new (cavity) node in the absence of one of its adjacent parity checks:

$$\eta = \Gamma^c(\text{cavity node free})$$

$$\geq \int d\Delta S [\Delta S] e^{\eta \Delta S} [\text{cavity node free}] e^{\Delta S z_d (1-\ell)(k-1)} ,$$

(38)

$$\Rightarrow \int d\Delta S [\Delta S] e^{\eta \Delta S} [\text{cavity node fixed}] e^{\Delta S z_d (1-\ell)(k-1)} ,$$

(39)

where $P_{\square}$ corresponds to $P_{\square}(\Delta S)$, taken either under the condition that the cavity node be free or that be is fixed. We obtain

$$\eta = \frac{p_d^2((2\xi^{2^{\eta}} - 1)^{1-\ell} + p_d(2^{x_d} - 1)(2\xi^{2^{x_d(1-\ell)}})^{1-\ell}) .$$

(40)

Alternatively, these equations can be obtained by differentiation of Eq. (35), which is variational with respect to the cavity $\eta$. The large deviation cavity equations (36) and (37) allow us to compute the cavity fields $\phi_d(x)$ using Eqs. (35) and (37), from which the rate function $L(s_1[v_d = \delta_d])$ is deduced by Legendre transformation as discussed in Sec. II E.

Again, two kinds of solutions, paramagnetic or ferromagnetic, can be present. For a given value of $\eta$, we find that a nontrivial, paramagnetic solution to Eq. (40) exists only for $x \geq x_d(p)$. In agreement with the observation reported in the previous section that the paramagnetic solution typically exists only when $p < p_d$, we have $x_d(p) < 0$ for $p < p_d$ and $x_d(p) = 0$ for $p > p_d$ (the typical case is indeed associated with $x=0$). We obtain the average error exponent by selecting the value of $L(s_2)$ where $s_1 = x_d$: our results are illustrated in Fig. 6. By extension of the concept of dynamical threshold $p_d$, one could define a “dynamical” error exponent as $E_d(p) = L(x_d(p)) - \phi_d(x_d(p))$, corresponding to the temperature of the spinodal for the paramagnetic solution. The relevance of this concept is, however, limited by the fact that the algorithmic interpretation presented in Sec. III A 3 does not extend to large deviations (see also Sec. III C 3).

More interestingly, we find an additional threshold (see Table III), denoted $p_{e,RSB}$, below which the equation $s_1(x) = 0$ has no longer a solution (see Fig. 6). This inconsistency of the 1RSB solution is indicative of the presence of a phase transition occurring at some $p_e > p_{e,RSB}$. The following section is devoted to computing $p_e$ and describing the nature of the new phase present for $p < p_e$. 
The generating function for the rate function $L_1(\epsilon)$ defined as

$$\phi_1(x) = \ln \left\{ p \int \prod_{a=1}^\ell du_a Q(u_a) \exp \left[ -x \left( \sum_{a=1}^\ell |u_a| - \sum_{a=1}^\ell u_a \right) \right] ight\} + (1-p) \int \prod_{a=1}^\ell du_a Q(u_a) \exp \left[ -2x \sum_{a=1}^\ell \delta_{u_a-1} \right]$$

$$- \frac{\ell(k-1)}{k} \ln \left\{ \prod_{i=1}^k dh_i P(h_i) \exp \left[ -x \delta \left( \prod_{i=1}^k h_i - 1 \right) \right] \right\}, \quad (43)$$

with

$$P(h \neq +\infty) \propto p \int \prod_{a=1}^{\ell-1} du_a Q(u_a)$$

$$\times \exp \left[ -x \left( \sum_{a=1}^{\ell-1} |u_a| - \sum_{a=1}^{\ell-1} u_a \right) \right]$$

$$\times \delta \left( h - \sum_{a=1}^{\ell-1} u_a \right), \quad (44)$$

$$P(h = +\infty) \propto (1-p) \int \prod_{a=1}^{\ell-1} du_a Q(u_a) \exp \left[ -x \sum_{a=1}^{\ell-1} \delta_{u_a-1} \right],$$

$$Q(u) = \prod_{i=1}^{k-1} dh_i P(h_i) \delta \left[ u - S \left( \prod_{i=1}^{k-1} h_i \right) \right], \quad (46)$$

where $S(x) = 1$ if $x > 0$, $-1$ if $x < 0$, and 0 if $x = 0$. Since $u$ only takes values in $\{-1, 0, +1\}$ and $h$ is restrained to integer values, we can introduce

$$Q(u) = q_+ \delta(u-1) + q_- \delta(u+1) + q_0 \delta(u) \quad (47)$$

and

$$p_+ = \int_{h>0} dh P(h), \quad p_- = \int_{h<0} dh P(h), \quad p_0 = 1 - p_+ - p_-.$$  

(48)

Our interest is here in zero-energy ground states, described by the limit $x \to \infty$, where the equations simplify to
We find that the only stable solution to these cavity equations satisfies $q_0 = p_0 = 0$, which allows us to further simplify the formulas

$$\phi_k(x = \infty) = -L(e = 0) = \ln[(1 - q_\ell)^k + p(1 - q_\ell)^k - pq_0^k]$$

$$-\frac{\ell (k - 1)}{k} \ln \left[ 1 - \frac{1}{2}((p_+ + p_-)^k - (p_+ - p_-)^k) \right],$$

with

$$p_+ \approx (1 - q_\ell)^{\ell - 1} - pq_0^{\ell - 1},$$

$$p_- \approx p(1 - q_\ell)^{\ell - 1} - pq_0^{\ell - 1},$$

$$p_0 \approx pq_0^{\ell - 1},$$

$$q_+ = \frac{1}{2}[(p_+ + p_-)^{\ell - 1} + (p_+ - p_-)^{\ell - 1}],$$

$$q_- = \frac{1}{2}[(p_+ + p_-)^{\ell - 1} - (p_+ - p_-)^{\ell - 1}],$$

$$q_0 = 1 - (p_+ + p_-)^{\ell - 1}.\tag{55}$$

We find that the only stable solution to these cavity equations satisfies $q_0=p_0=0$, which allows us to further simplify the formulas

$$\phi_k(x = \infty) = \ln[q_\ell^k + p(1 - q_\ell)^k]$$

$$-\frac{\ell (k - 1)}{k} \ln \left[ \frac{1}{2}[1 + (2p_+ - 1)^k] \right],$$

with

$$p_+ = \frac{q_\ell^{\ell - 1}}{q_\ell^{\ell - 1} + p(1 - q_\ell)^{\ell - 1}}.\tag{57}$$

The resulting RS average error exponent, given by $E_e(p) = -\phi(x = \infty)$, is represented in Fig. 7.

We identify the transition $p_c$ as the point where the 1RSB and RS error exponents coincide, which satisfies $p_c > p_{1RSB}$. We find that the RS solution is limited by a spinodal point and is only defined for $p \geq p_{1RSB}$. While we conjecture that the 1RSB estimate is exact for $p > p_c$, the existence of $p_{1RSB}$ suggests that either an additional phase transition occurs at some $p_c > p_{1RSB}$ or, more radically, that our description of the phase $p < p_c$ is incorrect. The limit case of random codes, however, indicates that the energetic method is valid in the limit $k, \ell \to \infty$.

### 3. Limit of random codes

The only limiting case where the average error exponent has been obtained integrally so far is the fully connected limit where $k, \ell \to \infty$ with $\ell/k = \alpha = 1 - R$ fixed. This limit corresponds to the random linear model, where an adjacency matrix is connected to each node with probability $1/2$. In this limit, the entropic 1RSB approach gives

$$E_e(k, \ell \to \infty) = L(s = 0) = D(1 - R \| p),$$

where $D(q \| p) = \alpha \ln(q/p) + (1 - \alpha) \ln[(1 - q)/(1 - p)]$ is known as the Kullback-Leibler divergence, while the energetic RS approach gives

$$E_e(k, \ell \to \infty) = -\phi_k(x = \infty) = -(R - 1) \ln 2 - \ln(1 + p)$$

(60)

(with $p_c = 1/1 + p$ and $q_c = 1/2$). The two expression coincide at the critical noise $p_c$, with

$$p_c = (1 - R)/(1 + R).\tag{61}$$

We thus predict the average error exponent of the RLM to be

$$E_e(\text{RLM}) = \begin{cases} (1 - R) \ln 2 - \ln(1 + p) & \text{if } p < \frac{1 - R}{1 + R}, \\ D(1 - R \| p) & \text{if } \frac{1 - R}{1 + R} < p < 1 - R. \end{cases}\tag{62}$$

### C. Typical error exponents

#### 1. Cavity equations

The typical error exponent is encoded into a potential $\phi(x,y)$, as defined in Eq. (13). The equations for $\phi(x,y)$ are obtained from the cavity method for large deviations by following very closely the path leading to $\phi(x)$ [31]. As noticed in Sec. II, the formalism with finite $y$ provides a generalization of the average case which is recovered by taking $y = 1$, with $\phi(x,y = 1) = \phi(x)$. We will therefore only quote our results. In the entropic (1RSB) case, we find
\[ \psi_{x}(x,y) = \ln\left[\left(\xi 2^{-xy} + 1 - \xi\right)^{\ell} - \left(\xi 2^{-xy}\right)^{\ell} + \xi^{\ell}(p 2^{x} + 1 - p)^{2^{-\ell xy}}\right] - \left(\frac{\ell (k-1)}{k}\right) \ln\left(1 - \eta\right)^{k} + \left[1 - (1 - \eta)^{k}\right] 2^{-xy}, \]  

with

\[ \eta = \frac{\xi^{1-p}}{(\xi 2^{-xy} + 1 - \xi)^{1} - (\xi 2^{-xy})^{1} + \xi(p 2^{x} + 1 - p)^{2} 2^{-1}}, \]

\[ \zeta = 1 - (1 - \eta)^{k-1}. \]

In the energetic (RS) case with \( x=+\infty \), we find

\[ \psi_{x}(x=+\infty,y) = \ln\left[q_{c}^{-1} + p^{y}(1-q_{c})^{\ell}\right] - \left(\frac{\ell (k-1)}{k}\right) \ln\left[\frac{1}{2}(1 + (2p_{s} - 1)^{k})\right], \]

with

\[ p_{s} = \frac{q_{c}^{-1}}{q_{c}^{-1} + p^{y}(1-q_{c})^{\ell-1}}, \]

\[ q_{c} = \frac{1}{2}[1 + (2p_{s} - 1)^{k-1}]. \]

In each case, from the potential \( \psi(x,y) \), the rate function is obtained as \( \mathcal{L}(\phi,x,y) = y \phi - \psi(x,y) \), with \( \phi(x) = \partial_{x} \psi(x,y) \). By definition, a typical code corresponds to a minimum of \( \mathcal{L} \), with \( \mathcal{L}=0 \), which, when \( \mathcal{L} \) is analytical at this minimum, is associated with \( y=\partial_{\phi} \mathcal{L}=0 \).

As a generic feature, we find that \( \mathcal{L}(y,x) \) is an increasing function of \( y \) for fixed \( x \), going from negative values for \( y < y_{c}(x) \) to positive ones for \( y > y_{c}(x) \). Negative rate functions, as thus obtained, are certainly unphysical. As negative entropies in the usual cavity-replica method, we attribute them to analytical continuations of physical solutions. The simplest way to circumvent them is, as with the frozen 1RSB ansatz in the replica method, to select \( y_{c}(x) \) with \( \mathcal{L}(y,x)=0 \). When \( y_{c}(x)<1 \), meaning that \( \mathcal{L}(y=1,x)>0 \), we consider that the average exponent is associated with atypical codes and therefore differs from the typical exponent, described by \( \mathcal{L}(y_{c}(x),x)=0 \). Using this criterion, we find that the two exponents indeed differ for the lowest values of \( p \), when \( p < p_{c} \), where \( p_{c} < p_{c} \) (see Fig. 8 for an illustration). In general the situation is complicated by the fact that the cavity equations may fail to provide solutions in this regime, as already seen in the average case when \( p < p_{RS} \) (corresponding here to \( y=1 \)); the random code limit, where this complication is absent, is thus the most instructive.

### 2. Limit of random codes

In the limit \( k, \ell \to \infty \), we obtain the following results. In the entropic regime, \( p > p_{c} \), the average and typical exponents are found to coincide. This conclusion extends in the energetic regime only for a restricted interval \([p_{s},p_{c}]\). When \( p < p_{c} \), we have \( y_{c}(x)<1 \) and average and typical error ex-

### IV. LDPC CODES OVER THE BSC

#### A. Definition

We now turn to error exponents for LDPC codes on the binary symmetric channels. One motivation for repeating the analysis with this channel is that it is representative of a broader class of channels, where bits are not simply erased as
with the BEC, but can be corrupted, in the sense that their content 0 or 1 is changed to other admissible values. This clearly complicates the decoding as corrupted bits cannot be straightforwardly identified; in fact, with the BSC, no scheme can guarantee to identify the corrupted bits and the receiver is never certain that his decoding is correct. We will, however, see that the overall phase diagram is very similar to that obtained with the BEC.

By definition, maximum-likelihood decoding consists in inferring the most probable realization of the noise a posteriori. The a posteriori probability can be expressed from the a priori probability thanks to Bayes’ theorem. If \( x \) denotes the transmitted message and \( y \) the received message, the a priori probability to receive \( y \) given \( x \) is

\[
Q(y|x) = \prod_{i=1}^{N} (1-p)^{\delta_{y_i}x_i}p^{1-\delta_{y_i}x_i}.
\]

To make contact with physical models of disordered systems [12], it is convenient to adopt a spin convention \( \sigma_i = (-1)^{y_i}, \tau_i = (-1)^{x_i} \), and to rewrite the previous relation as

\[
Q(\sigma|\tau) \propto \exp \left( \sum_{i=1}^{N} h_i \tau_i \right), \quad h_i = h_0 \sigma_i, \quad h_0 = \frac{1}{2} \ln \left( \frac{1-p}{p} \right).
\]

This formulation emphasizes the analogy with the random field Ising model [32], a prototypical disordered system. Using the group symmetry of the set of codewords, we can assume, without loss of generality, that the sent codeword is \( \sigma = (+1, \ldots, +1) \). With this simplification, the random field takes value \( h_i = h_0 \) with probability \( 1-p \) and \( -h_0 \) with probability \( p \), for the transmitted message and \( y \) the received message, the a priori probability to receive \( y \) given \( x \) is

\[
Q(y|x) = \prod_{i=1}^{N} (1-p)^{\delta_{y_i}x_i}p^{1-\delta_{y_i}x_i}.
\]

Numerical estimates of the error probability, based on \( 10^6 \) runs of exact maximum-likelihood decoding (using Gauss elimination) on samples of sizes ranging from \( N=500 \) to \( N=1500 \), yield reasonably good estimates of the error exponent using an exponential fit. These numerical results agree well with our theoretical prediction. The union bound (C11) and the random linear limit (62) are also represented for comparison.

In physical terms, the word-MAP procedure consists in finding the ground state of the system with partition function \( Z(\beta) \) given by the normalization in Eq. (72); this amounts to studying the zero-temperature limit \( \beta \to \infty \). Conversely, symbol MAP is equivalent to taking the sign of the local magnetizations at temperature \( \beta=1 \),

\[
p_{\text{hit}}^{\text{sym}} = \text{sgn}(\langle \tau_i \rangle) = \text{sgn} \left( \sum_{\tau} \tau_i P(\tau|\sigma) \right).
\]

We will treat the two cases in a common framework by considering an arbitrary temperature \( \beta \geq 1 \).
From the physical perspective, the original codeword is recovered if it dominates the Gibbs measure defined in Eq. (72). This can be expressed by decomposing the partition function $Z(\beta)$ as

$$Z(\beta) = Z_{\text{corr}}(\beta) + Z_{\text{err}}(\beta) = e^\beta \sum_i h_i,$$

$$Z_{\text{err}}(\beta) = \sum_{\tau \neq 1} e^\beta \sum_i h_i \tau_i \delta(\tau_i - 1).$$  

(74)

We define the corresponding free energies $F_{\text{corr}}(\beta) = -(1/\beta) \ln Z_{\text{corr}}(\beta)$ and $F_{\text{err}}(\beta) = -(1/\beta) \ln Z_{\text{err}}(\beta)$. The first one corresponds physically to a ferromagnetic phase (as with the BEC), while the second will be shown to correspond to either a paramagnetic or a glassy phase, depending on the values of $\beta$ and $p$. Decoding is successful if, and only if, the ferromagnetic phase has lower free energy, $F_{\text{corr}} < F_{\text{err}}$. The quantity $S_N(\xi, C)$ introduced in Sec. II E can therefore be defined here as

$$S_N = F_{\text{corr}}(\beta) - F_{\text{err}}(\beta),$$  

(75)

where the dependence in the noise $\xi$ and the code $C$ is implicitly understood.

### B. Cavity analysis and the 1RSB frozen ansatz

As with the BEC, explicit calculations can be performed by means of the replica or cavity methods. Details can be found in Appendix E, and we only discuss here the points where differences with the BEC arise. For any fixed $p$, a replica-symmetric calculation, whose derivation follows the derivation of the paramagnetic solution with the BEC, is found to undergo an entropy crisis—i.e., $s_{\text{RS}}(\beta) = \beta^2 \bar{\sigma}_{\text{RS}}(\beta) < 0$ for $\beta > \beta_c$. This feature is indicative of the presence of a glassy phase and points to the need to break the replica symmetry. The glassy phase of LDPC codes is, however, of the “frozen 1RSB” type, which implies that the glassy free energy $f_{\text{err}}$ can be completely inferred from the replica-symmetric solution $f_{\text{RS}}$. This simplicity stems from the “hard” nature of the constraints: changing a bit automatically violates all its surrounding checks, forcing the rearrangement of many variables [33,34]. When the degree of all nodes is $\ell_i \approx 2$, one can indeed show [24] that changing one bit while keeping all checks satisfied requires the rearrangement of an extensive ($\approx N$) number of variables (in the language of [24], factor graphs of LDPC codes have no leaves).

The consequence, expressed in the replica language, is that the 1RSB “states” are reduced to single configurations and thus have zero internal entropy. The 1RSB potential $\phi(\beta, m)$ whose optimization over $m \in [0, 1]$ is predicted to yield $f_{\text{err}}$ [20] thus simplifies to $\phi(\beta, m) = f_{\text{RS}}(\beta m)$ [35], since

$$e^{-N \beta m \phi(\beta, m)} = \sum_{\text{states } \alpha} e^{-N \beta m f_{\text{RS}}(\beta m)} = e^{-N \beta m e_{\text{err}}} = e^{-\beta m f_{\text{RS}}(\beta m)}.$$

(76)

According to whether one is above or below the freezing temperature $\beta^{-1}_c$, defined by

$$s_{\text{RS}}(\beta_c) = \beta_c^2 \bar{\sigma}_{\text{RS}}(\beta_c) = 0,$$

(77)

the free energy $f_{\text{err}}(\beta)$ is given either by $f_{\text{RS}}(\beta)$ (paramagnetic phase) or by $f_{\text{RS}}(\beta_c)$ (glassy phase). This is summarized as follows:

$$f_{\text{err}}(\beta) = \max_{\beta' = \beta} f_{\text{RS}}(\beta') = \begin{cases} f_{\text{RS}}(\beta) & \text{if } \beta < \beta_c, \\ f_{\text{RS}}(\beta_c) & \text{if } \beta > \beta_c. \end{cases}$$

(78)

Finally, we note that as in the BEC case, a nonferromagnetic solution $f_{\text{RS}}(\beta)$ exists only for large enough $p$. The threshold $p_{c}(\beta)$ giving the smallest noise level at which a nonferromagnetic solution exists is again called the dynamical threshold and can be shown here also to coincide with the dynamical arrest of BP [28].

### C. Average error exponent: LDPC codes

In the region relevant for error exponents, where $p < p_c$ and $\beta \geq 1$, the ferromagnetic solution is typically dominant (this is the definition of $p < p_c$) and metastable phases described by $f_{\text{err}}$ are typically glassy, since $\beta_c < 1$. Therefore, to compute error exponents, we have to consider $f_{\text{err}}(\beta) = f_{\text{RS}}(\beta_c)$ and not $f_{\text{err}}(\beta) = f_{\text{RS}}(\beta)$. This leads us to introduce an extra temperature $\beta_\epsilon$ distinct from the decoding temperature $\beta$, which is to be set to $\beta_c$ by requiring that the entropy $s_{\text{RS}}$ be zero. Similarly, we introduce a ferromagnetic tem-
nent is predicted to be the same for any consequence of the analysis is that the average error exponent based on the replica method given in (B14) are also represented for comparison.

The potential \( \phi_1 \) contains all the necessary information about both solutions:

\[
-\beta a \phi_a = \partial_a \phi_1, \quad s_a = \partial_a \phi_1 - \frac{\beta a}{x_a} \partial_{x_a} \phi_1,
\]

(80)

where the index \( a = e,f \) corresponds to the two possible phases. For the purpose of computing error exponents, we need only to control \( f_e - f_f \) and \( s_e \) for all temperatures \( \beta_e < \beta \). Note that the ferromagnetic solution \( f_f \) has no entropy, \( s_f = 0 \), which is here reflected by the fact that the potential \( \phi_f \) depends upon \( \beta_f \) and \( x_f \) only through \( m_f = \beta_f x_f \). These observations allow us to focus on a simplified potential

\[
\hat{\phi}(\beta, m) = \phi_1\left(\beta_c, x_c = \frac{m}{\beta_e}, m_f = -m\right),
\]

(81)

which satisfies

\[
\partial_{\beta_f} \hat{\phi} = f_f - f_e, \quad \partial_{x_f} \hat{\phi} = -m s_e.
\]

(82)

As with the BEC, the average error exponent is identified with the smallest value of \( L_1 \) such that \( s_e \geq 0 \) and \( f_e - f_f \geq 0 \). The present formulation is in fact equivalent to the presentation based on the replica method given in [10]. A remarkable consequence of the analysis is that the average error exponent is predicted to be the same for any \( \beta \approx 1 \). Indeed, both the glassy and the ferromagnetic free energies are temperature independent for \( \beta \approx \beta_e \). In particular, symbol and word MAP are predicted to have same error exponents.

Based on the cavity equations given in Appendix E, the potential \( \hat{\phi} \) can be computed numerically by population dynamics. As an illustration, we plot in Fig. 9 the rate function \( L_1(f_f - f_e, s_e = 0) \) for a regular code with \( k = 6, \ell = 3 \). As in the case of BEC, three regimes can be distinguished, according to the value of \( p \).

(i) \( p < p_{1RSB} \): no zero-entropy RS solution typically exists and \( f_e < f_f \) for the metastable solutions.

(ii) \( p_{1RSB} < p < p_{1A} \): no zero-entropy RS solution typically exists but the dominant metastable solutions have \( f_e > f_f \).

(iii) \( p' < p < p_c \): a zero-entropy RS solution is typically present.

The major difference with the BEC is that the threshold \( p_{1A} \) defined by \( p_{1A} = p_A(\beta(0)) \) does not coincide with the dynamical threshold \( p_A(\beta) \); indeed \( p_{1A} \) is defined in relation to the existence of a solution with positive entropy, while, in the framework of BP, the dynamical arrest \( p_g \) is related to the existence of a paramagnetic solution at decoding temperature \( \beta^{-1} \) [28]. In Fig. 10, we plot the average error exponent for regular codes with \( k = 6, \ell = 3 \).

**D. Random code limit**

1. **Average error exponent**

As with the BEC, the \( k, \ell \rightarrow \infty \) limit can be computed exactly, yielding

\[
E_1^{(1)} = L_1(f_f = f_e, s_e = 0) = D(\delta_{G2}(R) \parallel p),
\]

(83)

where \( \delta_{G2}(R) \) denotes the smallest solution to \( R - 1 + H(\delta) = 0 \). In this regime, errors are most likely to be caused by large noises driving the received message beyond the typical nearest-codeword distance.

As pointed out in [10], a second ferromagnetic solution is present in this limit (see Appendix E for details), yielding the error exponent

\[
E_1^{(2)} = -\frac{1}{2} \left[ 1 + 2 \sqrt{p(1-p)} \right] - R \ln 2.
\]

(84)

Such a solution also exists for finite \( k, \ell \), but is clearly unphysical (it predicts negative exponents for \( k = 6, \ell = 3 \)). Yet it correctly describes the low \( p \) phase (B14) in the \( k, \ell \rightarrow \infty \) limit, where failure is caused by the existence of one (or a
few) unusually close codewords. In that sense it plays the same role as the energetic solution in the BEC analysis, with the difference that it is not extensible to any case with finite connectivities. The critical noise $p_c$ below which such a scenario occurs is given by

$$\sqrt{p_c} = \delta_{C1}(R).$$  \hspace{1cm} (85)$$

We thus predict the average error exponent to be

$$E_1(\text{RLM}) = \begin{cases} 
D(\delta_{C1}(R) \parallel p) & \text{if } p < p_c < p_c', \\
- \ln \frac{1}{2} \left[ 1 + 2 \sqrt{p(1-p)} \right] - R \ln 2 & \text{if } p < p_c.
\end{cases}$$ \hspace{1cm} (86)

This expression coincides with the exact result (B14) of the RLM.

### 2. Typical error exponent

The typical exponent of the RLM can be evaluated using the two-step potential:

$$e^{N\hat{\phi}(\beta_e, m, y)} = \mathbb{E}_c \left[ e^{N\hat{\phi}(\beta_e, m)} \right] = \int d\phi e^{N\psi(\phi, \beta_e, m)}. \hspace{1cm} (87)$$

The details of the calculations by the cavity method are given in Appendix E. As in the average case, two distinct solutions appear. The first one is the counterpart of the solution discussed in Sec. IV C. It yields, in the random linear limit,

$$\psi(\beta_e, m, y) = y \hat{\phi}(\beta_e, m). \hspace{1cm} (88)$$

A consequence of the linear dependence on $y$ is that $\hat{\phi}$ always takes the value obtained from the average calculation,

$$E_0(\text{RLM}) = \begin{cases} 
L(y_c) = - \delta_{C1}(R) \ln \left[ 2 \sqrt{p(1-p)} \right] & \text{if } p < p_c', \\
L(y = 1) = E_1(\text{RLM}) & \text{if } p < p_c,
\end{cases} \hspace{1cm} (90)$$

where the critical noise $p_c(R)$ is a solution of

$$\frac{2 \sqrt{p(1-p)}}{1 + 2 \sqrt{p(1-p)}} = \delta_{C1}(R). \hspace{1cm} (91)$$

This exponent coincides with the RLM limit of the union bound (C18) and is rigorously established [7] to be the correct typical error exponent on the BSC.

### V. CONCLUSION

Since Shannon laid the basis for information theory, the analysis of error-correcting codes has been a major subject of study in this field of science [4]. Error-correcting codes aim at reconstructing signals altered by noise. Their performance is measured by their error probability—i.e., the probability that they fail in accomplishing this task. For block codes, where the messages are taken from a set of $2^M$ codewords of length $N$, it is known that when the rate $R = M/N$ is below the channel capacity $R_c$, the probability of error behaves, in the limit of large $N$, at best, as $P_e \sim \exp[-N \mathcal{E}(R)]$ [4]. This error exponent $\mathcal{E}(R)$, also called a reliability function, provides a particularly concise characterization of performance.

For a given code ensemble, two classes of error exponents can generally be distinguished, due to the presence of two levels of “disorder,” one associated with the choice of the code itself and a second associated with the realization of the noise. Average error exponents correspond to take the error
probability \( P_p \) with respect to these two levels simultaneously, while typical error exponents refer to fixed, typical, codes.

In the present paper, we tackled the computation of these two error exponents for a particular class of block codes, the low-density parity-check codes, with two particular channels, the binary erasure channel and the binary symmetric channel. We considered decoding under maximum-likelihood decoding, the best conceivable decoding procedure. We framed the problem in terms of large deviations and applied a recently proposed extension of the cavity method designed to probe atypical events in systems defined on random graphs [15]. This method provides an alternative to the replica method used in [10] to address similar problems, with the advantage of being based on explicitly formulated probabilistic assumptions. With respect to this earlier contribution, our work offers several clarifications, notably on the nature of the different phases, and various extensions, notably to the BEC channel. With this particular channel, our results are analytical, and in the high-noise regime, we conjecture them to be exact. Recent mathematical results on the typical phase diagram [36] foster hope for a confirmation of our results in that context.

From a statistical physics perspective, error exponents are interesting for the richness of their phase diagram, which comprises two phase transitions of different natures. These transitions are observed when the level of noise \( p \) is varied at fixed rate \( R \) (or, equivalently in the special case of random codes, when the rate \( R \) is varied at fixed \( p \)). Close to the static threshold, for \( p_c < p < p_e \), errors are mostly due to the proliferation of many incorrect codewords in the vicinity of the received message. We interpreted this feature in terms of the presence of a glassy phase, and accordingly, we were able to describe this regime by considering a one-step replica symmetry breaking approach. Below \( p_e \), errors become dominated by the effect of single isolated codewords, which we attributed to a transition towards a ferromagnetic state or 1RSB to RS transition. The noise \( p_e \) has its counterpart in the “critical rate” \( R_c \) of information theory [4], which marks the point below which only bounds on the reliability function are known. The replica-symmetric approach we employed to investigate the regime \( p < p_c \) also turns out to be only approximate, except in the limit of infinite connectivity, where we recovered the error exponents of random linear codes [7]. We also described a second transition occurring at \( p_r < p_e \), below which atypical codes come to dominate the average exponent, causing it to differ from the typical error exponent. As it takes place in the space of graphs, this is an example of a critical phenomenon whose description is not accessible to the standard cavity method [14], but only to its extension to large deviations [15] (see also [37] for another example). However, this second transition should be taken with utmost care, as it relies on an approximate ansatz.

The numerous efforts made in the information theory community to account for the low rate regime \( R < R_c \) have so far resulted only in upper and lower bounds for the reliability function [6]. Maybe not too surprisingly, this is also the region of the phase diagram where our methods encounter difficulties. Several examples are, however, now available which demonstrate that statistical physics methods can provide exact solutions to notoriously difficult mathematical problems. The solutions thus obtained generally sharpen our comprehension both of the system at hand and of the techniques themselves, besides often paving the way for rigorous derivations. In the light of some recent such achievements, extending the present statistical physics approach to reach a thorough understanding of error exponents seems to us a valuable challenge.

ACKNOWLEDGMENTS

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. thanks the Human Frontier Science Program for support.

APPENDIX A: A NOTE ON THE EXPONENTIAL SCALING

The thermodynamic approach is based on the assumption that the leading contribution to the probability of error decays exponentially with \( N \). However, as initially shown by Gallager, for ensembles of LDPC codes, the probability of error decays only polynomially in \( N \) to the leading order. In physical terms, this is due to a few codes (whose number is a polynomial in \( N \)) which display a second, metastable, ferromagnetic state at a smaller distance from the ground state (corresponding to the correct codeword) than the numerous configurations forming the paramagnetic state.

To overpass this spurious effect in the simplest, yet purely theoretical way, Gallager focused on the so-called “expurgated ensemble” where the half of the codes with smallest minimum distance is disregarded. On this restricted ensemble which excludes the codes with multiple ferromagnetic states, the error probability decays now exponentially in \( N \) at the leading order and can be characterized with an average error exponent. Needless to say, this construction only makes sense as a convenient theoretical way to access good codes.

As the large deviation method automatically overlooks any polynomial contribution, its results actually apply to the “expurgated ensemble”. This is, however, only true to the extent that the expurgation does not affect the distribution of graphs in the ensemble (i.e., does not change the distribution of degrees, of loops, etc.). This is presumably the case, as supported by the construction presented in [38], where an expurgated ensemble much tighter than Gallage’s one is defined by explicitly associating to any random code an expurgated code obtained by modifying only a number \( O(1) \) of small loops.

APPENDIX B: RANDOM LINEAR MODEL

Definition

A parity-check code is defined by a \( M \times N \) matrix \( A \) over \( \mathbb{Z}_2 \) and its codewords are the vectors \( x=(x_1,\ldots,x_N) \) satisfying \( Ax=0 \). Code ensembles are therefore subsets of the set of
all $2^{MN}$ possible matrices. Taking this complete set (with all possible matrices having some probability) defines the so-called random linear model. In contrast with LDPC codes, since a typical matrix from the RLM is not sparse, the belief propagation algorithm cannot be used to decode. While of little practical interest due to this absence of efficient decoding algorithm, the RLM has, however, two major theoretical advantages, both originating from its “maximally random” nature: typical codes from the RLM saturate the Shannon bounds, and error exponents can be derived rigorously. We review here some of the established results, which we used in the main text as a reference point to compare our nonrigorous results. Error exponents for the RLM are indeed expected to provide upper bounds for error exponents of LDPC ensemble, which are reached only in the limit of infinite connectivity $k, l \to \infty$ (this limit is similar to that in which $p$-spin models approach the random energy model when $p \to \infty$ [27]).

**Weight enumerator function**

We first characterize the geometry of the space of codewords by means of the so-called weight enumerator function. Given a code $C$ with matrix $A$, this function gives the number $N_C(d)$ of codewords $x$ at (Hamming) distance $d = |x|$ from the origin:

$$N_C(d) = \sum_x \delta(d, \sum_{i=1}^N x_i) \delta(Ax, 0),$$

where the sum is over all codewords and $\delta(x, y)$ enforces the constraint $x = y$. The average weight enumerator function is obtained by averaging over the code ensemble and satisfies

$$\bar{N}(d) = E_N[N_C(d)] = \binom{N}{d} d^{-M} \leq e^{N\Sigma(R, \delta = d/N)},$$

$$\Sigma(R, \delta) = (R - 1) \ln 2 + H(\delta),$$

where the limit of infinite block length, $N \to \infty$, is taken with $M = N(1 - R)$ and $d = N\delta$. The exponent $\bar{N}(d)$ defines the so-called average weight enumerator exponent. A critical distance is the distance $\delta_{G_Y}(R)$ defined as the smallest $\delta > 0$ such that $\Sigma(R, \delta) = 0$. Codewords at distance $d = N\delta$ with $\delta > \delta_{G_Y}(R)$ proliferate exponentially. On the other hand, the probability of existence of a codeword at distance $d = N\delta$ with $\delta < \delta_{G_Y}(R)$ is upper-bounded by $\bar{N}(d)$ and thus decays exponentially with $N$. Consequently, for any $\epsilon(N)$ such that $\epsilon(N) \to \infty$ [e.g., $\epsilon(N) = \sqrt{N}$], only an exponentially small fraction of the codes in the ensemble have a minimal nonzero distance $d = M \delta$ smaller than $N\delta_{G_Y}(R) - \epsilon(N)$. Excluding these “worst” codes from the RLM defines the expurgated RLM ensemble.

**Average error exponent over the BEC**

Due to the group symmetry of the set of codewords, we can assume without loss of generality that the transmitted codeword is $(0, \ldots, 0)$. For a given realization of the disorder due to a BEC, we denote by $E \subset \{1, \ldots, N\}$ the subset of erased bits in the received string and $d$ the number of elements in $E$. If $A$ is the $M \times N$ matrix representing the code, the submatrix $\bar{A}_E$ induced by $A$ on $E$ defines the decoding CSP problem: decoding is impossible if and only if the kernel of $\bar{A}_E$ is nonzero. When all matrices $A$ are sampled with uniform probabilities as in the RLM, the submatrices $\bar{A}_E$ are also represented with uniform probability. Given a noise realization $E$ of magnitude $d$, the error probability is the probability that a random $M \times d$ matrix $\bar{A}_E$ is noninjective,

$$E_C(\bar{A}^{(R)}_E(0)) = \sum_{d=0}^{N} \left( \binom{N}{d} \right) p^d(1-p)^{N-d} \times P(\exists x \neq 0 \text{ such that } \bar{A}_E x = 0).$$

When $d > M$, $\bar{A}_E$ is necessarily noninjective. When $d \leq M$, on the other hand, a straightforward inductive argument [8] gives

$$P(\exists x \neq 0 \text{ such that } \bar{A}_E x = 0) = 1 - \prod_{i=0}^{d-1} (1 - 2^{-iM}).$$

Consequently, the exact expression for the average error probability of the RLM reads

$$E_C(\bar{A}^{(R)}_E(0)) = \sum_{d=0}^{M} \left( \binom{N}{d} p^d(1-p)^{N-d} \left( 1 - \prod_{i=0}^{d-1} (1 - 2^{-iM}) \right) \right) + \sum_{d=M+1}^{N} \left( \binom{N}{d} p^d(1-p)^{N-d} \right).$$

In the $N \to \infty$, this expression can be evaluated by the saddle-point method. When $p < (1-R)/(1+R)$, the dominant contribution comes from the first sum, with

$$\sum_{d=0}^{M} \left( \binom{N}{d} p^d(1-p)^{N-d} \left( 1 - \prod_{i=0}^{d-1} (1 - 2^{-iM}) \right) \right) \approx e^{-N[(1-R)\ln 2 - \ln(1+p)]}$$

and typical number of errors $d = N2p/(1+p)$. When $p > (1-R)/(1+R)$ and $p < 1-R$, the dominant contribution comes from the second sum, with

$$\sum_{d=M+1}^{N} \left( \binom{N}{d} p^d(1-p)^{N-d} \approx e^{-ND(1-Rp)}$$

and the typical number of errors $d = N(1-R)$. We thus obtain for the average error exponent of the RLM the expression given in Eq. (62).
In physical terms, the transition between the two regimes can be interpreted as a transition between a ferromagnetic (RS) phase and a glassy (1RSB) phase. In the high-noise regime $p > (1-R)/(1+R)$, the error is indeed most probably due to the noise driving the received string into a “glassy phase” of exponentially numerous incorrect codewords, as reflected by the fact that then $\mathcal{P}(\exists \mathbf{x} \neq 0)$ such that $\hat{A}^T \mathbf{x} = \mathbf{0}$ = 1. In contrast, in the low-noise regime, $p < (1-R)/(1+R)$, the error is most probably due to the noise driving the received string into a “ferromagnetic phase” where an isolated incorrect codeword happens to be closer than the correct codeword; this is reflected by the fact that $\mathcal{P}(\mathbf{x} \neq 0)$ such that $\hat{A}^T \mathbf{x} = \mathbf{0}$ differs from 1 only by an exponentially small term in $N$, as seen from Eq. (B4).

**Average error exponent over the BSC**

With the binary symmetric channel, starting again from the transmitted codeword is $(0, \ldots, 0)$, the received string $\mathbf{y}$ cannot be decoded if there exists $\mathbf{x} \neq 0$ such that $A \mathbf{x} = 0$ and $|\mathbf{x} - \mathbf{y}| < |\mathbf{y}|$. Denoting $P_c(\mathbf{y})$ the probability of this event, the probability of error is

$$
E_c[\mathcal{P}_N^R(\mathbf{0})] = \sum_{d=0}^{N} \binom{N}{d} p^d (1-p)^{N-d} P_c(\mathbf{y}^{(d)}),
$$

(B9)

where $\mathbf{y}^{(d)}$ is a generic string of weight $d$—e.g., $y_i = 1$ if $i \leq d$, $y_i = 0$ if $i > d$. If $d/N > \delta_{\text{GS}}(R)$, $P_c(\mathbf{y}^{(d)})$ goes to 1 in the infinite block-length limit. Although no published proof is available in the literature, it is reported as proved [7] that, when $d/N < \delta_{\text{GS}}(R)$, $P_c(\mathbf{y}^{d})$ is asymptotically equivalent to its union bound approximation (see the following appendix)—i.e.,

$$
P_c(\mathbf{y}^{(d)}) \sim E_c \left[ \sum_{x \neq 0} \theta(d - |x - y^{(d)}|) \delta(A \mathbf{x}, \mathbf{0}) \right]
$$

(B10)

$$
\sim \sum_{d=0}^{d} E_c[\mathcal{N}_c(i, \mathbf{y}^{(d)})]
$$

(B11)

$$
\sim E_c[\mathcal{N}_c(d, \mathbf{y}^{(d)})],
$$

(B12)

where $\mathcal{N}_c(i, \mathbf{y}^{(d)})$ is the number of codewords at distance $i$ from $\mathbf{y}^{(d)}$ and $\theta(x) = 1$ if $x > 0$ and 0 otherwise. Straightforward combinatorics shows that the asymptotic behavior of $E_c[\mathcal{N}_c(i, \mathbf{y}^{d})]$ is given by the standard weight enumerator exponent $\Sigma(R,i/N)$. In the limit $N \to \infty$ where $\delta = d/N$ is kept fixed, a saddle-point evaluation leads to the following expression of the average error exponent:

$$
E_1(\text{RLM}) = - \max_{\delta < \delta_{\text{GS}}} \left[ \Sigma(R, \delta) - D(\delta \| p) \right]
$$

(B13)

$$
= \begin{cases} 
(1-R) \ln 2 - \ln[1+2\sqrt{p(1-p)}] & \text{if } \frac{\sqrt{p}}{1+\sqrt{1-p}} < \delta_{\text{GS}}(R), \\
D(\delta_{\text{GS}}(R) \| p) & \text{otherwise.}
\end{cases}
$$

(B14)
This result with two distinct regime is very similar to that obtained previously for the BEC.

APPENDIX C: UNION BOUNDS

The so-called union bound exponent is a rigorous lower bound of the average error exponent in the expurgated ensemble. We show in this appendix how the average weight enumerator exponent of (regular) LDPC codes can be used to derive this union bound exponent, for both the BEC and BSC. We will thus recover results first established by Gallager in [4,39]. In a nutshell, the idea of the union bound is to upper-bound the probability that at least one (bad) codeword causes an error by the sum of the probabilities that each does. Remarkably, this union bound turns out to be tight for the RLM ensemble.

Weight enumerator function

The weight enumerator function [see Eq. (B1) for the definition] of regular LDPC codes with \( k=6 \) and \( \ell=3 \) was computed in [4] and reads

\[
E_C[N_C(d)] = \sum_x \delta(x,d) E_C[\delta(Ax=0)] = \binom{N}{d} E_C[\delta(Ax^{(d)}=0)]
\]

(C1)

with

\[
\Sigma(k,l,\delta) = \min_{\mu} \left( 2 \mu \ell \delta + (1 - \ell)H(\delta) + \frac{\ell}{k} \ln C(\mu) \right),
\]

(C3)

and

\[
C(\mu) = \frac{1}{2} [(1+e^{-2\mu})^k + (1-e^{-2\mu})^k].
\]

(C4)

We introduce \( \delta_m \), the smallest \( \delta \) such that \( \Sigma(k,l,\delta) \geq 0 \). By construction, the average enumerator exponent in the expurgated ensemble is

\[
\Sigma_{\exp}(k,l,\delta) = \begin{cases} 
\Sigma(k,l,\delta) & \text{if } \Sigma(k,l,\delta) > 0 \text{ (i.e., if } \delta > \delta_m) \\
\infty & \text{otherwise.}
\end{cases}
\]

(C5)

This expurgated average enumerator exponent \( \Sigma_{\exp}(k,l,\delta) \) is believed to coincide with the typical enumerator exponent [40,41].

Union bound for the BEC

Given the set \( E \) of erased bits, we want to estimate the probability \( P_e(d) \) that the CSP-decoding problem has at least two solutions, when a code \( C \) is drawn at random from its ensemble. We call \( A \) the matrix characterizing \( C \), \( \tilde{A}^E \) the submatrix induced by \( A \) on \( E \), and \( d \) the number of erased bits. The union bound consists in the following inequality:

\[
P_e(d) = \mathbb{P}(\exists \bar{x} \in \{0,1\}^d \neq \emptyset \text{ such that } \tilde{A}^E \bar{x} = 0)
\]

(C6)

\[
\leq \min \left[ \sum_{\bar{x} \neq \emptyset} \mathbb{P}(\tilde{A}^E \bar{x} = 0), 1 \right].
\]

(C7)

Let \( w=|\bar{x}| \) and \( x \) be constructed from \( \bar{x} \) by setting \( x_i=\bar{x}_i \) for \( i \in E \), \( x_i=0 \) otherwise: \( \bar{x} \) belongs to the kernel of \( A \) if and only if \( x \) belongs to the kernel of \( A \). The probability of the latter event reads

\[
E_C[N_C(w)] \left( \frac{N}{w} \right)^{-1}.
\]

(C8)

The error probability is consequently bounded by

\[
E_C[N_C(w)] = \sum_{d=0}^{N} \binom{N}{d} p^d (1-p)^{N-d} P_e(d)
\]

\[
\leq \sum_{d=0}^{N} \binom{N}{d} p^d (1-p)^{N-d} \times \min \left[ \sum_{w=0}^{d} \binom{d}{w} E_C[N_C(w)] \left( \frac{N}{w} \right)^{-1}, 1 \right].
\]

(C10)

In the infinite block-length limit, a saddle-point estimate yields, as upper bound for the expurgated average error exponent, the exponent

\[
E_{\exp}(k,l) \geq E_{UB}
\]

\[
= - \max_{\delta} \left\{ -D(\delta \parallel p) + \min \left[ \max_{\omega} \left( \Sigma(\omega) + \delta H(\frac{\omega}{\delta}) - H(\omega) \right), 0 \right] \right\}
\]

\[
= - \max_{\delta < \delta_{UB}} \left\{ -D(\delta \parallel p) + \min_{\omega > \delta_m} \left[ \delta H(\frac{\omega}{\delta}) + 2 \mu \ell \omega - \ell H(\omega) + \frac{\ell}{k} \ln C(\mu) \right] \right\},
\]

(C11)

where \( \delta=d/N, \omega=w/N \), and \( \delta_{UB} \) is the largest \( \delta \) such that \( \max_{\delta} (\Sigma(\omega) + \delta H(\frac{\omega}{\delta}) - H(\omega)) \) is nonpositive.

As \( p \) is varied, three regimes can be distinguished. For small \( p \), the maximum over \( \omega \) is reached on the boundary \( \delta_m \), meaning that errors are dominated by the nearest codewords. For large \( p \) instead, the maximum over \( \delta \) is reached at \( \delta_{UB} \), in which case the union bound is simply replaced by 1, physically corresponding to a large number of bad codewords arising from the large amplitude of the noise. Finally, in the intermediate region of \( p \), the extremum is reached in the interior of the \( (\delta,\omega) \) domain. Note that this last regime is not always present when \( k \) and \( \ell \) are too small (for \( k=6 \) and \( \ell =3 \) in particular). These three regimes are given in the limit \( k, \ell \rightarrow \infty \) by
with $p_y$ defined as in Eq. (69). Union bounds for the BEC are plotted in Fig. 12 for several regular ensembles.

**Union bound for the BSC**

The union bound for the BSC is derived following the same steps than for the BEC. The counterpart of Eq. (C6) reads

$$P_e(d) = 1 - \mathbb{P}(\exists x \neq 0 \text{ such that } |x - y| < d \text{ and } Ax = 0),$$

with $y$ a generic string of weight $d$. Let $x$ be a string a weight $w$ and $Q(w,d,g)$ be the probability for $y$ to be at distance $g$ from $x$, conditioned on $|y| = d$:

$$Q(w,d,g) = \left( \frac{w}{(d-g+w)/2} \right) \left( \frac{N-w}{(d+g-w)/2} \right) \left( \frac{N}{d} \right)^{-1}.$$  

(C14)

The probability for $y$ to be at distance $g$ from any codeword $x$ is upper-bounded by

$$\sum_w E_{\mathcal{C}}[N_{\mathcal{C}}(w)] Q(w,d,g),$$

and we can write

$$P_e(d) \leq \min_{w,g} \left[ \sum_w E_{\mathcal{C}}[N_{\mathcal{C}}(w)] Q_{\mathcal{C}}(w,d,g), 1 \right] \leq \min_{w,g} \left[ \sum_w E_{\mathcal{C}}[N_{\mathcal{C}}(w)] Q_{\mathcal{C}}(w,d,g), 1 \right].$$

(C16)

From this inequality and Eq. (C9), we obtain the union bound for the error exponent via the saddle-point method:

$$E_{\exp}(k,l) \geq E_{UB} = -\max_{\delta} \left[ -D(\delta \| p) + \min_{w,a} \left[ \max_{\omega} \left( \sum_{\omega} \omega \right) + L(\omega, \delta, \delta) \right] \right]$$

$$= -\max_{\delta \leq \delta_{UB}} \left[ -D(\delta \| p) + \min_{\omega, a} \left[ 2 \mu \ell + \left( \omega - \ell \right) H(\omega) + \frac{\ell}{k} \ln C(\mu) + L(\omega, \delta, \delta) \right] \right],$$

$$L(\omega, \delta, \gamma) = \omega H\left( \frac{\delta - \gamma + \omega}{2 \omega} \right) + (1 - \omega) H\left( \frac{\delta + \gamma - \omega}{2(1 - \omega)} \right) - H(\delta).$$

(C17)

As for the BEC, three regimes can be distinguished, according to the value of $p$. In the limit $k, \ell \to \infty$, these three regimes are

$$E_0(RLM) = \begin{cases} 
-\delta_{GV}(R) \ln p & \text{if } p < p_y, \\
(1 - R) \ln 2 - \ln(1 + p) & \text{if } p_y < p < \frac{1 - R}{1 + R}, \\
D(1 - R \| p) & \text{if } \frac{1 - R}{1 + R} < p < 1 - R, 
\end{cases}$$

where $p_y$ and $p_e$ are given by Eq. (91) and (85). Union bounds for the BSC are plotted in Fig. 12.

**APPENDIX D: IRREGULAR CODES**

**Definition of the ensemble**

In this appendix we discuss the generalization to irregular graphs. We shall only treat the entropic large deviations with the BEC, but our arguments can easily be generalized to the other cases. With irregular codes, it is necessary to specify more precisely the definition of the ensemble. The usual definition is via the degree distributions $v_\ell$ and $c_\ell$. It is, however, possible to define different ensembles having same distribution and sharing the same typical properties, but differing at the level of atypical properties, including error exponents (see also [15] for similar nonequivalences in an other context).

The simplest construction takes all factor graphs with exactly $v_\ell N$ checks of degree $\ell$, $c_\ell M$ variables of degree $k$, and pick them with uniform probability. Such ensembles are used to build actual codes, and we shall therefore analyze them with some details.

**Average error exponent**

We revisit the arguments of Sec. III B and emphasize the differences with the regular case.

A crucial modification is the introduction of Lagrange multipliers enforcing the number of nodes of each degree. Call $N_\ell$ the number of variables of degree $\ell$ and $M_\ell$ the number of checks of degree $\ell$. Denote $n_\ell = N_\ell / N$ and $m_\ell = M_\ell / N$. The rate $L_\ell$ is now a function of the $n_\ell$ and $m_k$. Its multiple Legendre transform is defined as

$$\phi(x, \{\lambda_\ell\}, \{v_\ell\}) = x + \sum_\ell n_\ell + \sum_k v_\ell m_k - L_\ell,$$

(D1)

with

$$x = \partial_x L_1, \quad \lambda_\ell = \partial_{n_\ell} L_1, \quad v_\ell = \partial_{m_\ell} L_1.$$

Let us consider the addition of a new bit. $\ell$ checks are added along with it, where $\ell$ is drawn with probability $v_\ell$. Each of these checks, in turn, is connected to $k_a - 1$ old bits $(a=1, \ldots, \ell)$, where $k_a$ is drawn with probability $k_a c_{k_a} / \langle k \rangle$. Equation (31) is modified in the following way:
The addition of a variable of degree $\ell$ is reflected by a factor $e^{\eta/2}$ and the addition of a check of degree $k$ by a factor $e^{\mu k}$. Call the $k$ degree the degree of a variable with respect to checks of degree $k$. Here $z_k$ is related to the increase of $k$ degrees in the ensemble. Let us consider for a moment a $\ell$-degree variable $x_k$ as the expression of \( z_k \). Then $z_k$ is defined by

\[
    z_k = \sum_{\ell} \frac{\partial \phi}{\partial v_{\ell}} = \frac{\partial L_1(s, \{v_{\ell}\})}{\partial v_{\ell}},
\]

where $\partial \phi/\partial v_{\ell} = v_{\ell} - v_{\ell}^{(k)}$. $z_k$ is obtained in a very similar way as $z$ in Eq. (37):

\[
    z_k = - \frac{1}{k} \ln \int d\Delta S P_\ell^{(k)}(\Delta S) e^{\Delta S + \nu_k},
\]

where $P_\ell^{(k)}(\Delta S)$ now depends on the degree $k$.

The cavity equation (24) is modified in a very similar way as the expression of $\phi_1$ in Eq. (D2). The inversion of the Legendre transformation allows one to recover the relevant quantities:

\[
    s = \phi_k, \quad n_\ell = \phi_k, \quad m_k = \phi_k.
\]

Replacing $P^{(k_1, \ldots, k_\ell)}_\lambda(\Delta S)$ and $P^{(k)}_\lambda(\Delta S)$ by their values, we obtain

\[
    \phi_1 = x_S - L_1 = \ln[v(A) + p(2^\gamma - 1)v(B)],
\]

with

\[
    A = e^{x_S} \sum_k \frac{\Delta c_k}{k} e^{\gamma x_S^S} \left[ 2^{-x_S} + (1 - 2^{-x_S})(1 - \nu)^k \right],
\]

\[
    B = 2^{-x_S} e^{x_S} \sum_k \frac{\Delta c_k}{k} e^{\gamma x_S^S} \left[ 1 - (1 - \nu)^{x_S^S} \right],
\]

\[
    z_k = - \frac{1}{k} \ln \left[ 2^{-x_S} + (1 - 2^{-x_S})(1 - \nu)^k \right] - \frac{\nu_k}{k},
\]

\[
    \nu = \frac{p2^\gamma v(B)}{v(A) + p(2^{\gamma - 1})v(B)}.
\]

To evaluate $L_1$ as a function of $s$, we simply need to tune the parameters $\lambda_1$ and $m_k$ such that the conditions $n_\ell = v_{\ell}^{(k)}$ and $m_k = \Delta c_k$ are satisfied.

In Fig. 13, we represent the error exponent for the irregular ensemble with $v(x) = (1/2)x^2 + (1/2)x^3$ and $c(x) = (1/2)x^6 + (1/2)x^8$.

**APPENDIX E: CALCULATIONS IN THE BSC**

**Belief propagation and the Bethe approximation**

In this section we write down the BP equations for a given code over the BSC or, equivalently, the cavity equations at the RS level. The expression of the free energy is also given.

The cavity equations read

\[
    p_{\tau}^{(i-a)} \propto \prod_{b \in a} q_{\tau}^{(b-i)} e^{-\beta h_{\tau}},
\]

\[
    q_{\tau}^{(b-i)} = \sum_{\tau_b = 1} \prod_{j \in b-i} p_{\tau}^{(j-b)} \delta[\tau_b = 1].
\]

$p_{\tau}^{(i-a)}$ is the probability that the variable $i$ takes the value $\tau_i$ in the absence of $a$, and $q_{\tau}^{(b-i)}$ is proportional to the probability that the variable $i$ takes the value $\tau_i$ when connected to $b$ only.

Denoting $\tilde{p}_{\tau}^{(i-a)} = e^{\beta h_{\tau}/\sinh \beta h_{\tau}}$ and $\tilde{q}_{\tau}^{(b-i)} = e^{\beta h_{\tau}/\sinh \beta h_{\tau}}$, the cavity equations simplify to

\[
    h_{i-a} = \tilde{h}(h_{i-a+b-i}) = h_{i-b} + \sum_{b \in a} u_{b-i},
\]

\[
    u_{b-i} = u(h_{i-b}) = \frac{1}{\beta} \arctanh \left( \prod_{j \in b-i} \tanh \beta h_{j-\tau} \right).
\]

The local magnetization is given by $\langle \sigma \rangle = \beta H$, with $H_i = h_i + \sum_{a \in \mu_{i-a-i}} u_{a-i}$.

The Bethe approximation to the free energy reads

\[
    F_{RS}(\beta) = \sum_i \Delta F_i - \sum_k (k - 1) \Delta F_a,
\]

with

\[
    \Delta F_i = \Delta F_{\tau \rightarrow i}(u_{a-i}) = \frac{1}{\beta} \sum_{a \in i} \ln[2 \cosh(\beta u_{a-i})]
\]

\[
    - \frac{1}{\beta} \ln \left[ 2 \cosh \left( \beta h_{i} + \beta \sum_{a \in i} u_{a-i} \right) \right],
\]

\[
    \Delta F_a = \Delta F_{\tau \rightarrow a}(u_{a-i}) = \frac{1}{\beta} \sum_{a \in i} \ln[2 \cosh(\beta u_{a-i})]
\]

\[
    - \frac{1}{\beta} \ln \left[ 2 \cosh \left( \beta h_{i} + \beta \sum_{a \in i} u_{a-i} \right) \right].
\]
\[ \Delta F_a = \Delta F_{\square}(\{h_{i-a}\}) = -\frac{1}{\beta} \ln \left( 1 + \prod_{i \neq a} \tanh \beta h_{i-a} \right). \] (E4)

Define
\[ P(h) = \frac{1}{N(\ell)} e^{-\phi(h)}, \]
\[ Q(u) = \frac{1}{N(\ell)} e^{-\phi(u)}, \]

Averaging (E1) over the codes, the noise, and the edges, we obtain the self-consistency equations
\[ P(h) = \sum_{\ell} \frac{\ell \nu}{\langle \ell \rangle} \int_{\ell} \prod_{a=1}^{\ell-1} du_a Q(u_a) (\delta[h - \hat{h}(h, \{u_a\})]_{h_{i-a}}). \] (E6)

\[ P(h) \approx \int_{\ell} \prod_{a=1}^{\ell-1} du_a Q(u_a) \left( \frac{\delta[h - \sum_{a=1}^{\ell-1} u_a e^{\beta \phi(h)} (2 \cosh [\beta \phi(h) + \sum_{a=1}^{\ell-1} u_a])]}{\prod_{a=1}^{\ell-1} (2 \cosh [\beta u_a])^c} \right), \]
\[ Q(u) = \int_{\ell} \prod_{a=1}^{\ell-1} du_a Q(u_a) \delta[u - \frac{1}{\beta} \arctanh \left( \prod_{i=1}^{k-1} \tanh (\beta \phi(h_i)) \right)], \] (E9)

and the potential
\[ \phi(\beta, \beta_c, x_f, x_n) = \ln \int_{\ell} \prod_{a=1}^{\ell} du_a Q(u_a) \left( \frac{e^{\beta \phi(h)} (2 \cosh [\beta \phi(h) + \sum_{a=1}^{\ell} u_a])^c}{\prod_{a=1}^{\ell} (2 \cosh [\beta u_a])^c} \right)_{h_{i-a}} \]
\[ -\frac{\ell}{k} (k-1) \ln \int_{\ell} \prod_{a=1}^{\ell} du_a Q(u_a) \left[ 1 + \prod_{i=1}^{\ell} \tanh (\beta h_i) \right] \] (E10).

The solution to (E9) is obtained numerically. In the limit \( k, \ell \to \infty \), this solution simplifies:
\[ Q(u) = \delta(u), \]
\[ P(h) = (1-p) \delta[h - h_0] + p \delta[h + h_0], \] (E11)

yielding the error exponent (83).

Another solution, called "type I" in [10], also exists:
\[ Q(u) = \eta \delta_{x_f}(u) + (1-\eta) \delta_{x_n}(u), \]
\[ P(h) = \nu \delta_{x_f}(h) + (1-\nu) \delta_{x_n}(h), \] (E12)

with
\[ \nu = \frac{\eta^{\ell-1} + (1-\eta)^{\ell-1} e^{-2\eta h_0}}{\eta^{\ell-1} + (1-\eta)^{\ell-1} e^{-2\eta h_0}}, \]
\[ \eta = \frac{\nu^2}{1 + (2\nu - 1)^{\ell-1}}. \]

We automatically have \( s_p = 0 \), and the condition \( f_p = f_f \) implies \( m = \beta_c x_c = 1/2 \). Then the rate function reads
\[ L_1(f_p = f_f) = -\phi = -\ln \left[ \eta^f + (1-\eta)^f e^{-h_0 r_0} \right] \]
\[ -\frac{\ell}{k} (k-1) \ln \left[ \frac{1}{2} \left( 1 + (2\nu - 1)^2 \right) \right]. \] (E14)

This solution (E12) is numerically unstable, and the rate function thus obtained is clearly unphysical. However, for \( k, \ell \to \infty \), \( \ell/k = 1-R \), we have \( \eta = \nu = 1/2 \) and the resulting rate function
\[ L_1(f_p = f_f) = -\ln \left[ \frac{1}{2} \left( 1 + 2\sqrt{p(1-p)} \right) \right] \]
\[ -R \ln 2 = \ln 2[R_0(p) - R]. \] (E15)
Two-step large deviations

The potential $\psi(\beta_e, m, y)$ defined in Eq. (87) is obtained by extremizing the following expression with respect to $P(h)$ and $Q(u)$:

$$
\psi(\beta_e, m, y) = \ln \int \prod_{a=1}^{\ell} du_a Q(u_a) \left\{ \frac{e^{-mL \left[ \frac{1}{k}(k-1)\ln \int \prod_{i=1}^{k} dh_i P(h_i) \right.}}{\Pi_{a=1}^{\ell} \left[ 2 \cosh(\beta_a u_a) \right]^{m/\beta_a}} \right\}^y y
- \frac{\ell}{k} (k-1) \ln \int \prod_{i=1}^{k} dh_i P(h_i)
\times \left[ 1 + \prod_{i=1}^{k} \tanh(\beta_i h_i) \right]^{ym/\beta_e}.
$$

(E16)

We can only handle this calculation in the $k, \ell \to \infty$ limit. Equations (E11) are still a solution in this case and yield

$$
\psi(\beta_e, m, y) = y \hat{\phi}(\beta_e, m),
$$

(E17)

where $\hat{\phi}(\beta_e, m)$ is obtained from the average case. Therefore, the typical exponent is the same as the average error exponent in the high-$p$ regime.

There also exists a counterpart of solution (E12), which gives

$$
\psi(\beta_e, m, y) = (R-1) \ln 2 + \ln \left[ 1 + \left[ (1-p)^{1-m} p^m + p^{1-m}(1-p)^m \right]^y \right].
$$

(E18)

The condition $\partial_m \psi = 0$ is again enforced by setting $m = 1/2$. Thus we get

$$
\psi(y) = -yL - \mathcal{L} = (R-1) \ln 2 + \ln \left[ 2 \sqrt{p(1-p)} \right]^y.
$$

(E19)

This expression yields the rate function $\mathcal{L}(L)$ by inverse Legendre transformation.

---

[31] Contrary to what indicates the last equations of [15], the nature of the order parameter is unchanged when additional levels of disorder are taken into account. The reason is that the cavity method encodes in a unique spatial distribution both the statistics over the nodes of a single graph and the statistics over the graphs in a ensemble. The discrimination between the two levels is done only through the unequal weighting attributed to the different nodes, as controlled by the two independent temperatures $x$ and $y$.
[38] J. van Mourik and Y. Kabashima, e-print cond-mat/0310177.


In our case \( v^{(k)}_\ell = \sum_{\ell' \geq \ell} v^{(\ell')} \left( \frac{\ell'}{\ell} \right) c_k^\ell (1-c_k)^{\ell-\ell}. \)