Eur. Phys. J. B **18**, 121–136 (2000)

THE EUROPEAN PHYSICAL JOURNAL B

EDP Sciences

Turbo codes: the phase transition

A. Montanari[a,b]

Scuola Normale Superiore and INFN – Sezione di Pisa, 56100 Pisa, Italy

Received 14 March 2000

Abstract. Turbo codes are a very efficient method for communicating reliably through a noisy channel. There is no theoretical understanding of their effectiveness. In reference [1] they are mapped onto a class of disordered spin models. The analytical calculations concerning these models are reported here. We prove the existence of a no-error phase and compute its local stability threshold. As a byproduct, we gain some insight into the dynamics of the decoding algorithm.

PACS. 75.10.Hk Classical spin models – 75.10.Nr Spin-glass and other random models – 89.70.+c Information science

1 Introduction

Communication through a noisy channel is a central problem in Information Theory [2]. Error correcting codes are a widespread method for compensating the information corruption due to the noise, by cleverly increasing the redundancy of the message. Turbo codes [3–5] are a recently invented class of error correcting codes with nearly optimal performances. They allow reliable communication (*i.e.* very low error per bit probability) with practical communication rates.

It is known, since the work of Sourlas [6–9], that there exists a close relationship between the statistical behavior of error correcting codes and the physics of some disordered spin models. Recently the tools developed in statistical physics have been employed in studying Gallager-type codes [10–12].

In reference [1] the equivalence discovered by Sourlas is extended to turbo codes, and the basic features of the corresponding spin models are outlined. A remarkable property of a large family of turbo codes, presented in reference [1], is the existence of a no-error phase. In other words the error probability per bit vanishes beyond some critical (finite) signal to noise ratio. In reference [1] some intuitive arguments supporting this thesis are given. Some analytical results concerning the critical value of the signal to noise ratio are announced without giving any derivation. These results are compared with numerical simulations.

In this paper we present the analytical results in their full generality, and explain their derivation. We prove the existence of the no-error phase and find the condition for its local stability. This condition is derived in two different approaches. In the first one we study the asymptotic dynamics of the decoding algorithm. In the second approach we use replicas and establish the condition for stability in the full replica space. Local stability is a necessary but not sufficient condition for the stability of the no-error phase. The critical signal to noise ratio obtained from local stability is the correct one only if the phase transition is a second order one: in the general case it is only a lower bound.

The spin models which are equivalent to turbo codes have the following statistical weight [1]:

$$\mathcal{P}(\boldsymbol{\sigma}^{(1)},\boldsymbol{\sigma}^{(2)}|\mathbf{J},\beta) \equiv \frac{1}{Z(\mathbf{J},\beta)}\,\mathrm{e}^{-\beta\sum_{k=1}^{2}H^{(k)}(\boldsymbol{\sigma}^{(k)})} \times\prod_{i=1}^{N}\delta\left(\epsilon_{\rho(i)}(\boldsymbol{\sigma}^{(1)}),\epsilon_i(\boldsymbol{\sigma}^{(2)})\right), \quad (1.1)$$

$$H^{(k)}(\boldsymbol{\sigma}) \equiv -\sum_{i=1}^{N}J_i^{(k)}\epsilon_i(\boldsymbol{\sigma}) - \sum_{i=1}^{N}h_i^{(k)}\eta_i(\boldsymbol{\sigma}), \quad (1.2)$$

where $\delta(\cdot,\cdot)$ is the Kronecker δ function. The dynamical variables of the model are the $2N$ spins $\boldsymbol{\sigma}^{(k)} \equiv \{\sigma_1^{(k)},\dots,\sigma_N^{(k)}\}$ with $k = 1, 2$. They are divided in two chains $\boldsymbol{\sigma}^{(1)}$ and $\boldsymbol{\sigma}^{(2)}$ of length N. We shall choose them to be Ising spins[1], that is $\sigma_i^{(k)} = \pm 1$. The spins enter in the Hamiltonians $H^{(k)}(\boldsymbol{\sigma})$ through the local interaction terms $\epsilon_i(\boldsymbol{\sigma})$ and $\eta_i(\boldsymbol{\sigma})$ which are products of σ's. Their exact form can be encoded in two set of numbers $\kappa(j;1) = 0$ or 1, and $\kappa(j;2) = 0$ or 1 with $j = 0,\dots,r$, as follows: $\epsilon_i(\boldsymbol{\sigma}) \equiv \prod_{j=0}^{r}\sigma_{i-j}^{\kappa(j;1)}$ and $\eta_i(\boldsymbol{\sigma}) \equiv \prod_{j=0}^{r}\sigma_{i-j}^{\kappa(j;2)}$. In order to fix

[a] e-mail: montanar@cibs.sns.it

[b] *Present address:* Laboratoire de Physique Théorique de l'École Normale Supérieure, 24 rue Lhomond, 75231 Paris Cedex 05, France.

[1] This corresponds to considering codes which work with a binary alphabet.

completely our notation we set $\kappa(0;1) = \kappa(0;2) = 1$. Notice that the two Hamiltonians $H^{(1)}(\boldsymbol{\sigma}^{(1)})$ and $H^{(2)}(\boldsymbol{\sigma}^{(2)})$ have the same structure but different (random) couplings: $\{J_i^{(1)}; h_i^{(1)}\}$ for $H^{(1)}$, and $\{J_i^{(2)}; h_i^{(2)}\}$ for $H^{(2)}$. The δ function enforces the constraints $\epsilon_{\rho(i)}(\boldsymbol{\sigma}^{(1)}) = \epsilon_i(\boldsymbol{\sigma}^{(2)})$ for $i = 1, \ldots, N$, ρ being a random permutation of N objects. The quenched variables are listed below.

- The couplings $\mathbf{J} \equiv \{J_i^{(k)}; h_i^{(k)}\}$, whose distribution $\mathcal{P}(\mathbf{J}) \equiv \prod_{i=1}^{N} \prod_{k=1}^{2} P_J(J_i^{(k)})\ P_h(h_i^{(k)})$ satisfies the conditions $\int \mathrm{d}J_i^{(k)}\ P_J(J_i^{(k)})\ J_i^{(k)} > 0$ and $\int \mathrm{d}h_i^{(k)}\ P_h(h_i^{(k)})\ h_i^{(k)} > 0$. A typical choice is to take P_J and P_h Gaussian with positive mean. In the following we shall drop the subscripts in P_J and P_h.
- The permutation $\rho : \{1, \ldots, N\} \to \{1, \ldots, N\}$, which has uniform distribution: any of the $N!$ permutations of N objects is taken with the same probability $(1/N!)$.

It is useful to keep in mind an example of such models. A very simple example is constructed by taking $\kappa(0;1) = \kappa(1;1) = 1$, $\kappa(j;1) = 0$ for $j \geq 2$, and $\kappa(0;2) = 1$, $\kappa(j;2) = 0$ for $j \geq 1$. This yields $\epsilon_i(\boldsymbol{\sigma}) = \sigma_i \sigma_{i-1}$ and $\eta_i(\boldsymbol{\sigma}) = \sigma_i$. This example will be reconsidered in Section 3. The probability distribution (1.1) becomes in this case

$$\mathcal{P}_{\mathrm{ex}}(\boldsymbol{\sigma}^{(1)}, \boldsymbol{\sigma}^{(2)} | \mathbf{J}, \beta) \equiv \frac{1}{Z(\mathbf{J}, \beta)}\, \mathrm{e}^{-\beta \sum_{k=1}^{2} H^{(k)}(\boldsymbol{\sigma}^{(k)})} \times \prod_{i=1}^{N} \delta\left(\sigma_{\rho(i)}^{(1)} \sigma_{\rho(i)-1}^{(1)}, \sigma_i^{(2)} \sigma_{i-1}^{(2)}\right), \tag{1.3}$$

$$H_{\mathrm{ex}}^{(k)}(\boldsymbol{\sigma}) \equiv -\sum_{i=1}^{N} J_i^{(k)} \sigma_i \sigma_{i-1} - \sum_{i=1}^{N} h_i^{(k)} \sigma_i. \tag{1.4}$$

In this example each one the two Hamiltonians $H^{(1)}(\boldsymbol{\sigma}^{(1)})$ and $H^{(2)}(\boldsymbol{\sigma}^{(2)})$ describes a one-dimensional Ising model with random nearest-neighbour interactions and random magnetic field. However, the two spin chains $\boldsymbol{\sigma}^{(1)}$ and $\boldsymbol{\sigma}^{(2)}$ are not independent due to the δ function constraints, see equation (1.3), which impose $\sigma_{\rho(i)}^{(1)} \sigma_{\rho(i)-1}^{(1)} = \sigma_i^{(2)} \sigma_{i-1}^{(2)}$ for any $i = 1, \ldots, N$. With appropriate boundary conditions, this constraints allow to determine the spin variables $\sigma_i^{(1)}$, for $i = 1, \ldots, N$, once the configuration $\boldsymbol{\sigma}^{(2)}$ has been fixed (and *vice versa*). The independent spin degrees of freedom are only N rather than $2N$. This is a general feature of the models (1.1): it holds for any non-trivial choice of $\epsilon_i(\boldsymbol{\sigma})$. Nevertheless it is convenient to use the redundant formulation of the model adopted in equations (1.1, 1.2), *i.e.* in terms of both $\boldsymbol{\sigma}^{(1)}$ and $\boldsymbol{\sigma}^{(2)}$.

We shall impose a fixed boundary condition at one end of the chain (*i.e.* $\sigma_i^{(k)} = +1$ for $i \leq 0$ and $k = 1, 2$) and a free boundary condition at the other end. The model is composed by two one-dimensional substructures (chains), which interact through the Kronecker delta functions in equation (1.1). When the average over permutations is taken into account this interaction turns into a mean field one. This interplay between the two subsystems, each one possessing a one-dimensional structure, and the mean field interaction which couples them is clearly displayed by the analytical calculations. For further explanations on equations (1.1, 1.2) and their motivation we refer to [1].

The paper is organised as follows. In Sections 2 and 3 we present a first derivation of the stability condition. We write a "mean field" equation which describes the dynamics of the decoding algorithm (Sect. 2), we show that it possesses a no-error fixed point and then study its behavior in a neighbourhood of this fixed point (Sect. 3). Thanks to this derivation we will understand how this fixed point is reached. In Section 4 replicas are introduced in order to compute the average over the permutations. We exhibit the no-error saddle point. In Section 5 the stability of the no-error saddle point is studied by diagonalizing the second derivative of the free energy. Finally in Section 6 the validity of our calculations is discussed. Appendix A collects some useful (although simple) facts of algebra. In Appendix B the type of integral equations which appear in Section 3 is studied in detail. Finally in Appendix C we describe the derivation of the replicated partition function, which is the first step of Section 4.

2 A "mean field" equation for the decoding algorithm

Some properties concerning the models defined by equations (1.1, 1.2) can be obtained by considering the "turbo decoding" algorithm and making some factorization hypothesis. These hypothesis enable us to obtain a recursive integral equation for the probability distribution of a local field. They can be justified on heuristic grounds and arguments of this kind will be given later in this section. Moreover the replica calculation presented in the Section 4 does support our arguments. In particular this approach allows us to derive the critical noise below which "perfect" decoding is possible.

Turbo decoding is an iterative algorithm. The iteration variables are the fields $\boldsymbol{\Gamma}^{(k)} \equiv \{\Gamma_1^{(k)}, \ldots, \Gamma_N^{(k)}\}$ with $k = 1, 2$. The step t of the turbo decoding algorithm is defined as follows [1]:

$$\Gamma_i^{(1)}(t+1) = \frac{1}{\beta} \mathrm{arctanh}\left[\langle \epsilon_{\rho^{-1}(i)}(\boldsymbol{\sigma}) \rangle_{\Gamma^{(2)}(t)}^{(2)}\right] - \Gamma_{\rho^{-1}(i)}^{(2)}(t), \tag{2.1}$$

$$\Gamma_i^{(2)}(t+1) = \frac{1}{\beta} \mathrm{arctanh}\left[\langle \epsilon_{\rho(i)}(\boldsymbol{\sigma}) \rangle_{\Gamma^{(1)}(t)}^{(1)}\right] - \Gamma_{\rho(i)}^{(1)}(t)\,. \tag{2.2}$$

The expectation value $\langle \cdot \rangle_{\Gamma^{(k)}}^{(k)}$ is intended to be taken with respect to the Boltzmann weight with the modified Hamiltonian $H^{(k)}(\boldsymbol{\sigma}) - \sum_{i=1}^{N} \Gamma_i^{(k)} \epsilon_i(\boldsymbol{\sigma})$. The iteration variables $\Gamma_i^{(k)}$ should be interpreted as external fields conjugate to the operators $\epsilon_i(\boldsymbol{\sigma}^{(k)})$. They describe, in an approximate way, the action of each of the two chains on the other one.

In order to lighten the notation, let us write equations (2.1, 2.2) in the form:

$$\boldsymbol{\Gamma}^{(k)}(t+1) = F_\rho^{(k)}\left(\boldsymbol{\Gamma}^{(k')}(t), \mathbf{J}^{(k')}\right), \qquad (2.3)$$

with $k' = 2$ if $k = 1$, and $k' = 1$ if $k = 2$. Due to the randomness in the couplings $\mathbf{J}$, the fields $\boldsymbol{\Gamma}$ are random variables. Equation (2.3) implies an integral equation for the probability distribution of $\boldsymbol{\Gamma}$:

$$\mathcal{P}_{t+1}(\boldsymbol{\Gamma}^{(k)}) = \int \mathrm{d}\boldsymbol{\Gamma}^{(k')} \int \mathrm{d}\mathbf{J}^{(k')} \mathcal{P}_t(\boldsymbol{\Gamma}^{(k')}, \mathbf{J}^{(k')}) \times \delta\left[\boldsymbol{\Gamma}^{(k)} - F_\rho^{(k)}\left(\boldsymbol{\Gamma}^{(k')}, \mathbf{J}^{(k')}\right)\right]. \qquad (2.4)$$

Let us state a few approximations which allow us to reduce equation (2.4) to a much simpler one.

(1) We make the substitution $\mathcal{P}_t(\boldsymbol{\Gamma}^{(k')}, \mathbf{J}^{(k')}) \to \mathcal{P}_t(\boldsymbol{\Gamma}^{(k')})\mathcal{P}(\mathbf{J}^{(k')})$ in equation (2.4). This yields a closed integral equation describing the evolution of the distribution $\mathcal{P}_t(\boldsymbol{\Gamma}^{(k)})$.

(2) We neglect correlations between the fields at different sites:

$$\mathcal{P}_t(\boldsymbol{\Gamma}^{(k)}) \simeq \prod_{i=1}^N \pi_{i,t}^{(k)}(\Gamma_i^{(k)}|\rho), \qquad (2.5)$$

where we made explicit the dependence of the probability distributions $\pi_{i,t}^{(k)}$ upon the specific permutation ρ which defines the code.

These two hypothesis imply that equation (2.4) is equivalent to:

$$\pi_{i,t+1}^{(k)}(y|\rho) = \int_{-\infty}^{+\infty} \mathrm{d}\pi_t^{(k')}[\mathbf{x}|\rho] \times \int \mathrm{d}\mathcal{P}[\mathbf{J}] \delta\left(y - \frac{1}{\beta}\mathrm{arctanh}\left(\langle \epsilon_{\hat\rho(i)}(\boldsymbol{\sigma})\rangle_{\mathbf{J},\mathbf{x}}\right) + x_{\hat\rho(i)}\right), \qquad (2.6)$$

$$\mathrm{d}\pi_t^{(k')}[\mathbf{x}|\rho] \equiv \prod_{i=1}^N \mathrm{d}x_i\, \pi_{i,t}^{(k')}(x_i|\rho), \qquad (2.7)$$

where $\hat\rho$ is the appropriate permutation of $\{1,\dots,N\}$, *i.e.* $\hat\rho = \rho^{-1}$ if $k = 1$ and $\hat\rho = \rho$ if $k = 2$. The expectation value $\langle\cdot\rangle_{\mathbf{J},\mathbf{x}}$ on the right hand side of equation (2.6) has to be taken with respect to the Hamiltonian $H(\boldsymbol{\sigma}) \equiv -\sum_{i=1}^N (J_i + x_i)\epsilon_i(\boldsymbol{\sigma}) - \sum_{i=1}^N h_i\eta_i(\boldsymbol{\sigma})$.

Let us now define a field distribution averaged over the permutations and the sites:

$$\pi_t^{(k)}(x) \equiv \frac{1}{N!}\sum_\rho \frac{1}{N}\sum_{i=1}^N \pi_{i,t}^{(k)}(x|\rho). \qquad (2.8)$$

We can now state our last approximation.

(3) We make the substitution $\pi_{i,t}^{(k)}(x|\rho) \to \pi_t^{(k)}(x)$ on the right hand side of equation (2.6).

With this substitution, we can average equation (2.6) over ρ, obtaining a recursive equation for $\pi_t^{(k)}$:

$$\pi_{t+1}(y) = \frac{1}{N}\sum_{i=1}^N \int_{-\infty}^{+\infty} \mathrm{d}\pi_t[\mathbf{x}] \times \int \mathrm{d}\mathcal{P}[\mathbf{J}]\ \delta\left(y - \frac{1}{\beta}\mathrm{arctanh}\left(\langle\epsilon_i(\boldsymbol{\sigma})\rangle_{\mathbf{J},\mathbf{x}}\right) + x_i\right). \qquad (2.9)$$

The indices (k) and (k') have been dropped since we can define $\pi_t = \pi_t^{(1)}$ for t odd, and $\pi_t = \pi_t^{(2)}$ for t even, or *vice versa*. A byproduct of this heuristic derivation is the expression for the probability distribution of the expectation values $\langle\epsilon_i(\boldsymbol{\sigma})\rangle$ after t iterations of the turbo decoding algorithm: $\mathcal{P}_t(\epsilon) = \frac{1}{N}\sum_{i=1}^N \int_{-\infty}^{+\infty} \mathrm{d}\pi_t[\mathbf{x}] \int \mathrm{d}\mathcal{P}[\mathbf{J}]\ \delta\left(\epsilon - \langle\epsilon_i(\boldsymbol{\sigma})\rangle_{\mathbf{J},\mathbf{x}}\right)$.

Let us discuss the validity of the approximations made in deriving equation (2.9).

(1) and (2) These approximations should be accurate in the thermodynamic limit for a generic random permutation ρ. The reason is that the correlations produced by equations (2.1, 2.2) have short range: $\langle\epsilon_i(\boldsymbol{\sigma})\rangle$ and $\langle\epsilon_j(\boldsymbol{\sigma})\rangle$ have a significant correlation only if $|i-j|$ is less than some characteristic length. The random permutation ρ reshuffles the sites so that the correlation between two fields $\Gamma_i^{(k)}$ and $\Gamma_j^{(k)}$ is vanishing with high probability if $|i-j|$ is required to be "small". The correlations which "survive" (non vanishing only between "distant" sites) are irrelevant when computing the expectation values of local operators. In order to make this last assertion plausible, let us suppose that, for each site i, we can find a "large"[2] interval $[i - L(N), i + L(N)]$ of the chain, such that the correlations between the couplings inside the interval are negligible. The expectation value $\langle\epsilon_i(\boldsymbol{\sigma})\rangle_{\mathbf{J},\mathbf{x}}$ will not depend (as $N \to \infty$) upon the couplings outside $[i - L(N), i + L(N)]$ (this is always true in one dimension at non zero temperature) and can be then safely computed without taking into account the correlations. It is easy to find a similar argument concerning the correlations between $\boldsymbol{\Gamma}^{(k')}$ and $\mathbf{J}^{(k')}$ in equation (2.4).

(3) This is the probabilistic analogue of the replica symmetric approximation. Let us consider the fixed point equation $\pi_{t+1} = \pi_t$ corresponding to the dynamics defined by equation (2.9). It is remarkable that this fixed point equation coincides with the saddle point equation obtained by the standard replica method in the replica symmetric approximation (see Sect. 4). This fact confirms our conclusions about the relevance of the various approximations.

3 The behavior of the decoding algorithm

Equation (2.9) is the final outcome of our heuristic derivation. We want to study its behavior when the distribution

[2] Here "large" means that $\lim_{N\to\infty} L(N) = \infty$.

$\pi(x)$ is concentrated on large values of the field x, that is when the error probability is very small. In this regime the most relevant spin configuration satisfies $\epsilon_i(\boldsymbol{\sigma}) = +1$ for each $i = 1, \ldots, N$. The lowest excitations are such that $\epsilon_i(\boldsymbol{\sigma}) = -1$ only on a few sites. The first crucial point will be to understand that, for a class of Hamiltonians of the type (1.2) (which will be defined as "recursive"), the energy to be paid for flipping a single ϵ variable diverges in the thermodynamic limit. The second point will be to evaluate the energy to be paid for flipping two ϵ variables. In order to treat both these passages in full generality it is convenient to use an algebraic bookkeeping technique which we shall soon explain. The results concerning these two points will be useful again in Section 5.

A preliminary step consists in making the change of variables $X_i \equiv \mathrm{e}^{-2\beta x_i}$ and introducing the corresponding distribution function $Q_t(X)\mathrm{d}X = \pi_t(x)\mathrm{d}x$. Low X's correspond then to large local fields, *i.e.* to low error probability. The result is

$$Q_{t+1}(Y) = \frac{1}{N}\sum_{i=1}^{N}\int_0^\infty \mathrm{d}Q_t[\mathbf{X}] \times \int \mathrm{d}\mathcal{P}[\mathbf{J}]\ \delta\left(Y - \frac{1}{X_i}\,\frac{Z(\epsilon_i(\boldsymbol{\sigma}) = -1; \mathbf{J}, \mathbf{X})}{Z(\epsilon_i(\boldsymbol{\sigma}) = +1; \mathbf{J}, \mathbf{X})}\right), \quad (3.1)$$

where

$$Z(\epsilon_i(\boldsymbol{\sigma}) = \epsilon; \mathbf{J}, \mathbf{X}) \equiv Z_i(\epsilon) = \sum_{\boldsymbol{\sigma}:\epsilon_i(\boldsymbol{\sigma})=\epsilon} \mathrm{e}^{-\beta H(\boldsymbol{\sigma})} \prod_{k=1}^{N} X_k^{\frac{1}{2}(1-\epsilon_k(\boldsymbol{\sigma}))}, \quad (3.2)$$

with $H(\boldsymbol{\sigma}) = -\sum_i J_i\epsilon_i(\boldsymbol{\sigma}) - \sum_i h_i\eta_i(\boldsymbol{\sigma})$. Let us introduce some notations in order to write down the small X expansion of $Z_i(\epsilon)$: $(k_1, \ldots, k_l)$ is an l-uple (not ordered) of integers in $\{1, \ldots, i-1, i+1, \ldots, N\}$; $\boldsymbol{\sigma}_0$ is the configuration such that $\epsilon_i(\boldsymbol{\sigma}) = +1$ for all the sites i; $\boldsymbol{\sigma}(k, l, m, \ldots)$ is the configuration such that $\epsilon_j(\boldsymbol{\sigma}) = -1$ if $j = k, l, m, \ldots$ and $\epsilon_j(\boldsymbol{\sigma}) = 1$ otherwise (there is at most one such configuration once the boundary conditions have been specified); $E_0 \equiv H(\boldsymbol{\sigma}_0)$ is the energy of the ordered configuration; finally $\Delta(k, l, m, \ldots) \equiv H(\boldsymbol{\sigma}(k, l, m, \ldots)) - H(\boldsymbol{\sigma}_0)$. The following expressions are straightforward:

$$Z_i(+1) = \mathrm{e}^{-\beta E_0}\sum_{l=0}^{N-1}\sum_{(k_1,\ldots,k_l)} X_{k_1}\ldots X_{k_l}\mathrm{e}^{-\beta\Delta(k_1,\ldots,k_l)}, \quad (3.3)$$

$$Z_i(-1) = X_i\mathrm{e}^{-\beta E_0}\sum_{l=0}^{N-1}\sum_{(k_1,\ldots,k_l)} X_{k_1}\ldots X_{k_l}\mathrm{e}^{-\beta\Delta(i,k_1,\ldots,k_l)}. \quad (3.4)$$

The "bookkeeping technique" which we shall adopt in treating the above expansions consists in using the algebra of "generating polynomials" [1]. This approach allows us to consider a general Hamiltonian of the type (1.2). Let us define the following polynomials on $\mathbb{Z}_2$: $G(x) \equiv \sum_{j=1}^{\infty} G_j x^j$, with $\sigma_j = (-1)^{G_j}$; $g_n(x) = \sum_{j=0}^{r}\kappa(j;n)x^j$; $\mathcal{G}^{(n)}(x) \equiv g_n(x)\cdot G(x) \equiv \sum_{j=1}^{\infty}\mathcal{G}_j^{(n)}x^j$. Notice that the boundary condition on $\boldsymbol{\sigma}$ can be translated as follows: $G(x)$ is a series of strictly positive powers of x.

It is necessary to distinguish two types of models: in the first case $g_1(x)$ divides $g_2(x)$, *i.e.* $g_2(x)/g_1(x)$ is a polynomial (these are the "non recursive" models, a particular case being $\epsilon_i(\boldsymbol{\sigma}) = \sigma_i$); in the second one $g_1(x)$ does not divide $g_2(x)$, *i.e.* $g_2(x)/g_1(x)$ is a series ("recursive" models).

We shall treat the "recursive" models first. In this case the first order terms in the expansions (3.3, 3.4) are exponentially small in the size. In order to prove this assertion, let us consider the configuration $\boldsymbol{\sigma}(l)$. The relevant generating polynomials are $\mathcal{G}^{(1)}(x) = x^l$ and $\mathcal{G}^{(2)}(x) = x^l g_2(x)/g_1(x)$. The form of $\mathcal{G}^{(2)}(x)$ is given by the following result of algebra

Lemma 3.1 Let $g(x)$ and $f(x)$ be two polynomials on $\mathbb{Z}_2$ such that $g(0) = f(0) = 1$, $f(x) \not\equiv 1$, and their greatest common divisor $\gcd(f(x), g(x))$ is equal to 1. Then there exists an integer ω such that $g(x)/f(x) = \sum_{n=0}^{\infty} x^{n\omega}p_n(x)$ with $\deg[p_n(x)] < \omega$ and $p_n(x) = p_\infty(x) \neq 0$ if n is large enough. Hereafter we shall call $\omega(f)$ the smallest of such integers.

An explicit expression for $\omega(f)$ is given in the Appendix A. The Lemma 3.1 applies to our case if we divide both $g_1(x)$ and $g_2(x)$ by their greater common divisor: $f_k(x) \equiv g_k(x)/\gcd(g_1(x), g_2(x))$, so that $\gcd(f_1(x), f_2(x)) = 1$. It implies that if we write down the numbers $\eta_j(\boldsymbol{\sigma}(i)) = \pm 1$ we get an antiperiod followed by a non trivial periodic sequence with period $\omega(f_1)$. Let us consider a site "in the bulk": $N\delta < i < N(1-\delta)$ with δ a (small) positive number. Then, using the convention $h_j = 0$ for $j > N$, we get:

$$\Delta(i) = 2J_i + 2\sum_{j=1}^{N}\mathcal{G}_j^{(2)}h_j = 2J_i + 2\sum_{n=0}^{\infty}\sum_{k=0}^{\omega(f_1)-1} p_{n,k}h_{i+n\omega(f_1)+k}, \quad (3.5)$$

which diverges almost surely in the thermodynamic limit if $\langle h\rangle > 0$ (see the introduction on this point). In equation (3.1) we must sum also terms which are "near" the boundaries, *i.e.* $i \leq N\delta$ or $i \geq N(1-\delta)$. These give however a negligible contribution.

Let us now consider the second order terms of the expansions (3.3, 3.4). They involve configurations $\boldsymbol{\sigma}(k, l)$ with two flipped $\epsilon(\boldsymbol{\sigma})$'s. The only configurations which give a non negligible contribution are the ones which involve a finite (in the $N \to \infty$ limit) number of flipped $\eta(\boldsymbol{\sigma})$'s. This corresponds to choosing k and l such that $(x^k + x^l)g_2(x)/g_1(x)$ is a polynomial (and not an infinite series). The following useful result is proved in the Appendix A.

Lemma 3.2 Let $f(x)$ be a polynomial on $\mathbb{Z}_2$ such that $f(0) = 1$ and k an integer. Then there exists an integer $\omega(f)$ such that $f(x)$ divides $1 + x^k$ if and only if k is a strictly positive multiple of $\omega(f)$.

As suggested by the notation the $\omega(f)$'s cited in Lemmas 3.1 and 3.2 are indeed equal. The terms which give a non vanishing contribution at order X^2 in the expansions (3.3, 3.4) are the ones corresponding to configurations $\boldsymbol{\sigma}(k,l)$ such that $|k-l|$ is a multiple of $\omega(f_1)$. In order to evaluate these terms we must count the number of flipped $\eta(\boldsymbol{\sigma})$'s. This number is nothing but the number of non zero coefficients in the polynomial $(x^k+x^l)g_2(x)/g_1(x)$. Let us define the weight of a polynomial $p(x)=\sum_k p_k x^k$ over $\mathbb{Z}_2$ as the number of its non zero coefficients: $\text{weight}(p) \equiv \#\{p_k | p_k \neq 0\}$. The weight of $(x^k+x^l)g_2(x)/g_1(x)$ is given, for a large class of Hamiltonians, by the following lemma.

Lemma 3.3 Let $f(x)$ and $g(x)$ be two polynomial on $\mathbb{Z}_2$ such that $f(0)=g(0)=1$, $f(x)\not\equiv 1$, and $\gcd(f(x),g(x))=1$. If $\deg(g)\le\omega(f)$ then the weight of $s_m(x)\equiv(1+x^{m\omega(f)})g(x)/f(x)$ is given by $\text{weight}(s_m)=w_0(f,g)+w_1(f,g)m$ for each $m\ge 1$. The coefficients $w_0(f,g)$ and $w_1(f,g)$ are positive integers whose explicit expressions are given by equations (A.8, A.9).

Appendix A contains also an illustration of what could happen in the more general case.

By using Lemmas 3.2 and 3.3 we can linearize with respect to X the expression on the r.h.s. of equation (3.1):

$$\frac{1}{X_i}\,\frac{Z_i(-1)}{Z_i(+1)} = \sum_{m\neq 0} X_{i+m\omega(f_1)}\mathrm{e}^{-\beta\Delta(i,i+m\omega(f_1))} + O(X^2), \tag{3.6}$$

and defining $s_m(x) \equiv (1+x^{m\omega(f_1)})g_2(x)/g_1(x) = \sum_j s_{m,j}x^j$ we get

$$\Delta(k,l) = 2J_k + 2J_l + 2\sum_j s_{m,j}h_{\min(k,l)+j} \tag{3.7}$$

if $|k-l|=m\omega(f_1)$. Clearly equation (3.6) holds only for i in the "bulk" (*i.e.* $N\delta < i < (1-\delta)N$) up to terms which are exponentially small in the size N.

Our first important observation is that the right hand side of equation (3.6) vanishes if $X_k=0$ for $k=1,\dots,N$. This means that $Q_*(X)=\delta(X)$ is a fixed point of equation (3.1) for "recursive" models. Recall that the change of variables which yields equation (3.1) is $X=\mathrm{e}^{-2\beta x}$ and that x has the meaning of an effective field acting on $\epsilon_i(\boldsymbol{\sigma})$. The solution $Q_*(X)$ corresponds then to a phase with completely frozen spins: $\langle\epsilon_i(\boldsymbol{\sigma})\rangle=+1$.

We would like to understand if this phase is stable for some temperature β and some distribution of the couplings. A possible approach is to study the turbo decoding dynamics (as described by Eq. (3.1)) when starting from a distribution "near" $Q_*(X)$. Let us suppose that, for $Q_t(X)$ near enough to $Q_*(X)$, we can safely neglect $O(X^2)$ terms on the r.h.s. of equation (3.6):

$$Q_{t+1}(Y) = \frac{1}{N}\sum_{i=1}^{N}\int_0^\infty \mathrm{d}Q_t[\mathbf{X}] \times\int \mathrm{d}\mathcal{P}[\mathbf{J}]\;\delta\left(Y-\sum_{m\neq 0}X_{i+m\omega(f_1)}\mathrm{e}^{-\beta\Delta(i,i+m\omega(f_1))}\right). \tag{3.8}$$

This equation is very similar to a class of recursive equations which appear in a completely different context: polymers on disordered trees [13–17]. These are of the type

$$P_{t+1}(Z) = \int_0^\infty\prod_{i=1}^{K}\mathrm{d}Z_i\;P_t(Z_i) \times\int\rho(V_1,\dots,V_K)\,\mathrm{d}V_1\dots\mathrm{d}V_K\;\delta\left(Z-\sum_{i=1}^{K}\mathrm{e}^{-\beta V_i}Z_i\right). \tag{3.9}$$

The only non trivial difference is that the linear function of $\mathbf{X}$ appearing inside the delta function on the r.h.s. of equation (3.8) depends upon a macroscopic (indeed linear in N) number of X's. In equation (3.9), instead, only a finite number of variables appears: K is the coordination number of the tree minus one. Notice however that, for m large, $\Delta(i,i+m\omega(f_1)) \sim 2\,\text{weight}(s_m)\langle h\rangle \sim 2w_1(f_1,f_2)m\langle h\rangle$. We can thus truncate the sum in equation (3.8) to $m\le M$ by making an error of order $O(\mathrm{e}^{-cM})$ and we guess that the limit $M\to\infty$ can be taken at the end without problems[3].

Let us summarize some results of [13] which are useful in our discussion. It turns out that equation (3.9) is equivalent to a discretization of the Kolmogorov-Petrovsky-Piscounov (KPP) equation [18] (a well studied partial differential equation). Using this equivalence the large time limit of equation (3.9) is obtained:

$$P_t(X)\to\mathrm{e}^{-\beta c(\beta)t}\,\overline{P}(X\mathrm{e}^{-\beta c(\beta)t}), \tag{3.10}$$

corresponding to a wavefront solution of the KPP equation with front velocity $c(\beta)$. If we define the function

$$v(\beta) \equiv \frac{1}{\beta}\log\left(\sum_{i=1}^{K}\int\mathrm{d}V_1\dots\mathrm{d}V_K\;\rho(V_1,\dots,V_K)\,\mathrm{e}^{-\beta V_i}\right), \tag{3.11}$$

then the front velocity is given by the following construction:

$$c(\beta) = \begin{cases} v(\beta) & \text{if } \beta\le\beta_c\,,\\ v(\beta_c) & \text{if } \beta>\beta_c\,,\end{cases} \tag{3.12}$$

[3] This argument is not mathematically rigorous since it is not honest to use the central limit theorem in this case: we refer to Appendix B for more convincing arguments.

$$\mathrm{e}^{\beta v(\beta)} = \frac{2\left(\int \mathrm{d}J\ P(J)\ \mathrm{e}^{-2\beta J}\right)^2 \left(\int \mathrm{d}h\ P(h)\ \mathrm{e}^{-2\beta h}\right)^{w_0(f_1,f_2)+w_1(f_1,f_2)}}{1-\left(\int \mathrm{d}h\ P(h)\ \mathrm{e}^{-2\beta h}\right)^{w_1(f_1,f_2)}}\,. \tag{3.15}$$

with β_c given by

$$\left.\frac{\mathrm{d}}{\mathrm{d}\beta}\right|_{\beta_c} v(\beta) = 0\,. \tag{3.13}$$

At the critical temperature β_c a freezing phenomenon takes place with the front velocity sticking to its minimal value.

Let us apply these results to our case, *i.e.* to equation (3.8). The large time solution $Q_t(X) \sim \mathrm{e}^{-\beta c(\beta) t}\,\overline{Q}(X\mathrm{e}^{-\beta c(\beta)t})$ gives the correct behavior for $t\to\infty$ only if $c(\beta) < 0$. In this case $\lim_{t\to\infty} Q_t(X) = Q_*(X)$ and it is then correct to linearize equation (3.1): the frozen phase is stable. If, on the other hand, $c(\beta) \geq 0$ then we must take into account higher order terms in the low X expansion and the asymptotic form is no longer of the type defined by equation (3.10): the frozen phase is unstable.

In the thermodynamic limit we get

$$\begin{aligned}\mathrm{e}^{\beta v(\beta)} &= \sum_{m\neq 0} \int \mathrm{d}\mathcal{P}[\mathbf{J}]\mathrm{e}^{-\beta\Delta(i,i+m\omega(f_1))} \qquad (3.14)\\ &= 2\left(\int \mathrm{d}J\ P(J)\ \mathrm{e}^{-2\beta J}\right)^2 \\ &\quad\times \sum_{m=1}^{\infty}\left(\int \mathrm{d}h\ P(h)\ \mathrm{e}^{-2\beta h}\right)^{\mathrm{weight}(s_m)}\,.\end{aligned}$$

The front velocity $c(\beta)$ is obtained by applying the construction given in equations (3.12, 3.13) to equation (3.14). If the hypothesis of Lemma 3.3 are satisfied we can easily sum the series:

see equation (3.15) *above.*

We discuss now equation (3.15), the more general case being completely analogous. The series converges only if $\int \mathrm{d}h\ P(h)\ \mathrm{e}^{-2\beta h} < 1$. If $\int \mathrm{d}h\ P(h)\ h > 0$, as we supposed since the beginning, then convergence is assured for $0 < \beta < \beta_1$ with $\int \mathrm{d}h\ P(h)\ \mathrm{e}^{-2\beta_1 h} = 1$. It is easy to see that $\beta v(\beta)$ is strictly convex for $0 < \beta < \beta_1$ and thus $v(\beta)$ has either one global minimum or is strictly monotonic for $0 < \beta < \beta_1$. Since $\lim_{\beta\to 0^+} v(\beta) = \lim_{\beta\to\beta_1^-} v(\beta) = +\infty$ the first possibility is excluded and we conclude that $0 < \beta_c < \beta_1$. The important point is that the right hand side of equation (3.14) is well defined every time we need of it, *i.e.* for $0 < \beta < \beta_c$.

In applications to turbo codes a simplification occurs: we are interested in a particular temperature, $\beta = 1$, and we are left with a unique parameter: the signal to noise ratio $1/w^2$. Moreover the probability distributions of the couplings are fixed by the characteristics of the communication channel [1,6]. If we introduce the auxiliary variables $\hat{J}$ and $\hat{h}$, which correspond to the output of the channel, the probability distributions are obtained as follows

$$P(J)\ \mathrm{d}J = P(\hat{J}|+1)\ \mathrm{d}\hat{J} \quad \text{with} \quad J = \frac{1}{2}\log\frac{P(\hat{J}|+1)}{P(\hat{J}|-1)}, \tag{3.16}$$

where $P(\hat{J}|\tau)$ is the probability distribution of the output of the channel conditional to the input τ. A similar expression holds for h. If the channel is symmetric (*i.e.* if $P(\hat{J}|-1) = P(-\hat{J}|+1)$) one easily obtains $\beta_1 = 1$ and then $c(\beta = 1, w^2) = v(\beta_c, w^2)$. We can distinguish the two cases defined below.

- If $v(\beta, w^2) < 0$ for some $0 < \beta < 1$ then we are in the no-error phase and the turbo decoding algorithm converges to the message with "velocity" $c(\beta = 1, w^2) = \min_{0<\beta<1} v(\beta, w^2)$. We expect the condition $v(\beta_c, w^2) < 0$ to be verified in the "low noise" region $w^2 < w^2_{\mathrm{loc}}$.
- If $v(\beta, w^2) \geq 0$ in the interval $0 < \beta < 1$ then $c(\beta = 1, w^2) \geq 0$ and the linearization in equation (3.8) is no longer reliable. In this case $\pi_t(x)$ is expected to converge for $t\to\infty$ to some distribution supported on finite fields x. The decoded message will be plagued by a finite error probability per bit, no matter how many times do we iterate the turbo decoding algorithm.

Let us now study some examples. We consider a Gaussian channel with:

$$P(\hat{J}|\tau) = \frac{1}{(4\pi w^2)^{1/2}}\exp\left\{-\frac{(\hat{J}-\tau)^2}{4w^2}\right\}, \tag{3.17}$$

$$P(\hat{h}|\tau) = \frac{1}{(2\pi w^2)^{1/2}}\exp\left\{-\frac{(\hat{h}-\tau)^2}{2w^2}\right\}. \tag{3.18}$$

This choice of the variances is justified since it corresponds to a code with rate 1/3 (see Ref. [1]). It is useful to define the function

$$\begin{aligned} z(\beta, w^2) &= \int \mathrm{d}h\ P(h)\ \mathrm{e}^{-2\beta h} \\ &= \left(\int \mathrm{d}J\ P(J)\ \mathrm{e}^{-2\beta J}\right)^2 = \exp\left[\frac{2\beta(\beta-1)}{w^2}\right]. \end{aligned} \tag{3.19}$$

The three cases below have been already considered in reference [1]. We refer to the Appendix A for the calculation of the constants w_0 and w_1 to be used in equation (3.15).

(a) A model with nearest neighbours interaction is: $\epsilon_i(\boldsymbol{\sigma}) \equiv \sigma_i\sigma_{i-1}$ and $\eta_i(\boldsymbol{\sigma}) = \sigma_i$ (which corresponds to the generating polynomials $g_1(x) = 1 + x$ and $g_2(x) = 1$). This example has been already exhibited in the Introduction, see equations (1.3, 1.4). Using equation (3.15) and the fact that $w_0(f_1, f_2) = 0$ and $w_1(f_1, f_2) = 1$ we get

$$v(\beta, w^2) = \frac{1}{\beta} \log \frac{2z^2(\beta, w^2)}{1 - z(\beta, w^2)}. \qquad (3.20)$$

It is easy to see that $v(\beta, w^2) \geq 0$ for each $0 < \beta < 1$ if $w^2 \geq w^2_{\rm loc} = 1/\log 4$.

(b) For $\epsilon_i(\boldsymbol{\sigma}) \equiv \sigma_i\sigma_{i-1}\sigma_{i-2}$ and $\eta_i(\boldsymbol{\sigma}) = \sigma_i\sigma_{i-2}$ (generating polynomials: $g_1(x) = 1+x+x^2$ and $g_2(x) = 1+x^2$) we obtain $w_0(f_1, f_2) = 2$ and $w_1(f_1, f_2) = 2$ and then

$$v(\beta, w^2) = \frac{1}{\beta} \log \frac{2z^5(\beta, w^2)}{1 - z^2(\beta, w^2)}. \qquad (3.21)$$

Finally $w^2_{\rm loc} = -1/(2\log z_c)$ where z_c is the only real solution of the equation $2z^5 + z^2 = 1$.

(c) If we consider the model given by $\epsilon_i(\boldsymbol{\sigma}) \equiv \sigma_i\sigma_{i-1}\sigma_{i-2}\sigma_{i-3}\sigma_{i-4}$ and $\eta_i(\boldsymbol{\sigma}) = \sigma_i\sigma_{i-4}$ (generating polynomials: $g_1(x) = 1 + x + x^2 + x^3 + x^4$ and $g_2(x) = 1 + x^4$) we obtain $w_0(f_1, f_2) = 2$ and $w_1(f_1, f_2) = 2$ as in the previous example. Both $v(\beta, w^2)$ and $w^2_{\rm loc}$ coincide with the ones obtained above.

Let us make a few observations about the validity of our calculation. The threshold $w^2_{\rm loc}$ has been obtained by starting from a distribution $Q(X)$ very near to the "frozen" one $Q_*(X)$ and linearizing equation (3.1) in X. It must then be interpreted as a threshold for local stability of the "frozen" solution. Moreover, if we take seriously the heuristic derivation of equation (2.9), we can deduce something about the dynamics of the turbo decoding algorithm in the error-free phase: the probability distribution of the auxiliary fields $\Gamma^{(k)}_i(t)$ moves towards infinitely large fields with an average velocity $c(\beta, w^2)$. This conclusion is compared with numerical data in Figure 1: the agreement seems to be quite good. An interesting outcome of the previous calculation is that the approach to the perfect decoding becomes slower near to the critical signal to noise ratio.

Let us now discuss the "non recursive" models, that is models such that $g_1(x)$ divides $g_2(x)$. In this case the energy $\Delta(i)$ to be paid for flipping $\eta_i(\boldsymbol{\sigma})$ remains finite in the thermodynamic limit. The low X expansions in equations (3.3, 3.4) have a non vanishing term of order $O(X)$. This implies that $Q_*(X) = \delta(X)$ is no longer a fixed point of equation (3.1). Let us compute $\Delta(i)$. For "non recursive" models we can define the polynomial $s(x) \equiv \sum_k s_k x^k \equiv g_2(x)/g_1(x)$. It is easy to show that $\Delta(i) = 2J_i + 2\sum_k s_k h_{i+k}$. A simple approximation of the fixed point of equation (3.1) is:

$$Q_\infty(X) \sim \int {\rm d}J\ P(J) \times \int \prod_{i=1}^{w} {\rm d}h_i\ P(h_i)\, \delta\left(X - {\rm e}^{-2\beta J - 2\beta \sum_{i=1}^{w} h_i}\right), \qquad (3.22)$$

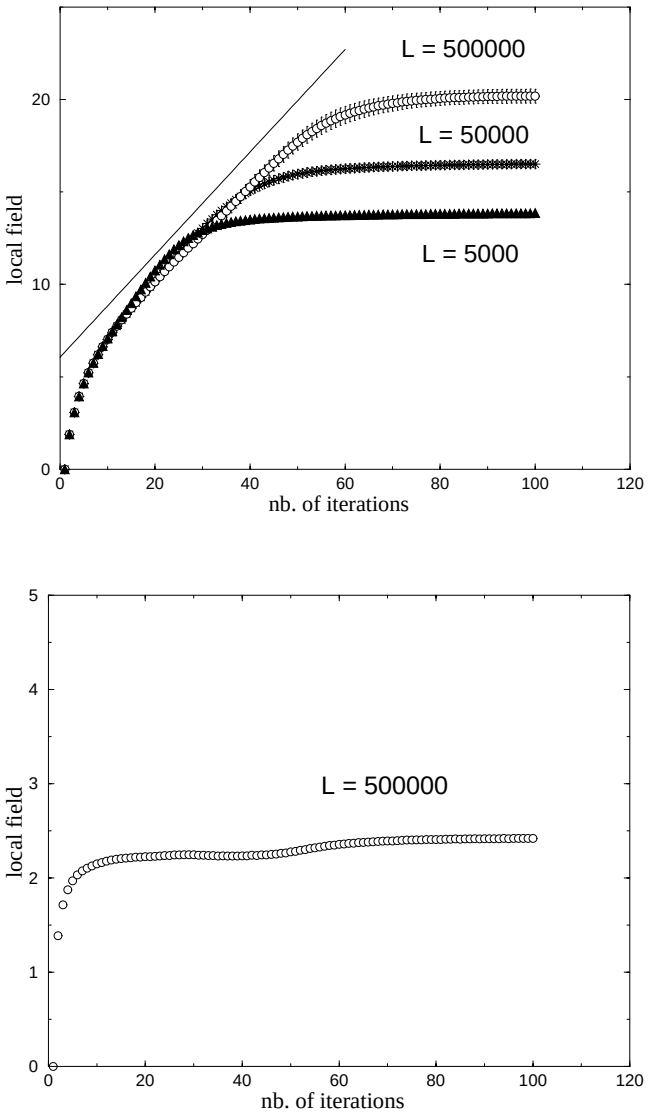

Fig. 1. The dynamics of the turbo decoding algorithm. The graph on the top gives the average of the local field Γ_i (see Eqs. (2.1, 2.2)) as a function of the number of iterations for different sizes of the system. The slope of the straight line on the same graph indicates the asymptotic velocity obtained in Section 3. The graph on the bottom gives the variance of the distribution of the local field.

with $w \equiv$ weight(s). This approximation is supposed to be good in the low noise region where we expect the distributions $Q_t(X)$ to be concentrated on small X's.

4 The replica calculation

The replica method [19] starts with the computation of the (integer) moments of the partition function. This can be done by introducing an appropriate order parameter (the choice is a matter of convenience) and by recurring

to standard tricks. Here we choose to use the (multi)-overlaps $q_{a_1\ldots a_l}$ and their complex conjugates $\hat{q}_{a_1\ldots a_l}$:

$$\overline{Z^n} = \int \frac{N}{\pi}\,\mathrm{d}q_0\,\mathrm{d}\hat{q}_0 \int \prod_a \frac{N}{\pi}\,\mathrm{d}q_a\,\mathrm{d}\hat{q}_a \times \int \prod_{(a,b)} \frac{N}{\pi}\,\mathrm{d}q_{ab}\,\mathrm{d}\hat{q}_{ab}\;\ldots\;\mathrm{e}^{-NS[q,\hat{q}]}, \quad (4.1)$$

$$S[q,\hat{q}] = -1 + q_0\hat{q}_0 + \sum_a q_a\hat{q}_a + \sum_{(a,b)} q_{ab}\hat{q}_{ab} + \ldots + n\log 2 + \beta\mathcal{F}_{1d,n}[q] + \beta\mathcal{F}_{1d,n}[\hat{q}], \quad (4.2)$$

$$\mathcal{F}_{1d,n}[q] \equiv -\lim_{N\to\infty}\frac{1}{N\beta}\log Z_{1d,n}[q], \quad (4.3)$$

$$Z_{1d,n}[q] \equiv \sum_{\{\sigma_i^a\}}\prod_{i=1}^N\left[q_0 + \sum_a q_a\epsilon_i(\boldsymbol{\sigma}^a) + \sum_{(a,b)} q_{ab}\epsilon_i(\boldsymbol{\sigma}^a)\epsilon_i(\boldsymbol{\sigma}^b) + \ldots\right] \times \int \mathrm{d}\mathcal{P}[\mathbf{J}]\exp\left\{-\beta\sum_a H(\boldsymbol{\sigma}^a;\mathbf{J})\right\}, \quad (4.4)$$

where $H(\boldsymbol{\sigma};\mathbf{J}) = -\sum_i J_i\epsilon_i(\boldsymbol{\sigma}) - \sum_i h_i\eta_i(\boldsymbol{\sigma})$, and the replica indices $a, b, \ldots$ run from 1 to n. For a detailed description of the manipulations which lead to equation (4.1) we refer to Appendix C.

The usual mean field models have no geometrical structure at all. In those cases the introduction of the order parameters leads to a (replicated) partition function which factorizes over the sites. In our case we are left with the problem of computing the one-dimensional partition functions $Z_{1d,n}[q]$. These correspond to the one-dimensional sub-structures which are not destroyed by the randomness of the model. The saddle point equations are easily written

$$\hat{q}_{a_1\ldots a_l} = \lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^N\left\langle\frac{\epsilon_i(\boldsymbol{\sigma}^{a_1})\cdot\cdots\cdot\epsilon_i(\boldsymbol{\sigma}^{a_l})}{[q_0 + \sum_a q_a\epsilon_i(\boldsymbol{\sigma}^a) + \ldots]}\right\rangle_q, \quad (4.5)$$

where the expectation values $\langle(\cdot)\rangle_q$, $\langle(\cdot)\rangle_{\hat{q}}$ are defined as follows

$$\langle(\,\cdot\,)\rangle_q \equiv \frac{1}{Z_{1d,n}[q]}\int \mathrm{d}\mathcal{P}[\mathbf{J}]\sum_{\{\sigma_i^a\}}(\,\cdot\,) \times\prod_{i=1}^N[q_0 + \sum_a q_a\epsilon_i(\boldsymbol{\sigma}^a) + \ldots]\;\mathrm{e}^{-\beta\sum_a H[\boldsymbol{\sigma}^a;\mathbf{J}]}. \quad (4.6)$$

In the recursive case equation (4.5) admits the following solution[4] corresponding to a no-error phase: $q^*_{a_1\ldots a_l} = \hat{q}^*_{b_1\ldots b_l} = 2^{-n/2}$. The free energy of this phase is $f_0(\beta) = -2\int \mathrm{d}J\;P(J)\;J - 2\int \mathrm{d}h\;P(h)\;h$. If we parametrize the replica symmetric ansatz as in reference [20]

$$q_{a_1\ldots a_l} = \int_{-\infty}^{+\infty}\mathrm{d}x\;\pi(x)\;\cosh^n(\beta x)\;\tanh^l(\beta x), \quad (4.7)$$

and analogously for $\hat{q}_{b_1\ldots b_m}$ (with a different distribution $\hat{\pi}(x)$), the following free energy functional can is obtained in the limit $n\to 0$:

$$f[\pi,\hat{\pi}] = \frac{1}{\beta}\int \mathrm{d}x\;\mathrm{d}y\;\pi(x)\hat{\pi}(y)\log\left[2\cosh(\beta x + \beta y)\right] + \mathcal{F}^{\mathrm{RS}}_{1d}[\pi] + \mathcal{F}^{\mathrm{RS}}_{1d}[\hat{\pi}], \quad (4.8)$$

$$\mathcal{F}^{\mathrm{RS}}_{1d}[\pi] \equiv -\lim_{N\to\infty}\frac{1}{\beta N}\int \mathrm{d}\mathcal{P}[\mathbf{J}]\int \mathrm{d}\pi[\mathbf{x}]\log Z^{\mathrm{RS}}_{1d}[\mathbf{J},\mathbf{x}], \quad (4.9)$$

$$Z^{\mathrm{RS}}_{1d}[\mathbf{J},\mathbf{x}] \equiv \sum_{\boldsymbol{\sigma}}\exp\left[\beta\sum_{i=1}^N(J_i + x_i)\epsilon_i(\boldsymbol{\sigma}) + \beta\sum_{i=1}^N h_i\eta_i(\boldsymbol{\sigma})\right]. \quad (4.10)$$

The distributions π and $\hat{\pi}$ are normalized ($\int \mathrm{d}x\;\pi(x) = \int \mathrm{d}y\;\hat{\pi}(y) = 1$) and satisfy the saddle point equation below:

$$\pi(y) = \lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^N\int_{-\infty}^{+\infty}\mathrm{d}\hat{\pi}[\mathbf{x}] \times\int \mathrm{d}\mathcal{P}[\mathbf{J}]\;\delta\left(y - \frac{1}{\beta}\mathrm{arctanh}\left(\langle\epsilon_i(\boldsymbol{\sigma})\rangle_{\mathbf{J},\mathbf{x}}\right) + x_i\right), \quad (4.11)$$

which is identical to the fixed point equation corresponding to equation (2.9), if we suppose the order parameters to be real at the saddle point.

Equation (4.11) is unpractical since it involves the unknown distributions $\pi(x)$ and $\hat{\pi}(x)$ infinitely many times. However due to the short range structure of the Hamiltonians defined in equation (1.2), it can be rewritten as a simple integral equation. Obviously the precise form of this equation depends upon the form of the Hamiltonian (1.2). In particular it becomes simpler as the range of the interaction becomes shorter. Let us illustrate this point by considering the model 3 of the previous section: $\epsilon_i(\boldsymbol{\sigma}) = \sigma_i\sigma_{i-1}$, $\eta_i(\boldsymbol{\sigma}) = \sigma_i$. We start by defining

[4] In fact there is a one parameter family of solutions which are degenerate. This fact is due to a (not very interesting) symmetry of the action (4.2): $S[q,\hat{q}] = S[\mathrm{e}^{\mathrm{i}\theta}q, \mathrm{e}^{-\mathrm{i}\theta}\hat{q}]$. However the integration over the parameter θ does not pose any problem. We shall fix this freedom by imposing q_0 to be real.

the following (right and left) partition functions:

$$Z^{(\mathrm{R})}_{i,M}(\sigma_i) \equiv \sum_{\sigma_{i+1}\dots\sigma_{i+M}} \exp\left[\beta \sum_{k=i+1}^{i+M} (J_k + x_k)\sigma_k\sigma_{k-1} + \beta \sum_{k=i}^{i+M} h_k\sigma_k\right], \quad (4.12)$$

$$Z^{(\mathrm{L})}_{i,M}(\sigma_i) \equiv \sum_{\sigma_{i-M}\dots\sigma_{i-1}} \exp\left[\beta \sum_{k=i-M+1}^{i} (J_k + x_k)\sigma_k\sigma_{k-1} + \beta \sum_{k=i-M}^{i} h_k\sigma_k\right], \quad (4.13)$$

and the (right and left) fields:

$$x_i^{\mathrm{R/L}} \equiv \lim_{M\to\infty} \frac{1}{2\beta} \log \frac{Z^{(\mathrm{R/L})}_{i,M}(+)}{Z^{(\mathrm{R/L})}_{i,M}(-)}. \quad (4.14)$$

We define now a new couple of order parameters, the probability distributions $\omega(x)$ and $\hat\omega(x)$ of the right (or left) fields:

$$\omega(x) = \int \prod_{i\geq 0} \mathrm{d}h_i\ P(h_i) \int \prod_{i\geq 1} \mathrm{d}J_i\ P(J_i) \times \int \prod_{i\geq 1} \mathrm{d}x_i\ \pi(x_i)\ \delta\left(x - x_0^{\mathrm{R}}[J_i; h_i; x_i]\right). \quad (4.15)$$

It is easy to show that, at the saddle point, $\omega(x)$ and $\hat\omega(x)$ satisfy the following integral equation:

$$\omega(z) = \int \mathrm{d}h\ P(h) \int \mathrm{d}J_1\ P(J_1) \int \mathrm{d}J_2\ P(J_2) \times \int \mathrm{d}x_1\ \hat\omega(x_1) \int \mathrm{d}x_2\ \hat\omega(x_2) \int \mathrm{d}z'\ \omega(z') \times \delta\left\{z - h - \Theta_\beta\left[z'; J_1 + J_2 + \Theta_\beta(x_1; x_2)\right]\right\}, \quad (4.16)$$

$$\Theta_\beta(x; y) \equiv \frac{1}{\beta} \mathrm{arctanh}[\tanh(\beta x)\tanh(\beta y)], \quad (4.17)$$

and that the solution of equation (4.11) is related to the solution of the previous equation as follows:

$$\pi(x) = \int \mathrm{d}J\ P(J) \int \mathrm{d}x_{\mathrm{L}}\ \hat\omega(x_{\mathrm{L}}) \times \int \mathrm{d}x_{\mathrm{R}}\ \hat\omega(x_{\mathrm{R}})\ \delta[x - J - \Theta_\beta(x_{\mathrm{R}}; x_{\mathrm{L}})]. \quad (4.18)$$

Equation (4.16) reduces to the Dyson Schmidt equation [21–23] for a one-dimensional model with nearest neighbour interaction if we keep the distribution $\hat\omega(x)$ fixed. The interaction between the two one-dimensional subsystems turns it into a nonlinear equation. Moreover equation (4.16) can be treated numerically more easily than equation (4.11). A possible approach consists in representing the unknown distribution as $\omega(x) = \sum_{j=1}^{K} \delta(x - x_j)$ and iterating equation (4.16) until a fixed point is reached. An example of this kind of computations is shown in Figure 2.

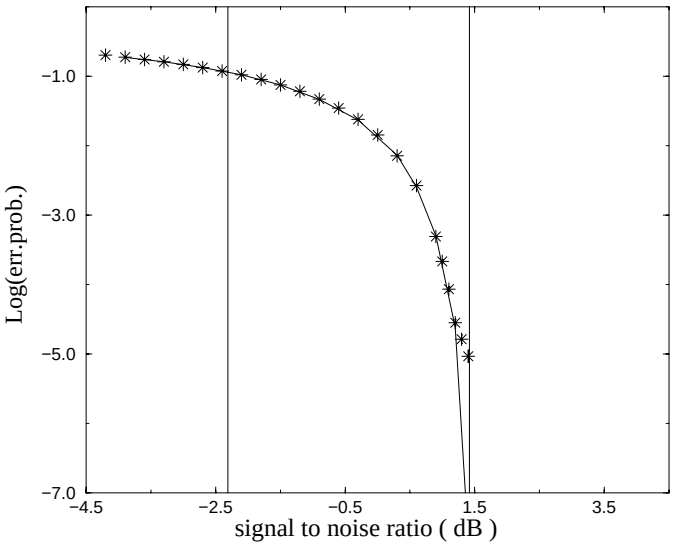

Fig. 2. The numerical results for the error probability per bit (stars, $*$), compared with the analytical prediction (continuous line). The analytical prediction is obtained, within the replica symmetric approximation, from equation (4.16). This graph refers to model 3 defined in Section 3.

It is simple to obtain the analogous of equation (4.16) for the simplest non recursive model, defined by: $\epsilon_i(\boldsymbol{\sigma}) = \sigma_i$, $\eta_i(\boldsymbol{\sigma}) = \sigma_i\sigma_{i-1}$. The final result is

$$\omega(z) = \int \mathrm{d}h\ P(h) \int \mathrm{d}J_1\ P(J_1) \int \mathrm{d}J_2\ P(J_2) \times \int \mathrm{d}x_1\ \hat\omega(x_1) \int \mathrm{d}x_2\ \hat\omega(x_2) \int \mathrm{d}z'\ \omega(z') \times \delta\left(z - \Theta_\beta\left[h; J_1 + J_2 + x_1 + x_2 + z'\right]\right), \quad (4.19)$$

$$\pi(x) = \int \mathrm{d}J\ P(J) \int \mathrm{d}x_{\mathrm{L}}\ \hat\omega(x_{\mathrm{L}}) \times \int \mathrm{d}x_{\mathrm{R}}\ \hat\omega(x_{\mathrm{R}})\ \delta(x - J - x_{\mathrm{L}} - x_{\mathrm{R}}). \quad (4.20)$$

A simple approximation to the solution of equation (4.19) can be obtained by starting from a distribution $\omega(x)$ supported on very large fields x and iterating equation (4.19) one time. The result is $\pi(x) \sim \int \mathrm{d}J\ P(J) \int \mathrm{d}h_1\ P(h_1) \int \mathrm{d}h_1\ P(h_1)\ \delta(x - J - h_1 - h_2)$, which coincides with the more general equation (3.22) after the change of variables $X = \mathrm{e}^{-2\beta x}$. No such approximation is possible for equation (4.16).

Expressions equivalent to equations (4.16, 4.19) can be derived for more complicated types of interaction. In general the distribution $\omega(x)$, which is defined on the real line, will be replaced by a distribution defined on $\mathbb{R}^{2^r-1}$, r being the range of the Hamiltonian.

5 The stability of the frozen solution

We would like to study local stability of the no-error phase in the context of the replica method. This can be done[5] by computing the eigenvalues of the matrices:

$$M^{\pm}_{a_1\dots a_l,b_1\dots b_m}[q] = \delta_{a_1\dots a_l,b_1\dots b_m} \pm \frac{\partial^2 \beta \mathcal{F}_{1d,n}[q]}{\partial q_{a_1\dots a_l}\partial q_{b_1\dots b_m}} \,. \tag{5.1}$$

$M^{\pm}[q]$ are the mass matrices for purely real ($M^{+}[q]$), or purely imaginary ($M^{-}[q]$), fluctuations of the order parameter around the value q. We are interested in the saddle point $q^*_{a_1\dots a_l} = 2^{-n/2}$. In order to write down all the 2^n eigenvectors of $M^{\pm}[q^*]$ it is convenient to change slightly our notation for the overlaps. Let us denote by $\Omega \subset \{1,2,\dots,n\}$ the set of $l \equiv |\Omega|$ different indices $(a_1^\Omega,\dots,a_l^\Omega)$. We can use the Ω's as indices for the overlaps with the natural identification $q_\Omega \equiv q_{a_1^\Omega\dots a_l^\Omega}$. It is not difficult to show that

$$\begin{aligned} T^{(N)}_{\Omega_a,\Omega_b} &\equiv \frac{1}{N}\frac{\partial^2 \log Z_{1d,n}[q]}{\partial q_{a_1\dots a_l}\partial q_{b_1\dots b_m}}\bigg|_{q=q^*} \\ &= \frac{2^{1-n}}{N}\left\{\sum_{(i,j)}\int \mathrm{d}\mathcal{P}[\mathbf{J}]\ \mathrm{e}^{nN\beta f - n\beta E_0}\right. \\ &\times \left.\left(1+\mathrm{e}^{-\beta\Delta(i,j)}\right)^n\left[\tanh\left(\frac{\beta\Delta(i,j)}{2}\right)\right]^u - \frac{N^2}{2}\right\}, \end{aligned} \tag{5.2}$$

where $\Delta(i,j)$ is defined in Section 3, $\mathrm{e}^{-nN\beta f} \equiv \int \mathrm{d}\mathcal{P}[\mathbf{J}]\ \mathrm{e}^{-n\beta H(\boldsymbol{\sigma}_0)}$ and $u \equiv u_{a_1\dots a_l,b_1\dots b_m}$ counts the indices which are either in the set in $\Omega_a \equiv (a_1,\dots,a_l)$ or in the set $\Omega_b \equiv (b_1,\dots,b_m)$ but not in both. If q is an eigenvector of $T^{(N)}$ with eigenvalue θ_N, then it is an eigenvector of $M^{\pm}[q^*]$ with eigenvalue $\mu^{\pm} = 1 \mp \lim_{N\to\infty}\theta_N$.

Notice that $T^{(N)}$ is an Hermitian matrix with respect to the scalar product:

$$\langle q, q'\rangle_n \equiv \sum_{l=0}^{n}\sum_{(a_1,\dots,a_l)} q^*_{a_1\dots a_l} q'_{a_1\dots a_l} = \sum_{\Omega} q^*_\Omega q'_\Omega. \tag{5.3}$$

We shall use another subset of $\{1,\dots,n\}$ (let us call it Λ) to label the different eigenvectors of $T^{(N)}$, which we now exhibit:

$$q^{(\Lambda)}_\Omega \equiv \frac{1}{2^{n/2}}(-1)^{|\Lambda\cap\Omega|}\,. \tag{5.4}$$

The vectors $\{q^{(\Lambda)}\}$ form an orthonormal set with respect to the scalar product defined in equation (5.3). This is easily proven by induction on n. The vector $q^{(\varnothing)}$ is nothing but the constant one. The corresponding eigenvalue is $\theta_N^{(\varnothing)} = -1$, whence $\mu^+_{(\varnothing)} = 2$ and $\mu^-_{(\varnothing)} = 0$. The eigenvalue $\mu^-_{(\varnothing)} = 0$ is a remnant of the invariance of the action under the symmetry cited in the footnote 4 of the previous section. In order to compute the eigenvalues in the subspace orthogonal to $q^{(\varnothing)}$, the following formula turns out to be useful:

$$\sum_{\Omega'} x^{|\Omega\triangle\Omega'|}\ q^{(\Lambda)}_{\Omega'} = (1-x)^{|\Lambda|}(1+x)^{n-|\Lambda|}\ q^{(\Lambda)}_\Omega\,, \tag{5.5}$$

where $\Omega\triangle\Omega'$ denotes the symmetric difference of Ω and Ω' (*i.e.* $\Omega\triangle\Omega' \equiv (\Omega\setminus\Omega')\cup(\Omega'\setminus\Omega)$). Using equation (5.5) and the results of algebra outlined in Section 3 we get (for $\Lambda \neq \varnothing$):

$$\theta_{N\to\infty}(\Lambda) = 2\zeta_J^2\sum_{m=1}^{\infty}\zeta_h^{\mathrm{weight}(s_m)}\,, \tag{5.6}$$

where weight(s_m) is defined in Section 3 and

$$\zeta_C = \zeta_C(|\Lambda|,n,\beta) = \frac{\displaystyle\int \mathrm{d}C\ P(C)\ \mathrm{e}^{(n-2|\Lambda|)\beta C}}{\displaystyle\int \mathrm{d}C\ P(C)\ \mathrm{e}^{n\beta C}}\,, \tag{5.7}$$

for $C\to h$ or $C\to J$. When the one-dimensional Hamiltonians (1.2) satisfy the hypothesis of Lemma 3.3, the sum in equation (5.6) can be explicitly computed yielding:

$$\theta_{N\to\infty}(\Lambda) = \frac{2\ \zeta_J^2\ \zeta_h^{w_0(f_1,f_2)+w_1(f_1,f_2)}}{1-\zeta_h^{w_1(f_1,f_2)}}. \tag{5.8}$$

If $n \geq 2|\Lambda|$ then $\theta(\Lambda,n;\beta)$ is positive and decreasing with β. Moreover $\lim_{\beta\to\infty}\theta(\Lambda,n;\beta) = 0$ and $\lim_{\beta\to 0}\theta(\Lambda,n;\beta) = \infty$. We can thus define the critical temperatures $\beta_{l,n}$ for $n/2 \geq l = |\Lambda| \geq 1$, by requiring[6]

$$\theta(\Lambda,n;\beta_{|\Lambda|,n}) = 1\,. \tag{5.9}$$

If $\beta > \beta_{|\Lambda|,n}$ the "frozen" saddle point is stable with respect to the direction $q^{(\Lambda)}$. If $\beta < \beta_{|\Lambda|,n}$ it becomes unstable: $\mu^+_{(\Lambda)} = 1-\theta(\Lambda) < 0$ while $\mu^-_{(\Lambda)} = 1+\theta(\Lambda) > 0$ (it could be guessed that the "imaginary" directions would be stable because of the physical interpretation of the overlaps). In the limit $n\to 0$, $\beta_{l,n}\to\beta_c/l$: the critical directions are the ones corresponding to $|\Lambda| = 1$. It is easy to see that the critical temperature β_c coincides with the one obtained in Section 3.

6 Conclusion

We have presented two derivations of the local stability condition for the no-error phase. Both will be object of the criticism of the skeptical reader. In the first one we obtained the "mean field" equation describing the dynamics of the decoding algorithm, equation (2.9), by making use

[5] For similar calculations see reference [24].

[6] Notice that equation (5.9) can have more than one solution for $n < 2|\Lambda|$. The "physical" critical point is obtained by taking the limit $n\to 0$ of the solution of equation (5.9) which exists for any n.

of heuristic arguments. Indeed we argued equation (2.9) to be valid only in the replica symmetric approximation. In the second derivation we made use of the replica method, which has not (yet) well founded mathematical basis.

We think that the two derivations compensate each other for their defects. Moreover they yield the same replica symmetric saddle point equation (4.11) and give the same picture of the instability which destroys the no-error (frozen) phase. This corresponds to couples of flipped $\epsilon(\boldsymbol{\sigma})$'s. Finally thanks to the first derivation we get some insight on the behavior of the decoding algorithm. In particular we have seen that, in the frozen phase, it approaches a no-error fixed point. This approach becomes slower near to the boundary of the frozen phase.

In reference [1] the local stability threshold computed here has been compared with numerical simulations for two types of code, respectively the models 3 and 3 presented in Section 3. Good agreement was found only for model 3. We propose two possible explanations of the disagreement for model 3:

- the phase transition is a first order one;
- the turbo decoding algorithm used in reference [1] gets stuck in some local minimum of the free energy, characterized by a finite error probability per bit.

We have not yet enough information for choosing between these two scenarios.

I thank G. Biroli, S. Caracciolo, R. Chirivì, B. Derrida, M. Mézard and R. Monasson for discussions about this work. Finally I am profoundly indebted with N. Sourlas for his advice and constant support.

Appendix A: Useful algebra results

In this Appendix we remind to the reader some known facts in the theory of finite fields and we prove the propositions stated in Section 3. These are nothing but simple exercises and we work out them in detail only for greater convenience of the reader. Finally we illustrate a few applications of the results obtained. The reader interested in a more complete treatment can consult references [25,26].

Let us begin with some elementary definitions. The basic object is $\mathbb{Z}_2$ *i.e.* the field of integer numbers modulo 2. A polynomial over $\mathbb{Z}_2$, $f(x) \in \mathbb{Z}_2[x]$ is simply a polynomial whose coefficients are in $\mathbb{Z}_2$. We say $f(x) \in \mathbb{Z}_2[x]$ to be irreducible if there do not exist two nonconstant polynomials $g(x), h(x) \in \mathbb{Z}_2[x]$ such that $f(x) = g(x)h(x)$. Any $f(x) \in \mathbb{Z}_2[x]$ possess an unique factorization, *i.e.* a decomposition of the form $f(x) = f_1(x)^{r_1} \dots f_h(x)^{r_h}$ where $f_i(x) \in \mathbb{Z}_2[x]$ are irreducible and $r_i \geq 1$ are integer numbers. Given two polynomials $f(x), g(x) \in \mathbb{Z}_2[x]$ we say that $f(x)$ divides $g(x)$ (in symbols $f(x)|g(x)$) if there exists $h(x) \in \mathbb{Z}_2[x]$ such that $g(x) = f(x)h(x)$[7]. For an irreducible polynomial $f(x) \in \mathbb{Z}_2[x]$ it does make sense to define the order $o(f)$: $o(f)$ is the smallest positive integer k such that $f(x)|x^k + 1$. The basic result which we shall employ in this appendix is the following:

Theorem A.1 Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}_2$. Then $f(x)|x^k + 1$ if and only if $o(f)|k$.

It is useful to know how to compute the order of an irreducible polynomial. The main tool is the theorem below:

Theorem A.2 Let $f(x)$ be an irreducible polynomial of degree d over $\mathbb{Z}_2$. Then d is the smallest positive integer for which $o(f)|2^d - 1$.

Moreover it is obvious from the definition that $o(f) \geq \deg(f)$.

Our first step will be the proof of Lemma 3.2 which we restate here as follows

Lemma A.1 Let $f(x)$ be a polynomial on $\mathbb{Z}_2$ with the following factorization

$$f(x) = f_1^{r_1}(x) \dots \ f_h^{r_h}(x); \qquad r_i \geq 1\,, \tag{A.1}$$

where the polynomials $f_i(x)$ are irreducible over $\mathbb{Z}_2$. Let p_i be the smallest integer such that $2^{p_i} \geq r_i$. Then $f(x)|(1 + x^k)$ if and only if $2^{p_i}|k$ and $o(f_i)|k$ for $i \in \{1, \dots, h\}$.

Proof of Lemma A.1. Let us begin by noticing that, since the $f_i(x)$ are irreducible, $f(x)|(1 + x^k)$ if and only if $f_i^{r_i}(x)|(1 + x^k)$ for $i \in \{1, \dots, h\}$. We can then limit ourselves to the case $f(x) = h^r(x)$ with $h(x)$ irreducible. It is convenient to work in an extension of $\mathbb{Z}_2$, *i.e.* in a field containing $\mathbb{Z}_2$ as a subfield. We choose an extension (let us call it S) of $\mathbb{Z}_2$ such that both $h(x)$ and $(1 + x^k)$ can be decomposed in linear factors. The existence of such an extension is a basic fact of field theory. We are then looking for the k such that all the root of $h(x)$ (in S) are roots of $(1 + x^k)$ with multiplicity at least r. It is then necessary to study the multiplicity of the roots of $(1+x^k)$. The first observation is that, if k is odd, all the roots are simple. In fact $\frac{\mathrm{d}}{\mathrm{d}x}(1 + x^k) = kx^{k-1}$ has no roots in common with $(1+x^k)$. The second observation consists in noticing that $(1 + x^{2k}) = (1 + x^k)^2$. We deduce that $(1 + x^{2^m k})$ with k odd has k distinct roots (the same as $(1 + x^k)$), each one with multiplicity 2^m. The final outcome is that $h^r(x)|(1+x^{2^m k})$ if and only if $2^m \geq r$ and $o(h)|k$. □

From Lemma A.1 the explicit form of the period $\omega(f)$ used in Section 3 is easily obtained:

$$\omega(f) = 2^{\max(p_1,\dots,p_h)}\ \mathrm{lcm}(o(f_1), \dots, o(f_h))\,. \tag{A.2}$$

The Lemmas 3.1 and 3.3 are easy consequences of Lemma 3.2.

Proof of Lemma 3.1. Let us begin by considering the series $1/f(x)$. We can always define the polynomials $\varphi_n(x)$ with $\deg(\varphi_n) < \omega(f)$ such that $1/f(x) = \sum_{n=0}^{\infty} \varphi_n(x)\ x^{n\omega(f)}$. Since $f(x)$ divides $(1 + x^{m\omega(f)})$ for all $m \geq 1$, we conclude that $\varphi_n(x) = \varphi_{n'}(x) \equiv \varphi(x)$ for all $n, n' \geq 0$ and $(1 + x^{m\omega(f)})/f(x) = \sum_{k=0}^{m-1} \varphi(x)\ x^{k\omega(f)}$. With the following definition

$$g(x)\varphi(x) \equiv \sum_{l=0}^{L} g_l(x)\ x^{l\omega(f)}, \quad \deg[g_l(x)] < \omega(f), \tag{A.3}$$

[7] Similarly, given two integer numbers $p, q \in \mathbb{Z}$, we say that p divides q (and write $p|q$) if there exists $m \in \mathbb{Z}$, such that $q = mp$.

we get

$$\frac{g(x)}{f(x)} = \sum_{n=0}^{\infty} x^{n\omega(f)} \sum_{l=0}^{\min(n,L)} g_l(x) \equiv \sum_{n=0}^{\infty} x^{n\omega(f)} p_n(x). \tag{A.4}$$

Notice that, for $n \geq L$, $p_n(x) = p_\infty(x) \equiv g(x)/f(x) \bmod x^{\omega(f)}$. An upper bound on L is easily obtained from equation (A.3) yielding[8] $p_n(x) = p_\infty(x)$ for $n \geq \lceil(\deg[g(x)]-1)/\omega(f)\rceil \geq L$. Clearly it cannot be $p_\infty(x) = 0$ otherwise we would conclude that $f(x)$ divides $g(x)$ in contradiction with the hypothesis. In order to complete the proof, let us suppose the following equation to hold

$$\frac{g(x)}{f(x)} = \sum_{n=0}^{\infty} x^{n\omega'} p'_n(x), \tag{A.5}$$

with $\omega' < \omega(f)$, $\deg(p'_n) < \omega'$ and $p'_n(x) = p'_\infty(x)$ for n large enough. This implies that $f(x)$ divides $g(x)(1+x^{\omega'})$ but, since $\gcd(f,g) = 1$, we would conclude that $f(x)$ divides $(1+x^{\omega'})$ contradicting Lemma 3.2. □

Proof of Lemma 3.3. It suffices to specialize the content of the previous paragraph to the case $\deg[g(x)] \leq \omega(f)$:

$$g(x)\varphi(x) = g_0(x) + g_1(x)\, x^{\omega(f)} \tag{A.6}$$

$$s_m(x) \equiv \frac{g(x)}{f(x)}(1+x^{m\omega(f)}) = g_0(x) + \{g_0(x)+g_1(x)\} \times \sum_{h=1}^{m-1} x^{h\omega(f)} + g_1(x), \tag{A.7}$$

whence

$$\begin{aligned} \text{weight}[s_m(x)] &= w_0 + w_1 m, && \text{(A.8)}\\ w_0 &\equiv \text{weight}[g_0(x)] + \text{weight}[g_1(x)] \\ &\quad -\text{weight}[g_0(x)+g_1(x)]\,, && \text{(A.9)}\\ w_1 &\equiv \text{weight}[g_0(x)+g_1(x)]. && \text{(A.10)} \end{aligned}$$

□

What does it happen when the hypothesis of Lemma 3.3 are not satisfied? It is easy to guess the answer. There exists a positive integer m_0 such that, for $m \geq m_0$, weight(s_m) grows linearly with m: weight$(s_m) = \tilde{w}_0(f,g)+\tilde{w}_1(f,g)\cdot m$ with $\tilde{w}_1(f,g) = \text{weight}(p_\infty)$. Thanks to this fact we can always sum the series in equation (3.14) in the interval $0 < \beta < \beta_1$. The discussion of the behavior of equation (3.8) presented in Section 3 is then completely general.

Let us return down to the earth and make a few examples. We shall consider the codes presented in reference [1]:

(a) The simplest non trivial case: $f(x) = 1+x$, $g(x) = 1$. Clearly both the polynomials are irreducible. The degree of $f(x)$ is $\deg[f(x)] = 1$. Because of Theorem A.2 $o(f)|2^1-1 = 1$ whence $o(f) = 1 = \omega(f)$. Theorem A.1 implies that $f(x)|1+x^k$ for each $k \geq 1$. This conclusion is easily confirmed by the well known formula $(1+x^k) = (1+x)(1+x+\cdots+x^{k-1})$. Lemma 3.1 tells us that $g(x)/f(x) = \sum_{n=0}^{\infty} p_n x^n$ with $p_n = p_\infty$ for $n \geq 0$ and that $p_\infty = 1$ (1 is the unique non zero polynomial of degree zero). We have thus rediscovered the simple fact that $(1+x)^{-1} = \sum_{n=0}^{\infty} x^n$. Finally we observe the hypothesis of Lemma 3.3 are satisfied and that (with the notation of Eq. (A.6)), $g_0(x) = 1$ and $g_1(x) = 0$. From equations (A.8–A.10) it follows that weight $[s_m(x) = (1+x^m)/(1+x)] = m$ which is easily confirmed by observing that $s_m(x) = 1+x+\cdots+x^{m-1}$.

(b) A less elementary example is: $f(x) = 1+x+x^2$, $g(x) = 1+x^2$. It is easy to see that $f(x)$ is irreducible and that $g(x) = (1+x)^2$ whence $\gcd(f,g) = 1$. From $o(f)|2^{\deg(f)}-1 = 3$ and $o(f) \geq \deg(f) = 2$ we deduce that $o(f) = 3 = \omega(f)$. In fact

$$\begin{aligned} \frac{1}{1+x+x^2} &= 1+x+x^3+x^4+x^6+\ldots \\ &= \sum_{n=0}^{\infty} \varphi(x) x^{3n}\,, && \text{(A.11)}\\ \varphi(x) &= 1+x\,. && \text{(A.12)} \end{aligned}$$

Thus by Lemma 3.2 $f(x)|(1+x^k)$ if and only if k is a multiple of 3. We can use Lemma 3.3 in order to compute the weight of $s_m(x) = (1+x^2)(1+x^{3m})/(1+x+x^2)$. We see that $g_0(x) = 1+x+x^2$ and $g_1(x) = 1$ whence weight$[h_m(x)] = 2+2m$. With some bookkeeping one can confirm this result:

$$h_m(x) = x + \sum_{l=0}^{m-1}(x^{3l+1}+x^{3l+2}) + x^{3m} \Rightarrow \text{weight}[h_m(x)] = 2+2m. \tag{A.13}$$

(c) Finally the generating polynomials used in reference [3] to build the first example of turbo code: $f(x) = 1+x+x^2+x^3+x^4$, $g(x) = 1+x^4$. Also in this case $f(x)$ is irreducible and $g(x) = (1+x)^4$ yielding $\gcd(f,g) = 1$. Since $o(f)|2^{\deg(f)}-1 = 15$ and $o(f) \geq \deg(f) = 4$, we deduce that either $o(f) = 5$ or $o(f) = 15$. However we know that $(1+x^5) = (1+x)(1+x+x^2+x^3+x^4)$ and we conclude that $o(f) = 5 = \omega(f)$. In fact

$$\begin{aligned} \frac{1}{1+x+x^2} &= 1+x+x^5+x^6+x^{10}+x^{11}+\ldots \\ &= \sum_{n=0}^{\infty} \varphi(x) x^{5n}\,, && \text{(A.14)}\\ \varphi(x) &= 1+x\,. && \text{(A.15)} \end{aligned}$$

Using the fact that $g_0(x) = 1+x+x^4$ and $g_1(x) = 1$ we get weight$[h_m(x)] = 2m+2$.

Appendix B: On the asymptotic behavior of the solutions of equation (3.8)

In this appendix we study equation (3.8) in order to extend to this case the results concerning equation (3.9)

[8] Here use the definition $\lceil x \rceil \equiv \min\{n \in \mathbb{Z} :\ n > x\}$.

used in Section 3. We shall examine both the approach of reference [13], which is based on the analogy with the KPP equation and is a non rigorous one, and the approach of reference [14], which employs probability theory and is entirely satisfactory from the mathematical point of view.

We would like to deal with this type of equation:

$$Q_{n+1}(Z) = \int_{-\infty}^{\infty} P(V)\,\mathrm{d}V \int_{-\infty}^{\infty} \prod_{i=1}^{\infty} p(h)\,\mathrm{d}h \times \int_{0}^{\infty} \prod_{i=1}^{\infty} Q_n(Z_i)\,\mathrm{d}Z_i \times \delta\left(Z - \sum_{i=1}^{\infty} \exp\left\{-\beta V - \beta \sum_{j=1}^{i-1} h_j\right\} Z_i\right), \quad \text{(B.1)}$$

with the requirement that $\int \mathrm{d}h\; p(h)\; h > 0$ and the initial condition $P_0(Z) = \delta(Z-1)$. Following reference [13] we introduce the function:

$$G_n(x) \equiv \int_0^{\infty} \mathrm{d}Z\; Q_n(Z) \exp\{-\mathrm{e}^{-\beta x} Z\}\,, \quad \text{(B.2)}$$

which satisfy this recurrence equation

$$G_{n+1}(x) = \int_{-\infty}^{\infty} P(V)\,\mathrm{d}V \int_{-\infty}^{\infty} \prod_{i=1}^{\infty} p(h_i)\,\mathrm{d}h_i \times \prod_{i=1}^{\infty} G_n(x + V + \sum_{j=1}^{i-1} h_j)\,. \quad \text{(B.3)}$$

Let us make a few elementary observations concerning equation (B.3): if $0 \le G_m(x) \le 1$ for some m and all x then $0 \le G_n(x) \le 1$ for all x and $n > m$; if $\limsup_{x\to\infty} G_n(x) = g_\infty < 1$ then $G_{n+1} = 0$; if $G_n(x)$ is increasing and $0 < G_n(x) < 1$ for some x (both these hypothesis are implied by Eq. (B.2)) then $\lim_{x\to-\infty} G_{n+1}(x) = 0$. The stationary uniform solutions of equation (B.3) are $G_n^A(x) = 0$ and $G_n^B(x) = 1$. The first one is obviously stable. If we consider a small fluctuation around $G_n^B(x)$, $G_n(x) = 1 + \rho_n(x)$ we get:

$$\rho_{n+1}(x) \simeq \int_{-\infty}^{\infty} P(V)\,\mathrm{d}V \times \int_{-\infty}^{\infty} \prod_{i=1}^{\infty} p(h)\,\mathrm{d}h \sum_{i=1}^{\infty} \rho_n(x + V + \sum_{j=1}^{i-1} h_j)\,, \quad \text{(B.4)}$$

which can be diagonalized in Fourier space:

$$\hat\rho_{n+1}(k) \simeq \frac{\hat P(k)}{1-\hat p(k)} \hat\rho_n(k) \equiv \lambda(k)\hat\rho_n(k)\,. \quad \text{(B.5)}$$

Notice that $|\lambda(k)| > 1$ for k small enough and that $|\lambda(k)|$ diverges at $k = 0$ in agreement with the previous observation that if $G_n(x) = 1 - \rho$ then $G_{n+1}(x) = 0$. The preceding observations lead us to the hypothesis that the $n \to \infty$ behavior of our problem is controlled by front-like solutions $G_n(x) = g(x - c(\beta)n)$ interpolating between the stable state $G_n^A(x) = 0$ at $x \to -\infty$ and $G_n^B(x) = 1$ at $x \to \infty$.

This scenario is easily confirmed in the case without disorder. If $P(V) = \delta(V - V_0)$ and $p(h) = \delta(h - h_0)$ one obtains $P_n(Z) = \delta(Z - \mathrm{e}^{\beta c(\beta) n})$, $G_n(x) = \exp\{-\mathrm{e}^{-\beta(x - c(\beta)n)}\}$ with

$$c(\beta) = \frac{1}{\beta} \log \frac{\mathrm{e}^{-\beta V_0}}{1 - \mathrm{e}^{-\beta h_0}}\cdot \quad \text{(B.6)}$$

In the general case we assume the existence of front-like solutions with the large x behavior $G_n(x) \sim 1 - \mathrm{e}^{-\beta(x-c(\beta)n)} + o(\mathrm{e}^{-\beta x})$. The front velocity is obtained through the construction given in equations (3.12, 3.13) with

$$v(\beta) \equiv \frac{1}{\beta} \log \phi(\beta) = \frac{1}{\beta} \log \frac{\langle \mathrm{e}^{-\beta V}\rangle}{1 - \langle \mathrm{e}^{-\beta h}\rangle}\cdot \quad \text{(B.7)}$$

Notice that $\langle h\rangle > 0$ implies that $\langle \mathrm{e}^{-\beta h}\rangle < 1$ in some interval $0 < \beta < \beta_1$ and that $\beta_c < \beta_1$. This remark allows us to sum the series $\sum_k \langle \mathrm{e}^{-\beta h}\rangle^k$ in the range $0 < \beta < \beta_c$, thus obtaining equation (B.7). The same remark will be useful in the following.

Let us consider now the more rigorous approach used in reference [14]. We start by defining the polymer model which corresponds to equation (B.1). We have to use a tree with a numerable set of branches stemming from each node. A node of the nth generation is identified by n integer numbers $\underline{\omega} \equiv (\omega_1, \ldots, \omega_n)$; its generation is denoted by $|\underline{\omega}|$. We denote by $\underline{0}$ the root node (*i.e.* the only node of the zeroth generation). We say that the node $\underline{\omega}'$ belonging to the mth generation is a descendant of the node $\underline{\omega}$ of the nth generation (and write $\underline{\omega} \prec \underline{\omega}'$ if $n < m$ or $\underline{\omega} \preceq \underline{\omega}'$ if $n \le m$) if $\omega_1 = \omega'_1, \ldots, \omega_n = \omega'_n$. The node $\underline{\omega}'$ is said to be an older brother of the node $\underline{\omega}$ with $|\underline{\omega}'| = |\underline{\omega}| = n$ if $\omega_1 = \omega'_1, \ldots, \omega_{n-1} = \omega'_{n-1}$ and $\omega_n > \omega'_n$. A pair of random variables $V(\underline{\omega})$ and $h(\underline{\omega})$ is attached at each node. All these variables are statistically independent and have marginal distributions $p(h)$ (the $h(\underline{\omega})$'s) and $P(V)$ (the $V(\underline{\omega})$'s). A directed polymer is given by a pair of nodes $\underline{\omega}^1 \prec \underline{\omega}^2$. To each polymer we assign an energy as follows:

$$E(\underline{\omega}^1, \underline{\omega}^2) = \sum_{\underline{\omega}^1 \prec \underline{\omega} \prec \underline{\omega}^2} V(\underline{\omega}) + \sum_{\underline{\omega}^1 \prec \underline{\omega} \preceq \underline{\omega}^2} \sum_{\substack{\underline{\omega}' : \underline{\omega}' \text{ is an older} \\ \text{brother of } \underline{\omega}}} h(\underline{\omega}'). \quad \text{(B.8)}$$

Moreover we use the shorthand $E(\underline{0}, \underline{\omega}) \to E(\underline{\omega})$ and define the following partition functions:

$$Z_n(\beta) \equiv \sum_{\underline{\omega}:\ |\underline{\omega}| = n} \mathrm{e}^{-\beta E(\underline{\omega})}\,, \quad \text{(B.9)}$$

$$Z_n(\beta|\underline{\omega}) = \sum_{\substack{\underline{\omega}' \succeq \underline{\omega}: \\ |\underline{\omega}'| - |\underline{\omega}| = n}} \mathrm{e}^{-\beta E(\underline{\omega}, \underline{\omega}')}\,. \quad \text{(B.10)}$$

The velocity of the wavefront studied in the previous paragraphs corresponds in this language to the random

variable:

$$c(\beta) \equiv \lim_{n\to\infty} \frac{1}{n\beta} \log Z_n(\beta)\,. \tag{B.11}$$

The model has two phases. In the high temperature phase ($\beta \le \beta_c$) the fluctuations of $Z_n(\beta)$ are small and

$$c(\beta) = \lim_{n\to\infty} \frac{1}{n\beta} \log\langle Z_n(\beta)\rangle = v(\beta)\,. \tag{B.12}$$

In the low temperature phase ($\beta > \beta_c$) the fluctuations become large and $c(\beta)$ is fixed by simple convexity and monotonicity arguments. The key point of the approach used in reference [14] is to estimate these fluctuations by proving that, for $\beta < \beta_c$:

$$\frac{\langle Z_n(\beta)^\alpha\rangle}{\langle Z_n(\beta)\rangle^\alpha} \le \mathrm{Bound}(\alpha,\beta) \tag{B.13}$$

for some $1 < \alpha < 2$ uniformly in n. This is enough for obtaining equation (B.12).

Let us define the normalized variables $M_n(\beta) \equiv Z_n(\beta)/\langle Z_n(\beta)\rangle$. In reference [14] the bound in equation (B.13) is obtained starting with the second moment of $M_n(\beta)$, and then refining the inequality for the fractional moments of order $1 < \alpha < 2$. Notice that looking at the mth moment of the partition function is a well known method [27] for obtaining an upper estimate on the critical temperature (the estimate becomes worser as m gets larger). Let us have a look at the first two integer moments:

$$\langle Z_{n+1}(\beta)\rangle = \langle \mathrm{e}^{-\beta V}\rangle \sum_{k=0}^{\infty} \langle \mathrm{e}^{-\beta h}\rangle^k \ \langle Z_n(\beta)\rangle\,, \tag{B.14}$$

$$\begin{aligned}\langle Z^2_{n+1}(\beta)\rangle = {} & \left(\langle \mathrm{e}^{-\beta V}\rangle \sum_{k=0}^{\infty} \langle \mathrm{e}^{-\beta h}\rangle^k\right)^2 \left[\langle Z^2_n(\beta)\rangle - Z_n(2\beta)\right] \\ & + \langle \mathrm{e}^{-2\beta V}\rangle \sum_{k=0}^{\infty} \langle \mathrm{e}^{-2\beta h}\rangle^k \left(1 + 2\sum_{l=1}^{\infty} \langle \mathrm{e}^{-\beta h}\rangle^l\right) \ \langle Z_n(2\beta)\rangle\,.\end{aligned} \tag{B.15}$$

In general the mth moment is finite (but not necessarily uniformly bounded) only if $\langle \mathrm{e}^{-m\beta h}\rangle < 1$ *i.e.* if $\beta < \beta_1/m$. There is no integer moment of order greater than one which remains finite in the interval $(0,\beta_c)$. This fact forces us to a slight modification of the proof presented in reference [14]. We use the trivial identity:

$$Z_{n+1}(\beta) = \sum_{\underline{\omega}:\ |\underline{\omega}|=1} \mathrm{e}^{-\beta E(\underline{\omega})} Z_n(\beta|\underline{\omega})\,, \tag{B.16}$$

and estimate the αth moment (with $1 < \alpha < 2$) as follows:

$$\begin{aligned} Z^\alpha_{n+1}(\beta) = {} & \left\{ \sum_{\substack{\underline{\omega}^1:\\ |\underline{\omega}^1|=1}} \sum_{\substack{\underline{\omega}^2:\\ |\underline{\omega}^2|=1}} \mathrm{e}^{-\beta[E(\underline{\omega}^1)+E(\underline{\omega}^2)]} \right. \\ & \left. \times Z_n(\beta|\underline{\omega}^1)\ Z_n(\beta|\underline{\omega}^2) \right\}^{\alpha/2} \\ \le {} & \sum_{\substack{\underline{\omega}^1:\\ |\underline{\omega}^1|=1}} \sum_{\substack{\underline{\omega}^2:\\ |\underline{\omega}^2|=1}} \mathrm{e}^{-\frac{\alpha\beta}{2}[E(\underline{\omega}^1)+E(\underline{\omega}^2)]} \\ & \times Z^{\alpha/2}_n(\beta|\underline{\omega}^1)\ Z^{\alpha/2}_n(\beta|\underline{\omega}^2)\,. \end{aligned} \tag{B.17}$$

For a temperature such that $\alpha\beta < \beta_1$ we can take the averages and sum up the series:

$$\begin{aligned} \langle Z^\alpha_{n+1}(\beta)\rangle \le {} & \sum_{\substack{\underline{\omega}:\\ |\underline{\omega}|=1}} \langle \mathrm{e}^{-\alpha\beta E(\underline{\omega})}\rangle\ \langle Z^\alpha_n(\beta)\rangle \\ & + \sum_{\substack{\underline{\omega}^1\neq\underline{\omega}^2:\\ |\underline{\omega}^i|=1}} \langle \mathrm{e}^{-\frac{\alpha\beta}{2}[E(\underline{\omega}^1)+E(\underline{\omega}^2)]}\rangle\ \langle Z^{\alpha/2}_n(\beta)\rangle^2 \\ \le {} & \phi(\alpha\beta)\langle Z^\alpha_n(\beta)\rangle + 2\phi(\alpha\beta)\sum_{l=1}^{\infty}\langle \mathrm{e}^{-\frac{\alpha\beta}{2}h}\rangle^l \langle Z_n(\beta)\rangle^\alpha. \end{aligned} \tag{B.18}$$

Rewriting this formula for the normalized variables we get

$$\begin{aligned} \langle M^\alpha_{n+1}(\beta)\rangle \le {} & \left[\frac{\phi(\alpha\beta)}{\phi(\beta)^\alpha}\right] \langle M^\alpha_n(\beta)\rangle + 2\left[\frac{\phi(\alpha\beta)}{\phi(\beta)^\alpha}\right] \sum_{l=1}^{\infty}\langle \mathrm{e}^{-\frac{\alpha\beta}{2}h}\rangle \\ \equiv {} & \psi(\alpha,\beta)\langle M^\alpha_n(\beta)\rangle + \chi(\alpha,\beta)\,. \end{aligned} \tag{B.19}$$

At this point we observe, following reference [14], that, if $\frac{\mathrm{d}v}{\mathrm{d}\beta}(\beta) < 0$ (*i.e.* $\beta < \beta_c$) then we can choose $\alpha > 1$ such that $\psi(\alpha,\beta) < 1$. The condition to be imposed on α for obtaining this inequality is $\alpha < \beta_c/\beta$ (notice that this inequality implies the previous one $\alpha < \beta_1/\beta$). The desired bound is obtained by using Gronwall lemma together with the fact that $\langle M^\alpha_0(\beta)\rangle = 1$:

$$\begin{aligned} \langle M^\alpha_n(\beta)\rangle \le {} & \psi^n(\alpha,\beta) + \frac{1-\psi^n(\alpha,\beta)}{1-\psi(\alpha,\beta)}\chi(\alpha,\beta) \\ \le {} & 1 + \frac{1}{1-\psi(\alpha,\beta)}\chi(\alpha,\beta)\,. \end{aligned} \tag{B.20}$$

Appendix C: The replicated partition function

In this appendix we describe in detail the derivation of the expression (4.1) for the replicated partition function. From equation (1.1) we get our starting point for this

calculation:

$$\overline{Z^n} = \frac{1}{N!}\sum_{\rho}\int \mathrm{d}\mathcal{P}[\mathbf{J}] \sum_{\{\boldsymbol{\sigma}^{(1),a}\}}\sum_{\{\boldsymbol{\sigma}^{(2),a}\}} \times \prod_{i=1}^{N}\prod_{a=1}^{n}\delta\left(\epsilon_{\rho(i)}(\boldsymbol{\sigma}^{(1),a}),\epsilon_i(\boldsymbol{\sigma}^{(2),a})\right) \times \exp\left[-\beta\sum_{k=1}^{2}\sum_{a=1}^{n}H^{(k)}(\boldsymbol{\sigma}^{(k),a})\right], \quad \text{(C.1)}$$

where the sum over ρ runs over all the $N!$ permutations of N objects. Equation (4.1) is easily obtained from equation (C.1) using the identity

$$\frac{1}{N!}\sum_{\rho}\prod_{i=1}^{N}\delta_{\underline{\epsilon}^{(1)}_{\rho(i)},\underline{\epsilon}^{(2)}_{i}} = \frac{\mathrm{e}^N}{2^{nN}}\int\frac{N}{\pi}\,\mathrm{d}q_0\,\mathrm{d}\hat{q}_0\int\prod_a\frac{N}{\pi}\,\mathrm{d}q_a\,\mathrm{d}\hat{q}_a \times\int\prod_{(a,b)}\frac{N}{\pi}\,\mathrm{d}q_{ab}\,\mathrm{d}\hat{q}_{ab}\,\cdots\prod_{i=1}^{N}[q_0 + \sum_a q_a\epsilon_i^{(1),a}+\dots]\prod_{j=1}^{N}[\hat{q}_0+\sum_a\hat{q}_a\epsilon_j^{(2),a}+\dots] \times\exp\left[-N\left(q_0\hat{q}_0+\sum_a q_a\hat{q}_a+\sum_{(a,b)}q_{ab}\hat{q}_{ab}+\dots\right)\right], \quad \text{(C.2)}$$

which, as we shall prove below, holds to the leading order in the $N\to\infty$ limit. In equation (C.2) the $\underline{\epsilon}_i^{(k)} \equiv (\epsilon_i^{(k),1},\dots,\epsilon_i^{(k),n})$ with $k=1,2$ are replicated spin variables, and $\delta_{\underline{\epsilon}^{(1)},\underline{\epsilon}^{(2)}} \equiv \prod_{a=1}^{n}\delta_{\epsilon^{(1),a},\epsilon^{(2),a}}$ is the corresponding delta function. The multi-overlaps $q_{a_1\dots a_l}$ and $\hat{q}_{a_1\dots a_l}$ are understood to be a complex conjugate pair.

In order to represent the random permutation ρ we introduce the matrix $C_{ij}^{\rho}\equiv\delta_{i,\rho(j)}$. We can then rewrite the l.h.s. of equation (C.2) as follows:

$$\frac{1}{N!}\sum_{\rho}\prod_{i,j=1}^{N}\prod_{a=1}^{n}\left[\left(1-\frac{1}{2}C_{ij}^{\rho}\right)+\frac{1}{2}C_{ij}^{\rho}\epsilon_i^{(1),a}\epsilon_j^{(2),a}\right]. \quad \text{(C.3)}$$

The matrix elements C_{ij}^{ρ} are all zeros or ones and satisfy the constraints: $\sum_{i=1}^{N}C_{ij}^{\rho}=1$ for each $j=1,\dots,N$, and $\sum_{j=1}^{N}C_{ij}^{\rho}=1$ for each $i=1,\dots,N$. There is a one-to-one correspondence between such matrices and the permutations of N objects. Rewriting the sum over the permutation ρ in equation (C.3) as a sum over these matrices C_{ij}, we get

$$\frac{1}{N!\omega_0^{N^2-N}\omega_1^N}\sum_{\{C_{ij}\}}\left(\prod_{j=1}^{N}\delta_{1,\sum_{i=1}^{N}C_{ij}}\prod_{i=1}^{N}\delta_{1,\sum_{j=1}^{N}C_{ij}}\right) \times\prod_{i,j=1}^{N}\left\{\omega_{C_{ij}}\prod_{a=1}^{n}\left[\left(1-\frac{1}{2}C_{ij}\right)+\frac{1}{2}C_{ij}\epsilon_i^{(1),a}\epsilon_j^{(2),a}\right]\right\}. \quad \text{(C.4)}$$

In equation (C.4) we introduced the weights $\omega_{C_{ij}}$ for later convenience. Since the number of entries C_{ij} such that $C_{ij}=1$ is N for any matrix satisfying the mentioned constraints, we can assign any non zero value to the weights ω_0 and ω_1. Our (quite natural) choice will be

$$\omega_0 = 1-\frac{1}{N}\,,\quad \omega_1=\frac{1}{N}\cdot \quad \text{(C.5)}$$

We rewrite now equation (C.4) using the following representation of the Kronecker δ function:

$$\delta_{1,A} = \oint\frac{\mathrm{d}z}{2\pi\mathrm{i}z^2}z^A\,, \quad \text{(C.6)}$$

where the integration contour encircles the origin in the complex z-plane. From equation (C.4) we get

$$\frac{1}{\mathcal{N}}\prod_{i=1}^{N}\oint\frac{\mathrm{d}z_i}{2\pi\mathrm{i}z_i^2}\prod_{j=1}^{N}\oint\frac{\mathrm{d}w_j}{2\pi\mathrm{i}w_j^2}\prod_{i,j=1}^{N}\sum_{C_{ij}=0}^{1}\omega_{C_{ij}}(z_iw_j)^{C_{ij}} \times\prod_{a=1}^{n}\left[\left(1-\frac{1}{2}C_{ij}\right)+\frac{1}{2}C_{ij}\epsilon_i^{(1),a}\epsilon_j^{(2),a}\right], \quad \text{(C.7)}$$

where $\mathcal{N}\equiv N!\omega_0^{N^2-N}\omega_1^N\simeq\mathrm{e}^{-2N}$. Summing over the numbers C_{ij} and proceeding to the leading order as $N\to\infty$, we obtain from equation (C.7)

$$\frac{1}{\mathcal{N}}\prod_{i=1}^{N}\oint\frac{\mathrm{d}z_i}{2\pi\mathrm{i}z_i^2}\prod_{j=1}^{N}\oint\frac{\mathrm{d}w_j}{2\pi\mathrm{i}w_j^2}\prod_{i,j=1}^{N}\left[1-\frac{1}{N}+\frac{z_iw_j}{2^nN} \times\prod_{a=1}^{n}(1+\epsilon_i^{(1),a}\epsilon_j^{(2),a})\right]\simeq\mathrm{e}^N\prod_{i=1}^{N}\oint\frac{\mathrm{d}z_i}{2\pi\mathrm{i}z_i^2} \times\prod_{j=1}^{N}\oint\frac{\mathrm{d}w_j}{2\pi\mathrm{i}w_j^2}\exp\left\{\frac{1}{2^nN}\sum_{i,j=1}^{N}\left[z_iw_j+\sum_a z_i\epsilon_i^{(1),a}w_j\epsilon_j^{(2),a} +\sum_{(a,b)}z_i\epsilon_i^{(1),a}\epsilon_i^{(1),b}w_j\epsilon_j^{(2),a}\epsilon_j^{(2),b}+\dots\right]\right\}. \quad \text{(C.8)}$$

We can now disentangle the dependence upon the spin variables $\underline{\epsilon}_i^{(1)}$ and $\underline{\epsilon}_j^{(2)}$ in equation (C.8), using the following identity:

$$\mathrm{e}^{ab/N} = \int\frac{N}{\pi}\,\mathrm{d}q\mathrm{d}\hat{q}\,\mathrm{e}^{-Nq\hat{q}+aq+b\hat{q}}, \quad \text{(C.9)}$$

which holds for complex conjugate q and $\hat{q}$. From equation (C.8) we get

$$\mathrm{e}^N \int \frac{N}{\pi}\,\mathrm{d}q_0\,\mathrm{d}\hat{q}_0 \int \prod_a \frac{N}{\pi}\,\mathrm{d}q_a\,\mathrm{d}\hat{q}_a \cdots \prod_{i=1}^{N} \oint \frac{\mathrm{d}z_i}{2\pi \mathrm{i} z_i^2} \prod_{j=1}^{N} \times \oint \frac{\mathrm{d}w_j}{2\pi \mathrm{i} w_j^2} \exp\left[\frac{1}{2^{n/2}} \sum_{i=1}^{N} \left(q_0 z_i + \sum_a q_a z_i \epsilon_i^{(1),a} + \dots\right) + \frac{1}{2^{n/2}} \sum_{j=1}^{N} \left(q_0 w_j + \sum_a q_a w_j \epsilon_j^{(2),a} + \dots\right)\right] \times \exp\left[-N\left(q_0\hat{q}_0 + \sum_a q_a \hat{q}_a + \dots\right)\right]. \quad \text{(C.10)}$$

The integration over the z_i and w_j variables can be done now yielding, after a few manipulations, equation (C.2).

References

1. A. Montanari, N. Sourlas, Eur. Phys. J. B **18**, 107 (2000).
2. T.M. Cover, J.A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
3. C. Berrou, A. Glavieux, P. Thitimajshima, *Proc. 1993 IEEE Int. Conf. Commun. (Geneva, Switzerland)*, pp. 1064–1070.
4. C. Berrou, A. Glavieux, IEEE Trans. Commun. **44**, 1261 (1996).
5. C. Berrou, R. Pyndiah, M. Jézéquel, A. Glavieux, P. Adde, La Recherche **315**, 34 (1998).
6. N. Sourlas, Nature **339**, 693 (1989).
7. N. Sourlas, *Statistical Mechanics of Neural Networks*, Lecture Notes in Physics **368**, edited by L. Garrido (Springer Verlag, 1990).
8. N. Sourlas, École Normale Supérieure preprint (April 1993).
9. N. Sourlas, *From Statistical Physics to Statistical Inference and Back,* edited by P. Grassberger, J.-P. Nadal (Kluwer Academic, 1994), p. 195.
10. D.J.C. MacKay, IEEE Trans. Inf. Theory **45**, 399 (1999).
11. R.G. Gallager, *Low Density Parity Check Codes*, Research Monograph Series Vol. 21 (MIT, Cambridge, MA., 1963).
12. I. Kanter, D. Saad, Phys. Rev. Lett. **83**, 2660 (1999).
13. B. Derrida, H Spohn, J. Stat. Phys. **51**, 817 (1988).
14. E. Buffet, A. Patrick, J.V. Pulé, J. Phys. A **26**, 1823 (1993).
15. B. Derrida, M.R. Evans, E.R. Speer, Commun. Math. Phys. **156**, 221 (1993).
16. J. Cook, B. Derrida, J. Stat. Phys. **61**, 961 (1990).
17. J. Cook, B. Derrida, J. Stat. Phys. **63**, 505 (1991).
18. A. Kolmogorov, I. Petrovsky, N. Piscounov, Moscou Univ. Math. Bull. **1**, 1 (1937).
19. M. Mézard, G. Parisi, M.A. Virasoro, *Spin Glass theory and Beyond* (World Scientific, Singapore, 1987).
20. K.Y.M. Wong, D. Sherrington, J. Phys. A **21**, L459 (1988).
21. F.J. Dyson, Phys. Rev. **92**, 1331 (1953).
22. H. Schmidt, Phys. Rev. **105**, 425 (1954).
23. J.M. Luck, *Systèmes désordonnés unidimensionels* (Aléa Saclay, 1992).
24. P. Mottishaw, C. De Dominicis, J. Phys. A **20**, L375 (1987).
25. S. Roman, *Field Theory* (Springer-Verlag, New York, 1995).
26. S. Roman, *Coding and Information Theory* (Springer-Verlag, New York, 1995).
27. B. Derrida, Phys. Rev. B **24**, 2613 (1981).