Zero-temperature error-correcting code for a binary symmetric channel

1995 J. Phys. A: Math. Gen. 28 135

(http://iopscience.iop.org/0305-4470/28/1/017)

J. Phys. A: Math. Gen. 28 (1995) 135–147. Printed in the UK

Zero-temperature error-correcting code for a binary symmetric channel

C Dress†§, E Amic‡‖ and J M Luck‡¶

† Laboratoire de Physique Théorique*, ENS, F-75231 Paris Cedex 05, France

‡ Service de Physique Théorique, Centre d'Etudes de Saclay, F-91191 Gif-sur-Yvette Cedex, France

Received 28 July 1994, in final form 17 October 1994

Abstract. We study a convolutional error-correcting code with a minimum error probability decoding procedure, which is designed to lower the distortion of messages transmitted through a noisy binary symmetric channel. The problem can be rephrased in terms of zero-temperature properties of a one-dimensional disordered spin model, with random two- and three-spin couplings. For instance the ground-state magnetization is related to the average error per bit of decoded output messages. The ground-state energy is evaluated exactly, whereas other relevant quantities are expanded as power series in the density p of impurity couplings, a measure of the level of channel noise. These analytic results are compared with the outcomes of numerical simulations.

1. Introduction

One of the standard topics in the mathematical theory of communication deals with the corruption of messages sent through a noisy channel [1–4]. The use of *error-correcting codes* usually arises in this framework to solve two key problems, namely the redundancy of source messages and the distortion of transmitted messages due to channel noise. Indeed the standard way of handling the latter point consists of encoding the emitted data, in order to strengthen the reliability of transmission. The communication system includes a coding device which converts a message, i.e. a sequence of information symbols $\{s_n\}_{1\leqslant n\leqslant N}$ drawn from the emitting source, into a new message $\{\gamma_\alpha\}_{1\leqslant\alpha\leqslant M}$. This procedure introduces some redundancy in the original message, measured by the *rate* $R = N/M$ of the code. The encoded message is then transmitted through a noisy channel which may corrupt each of its bits, thus delivering an output sequence $\{K_\alpha\}_{1\leqslant\alpha\leqslant M}$, whose components may either be real-valued, e.g. for a Gaussian channel, or integer-valued, e.g. for a binary channel. The capacity C of the channel is defined as the maximal amount of information per bit that can be transmitted through it. If $R > C$, the frequency of errors is bounded from below by a non-zero value, so that the communication system cannot be considered as reliable. Conversely, if $R < C$, it is possible to devise optimal error-correcting codes, together with appropriate decoding algorithms, such that the frequency of errors vanishes in the thermodynamical limit of infinitely long messages *(channel-coding theorem)* [1–4]. This

§ E-mail address: dress@physique.ens.fr

‖ E-mail address: amic@amoco.saclay.cea.fr

¶ E-mail address: luck@amoco.saclay.cea.fr

* Unité propre du CNRS, associée à l'Ecole Normale Supérieure et à l'Université de Paris Sud.

0305-4470/95/010135+13$19.50

result gave rise to many investigations which aimed at designing such optimal codes and decoding procedures. Sourlas [5] established that the decoding step of the general family of convolutional codes amounts to finding the ground state(s) of a suitably defined spin-glass Hamiltonian. In the present context the term *spin glass* is to be taken in the generic sense of a *disordered and frustrated magnetic model.* One of the known explicit examples of an ideal error-correcting code in the limit of a vanishing rate has been derived [6] from the random-energy model (REM) [7], well known in statistical mechanics.

This paper reports on analytical results concerning a simple error-correcting code, analogous to those actually used in telecommunications. The properties of this code can be rephrased in terms of a one-dimensional (1D) frustrated spin model, somewhat analogous to spin glasses and to random-field models. The main goal of this work is to investigate the zero-temperature properties of the spin model, and to interpret our predictions in the language of the theory of error-correcting codes. After recalling some general formalism in section 2, we present analytical results in section 3, whereas section 4 is devoted to numerical simulations and to a short discussion.

2. General formalism

Consider a source producing information messages. Each message is a sequence of the form $s = \{s_1, s_2, \ldots, s_N\}$, made of N bits $s_n = \pm 1$, and it occurs with a given *a priori* probability $P_s(s) \sim \exp[-\mathcal{H}_s(s)]$. A *convolutional error-correcting code* [3] transforms each information symbol into a product of some of the s_n's, thus converting the source message s into a new message $\gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_M\}$ of bits $\gamma_\alpha = \pm 1$, according to deterministic, translationally invariant rules of the form

$$\gamma_\alpha = \prod_{n \in \alpha} s_n \qquad \text{with} \quad \alpha \equiv \{n_1, n_2, \ldots, n_k\} \in \{1, \ldots, N\}^k \,. \tag{2.1}$$

We define the *range*, or *memory*, of the code as the maximal distance r between two n_ℓ's belonging to the same set of indices α [3], namely

$$r = 1 + \max_{\alpha} \max_{\{n_\ell, n_m\} \in \alpha} |n_\ell - n_m| \,. \tag{2.2}$$

The encoded message is then sent through a memoriless noisy binary channel, which delivers a distorted output sequence $K = \{K_1, K_2, \ldots, K_M\}$. In this case, the way each bit sent γ_α is corrupted does not depend on the other transmitted bits. Hence the conditional probability $P(K_\alpha|\gamma_\alpha)$ to have received the symbol K_α, knowing that the symbol γ_α was sent, determines the statistical properties of the channel completely.

It has been shown [5, 6] that the probability $P(\sigma|K)$ that the original message was $\sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_N\}$, knowing that the sequence K was received, can be expressed in terms of the Hamiltonian of a 1D spin model, whose coupling constants depend on the output message K, according to

$$P(\sigma|K) \sim \exp[-\mathcal{H}_K(\sigma) - \mathcal{H}_s(\sigma)] \tag{2.3}$$

where

$$\mathcal{H}_K(\sigma) = -\sum_{\alpha=1}^{M} J(K_\alpha) \prod_{n \in \alpha} \sigma_n \qquad \text{with} \quad J(K_\alpha) = \tfrac{1}{2} \ln \frac{P(K_\alpha|1)}{P(K_\alpha|-1)} \,. \tag{2.4}$$

The simplest procedure for inferring, from the received codeword K, what message s was sent as an input, consists of choosing the message $\sigma^{(d)}$ which maximizes the probability given in (2.3). This is the *minimum error probability decoding* (MED) scheme [3]. When all emitted words are equally probable, i.e. when $\mathcal{H}_s(\sigma)$ reduces to a constant, this is equivalent to finding the ground state(s) of the Hamiltonian $\mathcal{H}_K(\sigma)$.

We are thus led to consider zero-temperature properties of a disordered spin model, since the couplings $J(K_\alpha)$'s represent quenched disorder, whose realization is determined by the channel output, and where the dynamical spin variables σ_n represent the inferred source message. The *probability of error per bit*, or, equivalently, the *average error per bit*, in the inferred message $\sigma^{(d)}$ reads

$$p_e(s, \sigma^{(d)}) = \frac{1}{2}\left(1 - \frac{1}{N}\sum_{n=1}^{N} s_n \sigma_n^{(d)}\right) \tag{2.5}$$

where $\sigma^{(d)}$ depends implicitly on the quenched disorder.

In the case of a discrete channel, the Hamiltonian $\mathcal{H}_K(\sigma)$ may have many degenerate ground states, due to the combined effects of disorder and frustration. The number of such ground states then increases as $\exp(NS_0)$, with S_0 being the zero-temperature entropy per spin.

If we assume that the channel is *symmetric*, i.e. $P(-K_\alpha|-\gamma_\alpha) = P(K_\alpha|\gamma_\alpha)$, the invariance of $\mathcal{H}_K(\sigma)$ and $p_e(s, \sigma^{(d)})$ under the gauge transformation $s_n \to \varepsilon_n s_n$, $\sigma_n \to \varepsilon_n \sigma_n$, $K_\alpha \to (\prod_{n\in\alpha} \varepsilon_n) K_\alpha$, for any sequence of binary variables $\varepsilon_n = \pm 1$, implies that the whole procedure does not depend on the source message $\{s_n\}_{1\leqslant n\leqslant N}$. Taking $\varepsilon_n = s_n$, we can evaluate the probability of error per bit by considering a message consisting of 1's only. We thus obtain

$$p_e = \tfrac{1}{2}(1 - m) \tag{2.6}$$

where

$$m = \frac{1}{N}\sum_{n=1}^{N} \langle \sigma_n \rangle \tag{2.7}$$

is the magnetization per spin of the inferred ground state. Moreover, the explicit dependence on the ground state can be removed as well, since the magnetization is a *self-averaging quantity*: its value per spin is expected to be equal to a certain constant m, for almost all realizations of disorder in the thermodynamical limit ($N \to \infty$). There may be, however, exceptional realizations of disorder for which the ground states have a magnetization different from m, so that one should, in principle, determine the whole distribution of p_e. We shall come back to this point in section 3.2.

The above approach can be implemented numerically for any 1D disordered spin Hamiltonian built from a finite-range convolutional error-correcting code by means of the zero-temperature transfer-matrix algorithm, also called dynamical programming, or the Viterbi algorithm [3]. This procedure allows one to find the ground states in polynomial time, with a memory of size 2^{r-1}.

Ruján [8] recently proposed another decoding algorithm, which we refer to as the *finite-temperature decoding* (FTD) scheme, which merely focuses on the minimization of the probability of error p_e, rather than on the maximization of the conditional probability $P(\sigma|K)$. This scheme consists in taking the nth bit of the decoded sequence equal to the

sign of the local magnetization $m_n = \langle \sigma_n \rangle$ at temperature $T = 1$, in suitable units to be defined below. The value of p_e has been shown to be smaller than that obtained with MED. This result was proved rigorously by Nishimori [9] when the quenched disorder obeys laws of the form $P(K) = G(|K|)\exp(\gamma K)$; it was subsequently extended to any kind of randomness [10]. The algorithmic complexity of the procedure remains polynomial in time, but the required memory is now of order $2^{r-1}N$.

Throughout the following, we restrict the analysis to a convolutional error-correcting code of rate $R = \frac{1}{2}$ and range $r = 3$, that encodes each bit s_n of the original message, emitted by a uniform source, into two bits $\gamma_n^{(1)}$, $\gamma_n^{(2)}$, defined as follows:

$$\gamma_n^{(1)} = s_{n-1}s_{n+1} \qquad \gamma_n^{(2)} = s_{n-1}s_n s_{n+1} \,. \tag{2.8}$$

The encoded message $\gamma(s)$ is then sent through a memoriless *binary symmetric channel* (BSC). The level of channel noise is characterized by the probability p ($p \ll 1$ in practice) for any bit of information to get corrupted during transmission. Hence the conditional probability that the output message is $\{K_n, L_n\}_{1 \leqslant n \leqslant N}$, given that the encoded message was $\{\gamma_n^{(1)}, \gamma_n^{(2)}\}_{1 \leqslant n \leqslant N}$, reads

$$P(K_n|\gamma_n^{(1)}) = (1-p)\,\delta\big(K_n - \gamma_n^{(1)}\big) + p\,\delta\big(K_n + \gamma_n^{(1)}\big) \tag{2.9}$$

together with a similar formula for L_n.

Owing to the simple form $J(K_n)/K_n = J(L_n)/L_n = J(p)$ of the coupling constants in the binary case, with

$$J(p) = \tfrac{1}{2}\ln\frac{1-p}{p} \tag{2.10}$$

the Hamiltonian $\mathcal{H}_K(\sigma)$ defined in (2.4) reads

$$\mathcal{H}_K(\sigma) = J(p)\mathcal{H}'_K(\sigma)$$

with

$$\mathcal{H}'_K(\sigma) = -\sum_{n=1}^{N}(K_n\sigma_{n-1}\sigma_{n+1} + L_n\sigma_{n-1}\sigma_n\sigma_{n+1})\,. \tag{2.11}$$

The model defined by the reduced Hamiltonian $\mathcal{H}'_K$ of (2.11) is the central object of the present work. It can be viewed as a spin model living on a triangular ladder, with longitudinal nearest-neighbour binary interactions K_n, and ternary interactions L_n around the triangular *plaquettes* (see figure 1). The two- and three-spin couplings K_n and L_n are independent random variables, which assume the values (+1) and (−1), with respective

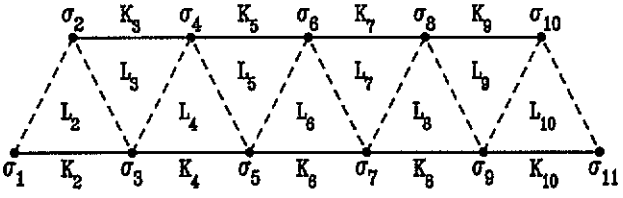

Figure 1. Triangular ladder geometry of the spin model associated with the reduced Hamiltonian $\mathcal{H}'_K(\sigma)$.

probabilities $(1-p)$ and p. It will become clearer in the following that the disordered spin model defined by the Hamiltonian (2.11) has some characteristic features in common with the random-field Ising chain, rather than with the 1D Ising spin glass. Indeed, the three-spin couplings L_n are, to some extent, analogous to a random magnetic field spread over three consecutive sites.

The regime of interest for the theory of error-correcting codes is that of a weak level of noise ($p \ll 1$). We shall therefore refer to the couplings equal to (-1) as *impurity couplings*. The temperature $T = 1$ of Ruján's FTD scheme corresponds to the so-called Nishimori temperature [11], where the binary spin-glass model (with only two-spin interactions) becomes exactly solvable, by virtue of the special form (2.10) of the strength of the interactions.

The Hamming distance between the received message K (the only available information for the decoder) and any possible codeword $\gamma(\sigma)$ in the coupling space $\{-1,+1\}^M$ can be expressed in terms of $\mathcal{H}'_K(\sigma)$, namely

$$d[K,\gamma(\sigma)] = \tfrac{1}{2}\sum_{n=1}^{N}\left[\left(K_n-\gamma_n^{(1)}\right)^2+\left(L_n-\gamma_n^{(2)}\right)^2\right] = 2N+\mathcal{H}'_K(\sigma)\,. \tag{2.12}$$

This formula underlines the interpretation of MED as the search of the set of messages lying closest to the received sequence. Defining d_f as the mean distance between any given codeword and its noisy realizations, Ruján's FTD method merely relies on the search of all the messages γ whose distance to the received message K equals d_f, which is obviously larger than $d[K,\gamma(\sigma^{(d)})]$.

3. Analytical results for the spin model

We now turn to the study of the zero-temperature properties of the reduced Hamiltonian $\mathcal{H}'_K(\sigma)$, and to their interpretation in the language of information theory. We shall consider successively the following thermodynamical quantities, defined per spin. The *ground-state energy* $E'_0(p) = E_0(p)/J(p)$ (related to the minimum distance between the original sequence and its inferred interpretations in the coupling space), the *zero-temperature entropy* $S_0(p)$ (related to the number of different inferred messages, a measure of the reliability of the decoder), and the *zero-temperature magnetization* $m(p)$ (related to the probability of error per bit in the decoded message). We shall derive an exact expression for $E'_0(p)$, whereas $S_0(p)$ and $m(p)$ will be obtained as power series in p, which are relevant in the small-p regime of interest.

3.1. Exact ground-state energy

We first recall the main lines of the transfer-matrix formalism for 1D Ising models [12, 13]. Let $Z_n^{\varepsilon_1,\varepsilon_2}$ be the constrained partition functions of a chain of length n at temperature $T = 1/\beta$, with the boundary conditions $\sigma_n = \varepsilon_1 = \pm 1$, $\sigma_{n-1} = \varepsilon_2 = \pm 1$. These four random variables obey linear recursion relations of the form

$$\begin{pmatrix} Z_{n+1}^{++} \\ Z_{n+1}^{-+} \\ Z_{n+1}^{+-} \\ Z_{n+1}^{--} \end{pmatrix} = \mathcal{T}_n \begin{pmatrix} Z_n^{++} \\ Z_n^{-+} \\ Z_n^{+-} \\ Z_n^{--} \end{pmatrix} \tag{3.1}$$

where $\mathcal{T}_n$ is the 4×4 transfer matrix

$$\mathcal{T}_n = \begin{pmatrix} z^{K_n+L_n} & z^{-K_n-L_n} & 0 & 0 \\ 0 & 0 & z^{K_n-L_n} & z^{-K_n+L_n} \\ z^{-K_n-L_n} & z^{K_n+L_n} & 0 & 0 \\ 0 & 0 & z^{-K_n+L_n} & z^{K_n-L_n} \end{pmatrix} \tag{3.2}$$

with $z = e^{\beta}$. The free energy per spin is given by the Lyapunov exponent of the product of non-commuting transfer matrices

$$-\beta F = \lim_{N\to\infty} \frac{1}{N} \ln \operatorname{tr} \prod_{n=1}^{N} \mathcal{T}_n . \tag{3.3}$$

The analysis of low-temperature properties goes as follows [12–14]. The partition functions obtained by iterating (3.1) have a leading power-law behaviour at low temperature, namely

$$\begin{aligned} Z_n^{++} &\approx A_n^{++} z^{x_n} & Z_n^{-+} &\approx A_n^{-+} z^{x_n+2a_n} \\ Z_n^{+-} &\approx A_n^{+-} z^{x_n+2b_n} & Z_n^{--} &\approx A_n^{--} z^{x_n+2c_n} \end{aligned} \qquad (z \to \infty) . \tag{3.4}$$

In order to evaluate the ground-state energy $E_0'(p)$, it is sufficient to keep track of the exponents a_n, b_n, and c_n. They obey the following recursion relations:

$$\begin{aligned} a_{n+1} &= \max(K_n + b_n, L_n + c_n) - \max(K_n + L_n, a_n) \\ b_{n+1} &= \max(0, K_n + L_n + a_n) - \max(K_n + L_n, a_n) \\ c_{n+1} &= \max(K_n + c_n, L_n + b_n) - \max(K_n + L_n, a_n) \end{aligned} \tag{3.5}$$

and the ground-state energy is given by

$$E_0'(p) = -2 + 4p - 2\langle\langle \max(K_n + L_n, a_n) \rangle\rangle \tag{3.6}$$

where the double brackets $\langle\langle \cdots \rangle\rangle$ denote an average over the stationary joint distribution of the three variables (a_n, b_n, c_n), which is invariant under the transformation (3.5). We have shown by iterating this transformation that the associated invariant distribution is supported by a finite set, which consists of 31 integer points in the three-dimensional space (a, b, c). The statistical weights associated with these points have been obtained by solving the linear system which expresses their invariance under the recursion (3.5).

We prefer to skip tedious calculations, and just give the following exact rational formula for the reduced ground-state energy

$$E_0'(p) = -2 + 2p \frac{N(p)}{D(p)} \tag{3.7}$$

with

$$
\begin{aligned}
N(p) &= 2 - 12p + 82p^2 - 322p^3 + 1002p^4 - 2542p^5 + 5060p^6 - 7873p^7 \\
&\quad + 14\,285p^8 - 55\,486p^9 + 248\,842p^{10} - 874\,448p^{11} + 2\,383\,088p^{12} \\
&\quad - 5\,206\,968p^{13} + 9\,349\,136p^{14} - 13\,992\,320p^{15} + 17\,566\,864p^{16} \\
&\quad - 18\,506\,368p^{17} + 16\,281\,888p^{18} - 11\,846\,592p^{19} + 7\,016\,576p^{20} \\
&\quad - 3\,302\,144p^{21} + 1\,189\,376p^{22} - 308\,224p^{23} + 51\,200p^{24} - 4096p^{25} \\
D(p) &= 1 - 6p + 46p^2 - 130p^3 + 419p^4 - 1030p^5 + 1607p^6 - 827p^7 - 5714p^8 \\
&\quad + 37\,267p^9 - 159\,858p^{10} + 556\,346p^{11} - 1\,653\,662p^{12} \\
&\quad + 4\,197\,065p^{13} - 8\,714\,696p^{14} + 13\,230\,758p^{15} - 8\,419\,724p^{16} \\
&\quad - 27\,952\,108p^{17} + 131\,054\,496p^{18} - 335\,734\,552p^{19} + 649\,530\,288p^{20} \\
&\quad - 1\,026\,616\,304p^{21} + 1\,367\,175\,616p^{22} - 1\,555\,663\,328p^{23} \\
&\quad + 1\,521\,159\,872p^{24} - 1\,278\,948\,928p^{25} + 921\,379\,840p^{26} \\
&\quad - 564\,579\,456p^{27} + 290\,795\,264p^{28} - 123\,716\,096p^{29} + 42\,372\,096p^{30} \\
&\quad - 11\,237\,376p^{31} + 2\,166\,784p^{32} - 270\,336p^{33} + 16\,384p^{34}.
\end{aligned}
\tag{3.8}
$$

The reduced ground-state energy is plotted as a full curve on figure 2. It is a monotonically increasing function of p, from $E_0'(0) = -2$ to $E_0'(1) = -\frac{4}{3}$. The broken curve on the figure shows a plot of the energy $E_0''(p)$ of the ground states associated with the error-correcting code problem, taking into account the sign of $J(p)$ defined in (2.10), namely

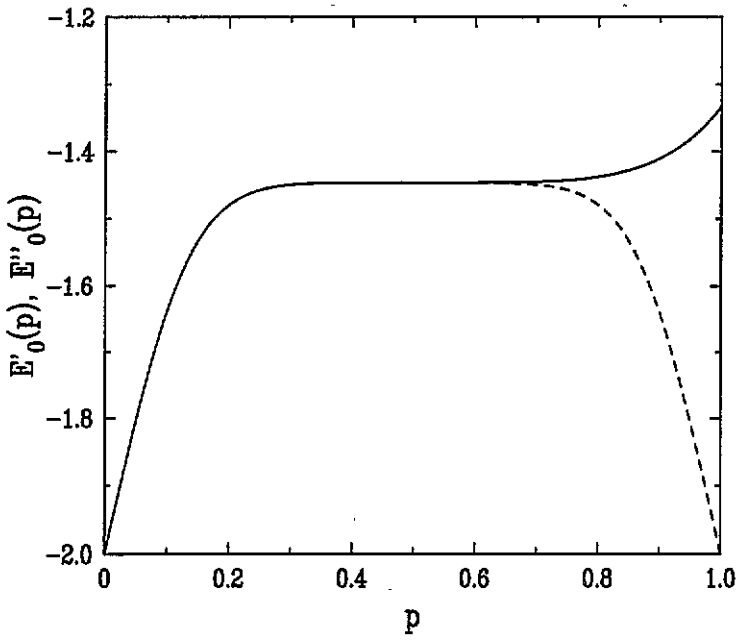

Figure 2. Exact ground-state energy $E_0'(p)$ of the reduced Hamiltonian $\mathcal{H}_K'(\sigma)$ (full curve), and its variant $E_0''(p)$ defined in (3.9) (broken curve).

$$E_0''(p) = \begin{cases} E_0'(p) & \text{for} \quad J(p) > 0 \quad \text{i.e.} \quad 0 < p < \frac{1}{2} \\ E_0'(1-p) & \text{for} \quad J(p) < 0 \quad \text{i.e.} \quad \frac{1}{2} < p < 1. \end{cases} \tag{3.9}$$

This expression is invariant under the change of p into $(1-p)$, as it should. The difference between E_0' and E_0'' originates in the fact that $\mathcal{H}_K(\sigma)$ and $\mathcal{H}_K'(\sigma)$ have identical ground states only for $p < \frac{1}{2}$.

For $p \to 0$, we have $E_0'(p) = -2+4p-20p^3-244p^4+\cdots$. The first two terms of this expansion are nothing but the energy $E_F = -(\overline{K}+\overline{L}) = -2(1-2p)$ of the ferromagnetic spin configuration ($\sigma_n = +1$ for $1 \leqslant n \leqslant N$), where the bar denotes an average over the quenched disorder. The next terms in the above expansion describe more complex configurations involving flipped spins ($\sigma_n = -1$). We shall come back to that point more extensively in section 3.2. For $p \to 1$, we have $E_0'(p) = -\frac{4}{3} - 32(1-p)/27 + \cdots$. The value $E_0'(1) = -\frac{4}{3}$ is the energy of the periodic ground state $(++-)^\infty$, which is three-fold degenerate. Finally, the reduced ground-state energy exhibits a very flat plateau around $p = \frac{1}{2}$. Indeed we have $E_0'(p) = -334/231 + 284\,800(p-\frac{1}{2})^5/53\,361 + \cdots$. This ensures that $E_0''(p)$ is continuous, together with its first four derivatives with respect to p, at the symmetric point $p = \frac{1}{2}$, where $J(p)$ vanishes.

The investigation of the complex singularities of thermodynamic functions often provides a useful alternative viewpoint (see [15] for a review). In the present case the ground-state energy $E_0'(p)$ is exactly known as a rational function of p. Figure 3 shows a plot of its poles and zeros in the complex p-plane. The 34 poles and 34 zeros turn out to come in closely grouped sets, either as pairs or larger neutral molecules. This phenomenon is to be put into perspective with the fact that $E_0'(p)$ is almost a constant over a large part of the physical range [0, 1].

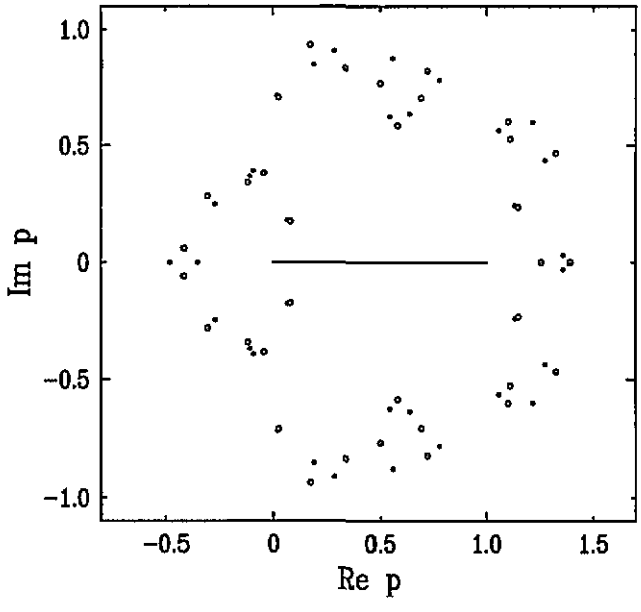

Figure 3. Exact poles (full symbols) and zeros (open symbols) of the reduced ground-state energy $E_0'(p)$ in the complex p-plane. The full line segment represents the physical range [0, 1].

3.2. Other zero-temperature observables

The exact treatment of other zero-temperature observables, besides the ground-state energy, is, in our opinion, beyond the possibility of analytical calculations. For instance the evaluation of the ground-state entropy requires the determination of the distribution of the prefactors $A_n^{\varepsilon_1,\varepsilon_2}$ which occur in the low-temperature behaviour (3.4) of the partition functions. This calculation cannot be worked out explicitly in degenerate situations such as the present one [12, 13].

Since in any case the regime of interest is that of a low noise level ($p \ll 1$), we have made use of an enumeration scheme which allows us to derive systematic expansions of various zero-temperature observables as power series in the concentration p of impurity interactions. The spirit of the approach is as follows. In order to expand observables up to order p^k included, introduce any number $\ell \leqslant k$ of impurity couplings K_n, L_n in a long enough chain, and look for all the spin configurations whose energies are less than or equal to that of the ferromagnetic state for that particular realization of disorder. The contributions of these realizations to physical observables are polynomials in the length N of the chain, but only the extensive terms (i.e. those linear in N) are to be kept, according to a well known argument used thoroughly, e.g. in high-temperature expansions in statistical mechanics (see [16]).

The enumeration algorithm starts being non-trivial for $k = 3$; indeed, the difference between the ground-state energy given in (3.7) and (3.8) and the energy of the ferromagnetic state scales as p^3, as already underlined in section 3.1. This behaviour can be explained as follows. Every spin σ_n occurs in five terms of the Hamiltonian $\mathcal{H}'_K$. At least three of those five coupling constants have to be impurity couplings, in order for the spin under consideration to be flipped in the ground state(s) of the chain. The statistical weight of such a realization of disorder is of order p^3 for small p. The same argument applies to other properties of the ground states, and therefore shows that thermodynamical quantities at zero temperature, such as the entropy $S_0(p)$ and the magnetization $m(p)$, will be non-trivial only at order p^3.

Apart from a non-zero value of the zero-temperature entropy, the presence of many degenerate ground states with different local spin ordering has another consequence. The limit magnetizations $m_+(p)$ (respectively, $m_-(p)$) of the spin chain in an infinitesimally positive (respectively, negative) external magnetic field $H \to 0^+$ (respectively, $H \to 0^-$) do not coincide, in general. Rather, we expect $m(p)$, $m_+(p)$ and $m_-(p)$ to be three different self-averaging quantities, obeying the thermodynamical inequalities $m_-(p) < m(p) < m_+(p) < 1$, with all the differences being of order p^3. The quantities $m_+(p)$ and $m_-(p)$ are to be identified with the upper and lower bounds of the distribution of the magnetization of all possible ground states, alluded to below (2.7).

We again skip details, and only give the following outcomes of the enumeration scheme, up to order p^4 included:

$$E'_0(p) = -2 + 4p - 20p^3 - 244p^4 + \mathcal{O}(p^5) \tag{3.10a}$$

$$S_0(p) = \underbrace{(30\ln 2 + 3\ln 3)}_{24.0902} p^3 + \underbrace{(-254\ln 2 + 87\ln 3 + 20\ln 5)}_{-48.2913} p^4 + \mathcal{O}(p^5) \tag{3.10b}$$

$$m_+(p) = 1 - 20p^3 - 608p^4 + \mathcal{O}(p^5) \tag{3.10c}$$

$$m(p) = 1 - 88p^3 - \underbrace{4244/5}_{848.8}\, p^4 + \mathcal{O}(p^5) \tag{3.10d}$$

$$m_-(p) = 1 - 154p^3 - 980p^4 + \mathcal{O}(p^5)\,. \tag{3.10e}$$

We wish to emphasize that an alternative method has been used in order to check all the above series, based on an expansion of the invariant distribution of the prefactors $A_n^{\varepsilon_1,\varepsilon_2}$ introduced in (3.4), and of similar quantities, along the lines of [14].

We have extended the enumeration technique to another observable of interest in the theory of error-correcting codes. For Ruján's FTD scheme, Nishimori [9] showed that the average error per bit reads in the thermodynamical limit

$$p_e = \tfrac{1}{2}(1 - S) \qquad \text{with} \quad S = \overline{\text{sign}(m_n)_{T=1}}\,. \tag{3.11}$$

Because of the peculiar dependence on p of the Boltzmann weight at unit temperature (see equation (2.10)), $\exp[-2J(p)] = p/(1-p)$, the FTD problem can also be dealt with by means of the enumeration scheme. It involves a few extra terms in the expansion of physical quantities, as compared with the zero-temperature expansion. Indeed, some of the low-lying excited states of the Hamiltonian $\mathcal{H}'_K(\sigma)$ with, for example, three impurity couplings, may give rise to contributions to the average defining S. Our final result reads

$$S = 1 - 86p^3 + \mathcal{O}(p^4)\,. \tag{3.12}$$

4. Numerical simulations and discussion

We now turn to a quantitative comparison of the analytical predictions derived in section 3 with the outcomes of numerical simulations.

Firstly, we have simulated the encoding model both for the MED ($T = 0$) procedure, by means of the zero-temperature transfer-matrix algorithm (Viterbi algorithm), and for Ruján's FTD ($T = 1$) procedure, using the finite-temperature transfer-matrix algorithm. The typical length of the input messages is of order 10^5 bits, and the error bars are obtained by averaging over up to 500 independent realizations, depending on the value of p.

Our data concerning the average error per bit p_e associated with the inferred messages are shown in figure 4, for both MED and FTD. In the first place, it is worth noticing that our data are far more accurate than those of previous simulations [8]. The numerical simulations become more and more difficult as $p \to 0$, because the rate of errors in decoded messages is extremely low. Indeed there is only an error of around 1.5 on average for an input message of length 3×10^5 bits and for $p = 0.005$ (the mean number of errors without encoding being 1500). We have nevertheless been able to obtain reliable estimates of p_e for values of p as small as $p = 0.0075$, i.e. roughly one order of magnitude better than previous works.

In the whole range of interest ($p \leqslant 0.15$) the frequency of errors is only slightly smaller for FTD than for MED. In the small-p regime a quantitative comparison between analytical and numerical results is possible. A least-squares fit of all data in the range $p \leqslant 0.03$ yields

$$\begin{aligned} p_e &\approx (43.67 \pm 0.48)p^3 + (423.6 \pm 19.2)p^4 \qquad \text{(MED)} \\ p_e &\approx (42.86 \pm 0.40)p^3 + (307.2 \pm 15.9)p^4 \qquad \text{(FTD)} \end{aligned} \tag{4.1}$$

in excellent agreement with the outcomes of the analytical small-p expansions (3.10d), (3.12), namely

$$\begin{aligned} p_e &= 44p^3 + 424.4p^4 + \mathcal{O}(p^5) \qquad \text{(MED)} \\ p_e &= 43p^3 + \mathcal{O}(p^4) \qquad \text{(FTD)}\,. \end{aligned} \tag{4.2}$$

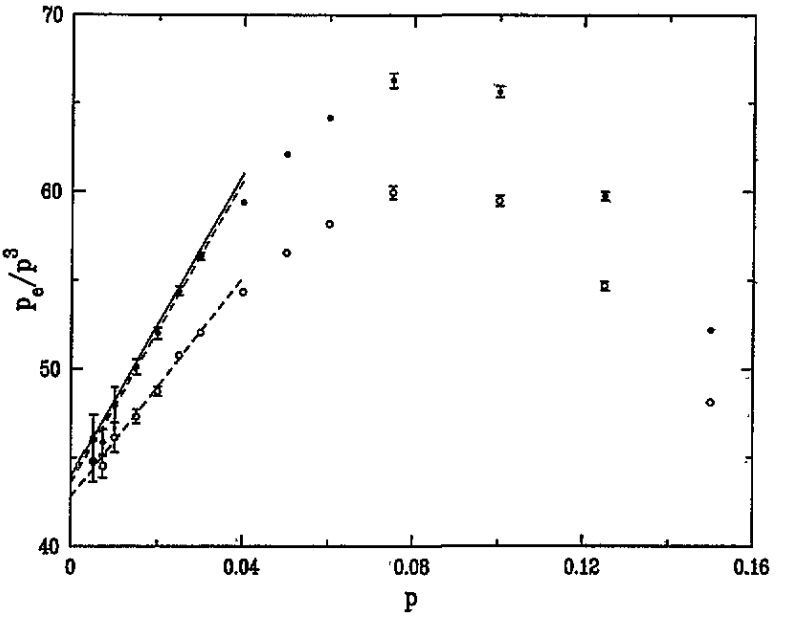

Figure 4. Results of numerical simulations concerning the ratio p_e/p^3, with p_e being the average error per bit for the MED (full symbols) and FTD (open symbols) approaches. The small-p expansion (4.2) for MED is shown as a full line, whereas the broken lines show the fits (4.1).

The leading behaviour $p_e \approx 44p^3$ for the probability of error per bit in MED improves in a significant way a previously known upper bound [3], scaling as $p^{5/2}$ for $p \to 0$.

The data shown in figure 4 also allow us to evaluate the threshold probability p_0 such that $p_e(p_0) = p_0$. We then have $p_e(p) < p$ for $p < p_0$ (the encoding procedure improves transmission), whereas $p_e(p) > p$ for $p > p_0$ (the encoding procedure worsens transmission, and thus becomes useless). We obtain two very similar threshold values for both decoding procedures, namely

$$\begin{aligned} p_0 &\approx 0.13 \qquad \text{(MED)} \\ p_0 &\approx 0.14 \qquad \text{(FTD)} \end{aligned} \tag{4.3}$$

the first value being in full agreement with that of [8].

Secondly, we have evaluated the full dependence on p of the zero-temperature entropy S_0, by means of a numerical iteration of the linear recursion relations, which can be derived for the four amplitudes $A_n^{\varepsilon_1,\varepsilon_2}$ introduced in (3.4). As a check of this approach we recover the ground-state energy $E_0'(p)$ given in (3.7) and (3.8), within an error of the order of 5×10^{-4}. The data concerning $S_0(p)$ are shown on figure 5. A quantitative agreement with the analytical prediction (3.10*b*) is only observed for $p \leqslant 0.05$. In the opposite limit ($p \to 1$), the entropy is found to vanish steeply, as $S_0(p) \approx \frac{1}{2}(1-p)\ln(1-p)$. This behaviour is a common characteristic feature of many 1D random magnetic models with diluted disorder, such as the random-field Ising chain [13, 14]. Finally, just like the ground-state energy, the zero-temperature entropy exhibits a very flat plateau near $p = \frac{1}{2}$, around the value $S_0(1/2) \approx 0.0284$.

To sum up this work, we have shown how to obtain analytical results about the ground-state energy and related zero-temperature properties of a simple error-correcting code. We

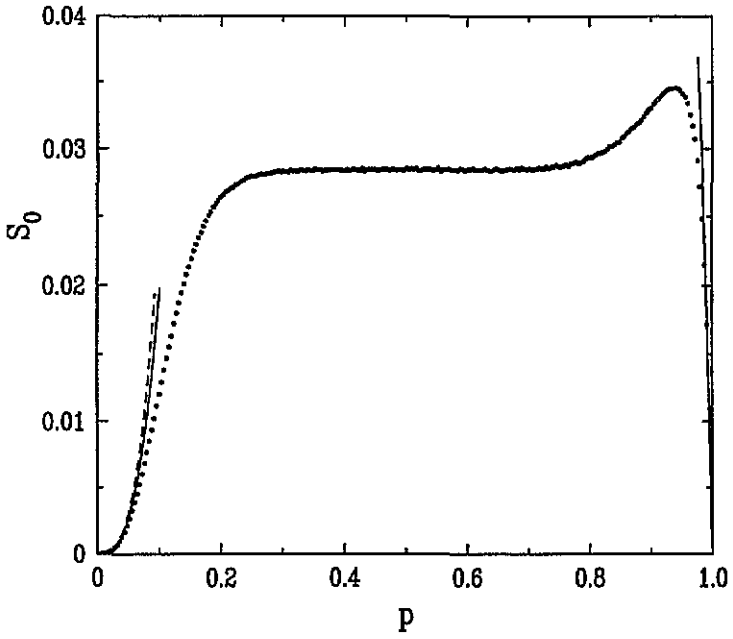

Figure 5. Plot of the zero-temperature entropy $S_0(p)$. Circles: numerical determination explained in the text. Full curve near $p = 0$: equation (3.10*b*). Broken curve near $p = 0$: *first term of (3.10b). Full curve near* $p = 1$: *logarithmic estimate given in the text.*

aim [17] at extending the present results to the more general situation where the two-spin and three-spin couplings have two different binary distributions, characterized by different magnitudes, and/or different probability weights. We also hope to extend the scope of the present paper to error-correcting codes commonly used in telecommunications, by means of the enumeration approach used to generate systematic power series in the level of noise p, although calculations will become more tedious for convolution codes with larger ranges.

Acknowledgments

One of us, CD, is very indebted to Nicolas Sourlas for introducing him to the area of error-correcting codes and their relationship with spin glasses. He would also like to thank CEA for their hospitality. Lorenzo Bergomi is warmly acknowledged for his careful reading of the manuscript. This work has been partly supported by a *Contrat de Formation Recherche* from Ecole Polytechnique.

References

[1] Shannon C E 1948 *Bell Syst. Tech. J.* **27** 379, 623
[2] Shannon C E and Weaver W 1962 *The Mathematical Theory of Communication* (University of Illinois Press)
[3] McEliece R J 1977 The theory of information and coding *Encyclopedia of Mathematics and its Applications* vol 3 (Reading, MA: Addison-Wesley)
[4] Clarck G C and Cain J B 1981 *Error-correction Coding for Digital Communication* (New York: Plenum)
[5] Sourlas N 1993 *Preprint* LPTENS 93/4
[6] Sourlas N 1989 *Nature* **339** 693

[7] Derrida B 1981 *Phys. Rev.* B **24** 2613
[8] Ruján P 1993 *Phys. Rev. Lett.* **70** 2968
[9] Nishimori H 1994 *Proc. 2nd Taipei Int. Symp. on Statistical Physics Physica* **205A** 1
[10] Sourlas N 1994 *Europhys. Lett.* **25** 159
[11] Nishimori H 1980 *J. Phys. C: Solid State Phys.* **13** 4071; 1981 *Prog. Theor. Phys.* **66** 1169
[12] Derrida B, Vannimenus J, and Pomeau Y 1978 *J. Phys. C: Solid State Phys.* **11** 4749
[13] Luck J M 1992 *Systèmes Désordonnés Unidimensionnels* (Collection Aléa-Saclay)
[14] Luck J M, Funke M, and Nieuwenhuizen Th M 1991 *J. Phys. A: Math. Gen.* **24** 4155
[15] Itzykson C and Luck J M 1985 *Proc. 1983 Brasov School Conf. on Critical Phenomena—Theoretical Aspects* (*Progress in Physics*) vol 11 (Boston: Birkhäuser)
[16] Domb C and Green M S (eds) 1974 *Phase Transitions and Critical Phenomena* vol 3 (London: Academic)
[17] Dress C 1995 *Thesis* University Paris VI to appear