Finite-connectivity systems as error-correcting codes

Renato Vicente and David Saad

The Neural Computing Research Group, Aston University, Birmingham B4 7ET, UK

Yoshiyuki Kabashima

Department of Computational Intelligence and Systems Science, Tokyo Institute of Technology, Yokohama 226, Japan

Abstract

We investigate the performance of parity check codes using the mapping onto Ising spin systems proposed by Sourlas. We study codes where each parity check comprises products of K bits selected from the original digital message with exactly C checks per message bit. We show, using the replica method, that these codes saturate Shannon's coding bound for $K \to \infty$ when the code rate K/C is finite. We then examine the finite temperature case to asses the use of simulated annealing methods for decoding, study the performance of the finite K case and extend the analysis to accommodate different types of noisy channels. The connection between statistical physics and belief propagation decoders is discussed and the dynamics of the decoding itself is analyzed. Further insight into new approaches for improving the code performance is given.

Typeset using REVTEX

I. INTRODUCTION

Error-correction is required whenever information has to be reliably transmitted through a noisy environment. The theoretical grounds for classical error-correcting codes were first presented in 1948 by Shannon [1]. He showed that it is possible to transmit information trough a noisy channel with a vanishing error probability by encoding up to a given critical rate R_c equivalent to the *channel capacity*. However, Shannon's arguments were non-constructive and devising such codes turned out to be a major practical problem in the area of information transmission.

In 1989 Sourlas [2,3] proposed that, due to the equivalence between addition over the field $\{0,1\}$ and multiplication over $\{\pm 1\}$, many error-correcting codes can be mapped onto many-body spin-glasses with appropriately defined couplings. This observation opened the possibility of applying techniques from statistical physics to study coding systems, in particular, these ideas were applied to the study of parity check codes. These linear block codes can be represented by matrices of N columns and M rows that transform N-bit messages to M $(> N)$ parity checks. Each row represents bits involved in a particular check and each column represents checks involving the particular bit. The number of bits used in each check and the number of checks per bit depends on the code construction. We concentrate on the case where exactly C checks are performed for each bit and exactly K bits compose each check.

The *code rate* R is defined as the information conveyed per channel use $R = H_2(f_s)N/M = H_2(f_s)K/C$, where $H_2(f_s) = -(1-f_s)\log_2(1-f_s) - f_s \log_2(f_s)$ is the binary entropy of the message with bias f_s.

In the mapping proposed by Sourlas a message is represented by a binary vector $\boldsymbol{\xi} \in \{\pm 1\}^N$ encoded to a higher dimensional vector $\boldsymbol{J^0} \in \{\pm 1\}^M$ defined as $J^0_{\langle i_1, i_2 \ldots i_K \rangle} = \xi_{i_1}\xi_{i_2}\ldots\xi_{i_K}$, where M sets of K indices are randomly chosen. A corrupted version $\boldsymbol{J}$ of the encoded message $\boldsymbol{J^0}$ has to be decoded for retrieving the original message. The decoding process can be viewed as a statistical Bayesian process [4] (see Fig.1). Decoding focuses

on producing an estimate $\widehat{\boldsymbol{\xi}}$ to the original message that minimizes a given expected loss $\langle\langle \mathcal{L}(\xi,\widehat{\xi})\rangle_{p(J|\xi)}\rangle_{p(\xi)}$ averaged over the indicated probability distributions. The definition of the loss depends on the particular task; the simple Hamming distance $\mathcal{L}(\xi,\widehat{\xi}) = \sum_j \xi_j \widehat{\xi}_j$ can be used for decoding binary messages. An optimal estimator for this particular loss function is $\widehat{\xi}_j = \mathrm{sign}\langle S_j\rangle_{p(S|J)}$ [4], where $\boldsymbol{S}$ is a N dimensional binary vector representing outcomes of the decoding process. Using Bayes' theorem, the posterior probability can be written as $\ln p(\boldsymbol{S} \mid \boldsymbol{J}) = \ln p(\boldsymbol{J} \mid \boldsymbol{S}) + \ln p(\boldsymbol{S}) + \text{const}$. Sourlas has shown [3] that for parity check codes this posterior can be written as a many-body Hamiltonian:

$$\begin{aligned} \ln p(\boldsymbol{S} \mid \boldsymbol{J}) &= -\beta\, \mathcal{H}(\boldsymbol{S}) \\ &= \beta \sum_{\mu} \mathcal{A}_\mu\, J_\mu \prod_{i\in\mu} S_i + \beta \mathcal{H}_{\text{prior}}(\boldsymbol{S}), \end{aligned} \tag{1.1}$$

where $\mu = \langle i_1, \ldots i_K\rangle$ is a set of indices and $\mathcal{A}$ is a tensor with the properties $\mathcal{A}_\mu \in \{0,1\}$ and $\sum_{\mu\setminus i} \mathcal{A}_\mu = C\ \forall i$, which determines the M components of the codeword $\boldsymbol{J}^0$. The second term $\mathcal{H}_{\text{prior}}(\boldsymbol{S})$ stands for the prior knowledge on the actual messages; it can be chosen as $\mathcal{H}_{\text{prior}}(\boldsymbol{S}) = F\sum_{j=1}^{N} S_j$ to represent the expected bias in the message bits. For the simple case of a memoryless binary symmetric channel (BSC), $\boldsymbol{J}$ is a corrupted version of the transmitted message $\boldsymbol{J}^0$ where each bit is independently flipped with probability p during transmission. The hyper-parameter β, that reaches an optimal value at Nishimori's temperature [4–6], is related to the channel corruption rate. The decoding procedure translates to finding the thermodynamical spin averages for the system defined by the Hamiltonian (1.1) at a certain temperature (Nishimori's temperature for optimal decoding); as the original message is binary, the retrieved message bits are given by the signs of the corresponding averages.

In the statistical physics framework the performance of the error-correcting process can be measured by the overlap between actual message and estimate for a given scenario characterized by a code rate, corruption process and information content of the message. To asses the typical properties we average this overlap over all possible codes $\mathcal{A}$ and noise realizations (possible corrupted vectors $\boldsymbol{J}$) given the message $\boldsymbol{\xi}$ and then over all possible messages:

$$m = \frac{1}{N} \left\langle \sum_{i=1}^{N} \xi_i \ \langle \mathrm{sign} \langle S_i \rangle \rangle_{\mathcal{A},J|\xi} \right\rangle_{\xi} \tag{1.2}$$

Here $\mathrm{sign}\langle S_i \rangle$ is the sign of the spins thermal average corresponding to the Bayesian optimal decoding. The average error per bit is then given by $p_e = (1-m)/2$. Although this performance measure is not the usual physical magnetization (it can be better described as a measure of misalignment of the decoded message), for brevity, we will refer to it as *magnetization*.

From the statistical physics point of view, the number of checks per bit is analogous to the spin system connectivity and the number of bits in each check is analogous to the number of spins per interaction. Sourlas' code has been studied in the case of extensive connectivity , where the number of bonds $C \sim \begin{pmatrix} N-1 \\ K-1 \end{pmatrix}$ scales with the system size. In this case it can be mapped onto known problems in statistical physics such as the SK [7] (K=2) and Random Energy (REM) [8] ($K \to \infty$) models. It has been shown that the REM saturates Shannon's bound [2]. However, it has a rather limited practical relevance as the choice of extensive connectivity corresponds to a vanishingly small code rate.

Here we present an analysis of Sourlas' code for the case of finite connectivity where the code rate is non-vanishing, detailing and extending our previous brief reports [9,10]. We show that Shannon's bound can also be attained at finite code rates. We study the decoding dynamics and discuss the connections between statistical physics and belief propagation methods.

This paper is organized as follows: in Section II we introduce a naive mean-field model that contains all the necessary ingredients to understand the system qualitatively. Section III describes the statistical physics treatment of Sourlas' code showing that Shannon's bound can be attained for finite code rates if $K \to \infty$. The finite K case and the Gaussian noise are also discussed in Section III. The decoding dynamics is analyzed in Section IV. Concluding remarks are given in Section V. Appendices with detailed calculations are also provided.

II. NAIVE MEAN FIELD THEORY

A. Equilibrium

To gain some insight into the code behavior one can start by considering that the original message is $\xi_j = 1$ for all j (so $m = 1$ will correspond to perfect decoding) and use Weiss' mean-field theory as a first (naive) approximation. The idea is to consider an effective field given by (for unbiased messages with $F = 0$):

$$h_j^{\text{eff}} = \sum_{\{\mu: j\in\mu\}} J_\mu \prod_{i\in\mu\setminus j} S_i \tag{2.1}$$

acting in every site. The first strong approximation here consists in disregarding the reaction fields that describe the influence of site j back over the system. The local magnetization can then be calculated:

$$m_j = \left\langle \tanh\left(\beta h_j^{\text{eff}}\right)\right\rangle_{J,S} \simeq \tanh\beta \left\langle h_j^{\text{eff}}\right\rangle_{J,S}, \tag{2.2}$$

where we introduced a further approximation taking averages inside the function that can be seen as a high temperature approximation. Disregarding correlations among spins and computing the proper averages one can write:

$$m = \tanh\left(\beta\, C(1-2p)\, m^{K-1}\right), \tag{2.3}$$

where p is the noise level in the channel. An alternative way to derive the above equation is by considering the free-energy:

$$f(m) = -(1-2p)\frac{C}{K}m^K - \frac{s(m)}{\beta}. \tag{2.4}$$

The entropic term $s(m)$ is:

$$s(m) = -\frac{1+m}{2}\ln\left(\frac{1+m}{2}\right) - \frac{1-m}{2}\ln\left(\frac{1-m}{2}\right). \tag{2.5}$$

Minimizing this free-energy one can obtain Eq.(2.3) whose solutions give the possible phases after the decoding process. In Fig. 2 we show the maximum magnetization solutions m for

Eq.(2.3) as a function of the flip rate p at code rate $R = 1/2$ and $K = 2, 3, 4$. For $K = 2$ the performance degrades faster with the noise level than in the $K > 2$ case. The dashed line indicates coexistence between paramagnetic (PARA) $m = 0$ and ferromagnetic (FERRO) $m > 0$ phases.

B. Decoding Dynamics

In a naive mean-field framework the decoding process can be seen as an iterative solution for (2.3) starting from a magnetization value that depends on the prior knowledge about the original message. The fixed points of this dynamics correspond to the minima of the free-energy; a specific minimum is reached depending on the initial condition. In the insets of Fig.2 we show, as a measure for the basin of attraction, the maximal deviation between the initial condition and the original message $\lambda = 1 - m_0$ that allows convergence to a FERRO solution. At the bottom inset we show the deviation λ at code rate $R = 1/2$, increasing values of K and noise level $p = 0.1$. An increasing initial magnetization is needed when K increases, decoding without prior knowledge is only possible for $K = 2$. The top inset shows λ for $K = 3$, $p = 0.1$; as C increases (code rate decreases), the basin of attraction increases.

One can understand intuitively how the basin of attraction depends on the connectivities by representing the code in a graph with bit and check nodes and looking at the mean-field behavior of a single bit node (see Fig.3). The corrupted checks contribute wrong (-1 for the "all ones" message case) values to the bit nodes ($m < 1$ in the mean field). Since check node values correspond to a product of $K - 1$ bit values, the probability of updating these nodes to the wrong values increases with K, degrading the overall performance. On the other hand, if C increases for a fixed K the bit nodes gather more information and are less sensitive to the presence of (a limited amount of) wrong bits .

Although this naive picture indicates some of the qualitative features of real codes, one certainly cannot rely in its numerical predictions. In the following sections we will study Sourlas' codes using more sophisticated techniques that will substantially refine the analysis.

III. EQUILIBRIUM

A. Replica Theory

In the following subsections we will develop the replica symmetric theory for Sourlas' codes and show that, in addition to providing a good description of the equilibrium, it describes the typical decoding dynamics using belief propagation methods.

The previous naive "all ones" messages assumption can be formally translated to the gauge transformation [11] $S_i \mapsto S_i \xi_i$ and $J_\mu \mapsto J_\mu \prod_{i\in\mu} \xi_i$ that maps any general message to the FERRO configuration defined as $\xi_i^* = 1 \ \forall i$. One can then rewrite the Hamiltonian in the form:

$$\mathcal{H}(\boldsymbol{S}) = -\sum_{\mu} \mathcal{A}_\mu \ J_\mu \ \prod_{i\in\mu} S_i - F \sum_k \xi_k S_k \ , \tag{3.1}$$

With this transformation, the bits of the uncorrupted encoded message are $J_i^0 = 1 \ \forall i$ and, for a BSC, the corrupted bits are random variables with probability:

$$\mathcal{P}\left(J_\mu\right) = (1-p)\ \delta\left(J_\mu - 1\right) + p\ \delta\left(J_\mu + 1\right), \tag{3.2}$$

where p is the channel flip rate. For deriving typical properties of these codes one has obtain an expression for the free-energy by invoking the replica approach where the free-energy is defined as:

$$f = -\frac{1}{\beta} \lim_{N\to\infty} \frac{1}{N} \left.\frac{\partial}{\partial n}\right|_{n=0} \langle \mathcal{Z}^n \rangle_{\mathcal{A},\xi,J}, \tag{3.3}$$

where $\langle \mathcal{Z}^n \rangle_{\mathcal{A},\xi,J}$ represents an analytical continuation in the interval $n \in [0,1]$ of the replicated partition function defined as:

$$\langle \mathcal{Z}^n \rangle_{\mathcal{A},\xi,J} = \mathrm{Tr}_{\{S_j^\alpha\}} \left[\left\langle e^{\beta F \sum_{\alpha,k} \xi_k S_k^\alpha} \right\rangle_\xi \left\langle \exp\left(\beta \sum_{\alpha,\mu} \mathcal{A}_\mu \ J_\mu \ \prod_{i\in\mu} S_i^\alpha \right) \right\rangle_{\mathcal{A},J} \right]. \tag{3.4}$$

The magnetization can be rewritten in the gauged variables as :

$$m = \left\langle \langle \mathrm{sign}\langle S_i \rangle \rangle_{\mathcal{A},J|\xi^*} \right\rangle_\xi, \tag{3.5}$$

where ξ^* denotes the transformation of a message ξ into the FERRO configuration. The usual magnetization per site can be easily obtained by calculating

$$\langle\langle S_i\rangle\rangle_{\mathcal{A},J,\xi} = -\left(\frac{\partial f}{\partial(\xi F)}\right). \tag{3.6}$$

From this derivative one can find the distribution of the effective local fields h_j that can be used to asses the magnetization m, since $\text{sign}\left(\langle S_j\rangle\right) = \text{sign}(h_j)$.

To compute the replicated partition function we closely follow Ref. [12]. We average uniformly over all codes $\mathcal{A}$ such that $\sum_{\mu\setminus i}\mathcal{A}_\mu = C\ \forall i$ to find:

$$\begin{aligned}\langle\mathcal{Z}^n\rangle_{\mathcal{A},\xi,J} = \exp\Bigg\{ N\ Extr_{q,\widehat{q}}\Bigg[& C - \frac{C}{K} + \frac{C}{K}\left(\sum_{l=0}^{n}\mathcal{T}_l \sum_{\langle\alpha_1\ldots\alpha_l\rangle} q^K_{\alpha_1\ldots\alpha_l}\right) \\ & -\ C\left(\sum_{l=0}^{n}\sum_{\langle\alpha_1\ldots\alpha_l\rangle} q_{\alpha_1\ldots\alpha_l}\widehat{q}_{\alpha_1\ldots\alpha_l}\right) \\ & +\ \ln \text{Tr}_{\{S^\alpha\}}\left\langle e^{\beta F\xi\sum_\alpha S^\alpha}\right\rangle_\xi \left(\sum_{l=0}^{n}\sum_{\langle\alpha_1\ldots\alpha_l\rangle}\widehat{q}_{\alpha_1\ldots\alpha_l}S^{\alpha_1}\ldots S^{\alpha_l}\right)^C\Bigg]\Bigg\},\end{aligned} \tag{3.7}$$

where $\mathcal{T}_l = \langle\tanh^l(\beta J)\rangle_J$, as in [13], and $q_0 = 1$. We give details of this calculation in the Appendix A. At the extremum the order parameters acquire expressions similar to those of Ref. [12]:

$$\begin{aligned}\widehat{q}_{\alpha_1,\ldots,\alpha_l} &= \mathcal{T}_l\ q^{K-1}_{\alpha_1,\ldots,\alpha_l} \\ q_{\alpha_1,\ldots,\alpha_l} &= \left\langle\left(\prod_{i=1}^{l}S^{\alpha_i}\right)\left(\sum_{l=0}^{n}\sum_{\langle\alpha_1\ldots\alpha_l\rangle}\widehat{q}_{\alpha_1\ldots\alpha_l}S^{\alpha_1}\ldots S^{\alpha_l}\right)^{-1}\right\rangle_{\mathcal{X}}.\end{aligned} \tag{3.8}$$

where

$$\mathcal{X} = \left\langle e^{\beta F\xi\sum_\alpha S^\alpha}\right\rangle_\xi \left(\sum_{l=0}^{n}\sum_{\langle\alpha_1\ldots\alpha_l\rangle}\widehat{q}_{\alpha_1\ldots\alpha_l}S^{\alpha_1}\ldots S^{\alpha_l}\right)^C, \tag{3.9}$$

and $\langle\ldots\rangle_{\mathcal{X}} = \text{Tr}_{\{S^\alpha\}}\left[(\ldots)\mathcal{X}\right]/\text{Tr}_{\{S^\alpha\}}\left[(\ldots)\right]$. The term $\widehat{p}(\underline{S}) = \sum_{l=0}^{n}\sum_{\langle\alpha_1\ldots\alpha_l\rangle}\widehat{q}_{\alpha_1\ldots\alpha_l}S^{\alpha_1}\ldots S^{\alpha_l}$ represents a probability distribution over the space of replicas and $p_0(\underline{S}) = \left\langle e^{\beta F\xi\sum_\alpha S^\alpha}\right\rangle_\xi$ is a prior distribution over the same space. For reasons that will become clear in Section IV, $q_{\alpha_1,\ldots,\alpha_l}$ represents one l-th momentum of the equilibrium distribution of a bit-check edge in a belief network during the decoding process and $\widehat{q}_{\alpha_1\ldots\alpha_l}$ represents l-th moments of a

check-bit edge equilibrium distribution . The distribution $\mathcal{X}$ represents the probability of a certain site (bit node) configuration subjected to exactly C interactions and with prior probability given by p_0.

B. Replica Symmetric Solution

The replica symmetric (RS) ansatz can be introduced via the auxiliary fields $\pi(x)$ and $\widehat{\pi}(y)$ in the following way (see also [12]):

$$\begin{aligned} \widehat{q}_{\alpha_1 \ldots \alpha_l} &= \int dy\ \widehat{\pi}(y) \tanh^l(\beta y), \\ q_{\alpha_1 \ldots \alpha_l} &= \int dx\ \pi(x) \tanh^l(\beta x) \end{aligned} \tag{3.10}$$

for $l = 1, 2, \ldots$.

Plugging it into the replicated partition function (3.7), performing the limit $n \to 0$ and using Eq.(3.3) (see Appendix B for details) one obtains:

$$\begin{aligned} f = -\frac{1}{\beta}\, Extr_{\pi,\widehat{\pi}} \{ & \alpha \ln \cosh \beta \\ & + \alpha \int \left[\prod_{l=1}^{K} dx_l\ \pi(x_l) \right] \left\langle \ln \left[1 + \tanh \beta J\ \prod_{j=1}^{K} \tanh \beta x_j \right] \right\rangle_J \\ & - C \int dx\ dy\ \pi(x)\ \widehat{\pi}(y)\ \ln \left[1 + \tanh \beta x\ \tanh \beta y \right] \\ & - C \int dy\ \widehat{\pi}(y)\ \ln \cosh \beta y \\ & + \int \left[\prod_{l=1}^{C} dy_l\ \widehat{\pi}(y_l) \right] \left\langle \ln \left[2 \cosh \beta \left(\sum_{j=1}^{C} y_j + F\xi \right) \right] \right\rangle_\xi \Bigg\}, \end{aligned} \tag{3.11}$$

where $\alpha = C/K$. The saddle-point equations, obtained by varying Eq.(3.11) with respect to the probability distributions, provide a set of relations between $\pi(x)$ and $\widehat{\pi}(y)$

$$\begin{aligned} \pi(x) &= \int \left[\prod_{l=1}^{C-1} dy_l\ \widehat{\pi}(y_l) \right]\ \left\langle \delta \left[x - \sum_{j=1}^{C-1} y_j - F\xi \right] \right\rangle_\xi \\ \widehat{\pi}(y) &= \int \left[\prod_{l=1}^{K-1} dx_l\ \pi(x_l) \right]\ \left\langle \delta \left[y - \frac{1}{\beta} \tanh^{-1} \left(\tanh \beta J\ \prod_{j=1}^{K-1} \tanh \beta x_j \right) \right] \right\rangle_J . \end{aligned} \tag{3.12}$$

Later we will show that this self-consistent pair of equations can be seen as a mean-field version for the belief propagation decoding.

Using Eq.(3.6) one finds that the local field distribution is :

$$P(h) = \int \left[\prod_{l=1}^{C} dy_l \; \widehat{\pi}(y_l)\right] \; \left\langle \delta \left[h - \sum_{j=1}^{C} y_j - F\xi \right] \right\rangle_{\xi} , \tag{3.13}$$

where $\widehat{\pi}(y)$ is given by the saddle point equations above.

The magnetization (1.2) can then be calculated using:

$$m = \int dh \, \mathrm{sign}(h) \, P(h). \tag{3.14}$$

The code performance can be assessed by assuming a particular prior distribution for the message bits, solving the saddle-point equations (3.12) numerically and then computing the magnetization.

Instabilities in the solution within the space of symmetric replicas can be probed looking at second derivatives of the functional whose extremum defines the free-energy (3.11). The simplest necessary condition for stability is having non-negative second functional derivatives in relation to $\pi(x)$ (and $\widehat{\pi}(y)$) :

$$\frac{1}{\beta} \int \left[\prod_{l=1}^{K-2} dx_l \; \pi(x_l)\right] \left\langle \ln \left[1 + \tanh \beta J \; \tanh^2 \beta x \prod_{j=1}^{K-2} \tanh \beta x_j \right] \right\rangle_{J} \geq 0, \tag{3.15}$$

for all x. The replica symmetric solution is expected to be unstable for sufficiently low temperatures (large β). For high temperatures we can expand the above expression around small β to find the stability condition:

$$\langle J \rangle_J \langle x \rangle_{\pi}^{K-2} \geq 0 \tag{3.16}$$

We expect the average $\langle x \rangle_{\pi} = \int dx \, \pi(x) \, x$ to be zero in PARA phase and positive in FERRO phase, satisfying the stability condition. This result is still generally inconclusive, but provides some evidence that can be examined numerically. In Section III D we will test the stability of our solutions using condition (3.15).

In the next sections we restrict our study to the unbiased case ($F = 0$), which is of practical relevance, since it is always possible to compress a biased message to an unbiased one.

C. Case $K \to \infty$, $C = \alpha K$

For this case one can obtain solutions to the saddle-point equations for arbitrary temperatures. In the first saddle-point equation (3.12) one can write:

$$x = \sum_{l=1}^{C-1} y_l \approx (C-1)\langle y \rangle_{\widehat{\pi}} = (C-1) \int dy \; y \; \widehat{\pi}(y). \tag{3.17}$$

It means that if $\langle y \rangle_{\widehat{\pi}} = 0$ (as it is the in PARA and spin glass (SG) phases) then $\pi(x)$ must be concentrated at $x = 0$ implying that $\pi(x) = \delta(x)$ and $\widehat{\pi}(y) = \delta(y)$ are the only possible solutions. Moreover, Eq.(3.17) implies that in FERRO phase one can expect $x \approx \mathcal{O}(K)$.

Using Eq.(3.17) and the second saddle-point equation (3.12) one can find a self-consistent equation for the mean-field $\langle y \rangle_{\widehat{\pi}}$:

$$\langle y \rangle_{\widehat{\pi}} = \left\langle \frac{1}{\beta} \tanh^{-1} \left[\tanh(\beta J) \left(\tanh(\beta(C-1)\langle y \rangle_{\widehat{\pi}}) \right)^{K-1} \right] \right\rangle_J . \tag{3.18}$$

For a BSC the above average is over distribution (3.2). Computing the average, using $C = \alpha K$ and rescaling the temperature as $\beta = \tilde{\beta}(\ln K)/K$, in the limit $K \to \infty$ one obtains:

$$\langle y \rangle_{\widehat{\pi}} = (1-2p) \left[\tanh(\tilde{\beta}\alpha \langle y \rangle_{\widehat{\pi}} \ln(K)) \right]^K , \tag{3.19}$$

where p is the channel flip probability. The mean-field $\langle y \rangle_{\widehat{\pi}} = 0$ is always a solution to this equation (either PARA or SG); at $\beta_c = \ln(K)/(2\alpha K(1-2p))$ an extra non-trivial FERRO solution emerges with $\langle y \rangle_{\widehat{\pi}} = 1 - 2p$. As the connection with the magnetization m is given by Eq. (3.13) and Eq. (3.14); it is not difficult to see that it implies $m = 1$ for FERRO solution. One remarkable point is that the temperature were the FERRO solution emerges is $\beta_c \sim \mathcal{O}(\ln(K)/K)$; it means that in a simulated annealing process PARA-FERRO barriers emerge quite early for large K values implying metastability and, consequently, a very slow convergence. It seems to advocate the use of small K values in practical applications. This case is analyzed in Section III E. For $\beta > \beta_c$ both PARA and FERRO solutions exist.

The FERRO free-energy can be obtained from Eq.(3.11) using Eq.(3.17), being $f_{\text{FERRO}} = -\alpha(1-2p)$. The corresponding entropy is $s_{\text{FERRO}} = 0$ indicating a single solution. The PARA free-energy is obtained by plugging $\pi(x) = \delta(x)$ and $\widehat{\pi}(y) = \delta(y)$ into Eq. (3.11):

$$f_{\text{PARA}} = -\frac{1}{\beta}(\alpha \ \ln(\cosh \ \beta) + \ln \ 2), \tag{3.20}$$

$$s_{\text{PARA}} = \alpha(\ln(\cosh \ \beta) - \beta \ \tanh \ \beta) + \ln \ 2. \tag{3.21}$$

PARA solutions are unphysical for $\alpha > (\ln \ 2)/(\beta \ \tanh \ \beta - \ln \ \text{ch} \ \beta)$, since the corresponding entropy is negative. To complete the phase diagram picture we have to assess the spin-glass free-energy and entropy. We have seen in the beginning of this section that replica symmetric SG and PARA solutions consist of the same field distributions for $K \to \infty$, implying unphysical behavior. In order to produce a solution with non-negative entropy one has to break the replica symmetry. We use here a pragmatic way to build this solution, using the simplest one-step replica symmetry breaking known as *frozen spins*.

It was observed in Ref. [14] that for the REM a one-step symmetry breaking scheme gives the exact solution. In this scheme the n replicas' space is divided to groups of m identical solutions. It was shown that an abrupt transition in the order parameter from a unique solution (Edwards-Anderson parameter $q = 1$, SG phase) to a completely uncorrelated set of solutions ($q = 0$, PARA phase) occurs. This transition takes place at a critical temperature β_g that can be found by solving the appropriate saddle-point equations; this temperature is given by the root of the replica symmetric entropy ($s_{RS} = 0$) meaning that the RS-RSB transition occurs at the same point as the PARA-SG in this model. The symmetry breaking parameter was found to be $m_g = \beta_g/\beta$, indicating that this kind of solution is physical only for $\beta > \beta_g$, since $m_g \leq 1$ [15], indicating a PARA-SG phase transition. The free-energy can be computed by plugging the order parameters in the effective Hamiltonian, obtained after averaging over the disorder and taking the proper limits. It shows no dependence on the temperature, since for $\beta > \beta_g$ the system is completely frozen in a single configuration.

For the Sourlas' code, in the regime we are interested in, SG solutions to the saddle-point equations are given by $\pi(x) = \delta(x)$ and $\widehat{\pi}(y) = \delta(y)$. The RSB-SG free-energy that guaranties continuity in the SG-PARA transition is identical to f_{PARA}, since the SG and PARA solutions have exactly the same structure, to say:

$$f_{\text{RSB-SG}} = -\frac{1}{\beta_g}\,(\alpha\,\ln(\cosh\ \beta_g) + \ln\ 2), \tag{3.22}$$

where β_g is a solution for $s_{\text{RS-SG}} = \alpha\,(\ln(\cosh\ \beta) - \beta\tanh\ \beta) + \ln\ 2 = 0$.

In Fig.4 we show the phase diagram for a given code rate R in the temperature T versus noise level p plane.

D. Shannon's Limit

Shannon's analysis shows that up to a critical code rate R_c, which equals the channel capacity, it is possible to recover information with arbitrarily small error probability for a given noise level. For the BSC :

$$R_c = \frac{1}{\alpha_c} = 1 + p\,\log_2\,p + (1-p)\,\log_2\,(1-p). \tag{3.23}$$

Sourlas' code, in the case where $K \to \infty$ and $C \sim \mathcal{O}(N^K)$ can be mapped onto the REM and has been shown to be capable of saturating Shannon's bound in the limit $R \to 0$ [2]. In this section we extend the analysis to show that Shannon's bound can be attained by Sourlas' code at zero temperature also for $K \to \infty$ limit but with connectivity $C = \alpha K$. In this limit the model is analogous to the diluted REM analyzed by Saakian in [16]. The errorless phase is manifested in a FERRO phase with perfect alignment ($m = 1$) (condition that is only possible for infinite K) up to a certain critical noise level; a further noise level increase produces frustration leading to a SG phase where the misalignment is maximal ($m = 0$). The FERRO-SG transition is analogous to the transition from errorless decoding to decoding with errors described by Shannon. A PARA phase is also present when the transmitted information is insufficient to recover the original message ($R > 1$).

At zero temperature saddle-point equations (3.12) can be rewritten as:

$$\begin{aligned}
\pi(x) &= \int \left[\prod_{l=1}^{C-1} dy_l\ \widehat{\pi}(y_l)\right]\ \delta\left[x - \sum_{j=1}^{C-1} y_j\right] \\
\widehat{\pi}(y) &= \int \left[\prod_{l=1}^{K-1} dx_l\ \pi(x_l)\right]\ \left\langle \delta\left[y - \text{sign}(J\prod_{l=1}^{K-1} x_l)\min(\mid J \mid, ..., \mid x_{K-1} \mid)\right]\right\rangle_J\ ,
\end{aligned} \tag{3.24}$$

The solutions for these saddle-point equations may, in general, result in probability distributions with singular and regular parts. As a first approximation we choose the simplest self-consistent family of solutions which are, since $J = \pm 1$, given by:

$$\widehat{\pi}(y) = p_+ \delta(y-1) + p_0 \delta(y) + p_- \delta(y+1) \tag{3.25}$$

$$\pi(x) = \sum_{l=1-C}^{C-1} T_{[p_\pm, p_0; C-1]}(l)\, \delta(x-l), \tag{3.26}$$

with

$$T_{[p_+, p_0, p_-; C-1]}(l) = \sum_{\{k,h,m\}}{}' \frac{(C-1)!}{k!\; h!\; m!}\; p_+^k\; p_0^h\; p_-^m, \tag{3.27}$$

where the prime indicates that k, h, m are such that $k - h = l;\ k + h + m = C - 1$. Evidence for this simple ansatz comes from Monte-carlo integration of Equation (3.12) at very low temperatures, that shows solutions comprising three dominant peaks and a relatively weak regular part. Inside FERRO and PARA phases a more complex singular solution comprising five peaks $\widehat{\pi}(y) = p_{+2}\delta(y-1) + p_+\delta(y-0.5) + p_0\delta(y) + p_-\delta(y+0.5) + p_{-2}\delta(y+1)$ collapses back to the simpler three peak solution. In Fig.5 we show a typical result of a Monte-carlo integration for the field $\widehat{\pi}(y)$. The two peak that emerge by using either the three peak ansatz or the five peak ansatz are shown as dotted lines. In the inset we show the weak regular part of the Monte-carlo solution.

Plugging the above ansatz in the saddle-point equations one can write a closed set of equations in $p_\pm$ and p_0 that can be solved numerically (see appendix D for details).

The three peak solution can be of three types: FERRO ($p_+ > p_-$), PARA ($p_0 = 1$) or SG ($p_- = p_+$). Computing free-energies and entropies enables one to construct the phase diagram. At zero temperature the PARA free-energy is $f_{\rm PARA} = -\alpha$ and the entropy is $s_{\rm PARA} = (1-\alpha)\ln 2$, this phase is physical only for $\alpha < 1$, what is expected since it corresponds exactly to the regime where the transmitted information is not sufficient to recover the actual message ($R > 1$).

The FERRO free-energy does not depend on the temperature, having the form $f_{\rm FERRO} = -\alpha(1-2p)$ with entropy $s_{\rm FERRO} = 0$. One can find the FERRO-SG coexistence line that

corresponds to the maximum performance of a Sourlas' code by equating Eq.(3.22) and $f_{\rm FERRO}$. Observing that $\beta_g = \beta_N(p_c)$ (as seen in Fig.4) we found that this transition coincides with Shannon's bound Eq.(3.23). It is interesting to note that in the large K regime both RS-FERRO and RSB-SG free-energies (for $T < T_g$) do not depend on the temperature, it means that Shannon's bound is valid also for finite temperatures up to T_g. In Fig.6 we give the complete zero temperature phase diagram.

The stability of replica symmetric FERRO and PARA solutions used to obtain Shannon's bound can be checked using Eq.(3.15) at zero temperature:

$$\lim_{\beta\to\infty} \frac{1}{\beta} \int \left[\prod_{l=1}^{K-2} dx_l \ \pi(x_l)\right] \left\langle \ln \left[1 + \tanh\beta J \ \tanh^2\beta x \prod_{j=1}^{K-2} \tanh\beta x_j\right]\right\rangle_J \geq 0, \tag{3.28}$$

for all x.

For PARA solutions the above integral vanishes, trivially satisfying the condition, while for FERRO solution in the K large regime, $x_l \approx \mathcal{O}(K)$ and the integral becomes

$$-2p\left[(1-\Theta(x+1)) + |x|\left(\Theta(x+1) - \Theta(x-1)\right) + \Theta(x-1)\right], \tag{3.29}$$

where $\Theta(x) = 1$ for $x \geq 0$ and 0 otherwise, indicating instability for $p > 0$. For the noiseless case $p = 0$ the stability condition is satisfied. The instability of FERRO phase opens the possibility that Sourlas' code does not saturate Shannon's bound, since a correction to the FERRO solution could change FERRO-SG transition line. However, it was shown in Section III B that this instability vanishes for large temperatures, what supports, to some extent, the FERRO-SG line obtained and the saturation of Shannon's bound in some region, as long as the temperature is lower than Nishimori's temperature. For finite temperatures the stability condition for FERRO solution can be rewritten as:

$$\left(1 + \tanh(\beta)\tanh^2(\beta x)\right)^{(1-p)} \left(1 - \tanh(\beta)\tanh^2(\beta x)\right)^{p} \geq 1 \ \forall x. \tag{3.30}$$

For $p = 0$ the condition is clearly satisfied. For finite p a critical temperature above which the stability condition is fulfilled can be found numerically. In Fig.4 we show this critical temperature in the phase diagram; one can see that there is a considerable region in which our

result that Sourlas' code can saturate Shannon's bound is supported. Conclusive evidence to that will be given by simulations presented in Section IV.

E. Finite K Case

Although Shannon's bound only can be attained in the limit $K \to \infty$, it was shown in the Section III C that there are some possible drawbacks, mainly in the decoding of messages encoded by large K codes, due to large barriers which are expected to occur between PARA and FERRO states. In this section we consider the finite K case, for which we can solve the RS saddle-point equations (3.12) for arbitrary temperatures using Monte-carlo integration. We can also obtain solutions for the zero temperature case using the simple iterative method described in Section III D.

We expect the FERRO-SG transition for $K > 2$ to be properly described by the frozen spins RSB solution. It has been shown that $K > 2$ extensively connected models [14] exhibit Parisi-type order functions with similar discontinuous structure as found in the $K \to \infty$ case; it was also shown that the PARA-like solution, employed to describe PARA and SG phases, is locally stable within the complete replica space and zero field (unbiased messages case) at all temperatures.

At the top of Fig.7 we show the zero temperature magnetization m as a function of the noise level p at code rate $R = 1/2$. These curves were obtained by using the three peak ansatz of the Section III D. It can be seen that the transition is of second order for $K = 2$ and first order for $K > 3$ similarly to extensively connected models. The transition as described by the RS solution tends to $p = 0.5$ as K grows. Note that this does not correspond to perfect retrieval since the RSB spin glass phase dominates for $p > p_c$ (see bottom of Fig.7). In the bottom figure we plot RS free-energies and RSB frozen spins free-energy, from which we determine the critical probability p_c where the transition occurs (pointed by an arrow). After the transition, free-energies for $K = 3, 4, 5$ and 6 acquire values that are lower than the SG free-energy; nevertheless, the entropy is negative and these free-energies are therefore

unphysical. It is remarkable that this critical value does not change significantly for finite K in comparison to infinite K. Observe that Shannon's bound cannot be attained for finite K, since $m = 1$ exactly only if $K \to \infty$.

The $K = 2$ model with extensive connectivity (SK) is known to be somewhat special, a full Parisi solution is needed to recover the concavity of the free-energy and the Parisi order function has a continuous behavior [17]. No stable solution is known for the intensively connected model (Viana-Bray model). In order to check the theoretical result obtained one relies on simulations of the decoding process at low temperatures. In Section VIII we show that the simulations are in good agreement with the theoretical results.

F. Gaussian Noise

Using the replica symmetric free-energy (3.11) and the frozen spins RSB free-energy (3.22) one can easily extend the analysis to other noise types. The general PARA free-energy and entropy can be written:

$$\begin{aligned} f_{\text{PARA}} &= -\frac{1}{\beta}\ (\alpha\ \langle \ln (\text{ch}\ \beta J)\rangle_J + \ln\ 2) \\ s_{\text{PARA}} &= \alpha\ (\langle \ln (\text{ch}\ \beta J)\rangle_J - \beta \langle J\ \tanh (\beta J)\rangle_J) + \ln\ 2. \end{aligned} \tag{3.31}$$

The SG-RSB free-energy is given by :

$$f_{\text{SG-RSB}} = -\frac{1}{\beta_g}\ (\alpha\ \langle \ln\ (\text{ch}\ \beta_g J)\rangle_J + \ln\ 2)\,, \tag{3.32}$$

with β_g defined as the solution of

$$\alpha\ (\langle \ln\ (\text{ch}\ \beta_g J)\rangle_J - \beta_g \langle J\ \tanh\ (\beta_g J)\rangle_J) + \ln\ 2 = 0. \tag{3.33}$$

The FERRO free-energy is in general given by $f_{\text{FERRO}} = -\alpha\ \langle J\rangle_J = -\alpha\ \langle J\ \tanh\ (\beta_N J)\rangle_J$ (see Appendix D). The maximum performance of the code is defined by the critical line :

$$\alpha\,(\langle \ln(\text{ch}\ \beta_g J)\rangle_J - \beta_g \langle J\ \tanh(\beta_N J)\rangle_J) + \ln\ 2 = 0, \tag{3.34}$$

obtained by equating free-energies in PARA and FERRO phases. Comparing this expression with entropy (3.33) it can be seen that $\beta_g = \beta_N$ at the critical line; the same behavior observed in the BSC case. From Eq.(3.34) one can write:

$$R_c = \beta_N^2 \frac{\partial}{\partial \beta} \left[\frac{1}{\beta} \langle \log_2 \cosh(\beta J) \rangle_J \right]_{\beta=\beta_N}, \tag{3.35}$$

that can be used to compute the performance of the code for arbitrary symmetric noise.

Supposing that the encoded bits can acquire totally unconstrained values Shannon's bound for Gaussian noise is given by $R_c = \frac{1}{2} \log_2(1 + S/N)$, where S/N is the signal to noise ratio, defined as the ratio of source energy per bit (squared amplitude) over the spectral density of the noise (variance). If one constrains the encoded bits to binary values $\{\pm 1\}$ the capacity of a Gaussian channel is:

$$R_c = \int dJ \; P(J \mid 1) \log_2 P(J \mid 1) - \int dJ \; P(J) \log_2 P(J), \tag{3.36}$$

where $P(J \mid J^0) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{(J-J^0)^2}{2\sigma^2})$.

In Fig.8 we show the performance of Sourlas' code in a Gaussian channel together with the capacities of the unconstrained and binary Gaussian channels. We show that $K \to \infty$, $C = \alpha K$ Sourlas' code saturates Shannon's bound for the binary Gaussian channel as well. The significantly lower performance in the unconstrained Gaussian channel can be trivially explained by the binary coding scheme while signal and noise are allowed to acquire real values.

IV. DECODING DYNAMICS

A. Belief Propagation

The decoding process of an error-correcting code relies on computing averages over the marginal posterior probability $P(S_j \mid \boldsymbol{J})$ for each one of the N message bits S_j given the corrupted encoded bits J_μ (checks), where $\mu = \langle i_1 \dots i_K \rangle$ is one of the M sets chosen by the tensor $\mathcal{A}_\mu$. The probabilistic dependencies existing in the code can be represented as

a bipartite graph known as a *belief network* where nodes in one layer correspond to the M checks J_μ while nodes in the other to the N bits S_j. Each check is connected to exactly K bits and each bit is connected exactly to C checks (see Fig.9a).

Pearl [18] proposed an iterative algorithm for computation of marginal probabilities in belief networks. These algorithms operate by updating beliefs (conditional probabilities) locally and propagating them. Generally the convergence of these iterations depends on the absence of loops in the graph. As can be seen in Fig.9a, networks that define error-correcting codes may include loops and convergence problems may occur. Recently it was shown that in some cases Pearl's algorithm works even in the presence of loops [19].

The particular use of belief networks as decoding algorithms for error-correcting codes based on sparse matrices was discussed by MacKay in [20]. In this work a loop-free approximation for the graph in Fig.9a was proposed (see [18] for a general discussion on such approximations). In fact, it was shown in [21] that the probability of finite length loops in these graphs vanishes with the system size.

In this framework the network is decomposed in a way to avoid loops and the conditional probabilities $q_{\mu j}^{(S)}$ and $r_{\mu j}^{(S)}$ are computed. The set of bits in a check μ is defined as $\mathcal{L}(\mu)$ and the set of checks over the bit j as $\mathcal{M}(j)$. The probability that $S_j = S$ given information on all checks other than μ is denoted $q_{\mu j}^{(S)} = P(S_j = S \mid \{J_\nu : \nu \in \mathcal{M}(j) \setminus \mu\})$ and $r_{\mu j}^{(S)} = \mathrm{Tr}_{\{S_l : l \in \mathcal{L}(\mu)\setminus j\}} P(J_\mu \mid S_j = S, \{S_l : l \in \mathcal{L}(\mu) \setminus j\}) \prod_{l \in \mathcal{L}(\mu)\setminus l} q_{\mu l}^{(S_l)}$ is the probability of the check J_μ if the bit j is fixed to $S_j = S$ and the other bits involved are supposed to have distributions given by $q_{\mu i}^{(S_i)}$. In Fig.9b one can see a graphical representation of $r_{\mu j}^{(S)}$ that can be interpreted as the influence of the bit S_j and the mean-field $\prod_{l \in \mathcal{L}(\mu)\setminus l} q_{\mu l}^{(S_l)}$ (representing bits in $\mathcal{L}(\mu)$ over than l) over the check J_μ. In the Fig.9c we see that each field $q_{\mu l}^{(S)}$ represents the influence of the checks in $\mathcal{M}(l)$, excluding μ, over each bit S_l, this setup excludes the loops that may exist in the actual network.

Employing Bayes theorem, $q_{\mu j}^{(S)}$ can be rewritten as:

$$q_{\mu j}^{(S)} = a_{\mu j}\, P(\{J_\nu : \nu \in \mathcal{M}(j) \setminus \mu\} \mid S_j)\, p_j^{(S)}, \tag{4.1}$$

where $a_{\mu j}$ is a normalization constant such that $q_{\mu j}^{(+1)} + q_{\mu j}^{(-1)} = 1$ and $p_j^{(S)}$ is the prior probability over the bit j. The distribution $P(\{J_\nu : \nu \in \mathcal{M}(j) \setminus \mu\} \mid S_j)$ can be replaced by a mean-field approximation by factorizing dependencies using fields $r_{\mu j}^{(S)}$:

$$
\begin{aligned}
q_{\mu j}^{(S)} &= a_{\mu j} p_j^{(S)} \prod_{\nu \in \mathcal{M}(j) \setminus \mu} r_{\nu j}^{(S)} \\
r_{\mu j}^{(S)} &= \mathrm{Tr}_{\{S_l : l \in \mathcal{L}(\mu) \setminus j\}} P(J_\mu \mid S_j = S, \{S_i : i \in \mathcal{L}(\mu) \setminus j\}) \prod_{i \in \mathcal{L}(\mu) \setminus j} q_{\mu i}^{(S_i)}.
\end{aligned} \tag{4.2}
$$

A message estimate $\widehat{\xi}_j = \mathrm{sign}\left(\langle S_j \rangle_{q_j^{(S)}} \right)$ can be obtained by solving the above equations and computing the pseudo-posterior:

$$
q_j^{(S)} = a_j p_j^{(S)} \prod_{\nu \in \mathcal{M}(j)} r_{\nu j}^{(S)}, \tag{4.3}
$$

where a_j is a normalization constant.

By taking advantage of the normalization conditions for the distributions $q_{\mu j}^{(+1)} + q_{\mu j}^{(-1)} = 1$ and $r_{\mu j}^{(+1)} + r_{\mu j}^{(-1)} = 1$ one can change variables and reduce the number of equations (4.2) to the couple $\delta q_{\mu j} = q_{\mu j}^{(+1)} - q_{\mu j}^{(-1)}$ and $\delta r_{\mu j} = r_{\mu j}^{(+1)} - r_{\mu j}^{(-1)}$. Solving these equations, one can find back $r_{\mu j}^{(S)} = \frac{1}{2}(1 + \delta r_{\mu j} S_j)$ and the pseudo-posterior can be calculated to obtain the estimate.

B. Connection with Statistical Physics

The belief propagation algorithm was shown in [20] to outperform other methods such as simulated annealing. In [9] it was proposed that this framework can be reinterpreted using statistical physics. The main ideas behind the approximations contained in (4.2) are somewhat similar to the Bethe [22] approximation to diluted two-body spin glasses. Actually, for systems involving two-body interactions it is known that the Bethe approximation is equivalent to solving exactly a model defined on a Cayley tree and that this is a good approximation for finitely connected systems in the thermodynamical limit [23]. In fact, loops in the connections become rare as the system size grows and can be neglected without intro-

ducing significant errors. The belief propagation can be seen as a Bethe-like approximation for multiple bodies interaction systems.

The mean-field approximations used here are also quite similar to the TAP approach [24]. The fields $q_{\mu j}^{(S)}$ correspond to the mean influence of other sites other the site j and the fields $r_{\nu j}^{(S)}$ represent the influence of j back over the system (reaction fields).

The analogy can be exposed by observing that the likelihood $p(J_\mu \mid \boldsymbol{S})$ is proportional to the Boltzmann weight:

$$w_B(J_\mu \mid \{S_j : j \in \mathcal{L}(\mu)\}) = \exp\left(-\beta J_\mu \prod_{i \in \mu} S_i\right). \tag{4.4}$$

That can be also written in the more convenient form:

$$w_B(J_\mu \mid \{S_j : j \in \mathcal{L}(\mu)\}) = \frac{1}{2}\cosh(\beta J_\mu)\left(1 \; + \; \tanh(\beta J_\mu) \prod_{j \in \mathcal{L}(\mu)} S_j\right). \tag{4.5}$$

The variable $r_{\mu j}^{(S_j)}$ can then be seen as proportional to the effective Boltzmann weight obtained by fixing the bit S_j:

$$w_{\text{eff}}(J_\mu \mid S_j) = \text{Tr}_{\{S_l \,:\, l \in \mathcal{L}(\mu)\setminus j\}}\, w_B(J_\mu \mid \{S_l \; : \; l \in \mathcal{L}(\mu)\}) \prod_{l \in \mathcal{L}(\mu)\setminus j} q_{\mu l}^{(S_l)}. \tag{4.6}$$

Plugging Eq.(4.5) for the likelihood in equations (4.2), using the fact that the prior probability is given by $p_j^{(S)} = \frac{1}{2}\left(1 + \tanh(\beta S F)\right)$ and computing $\delta q_{\mu j}$ and $\delta r_{\mu j}$:

$$\begin{aligned} \delta r_{\mu j} &= \tanh(\beta J_\mu) \prod_{l \in \mathcal{L}(\mu)\setminus j} \delta q_{\mu l} \\ \delta q_{\mu j} &= \tanh\left(\sum_{\nu \in \mathcal{M}(l)\setminus \mu} \tanh^{-1}(\delta r_{\nu j}) + \beta F\right). \end{aligned} \tag{4.7}$$

The pseudo-posterior can then be calculated:

$$\delta q_j = \tanh\left(\sum_{\nu \in \mathcal{M}(l)} \tanh^{-1}(\delta r_{\nu j}) + \beta F\right), \tag{4.8}$$

providing Bayes' optimal decoding $\widehat{\xi}_j = \text{sign}(\delta q_j)$. It is important at this point to support the mean-field assumptions used here by methods of statistical physics [9]. The factorizability of the probability distributions can be explained by weak correlations between connections (checks) and by the cluster property:

$$\lim_{N\to\infty}\frac{1}{N^2}\sum_{i\neq j}\left(\langle S_iS_j\rangle_{p(S|J)}-\langle S_i\rangle_{p(S|J)}\langle S_j\rangle_{p(S|J)}\right)^2\to 0 \tag{4.9}$$

that bits S_j obey within a pure state [17].

One can push the above connections even further. Eqs.(4.7), of course, depend on the particular received message $\boldsymbol{J}$. In order to make the analysis message independent, one can use a gauge transformation $\delta r_{\mu j}\mapsto\xi_j\delta r_{\mu j}$ and $\delta q_{\mu j}\mapsto\xi_j\delta q_{\mu j}$ to write:

$$\begin{aligned}\delta r_{\mu j}&=\tanh(\beta J)\prod_{l\in\mathcal{L}(\mu)\backslash j}\delta q_{\mu l}\\ \delta q_{\mu j}&=\tanh\left(\sum_{\nu\in\mathcal{M}(l)\backslash\mu}\tanh^{-1}(\delta r_{\nu j})+\beta\xi_jF\right).\end{aligned} \tag{4.10}$$

In this form a success in the decoding process correspond to $\delta r_{\mu j}>0$ and $\delta q_{\mu j}=1$ for all μ and j. For a large number of iterations, one can expect the ensemble of belief networks to converge to an equilibrium distribution where δr and δq are random variables sampled from distributions $\widehat{\rho}(y)$ and $\rho(x)$ respectively. By transforming these variables as $\delta r=\tanh(\beta y)$ and $\delta q=\tanh(\beta x)$ and considering the actual message and noise as quenched disorder, Eqs.(4.10) can be rewritten as:

$$\begin{aligned}y&=\frac{1}{\beta}\left\langle\tanh^{-1}\left(\tanh(\beta J)\prod_{j=1}^{K-1}\tanh(\beta x_j)\right)\right\rangle_J\\ x&=\left\langle\sum_{j=1}^{C-1}y_j+\xi F\right\rangle_\xi.\end{aligned} \tag{4.11}$$

The above relations lead to a dynamics on the distributions $\widehat{\rho}(y)$ and $\rho(x)$, that is exactly the same obtained when solving iteratively RS saddle-point equations (3.12). The probability distributions $\widehat{\rho}(y)$ and $\rho(x)$ can be ,therefore, identified with $\widehat{\pi}(y)$ and $\pi(x)$ respectively and the RS solutions correspond to decoding a generic message using belief propagation averaged over an ensemble of different codes, noise and signals.

Eqs.(4.7) are now used to show the agreement between the simulated decoding and analytical calculations. For each run, a fixed code is used to generate 20000 bit codewords from 10000 bit messages, corrupted versions of the codewords are then decoded using (4.7). Numerical solutions for 10 individual runs are presented in Figs.10 and 11, initial conditions

are chosen as $\delta r_{\mu l} = 0$ and $\delta q_{\mu l} = \tanh(\beta F)$ reflecting prior beliefs. In Fig.10 we show results for $K = 2$ and $C = 4$ in the unbiased case, at code rate $R = 1/2$ (prior probability $p_j^{(1)} = f = 0.5$) at a low temperature $T = 0.26$ (we avoided $T = 0$ due to numerical difficulties). Solving saddle-point equations (3.12) numerically using Monte-carlo integration methods we obtain solutions with good agreement to simulated decoding. In the same figure we show the performance for the case of biased messages ($p_j^{(1)} = f_s = 0.1$), at code rate $R = 1/4$. Also here the agreement with Monte-carlo integrations is rather convincing. The third curve in Fig.10 shows the performance for biased messages at Nishimori's temperature T_N, as expected, it is far superior compared to low temperature performance and the agreement with Monte-carlo results is even better.

In Fig.11 we show the results obtained for $K = 5$ and $C = 10$. For unbiased messages the system is extremely sensitive to the choice of initial conditions and does not perform well in average even at Nishimori's temperature. For biased messages ($f_s = 0.1$, $R = 1/4$) results are far better and in agreement with Monte-carlo integration of the RS saddle-point equations.

The experiments show that belief propagation methods may be used successfully for decoding Sourlas-type codes in practice, and provide solutions that are well described by RS analytical solutions.

C. Basin of Attraction

To asses the size of the basin of attraction we consider the decoding process as a dynamics in the graphs space where edges $\delta q_{\mu j}$ are considered as dynamical variables. In gauged transformed equations (4.10) , the perfect decoding of a message correspond to $\delta q_{\mu j} = 1$. To analyse the basin of attraction we start with random initial values with a given normalized deviation from the perfect decoding $\lambda = \frac{1}{NC} \sum_{\mu j} (1 - \delta q^0_{\mu j})$. It is analogous to the finite magnetizations used in the naive mean-field of Section II, since a given $\delta q^0_{\mu j}$ corresponds to a given magnetization value by using Eq.(4.8).

In Fig.12 we show the maximal deviation in initial conditions required for successful decoding. Top figure shows an average over 10 different codes with $N = 300$ (circles) for a fixed code rate $R = 1/3$, fixed noise level $p = 0.1$ and increasing K. Bottom figure shows the maximal deviation in initial conditions for a fixed number of spins per interaction $K = 3$, noise level $p = 0.1$ and increasing C. We confirm the fidelity of the RS description by comparing the experimental results with the basin of attraction predicted by saddle-point equations (3.12). One can interpret these equations as a dynamics in the space of distributions $\pi(x)$. Performing the transformation $X = \tanh(\beta x)$, one can move to the space of distributions $\Pi(X)$ with support over $[-1, +1]$. The initial conditions can then be described simply as $\Pi^0(X) = (1 - \frac{\lambda}{2})\delta(X - 1) + \frac{\lambda}{2}\delta(X + 1)$. In Fig.12 we show the basin of attraction of this dynamics as lines and $\times$'s.

The $K = 2$ case is the only practical code from a dynamical point of view, since it has the largest basin of attraction and no prior knowledge on the message is necessary for decoding. Nevertheless, this code's performance degrades faster than the $K > 2$ case as shown in Section III, which points to a compromise between good dynamical properties in one side and good performance in the other. One idea could be having a code with changing K, starting with $K = 2$ to guarantee convergence and progressively increasing its values to improve the performance [25].

On the other hand, the basin of attraction increases with C. Again it points to a trade off between good equilibrium properties (small C and large code rates) and good dynamical properties (large C, large basin of attraction). Mixing small and large C values in the same code seems to be a way to take advantage of this trade-off [26–28].

V. CONCLUDING REMARKS

In this paper we studied, using the replica approach, a finite connectivity many-body spin glass that corresponds to Sourlas' codes for finite code rates. We have shown, using a simplified one step RSB solution for spin glass phase, that for $K \to \infty$ and $C = \alpha K$ regime

at low temperatures the system exhibits a FERRO-SG phase transition that corresponds to Shannon's bound. However, we have also shown that the decoding problem for large K has bad convergence properties when simulated annealing strategies are used.

We were able to find replica symmetric solutions for finite K and found good agreement with practical decoding performance using belief networks. Moreover, we have shown that RS saddle-point equations actually describe the mean behavior of belief propagation algorithms.

We studied the dynamical properties of belief propagation and compared to statistical physics predictions, confirming the validity of the description. The basin of attraction was shown to depend on K and C. Strategies for improving the performance were discussed.

The same methodology has been recently employed successfully [29] to state-of-the-art algorithms as the recent rediscovered Gallager codes [30] and its variations [25,28]. We believe that the connections found between belief networks and statistical physics can be further developed to provide deeper insights into the typical performance of general error-correcting codes.

ACKNOWLEDGMENTS

This work was partially supported by the program "Research For The Future" (RFTF) of the Japanese Society for the Promotion of Science (YK) and by EPSRC grant GR/L52093 and a Royal Society travel grant (DS and RV).

APPENDIX A: FREE ENERGY

In order to compute free-energies one needs to calculate the replicated partition function (3.7). One can start from Eq. (3.4):

$$\langle \mathcal{Z}^n \rangle_{\mathcal{A},\xi,J} = \mathrm{Tr}_{\{S_j^\alpha\}} \left[\left\langle \exp\left(-\beta \mathcal{H}^{(n)}(\{ \boldsymbol{S}^{\boldsymbol{\alpha}} \}) \right) \right\rangle_{\mathcal{A},J,\xi} \right], \tag{A1}$$

where $\mathcal{H}^{(n)}(\{\boldsymbol{S}^{\boldsymbol{\alpha}}\})$ represents the replicated Hamiltonian and α the replica indices. First one averages over the parity check tensors $\mathcal{A}$, for that an appropriate distribution has to be introduced, denoting $\mu \equiv \langle i_1, ..., i_K \rangle$ for a specific set of indices:

$$\langle \mathcal{Z}^n \rangle = \left\langle \frac{1}{\mathcal{N}} \sum_{\{\mathcal{A}\}} \prod_i \delta \left(\sum_{\mu \setminus i} \mathcal{A}_\mu - C \right) \mathrm{Tr}_{\{S_j^\alpha\}} \exp\left(-\beta \, \mathcal{H}^{(n)}(\{\boldsymbol{S}^{\boldsymbol{\alpha}}\}) \right) \right\rangle_{J,\xi}, \tag{A2}$$

where the δ distribution imposes a restriction on the connectivity per spin, $\mathcal{N}$ is a normalization coefficient and the notation $\mu \setminus i$ means the set μ minus the element i. Using integral representations for the delta functions and rearranging:

$$\langle \mathcal{Z}^n \rangle = \mathrm{Tr}_{\{S_j^\alpha\}} \left\langle \frac{1}{\mathcal{N}} \left(\prod_i \oint \frac{dz_i}{2\pi i} \frac{1}{z_i^{C+1}} \right) \sum_{\{\mathcal{A}\}} \left(\prod_\mu (\prod_{i \in \mu} z_i)^{\mathcal{A}_\mu} \right) \exp\left(-\beta \mathcal{H}^{(n)}(\{\boldsymbol{S}^{\boldsymbol{\alpha}}\}) \right) \right\rangle_{J,\xi}. \tag{A3}$$

Remembering that $\mathcal{A} \in \{0, 1\}$, and using the expression (1.1) for the Hamiltonian one can change the order of the summation and the product above and sum over $\mathcal{A}$:

$$\begin{aligned} \langle \mathcal{Z}^n \rangle = \mathrm{Tr}_{\{S_j^\alpha\}} \Bigg\langle \frac{1}{\mathcal{N}} \left(\prod_i \oint \frac{dz_i}{2\pi i} \frac{1}{z_i^{C+1}} \right) e^{\beta F \sum_{\alpha,i} \xi_i S_i^\alpha} \\ \times \prod_\mu \left[1 + (\prod_{i \in \mu} z_i) \exp\left(\beta J_\mu \sum_\alpha \prod_{i \in \mu} S_i^\alpha \right) \right] \Bigg\rangle_{J,\xi}. \end{aligned} \tag{A4}$$

Using the identity $\exp(\beta J_\mu \prod_{i \in \mu} S_i^\alpha) = \cosh(\beta) \left[1 + \left(\prod_{i \in \mu} S_i^\alpha \right) \tanh(\beta J_\mu) \right]$ one can perform the product over α to write:

$$\langle \mathcal{Z}^n \rangle = \mathrm{Tr}_{\{S_j^\alpha\}} \frac{1}{\mathcal{N}} \left(\prod_i \oint \frac{dz_i}{2\pi i} \frac{1}{z_i^{C+1}} \right) \left\langle e^{\beta F \sum_{\alpha,i} \xi_i S_i^\alpha} \right\rangle_\xi \tag{A5}$$

$$\begin{aligned} \times \prod_\mu \Bigg[1 + \left(\prod_{i \in \mu} z_i \right) \cosh^n(\beta) \Bigg(1 + \langle \tanh(\beta J) \rangle_J \sum_\alpha \prod_{i \in \mu} S_i^\alpha \\ + \langle \tanh^2(\beta J) \rangle_J \sum_{\langle \alpha_1 \alpha_2 \rangle} \prod_{i \in \mu} S_i^{\alpha_1} \prod_{j \in \mu} S_j^{\alpha_2} + ... \Bigg) \Bigg]. \end{aligned}$$

Defining $\langle \mu_1, \mu_2, ..., \mu_l \rangle$ as an ordered set of sets, and observing that for large N, $\sum_{\langle \mu_1 ... \mu_l \rangle} (...) = \frac{1}{l!} \left(\sum_\mu (...) \right)^l$ one can perform the product over the sets μ and replace the series that appears by an exponential:

$$\langle \mathcal{Z}^n \rangle = \mathrm{Tr}_{\{S_j^\alpha\}} \frac{1}{\mathcal{N}} \left(\prod_i \oint \frac{dz_i}{2\pi i} \frac{1}{z_i^{C+1}} \right) \left\langle e^{\beta F \sum \alpha, i \xi_i S_i^\alpha} \right\rangle_\xi \tag{A6}$$

$$\times \exp\left[\cosh^n(\beta)\left(\sum_\mu(\prod_{i\in\mu} z_i) + \langle\tanh(\beta J)\rangle_J \sum_\alpha\sum_\mu\prod_{i\in\mu} z_i S_i^\alpha \right.\right.$$
$$\left.\left. + \langle\tanh^2(\beta J)\rangle_J \sum_{\langle\alpha_1\alpha_2\rangle}\sum_\mu\prod_{i\in\mu} z_i S_i^{\alpha_1} S_i^{\alpha_2} + ...\right)\right].$$

Observing that $\sum_\mu = 1/K!\sum_{i_1,...i_K}$, defining $\mathcal{T}_l = \langle\cosh^n(\beta J)\tanh^l(\beta J)\rangle_J$ and introducing auxiliary variables $q_{\alpha_1...\alpha_m} = \frac{1}{N}\sum_i z_i S_i^{\alpha_1}...S_i^{\alpha_m}$ one finds:

$$\langle\mathcal{Z}^n\rangle_{\mathcal{A},\xi,J} = \frac{1}{\mathcal{N}}\left(\prod_i\oint\frac{dz_i}{2\pi i}\frac{1}{z_i^{C+1}}\right)\left(\int\frac{dq_0 d\widehat{q}_0}{2\pi i}\right)\left(\prod_\alpha\int\frac{dq_\alpha d\widehat{q}_\alpha}{2\pi i}\right)\ldots \tag{A7}$$
$$\times\exp\left[\frac{N^K}{K!}\left(\mathcal{T}_0 q_0^K + \mathcal{T}_1\sum_\alpha q_\alpha^K + \mathcal{T}_2\sum_{\langle\alpha_1\alpha_2\rangle} q_{\alpha_1\alpha_2}^K + \ldots\right)\right]$$
$$\times\exp\left[-N\left(q_0\widehat{q}_0 + \sum_\alpha q_\alpha\widehat{q}_\alpha + \sum_{\langle\alpha_1\alpha_2\rangle} q_{\alpha_1\alpha_2}\widehat{q}_{\alpha_1\alpha_2} + \ldots\right)\right]$$
$$\times\mathrm{Tr}_{\{S_j^\alpha\}}\left[\left\langle e^{\beta F\sum_{\alpha,i}\xi_i S_i^\alpha}\right\rangle_\xi \exp\sum_i\left(\widehat{q}_0 z_i + \sum_\alpha\widehat{q}_\alpha z_i S_i^\alpha + \ldots\right)\right].$$

The normalization constant is given by:

$$\mathcal{N} = \sum_{\{\mathcal{A}\}}\prod_i\delta\left(\sum_{\mu\backslash i}\mathcal{A}_\mu - C\right), \tag{A8}$$

and can be computed using exactly the same methods as above, resulting in:

$$\mathcal{N} = \left(\prod_i\oint\frac{dz_i}{2\pi i}\frac{1}{z_i^{C+1}}\right)\left(\int\frac{dq_0 d\widehat{q}_0}{2\pi i}\right)\exp\left[\frac{N^K}{K!}q_0^K - N q_0\widehat{q}_0 + \widehat{q}_0\sum_i z_i\right]. \tag{A9}$$

Computing the integrals over z_i's and using Laplace's method to compute the integrals over q_0 and $\widehat{q}_0$ one get:

$$\mathcal{N} = \exp\left\{\mathrm{Extr}_{q_0,\widehat{q}_0}\left[\frac{N^K}{K!}q_0^K - N q_0\widehat{q}_0 + N\ln\left(\frac{\widehat{q}_0^C}{C!}\right)\right]\right\}. \tag{A10}$$

The extremum point is given by $q_0 = N^{(1-K)/K}[(K-1)!C]^{1/K}$ and $\widehat{q}_0 = (C\,N)^{(K-1/K)}\left[(K-1)!\right]^{-1/K}$. Replacing the auxiliary variables in Eq.(A7) using $q_{\alpha_1...\alpha_m}/q_0 \to q_{\alpha_1...\alpha_m}$ and $\widehat{q}_{\alpha_1...\alpha_m}/q_0 \to \widehat{q}_{\alpha_1...\alpha_m}$, computing the integrals over z_i and using Laplace's method to evaluate the integrals one finally finds Eq.(3.7).

APPENDIX B: REPLICA SYMMETRIC SOLUTION

The replica symmetric free-energy (3.11) can be obtained by plugging the ansatz (3.10) into Eq.(A7). After computing the normalization $\mathcal{N}$ and using Laplace's method one has:

$$\langle \mathcal{Z}^n \rangle_{\mathcal{A},\xi,J} = \exp\left\{ N \, \mathrm{Extr}_{\pi,\widehat{\pi}} \left[\frac{C}{K} \mathcal{G}_1 \; - \; C \, \mathcal{G}_2 \; + \; \mathcal{G}_3 \right] \right\}, \tag{B1}$$

where:

$$\begin{aligned} \mathcal{G}_1 &= \mathcal{T}_0 + \mathcal{T}_1 \sum_{\alpha} \int \prod_{j}^{K} \left(dx_j \, \pi(x_j) \tanh(\beta x_j) \right) \\ &+ \mathcal{T}_2 \sum_{\langle \alpha_1 \alpha_2 \rangle} \int \prod_{j}^{K} \Big(dx_j \, \pi(x_j) \tanh^2(\beta x_j) \Big) + \ldots, \end{aligned} \tag{B2}$$

$$\begin{aligned} \mathcal{G}_2 &= 1 + \sum_{\alpha} \int dx \, dy \, \pi(x) \, \widehat{\pi}(y) \tanh(\beta x) \tanh(\beta y) \\ &+ \sum_{\langle \alpha_1 \alpha_2 \rangle} \int dx \, dy \, \pi(x) \, \widehat{\pi}(y) \tanh^2(\beta x) \tanh^2(\beta y) + \ldots \end{aligned} \tag{B3}$$

and

$$\begin{aligned} \mathcal{G}_3 = \frac{1}{N} \ln \Bigg\{ \Bigg(\prod_i \oint \frac{dz_i}{2\pi i} \frac{1}{z_i^{C+1}} \Bigg) \mathrm{Tr}_{\{S_j^\alpha\}} \Bigg[\Bigg\langle \exp \, \beta F \sum_{\alpha,i} \xi_i S_i^\alpha \Bigg\rangle_{\xi} \\ \times \exp \, \widehat{q}_0 \Bigg(\sum_i z_i + \sum_\alpha \sum_i z_i S_i^\alpha \int dy \, \widehat{\pi}(y) \tanh(\beta y) \\ + \sum_{\langle \alpha_1 \alpha_2 \rangle} \sum_i z_i S_i^{\alpha_1} S_i^{\alpha_2} \int dy \, \widehat{\pi}(y) \tanh^2(\beta y) + \ldots \Bigg) \Bigg] \Bigg\}. \end{aligned} \tag{B4}$$

The equation for $\mathcal{G}_1$ can be worked out by using the definition of $\mathcal{T}_m$ and the fact that $\left(\sum_{\langle \alpha_1 \ldots \alpha_l \rangle} 1\right) = \begin{pmatrix} n \\ l \end{pmatrix}$ to write:

$$\mathcal{G}_1 = \left\langle \cosh^n(\beta J) \int \left(\prod_{j=1}^{K} dx_j \, \pi(x_j) \right) \left(1 + \tanh(\beta J) \prod_{j=1}^{K} \tanh(\beta x_j) \right)^n \right\rangle_J . \tag{B5}$$

Following exactly the same steps one obtains:

$$\mathcal{G}_2 = \int dx \, dy \pi(x) \, \widehat{\pi}(y) \; \left(1 + \tanh(\beta x) \tanh(\beta y) \right)^n , \tag{B6}$$

and

$$\mathcal{G}_3 = \ln \left\{ \mathrm{Tr}_{\{S^\alpha\}} \left[\left\langle \exp \left(\beta F \xi \sum_\alpha S^\alpha \right) \right\rangle_\xi \right.\right.$$
$$\left.\left. \times \oint \frac{dz}{2\pi i} \frac{1}{z^{C+1}} \exp \left(\widehat{q}_0 \, z \int dy \, \widehat{\pi}(y) \prod_{\alpha=1}^{n} (1 + S^\alpha \tanh(\beta y)) \right) \right] \right\}. \tag{B7}$$

Computing the integral over z_i and the trace one finally finds:

$$\mathcal{G}_3 = \ln \left\{ \frac{\widehat{q}_0}{C!} \int \prod_{l=1}^{C} dy_l \widehat{\pi}(y_l) \left[\sum_{\sigma=\pm 1} \left\langle e^{\sigma \beta F \xi} \right\rangle_\xi \prod_{l=1}^{C} (1 + \sigma \tanh(\beta y_l)) \right]^n \right\}. \tag{B8}$$

Putting everything together, using Eq.(3.3) and some simple manipulation one finds Eq.(3.11).

APPENDIX C: ZERO TEMPERATURE SELF-CONSISTENT EQUATIONS

In this appendix we describe how one can write a set of self-consistent equations to solve the zero temperature saddle-point equations (3.24). Supposing a three peaks ansatz given by:

$$\widehat{\pi}(y) = p_+ \delta(y-1) + p_0 \delta(y) + p_- \delta(y+1) \tag{C1}$$
$$\pi(x) = \sum_{l=1-C}^{C-1} T_{[p_\pm, p_0; C-1]}(l) \; \delta(x-l), \tag{C2}$$

with

$$T_{[p_+,p_0,p_-;C]}(l) = \sum_{\{k,h,m \; ; \; k-h=l \; ; \; k+h+m=C-1\}} \frac{(C-1)!}{k! \; h! \; m!} \; p_+^k \; p_0^h \; p_-^m. \tag{C3}$$

One can consider the problem as a random walk, where $\widehat{\pi}(y)$ describes the probability of one step of length y ($y > 0$ means one step to the right) and $\pi(x)$ describes the probability of being at distance x from the origin after $C-1$ steps. With this idea in mind it is relatively easy to understand $T_{[p_+,p_0,p_-;C-1]}(l)$ as the probability of walking the distance l after $C-1$ steps with the probabilities p_+, p_- and p_0 of respectively moving right, left and staying at the same position. We define the probabilities of walking right/left as $\psi_\pm = \sum_l^{C-1} T_{[p_+,p_0,p_-;C-1]}(\pm l)$. Using second saddle-point equations (3.24):

$$p_+ = \int \left[\prod_{l=1}^{K-1} dx_l\, \pi(x_l)\right] \left\langle \delta \left[1 - \mathrm{sign}(J \prod_{l=1}^{K-1} x_l)\min(\mid J \mid, \mid x_1 \mid, \ldots, \mid x_{K-1} \mid\right]\right\rangle_J \qquad \text{(C4)}$$

The left side of the above equality can be read as the probability of making $K-1$ independent walks such that after $C-1$ steps all of them are not in the origin and an even (for$J=+1$) or odd (for $J=-1$) number of walks are at the left side. Using this reasoning for p_- and p_0 one can finally write :

$$p_+ = (1-p) \sum_{j=0}^{\lfloor \frac{K-1}{2} \rfloor} \binom{K-1}{2j} \psi_-^{2j} \psi_+^{K-2j-1} + p \sum_{j=0}^{\lfloor \frac{K-1}{2} \rfloor - 1} \binom{K-1}{2j+1} \psi_-^{2j+1} \psi_+^{K-2j-2} + p\, \psi_-^{K-1} \mathrm{odd}(K-1) \qquad \text{(C5)}$$

$$p_- = (1-p) \sum_{j=0}^{\lfloor \frac{K-1}{2} \rfloor - 1} \binom{K-1}{2j+1} \psi_-^{2j+1} \psi_+^{K-2j-2} + p \sum_{j=0}^{\lfloor \frac{K-1}{2} \rfloor - 1} \binom{K-1}{2j} \psi_-^{2j} \psi_+^{K-2j-1} + (1-p)\, \psi_-^{K-1} \mathrm{odd}(K-1), \qquad \text{(C6)}$$

where $\mathrm{odd}(x) = 1(0)$ if x is odd (even). Using that $p_+ + p_- + p_0 = 1$ one can obtain p_0. A similar set of equations can be obtained for a five peaks ansatz leading to the same set of solutions for the FERRO and PARA phases. The PARA solution $p_0 = 1$ is always a solution, for $C > K$ a FERRO solution with $p_+ > p_- > 0$ emerges.

APPENDIX D

In this appendix we establish the identity $\langle J \rangle_J = \langle J \tanh(\beta_N J) \rangle_J$ for symmetric channels. It was shown in [3] that :

$$\beta_N\, J = \frac{1}{2} \ln \left(\frac{p(J \mid 1)}{p(J \mid -1)} \right), \qquad \text{(D1)}$$

where β_N is the Nishimori's temperature and $p(J \mid J^0)$ are the probabilities that a transmitted bit J^0 is received as J. From this we can easily find:

$$\tanh\,(\beta_N\, J) = \frac{p(J \mid 1) - p(J \mid -1)}{p(J \mid 1) + p(J \mid -1)}. \qquad \text{(D2)}$$

In a symmetric channel ($p(J \mid -J^0) = p(-J \mid J^0)$), it is also represented as

$$\tanh\,(\beta_N\,J) = \frac{p(J\mid 1) - p(-J\mid 1)}{p(J\mid 1) + p(-J\mid 1)}. \tag{D3}$$

Therefore,

$$\begin{aligned}
\langle J\,\tanh\,(\beta_N\,J)\rangle_J &= \mathrm{Tr}_J\; p(J\mid 1)\;\frac{J\;p(J\mid 1)}{p(J\mid 1)+p(-J\mid 1)} \\
&\quad + \mathrm{Tr}_J\; p(J\mid 1)\;\frac{(-J)\;p(-J\mid 1)}{p(J\mid 1)+p(-J\mid 1)} \\
&= \mathrm{Tr}_J\; p(J\mid 1)\;\frac{J\;p(J\mid 1)}{p(J\mid 1)+p(-J\mid 1)} \\
&\quad + \mathrm{Tr}_J\; p(-J\mid 1)\;\frac{J\;p(J\mid 1)}{p(-J\mid 1)+p(J\mid 1)} \\
&= \mathrm{Tr}_J\; J\;p(J\mid 1) = \langle J\rangle_J.
\end{aligned} \tag{D4}$$

REFERENCES

[1] C. Shannon, Bell. Sys. Tech. J. **27**, 379 (1948).

[2] N. Sourlas, Nature **339**, 693 (1989).

[3] N. Sourlas, Europhys. Lett. **25**, 159 (1994).

[4] Y. Iba, J. Phys. A **32**, 3875 (1999).

[5] P. Ruján, Phys. Rev. Lett. **70**, 2968 (1993).

[6] H. Nishimori, J. Phys. Soc. of Japan **62**, 2973 (1993).

[7] S. Kirkpatrick and D. Sherrington, Phys. Rev. B **17**, 4384 (1978).

[8] B. Derrida, Phys. Rev. B **24**, 2613 (1981).

[9] Y. Kabashima and D. Saad, Europhys. Lett. **44**, 668 (1998).

[10] Y. Kabashima and D. Saad, Europhys. Lett. **45**, 97 (1999).

[11] E. Fradkin, B. Huberman, and S. Shenker, Phys. Rev. B **18**, 4879 (1978).

[12] K. Wong and D. Sherrington, J. Phys A **20**, L793 (1987).

[13] L. Viana and A. Bray, J. Phys. C **18**, 3037 (1985).

[14] D. Gross and M. Mezard, Nuclear Phys. B **240**, 431 (1984).

[15] G. Parisi, J.Phys. A **13**, 1101 (1980).

[16] D. B. Saakian, JETP Letters **67**, 440 (1998).

[17] M. Mezard, G. Parisi, and M. Virasoro, *Spin glass theory and beyond* (World Scientific, NJ, 1987).

[18] J. Pearl, *Probabilistic reasoning in intelligent systems* (Morgan Kauffman Publishers, CA, 1988).

[19] Y. Weiss, Technical Report No. A.I. Memo 1616, MIT (unpublished).

[20] D. MacKay, IEEE Trans. Inf. Theor. **45**, 399 (1999).

[21] T. Richardson and R. Urbanke (unpublished).

[22] H. Bethe, Proc. R. Soc. London, Ser. A **151**, 540 (1935).

[23] D. Sherrington and K. Wong, J. Phys A **20**, L785 (1987).

[24] D. Thouless, P. Anderson, and R. Palmer, Philos. Mag. **35**, 593 (1993).

[25] I. Kanter and D. Saad (unpublished).

[26] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman (unpublished).

[27] D. MacKay, S. Wilson, and M. Davey (unpublished).

[28] R. Vicente, D. Saad, and Y. Kabashima (unpublished).

[29] Y. Kabashima, T. Murayama, and D. Saad (unpublished).

[30] D. MacKay and R. Neal, Lec. Notes in Comp. Sc. **1025**, 100 (1995).

FIGURES

FIG. 1. The encoding, message corruption in the noisy channel and decoding can be represented as a Markovian process. The aim is to obtain a good estimative $\widehat{\boldsymbol{\xi}}$ for the original message ξ.

FIG. 2. Code performance measured by the magnetization m as a function of the noise level p as given by the naive mean-field theory at code rate $R = 1/2$ and $K = 2, 3, 4$ respectively from the bottom. The long-dashed line indicates PARA-FERRO coexistence. Insets: Maximum initial deviation λ for convergence at a noise level $p = 0.1$. Top inset: $K = 3$ and increasing C. Bottom inset: Code rate $R = 1/2$ and increasing K.

FIG. 3. Graph representation of the code.

FIG. 4. Phase diagram in the plane temperature T versus noise level p for $K \to \infty$ and $C = \alpha K$, with $\alpha = 4$. The dotted line indicates Nishimori's temperature T_N . Full lines represent coexistence. The critical noise level is p_c. The necessary condition for stability in the FERRO phase is satisfied above the dashed line.

FIG. 5. Histogram representing the mean-field distribution $\widehat{\pi}(y)$ obtained by Monte-carlo integration at low temperature ($\beta = 10$, $K = 3$,$C = 6$ and $p = 0.1$). Dotted lines represent solutions obtained by iterating self-consistent equations both with five peak and three peak ansätze. Inset: detailed view of the weak regular part arising in the Monte-carlo integration.

FIG. 6. Phase diagram in the plane code rate R versus noise level p for $K \to \infty$ and $C = \alpha K$ at zero temperature. The FERRO-SG coexistence line corresponds to the Shannon's bound.

FIG. 7. Top: zero temperature magnetization m as a function of the noise level p for various K values at code rate $R = 1/2$, as obtained by the iterative method . Notice that the RS theory predicts a transition of second order for $K = 2$ and first order for $K > 2$. Bottom: RS-FERRO free-energies (white circles for $K = 2$ and from the left: $K = 3, 4, 5$ and 6) and RSB-SG free-energy (dotted line) as functions of the noise level p. The arrow indicates the region where the RSB-SG phase starts to dominate. Inset: a detailed view of the RS-RSB transition region.

FIG. 8. Critical code rate R_c and channel capacity for a binary Gaussian channel as a function of the signal to noise rate S/N (solid line). Sourlas' code saturates Shannon's bound. Channel capacity of the unconstrained Gaussian channel (dashed line).

FIG. 9. (a) Belief network representing an error-correcting code. Each bit S_j (white circles) is linked to exactly C checks and each check (black circles) J_μ is linked to exactly K bits. (b) Graphical representation of the field $r_{\mu j}$. The grey box represents the mean field contribution $\prod_{l \in \mathcal{L}(\mu) \setminus j} q_{\mu l}$ of the other bits on the check J_μ. (c) Representation of one of the fields $q_{\mu l}$.

FIG. 10. Magnetization as a function of the flip probability p for decoding using TAP equations for $K = 2$. From the bottom: Monte-carlo solution of the RS saddle-point equations for unbiased messages ($f_s = 0.5$) at $T = 0.26$ (line) and 10 independent runs of TAP decoding for each flip probability (plus signs), $T = 0.26$ and biased messages ($f_s = 0.1$) at Nishimori's temperature T_N.

FIG. 11. Magnetization as a function of the flip probability p for decoding using TAP equations for $K = 5$. The dotted line is the replica symmetric saddle-point equations Monte-carlo integration for unbiased messages ($f_s = 0.5$) at the Nishimori's temperature T_N. The bottom error bars correspond to 10 simulations using the TAP decoding. The decoding performs badly on average in this scenario. The upper curves are for biased messages ($f_s = 0.1$) at the Nishimori's temperature T_N. The simulations agree with results obtained using the replica symmetric ansatz and Monte-carlo integration.

FIG. 12. Top: Maximum initial deviation λ for decoding. Top: λ as function of the number of interactions K. Circles are averages over 10 different codes with $N = 300$, $R = 1/3$ and noise level $p = 0.1$. Bottom: λ as function of the connectivity C. Circles are averages over 10 codes with $N = 300$, $K = 3$ and noise level $p = 0.1$. Lines and $\times$'s correspond to the RS dynamics described by the saddle-point equations.