

Statistical mechanics of error-correcting codes

Y. KABASHIMA¹(*) and D. SAAD²(**)

¹ *Department of Computational Intelligence and Systems Science
Tokyo Institute of Technology - Yokohama 226, Japan*

² *The Neural Computing Research Group, Aston University
Birmingham B4 7ET, UK*

(received 8 June 1998; accepted 9 October 1998)

PACS. 89.90+n – Other areas of general interest to physicists.

PACS. 89.70+c – Information science.

PACS. 05.50+q – Lattice theory and statistics; Ising problems.

Abstract. – We investigate the performance of error-correcting codes, where the code word comprises products of K bits selected from the original message and decoding is carried out utilizing a connectivity tensor with C connections per index. Shannon's bound for the channel capacity is recovered for large K and zero temperature when the code rate K/C is finite. Close to optimal error-correcting capability is obtained for finite K and C . We examine the finite-temperature case to assess the use of simulated annealing for decoding and extend the analysis to accommodate other types of noisy channels.

Error-correcting codes are of significant practical importance as they provide mechanisms for retrieving the original message after possible corruption due to noise during transmission. They are being used extensively in most means of information transmission from satellite communication to the storage of information on hardware devices. The coding efficiency, measured in the percentage of informative transmitted bits, plays a crucial role in determining the speed of communication channels and the effective storage space on hard-disks. Rigorous bounds [1] have been derived for the maximal channel capacity for which codes, capable of achieving arbitrarily small error probability, can be found. However, existing practical error-correcting codes do not saturate this bound and the quest for more efficient error-correcting codes has been going on ever since.

A new family of error-correcting codes, based on insights gained from the statistical mechanical analysis of Ising spin models, has recently been suggested by Sourlas [2], investigating the use of statistical mechanics for constructing and investigating novel coding methods [3, 12]. However, the codes suggested and analyzed so far are of no practical significance as they imply an infinite ratio between the length of the transmitted word and the original message. Consequently, they had little impact on the design and the understanding of practical codes.

(*) E-mail: kaba@fe.dis.titech.ac.jp

(**) E-mail: saadd@aston.ac.uk

In this letter we extend the framework suggested by Sourlas to accommodate practical codes, where the ratio between the transmitted and the original message is finite and arbitrarily close to the bound presented by Shannon [1]. We analyze the performance of these codes using methods adopted from the statistical mechanics of diluted spin systems and validate the analytical solution by comparing it to results obtained by numerical solutions.

In a general scenario, a message represented by an N -dimensional binary vector $\boldsymbol{\xi}$ is encoded by a vector \boldsymbol{J}^0 which is then transmitted through a noisy channel with some flipping probability p per bit. The received message \boldsymbol{J} is then decoded to retrieve the original message.

We will consider a family of codes, suggested originally by Sourlas [2], in which the encoded message is of the form: $J_{i_1, i_2, \dots, i_K}^0 = \xi_{i_1} \xi_{i_2} \dots \xi_{i_K}$. The original message is then retrieved by exploring the ground state of the related Hamiltonian

$$\mathcal{H} = - \sum_{\langle i_1, \dots, i_K \rangle} \mathcal{A}_{\langle i_1, \dots, i_K \rangle} J_{\langle i_1, \dots, i_K \rangle} S_{i_1} \dots S_{i_K} - F \sum_k S_k, \quad (1)$$

where \boldsymbol{S} is the N -dimensional binary vector of dynamical variables and \mathcal{A} is a sparse tensor with C unit elements per index setting the rest of the elements to zero, which determines the components of the transmitted code word \boldsymbol{J}^0 . The last term on the right is required in the case of sparse or biased messages and will require assigning a certain value to the additive field F , which can be related to the prior belief in the Bayesian framework.

Codes of this type have been studied by Sourlas [2, 3], by mapping them onto known problems in statistical mechanics such as the SK [4] ($K = 2$) and Random Energy [5] ($K \rightarrow \infty$) models. However, these studies [2,3] have been carried out in the case of extensive connectivity, where the ratio between the number of bonds $C \sim \binom{N-1}{K-1}$, and the number of sites used for encoding K is infinite, corresponding to the case of a vanishing code rate which is of limited practical significance. In this letter we will examine the case where the code rate $R = K/C$ is finite, defining $\alpha \equiv 1/R$.

Since the first part of the Hamiltonian (eq. (1)) is invariant under the transformation $S_i \rightarrow S_i \xi_i$ and $J_{\langle i_1, \dots, i_K \rangle} \rightarrow J_{\langle i_1, \dots, i_K \rangle} \xi_{i_1} \xi_{i_2} \dots \xi_{i_K}$, it would be useful to decouple the vectors \boldsymbol{S} and $\boldsymbol{\xi}$, obtaining a similar expression to (eq. (1)) apart from the last term on the right which becomes $F \sum_k S_k \xi_k$, retaining pattern dependence. Note that we have three types of random variables, the corruption process, the original message and, most importantly, the selection of code bits represented by the tensor \mathcal{A} . These infinitely large sets of random variables justify the assumption of self-averaging free energy and enables us to use the tools of statistical physics.

For calculating the partition function $\mathcal{Z}(\boldsymbol{J}, \boldsymbol{\xi}, \mathcal{A}) = \text{Tr}_{\{S\}} \exp[-\beta \mathcal{H}]$ we invoke the replica method following ref. [6]. We use an integral representation of the δ -function to enforce the restriction, of C bonds per index, on the tensor \mathcal{A} :

$$\delta \left(\sum_{\langle i_2, i_3, \dots, i_K \rangle} \mathcal{A}_{\langle i, i_2, \dots, i_K \rangle} - C \right) = \int_0^{2\pi} \frac{dZ}{2\pi} Z^{-(C+1)} Z^{\sum_{\langle i_2, i_3, \dots, i_K \rangle} \mathcal{A}_{\langle i, i_2, \dots, i_K \rangle}}, \quad (2)$$

giving rise to a set of order parameters $q_{\alpha, \beta, \dots, \gamma} = (1/N) \sum_{i=1}^N Z_i S_i^\alpha S_i^\beta \dots S_i^\gamma$, where α, β, \dots represent replica indices. The averages over \boldsymbol{J} and $\boldsymbol{\xi}$ are taken with respect to the probability distributions

$$\begin{aligned} \mathcal{P}(J_{\langle i_1, \dots, i_K \rangle}) &= (1-p) \delta(J_{\langle i_1, \dots, i_K \rangle} - 1) + p \delta(J_{\langle i_1, \dots, i_K \rangle} + 1), \\ \mathcal{P}(\xi_i) &= \frac{1+\rho}{2} \delta(\xi_i - 1) + \frac{1-\rho}{2} \delta(\xi_i + 1), \end{aligned} \quad (3)$$

respectively, where $0 \leq p, \rho \leq 1$ are small coefficients representing the channel noise (flip probability) and pattern bias (or sparsity), respectively. As a first approximation we will assume replica symmetry [6]; one step replica symmetry breaking will be employed later on for the spin-glass phase where its effect is most crucial and the validity of the approximation will be examined by numerical methods. We use the following representation for the order parameters and the related conjugate variables [6]:

$$q_{\alpha, \beta, \dots, \gamma} = a \int dx \pi(x) \tanh^l(\beta x) \quad \text{and} \quad \hat{q}_{\alpha, \beta, \dots, \gamma} = b \int dy \hat{\pi}(y) \tanh^l(\beta y), \quad (4)$$

where l is the number of replica indices, $a = [(K-1)! N^{1-K} C]^{1/K}$ and $b = [(K-1)!]^{-1/K} [N C^{1/K}]^{K-1}$ are normalization coefficients, and $\pi(x)$ and $\hat{\pi}(y)$ represent probability distributions related to the integration variables. Throughout the letter, integrals with unspecified limits will denote integrals over the range $(-\infty, +\infty)$. One then obtains an expression for the free energy per spin expressed in terms of the probability distributions $\pi(x)$ and $\hat{\pi}(y)$:

$$\begin{aligned} \frac{1}{N} \langle \ln \mathcal{Z} \rangle_{J, \xi, \mathcal{A}} &= \frac{C}{K} \ln \cosh \beta + \frac{C}{K} \int \left[\prod_{l=1}^K dx_l \pi(x_l) \right] \left\langle \ln \left[1 + \tanh \beta J \prod_{j=1}^K \tanh \beta x_j \right] \right\rangle_J - \\ &- C \int dx dy \pi(x) \hat{\pi}(y) \ln [1 + \tanh \beta x \tanh \beta y] - C \int dy \hat{\pi}(y) \ln \cosh \beta y + \\ &+ \int \left[\prod_{l=1}^C dy_l \hat{\pi}(y_l) \right] \left\langle \ln \left[2 \cosh \beta \left(\sum_{j=1}^C y_j + F\xi \right) \right] \right\rangle_{\xi}. \end{aligned} \quad (5)$$

One should also point out that although the parameters \mathbf{x} and \mathbf{y} have been derived from the somewhat artificial set of conjugate variables they have been shown to have a physical meaning [7]: $\pi(x)$ representing the spin field distribution when a single connection is removed from the system, and $\hat{\pi}(y)$ is the cavity field distribution.

The saddle point equations, obtained by varying eq. (5) with respect to the probability distributions, provide a set of relations between $\pi(x)$ and $\hat{\pi}(y)$:

$$\begin{aligned} \pi(x) &= \int \left[\prod_{l=1}^{C-1} dy_l \hat{\pi}(y_l) \right] \left\langle \delta \left[x - \sum_{j=1}^{C-1} y_j - F\xi \right] \right\rangle_{\xi}, \\ \hat{\pi}(y) &= \int \left[\prod_{l=1}^{K-1} dx_l \pi(x_l) \right] \left\langle \delta \left[y - \frac{1}{\beta} \tanh^{-1} \left(\tanh \beta J \prod_{j=1}^{K-1} \tanh \beta x_j \right) \right] \right\rangle_J, \end{aligned} \quad (6)$$

from which the magnetization M , constituting our performance measure, can be calculated:

$$M = \frac{1}{N} \left\langle \sum_{i=1}^N \xi_i \text{sign} \langle S_i \rangle_T \right\rangle_{\xi} = \int dh \text{sign}(h) \int \left[\prod_{l=1}^C dy_l \hat{\pi}(y_l) \right] \left\langle \delta \left[h - \sum_{j=1}^C y_j - F\xi \right] \right\rangle_{\xi}, \quad (7)$$

where the subscript T denotes thermal averaging. The magnetization M represents our performance measure, denoting the normalized mean overlap between the dynamical vector $\text{sign}(\mathbf{S})_T$ and the original message ξ .

This set of equations may be solved numerically for general β , K and C . However, in the limit of $\beta \rightarrow \infty$ they can be simplified significantly and analytical results may be obtained. To

simplify the treatment we will consider only the case of unbiased patterns where $F = 0$; the case of biased patterns will be examined in future publications. We obtain the solutions

$$\begin{aligned}\pi(x) &= \int \left[\prod_{l=1}^{C-1} dy_l \hat{\pi}(y_l) \right] \delta \left[x - \sum_{j=1}^{C-1} y_j \right], \\ \hat{\pi}(y) &= \int \left[\prod_{l=1}^{K-1} dx_l \pi(x_l) \right] \langle \delta [y - \text{sign}(J x_1 \dots x_{K-1}) \min(|J|, x_1, \dots, x_{K-1})] \rangle_J. \quad (8)\end{aligned}$$

The general solution of these equations may result in probability distributions which comprise both singular (delta functions) and regular (continuous) distributions [8]. However, as the replica symmetric solution already represents an approximation (as in fact do higher-order replica symmetry-breaking steps), we will choose the simplest *self-consistent* set of solutions which will be validated later on by numerical solutions using different methods [7].

Since $J = \pm 1$, we choose an integer distribution of the form $\hat{\pi}(y) = p_+ \delta(y-1) + p_0 \delta(y) + p_- \delta(y+1)$ and the corresponding distribution $\pi(x) = \sum_{l=1-C}^{C-1} T_{[p_{\pm}, p_0; C]}(l)$, where

$$T_{[p_+, p_0, p_-; C]}(l) = \sum_{\{k, h, m; k-h=l; k+h+m=C-1\}} \frac{(C-1)!}{k! h! m!} p_+^k p_0^h p_-^m. \quad (9)$$

One then solves the closed set of equations for p_{\pm} , p_0 , and $\psi_{\pm} = \sum_{l=1}^{C-1} T_{[p_{\pm}, p_0; C]}(\pm l)$ iteratively [6].

We first consider the case of $K, C \rightarrow \infty$ (but $K, C \ll N$). Three different solutions emerge, corresponding to the paramagnetic, ferromagnetic and spin-glass phases. The paramagnetic solution ($M = 0$), which is valid also for general β , K and C , is of the form $\hat{\pi}(y) = \delta(y)$, $\pi(x) = \delta(x)$; it has the lowest possible free energy $-f_{\text{para}} = \alpha$ but its entropy $s_{\text{para}} = (1 - \alpha) \ln 2$ is positive only for $\alpha \leq 1$, corresponding to $R \geq 1$ which is irrelevant for the case of error-correcting codes. The ferromagnetic solution ($M = 1$), characterized by asymmetric distributions for both $\hat{\pi}(y)$ and $\pi(x)$ has a free energy $-f_{\text{ferro}} \rightarrow \alpha(1 - 2p)$ with a vanishing entropy $s_{\text{ferro}} \rightarrow 0$ as $K \rightarrow \infty$, indicating a unique solution in this limit.

The spin-glass solution has been calculated for both replica symmetric and the one-step replica symmetry-breaking (frozen spin glass, where the n replica are divided into groups of m identical solutions) ansätze. The former reduces to the paramagnetic solution, which is unphysical for $\alpha > 1$, while the latter yields $\hat{\pi}_{\text{IRSB}}(y) = \delta(y)$, $\pi_{\text{IRSB}}(x) = \delta(x)$ with $m = \beta_g(\alpha)/\beta$ and β_g obtained from the root of the replica symmetric entropy [9, 5] $s_{\text{RS}} = \alpha [\ln \cos \beta - \beta \tanh \beta] + \ln 2 = 0$. This implies a frozen state below $T_g = 1/\beta_g$ with a free energy $-f_{\text{IRSB}} = (\alpha/\beta_g) \ln \cos \beta_g + 1/\beta_g \ln 2$. One of the major results of this paper is the phase transition between the ferromagnetic and the spin-glass phases, depicted by the curved line in fig. 1a. This transition marks the critical value α_c for which error-free transmission can be obtained, given a flip rate p , constituting the maximal channel capacity. It can be calculated by equating f_{IRSB} and f_{ferro} to obtain

$$R_c = \frac{1}{\alpha_c} = 1 + (p \log_2 p + (1-p) \log_2(1-p)), \quad (10)$$

thus *retrieving Shannon's maximal channel capacity*.

This result seems to advocate the use of high values for K and C for obtaining high channel capacity. However, this result alone has little practical relevance without considering the decoding method used. Since simulated annealing and related methods may be the most natural approaches to the decoding task, we will examine the finite β solutions to eqs. (6).

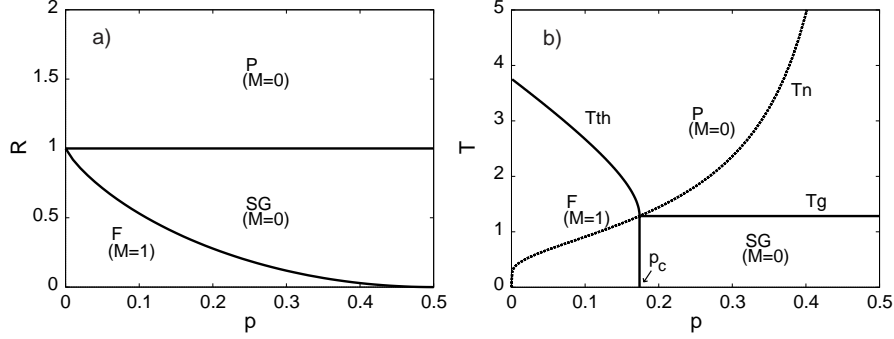


Fig. 1. – Phase diagrams for the case $K, C \rightarrow \infty$ as a function of the flip rate p . (a) For the zero-temperature case ($\beta \rightarrow \infty$) we retrieve Shannon’s maximal channel capacity represented by the phase transition between the ferromagnetic (F) and the spin-glass (SG) phases. (b) For finite temperatures we obtain different transition boundaries, shown here for $\alpha = 3$, which collapse to the critical flip probability p_c (Shannon’s limit) as $T \rightarrow T_g$; the dotted line represents Nishimori’s temperature T_n .

For the case $K, C \rightarrow \infty$ one can obtain solutions for finite temperatures, as long as $1 - 2p \gg \mathcal{O}(K^{-1/2})$, by exploiting the fact that $x = \sum_{l=1}^{C-1} y_l \approx (C-1) \langle y \rangle$ in the case of $C \rightarrow \infty$, where $\langle y \rangle \equiv \int dy y \hat{\pi}(y)$. The solution obtained for $\langle y \rangle$ suggests scaling the temperature with $(\ln K)/K$ and the emergence of a non-trivial ferromagnetic solution with $\langle y \rangle = 1 - 2p$ at $\beta_c = \ln K / 2\alpha K (1 - 2p)$. One can also obtain an expression for the free energy in the various phases as well as the phase diagram shown in fig. 1b for $\alpha = 3$ and different flip probabilities and temperatures. From fig. 1b we see that the transition boundaries collapse to Shannon’s limit as $T \rightarrow T_g$ which coincides with Nishimori’s temperature [10] for this flip rate. This is not surprising as the average spin alignment M in these systems calculated at Nishimori’s temperature provides an upper bound for the achievable alignment [11, 12] (although the fact that Shannon’s limit is achievable also in this case *is* significant).

The free energies for the ferromagnetic, paramagnetic and spin-glass phases at this point,

$$\begin{aligned}
 -f_{\text{ferro}} &= \alpha (1 - 2p), & -f_{\text{para}} &= (\alpha \ln \cosh \beta + \ln 2) / \beta \\
 \text{and} & & -f_{\text{IRSB}} &= (\alpha \ln \cosh \beta_g + \ln 2) / \beta_g,
 \end{aligned} \tag{11}$$

suggest a paramagnetic-to-ferromagnetic transition at temperatures of $\mathcal{O}(1)$, while the ferromagnetic solution emerges at $1/\beta_c$. This indicates the existence of high-energy barriers of $\mathcal{O}(1/\beta_c) \sim \mathcal{O}(K/\ln K)$ between the ferromagnetic and the paramagnetic phases at the transition point, which will require a prohibitively long time to allow for the transition itself, thus preventing the annealing process from converging to the global minimum⁽¹⁾. Although these expressions (eqs. (11)) have been obtained for $K, C \rightarrow \infty$, we may expect the energy barriers for finite K and C values to be small.

In the remainder of this paper we will therefore investigate the case of finite K and C when $\beta \rightarrow \infty$ which is of considerable practical relevance. From the numerical solutions of eqs. (8), obtained by solving iteratively the equations for p_{\pm} , p_0 , and ψ_{\pm} , we can plot the magnetization and the free energy as functions of the flipping rate p for $K = 2 \dots 6$, shown in fig. 2a. The results presented in fig. 2a for $\alpha = 2$ enable us to assess the efficiency of codes based on

⁽¹⁾ The annealing process commences at high temperatures, where the system is typically in the paramagnetic phase, and should be terminated below the transition temperature, allowing the system to settle in the ferromagnetic solution.

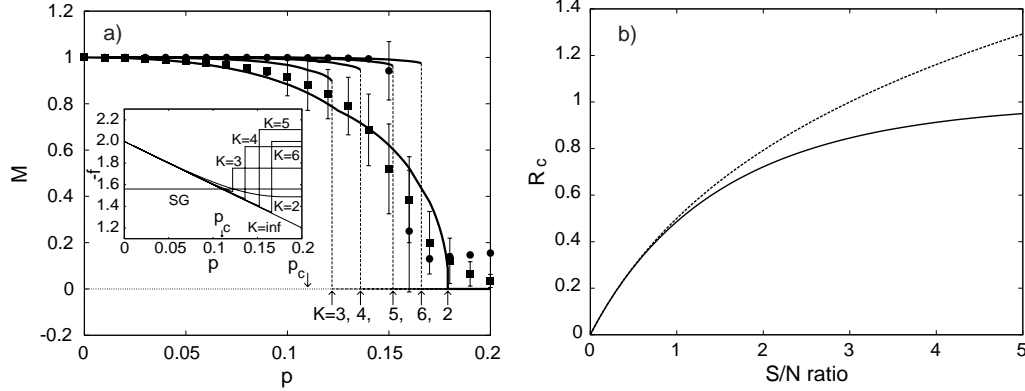


Fig. 2. – (a) The dependence of M on the flip rate p for $K = 2 \dots 6$; note the second-order phase transition characterizing the $K = 2$ case in contrast to the first-order transition for $K \geq 3$. Numerical results for the cases of $K = 2, 5$ are consistent with the theoretical solutions. Inset: free energies obtained for the ferromagnetic and the spin-glass solutions. (b) Critical code rate R_c as a function of the signal-to-noise ratio in the case of a Gaussian channel (solid line); Shannon's bound is represented by the dashed curve.

different choices of K . We note that the case $K = 2$ shows a second-order phase transition in contrast to the first-order phase transition characterizing the other cases; spinodal points for higher K values are obtained for higher values of p , converging to $p = 0.5$ as $K \rightarrow \infty$. To validate the replica symmetric ansatz and the discrete solutions assumed for the probabilities $\pi(x)$ and $\hat{\pi}(y)$, we also plotted numerical solutions obtained by employing a different method based on the TAP approach for diluted systems [7]. The numerical results, showing the mean and variance of 100 iterative solutions obtained after 30 and 10 iterations for the cases of $K = 2$ and 5, respectively, show consistency with the theoretical solutions. Initial conditions were chosen at random for the case of $K = 2$ and close to the theoretical solution for the case of $K = 5$ to avoid getting stuck in glassy solutions. The $M > 0$ solutions after the phase transition for $K = 5$ are an artifact of the spin-glass phase where an exponentially long time is required before converging to the system's ground state.

The free energies presented in the inset (including $K \rightarrow \infty$) show how the solutions are dominated initially by the ferromagnetic phase until a certain value p_c , in which the spin-glass phase takes over (lower free energy). Solutions obtained after the phase transition for $K = 3 \dots 6$, which seem to have lower free energies, are unphysical as the related entropies become negative. Note that the values obtained for p_c become almost identical for $K > 3$, indicating a modest loss in corrective capabilities due to the use of small K values. The nature of the solutions and of the phase transitions will be described elsewhere.

The analysis presented in this letter has been restricted so far to the case of Binary Symmetric Channel, characterized by some flip rate probability p . The methods used here may be also employed for analyzing general noisy channels and other encoding/decoding methods. For instance, in the case of $K, C \rightarrow \infty$ ($K, C \ll N$), analyzing the capacity of a noisy channel, whereby the encoded message is corrupted by a zero mean Gaussian noise, one obtains the following expressions for the ferromagnetic and spin-glass free energies:

$$-f_{\text{ferro}} = \alpha \langle J \rangle_J = \alpha \langle J \tanh \beta_n J \rangle_J \quad \text{and} \quad -f_{\text{1RSB}} = \alpha / \beta_g \langle \ln \cosh \beta_g J \rangle_J + (\ln 2) / \beta_g, \quad (12)$$

where β_n is Nishimori's temperature [10,11] for the particular type of noise examined. Equating the free energies for the ferromagnetic and spin-glass solutions (eq. (12)), one obtains an

expression for the critical code rate R_c , using the fact that at the critical point $\beta_g = \beta_n$

$$R_c = \frac{1}{\alpha_c} = \frac{\beta^2}{\ln 2} \frac{\partial}{\partial \beta} \left[\frac{1}{\beta} \langle \ln \cosh \beta J \rangle_J \right] \Big|_{\beta=\beta_n} . \quad (13)$$

The dependency of the critical rate R_c on the signal-to-noise ratio (solid line), shown in fig.2b, indicates a significantly lower critical rate than Shannon's bound in this case (dashed line, $1/2 \log(1 + v/\sigma^2)$, where v/σ^2 is the signal-to-noise ratio) due to the use of a binary code while allowing the signal (and the noise) to acquire real values.

In this letter we examined an encoding scheme, analyzed previously by Sourlas for the limited case of an infinite ratio between the connectivity C and the number of sites sampled K , where the code rate R vanishes. Our study tackles the practical case of finite R , showing that for zero temperature and $K, C \rightarrow \infty$, one retrieves Shannon's bound for the channel capacity. However, studying the solution for finite temperatures reveals high-energy barriers which evolve in an annealing decoding schedule, separating the desired global solution from those obtained earlier in the annealing process. Examining the solutions for low K and C values shows that one may avoid these barriers with some modest loss in performance. The results and the approximations taken have been validated by numerical solutions using other methods. In addition, we extended the calculation to the case of Gaussian transmission noise, obtaining an expression for the critical code rate; the deviation between the code rate achieved by using Sourlas's code and Shannon's bound in this case may be explained by the use of binary transmitted bits in comparison to the real-valued nature of the corruption process.

A refinement of our approximation as well as the study of different noise types and of biased messages is under way. We also currently examine state of the art encoding/decoding schemes, focusing on the efficiency of Gallager codes [13], which have recently been rediscovered [14] and seem to have a significant practical potential.

This work was partially supported by the RFTF program of the Japanese Society for the Promotion of Science (YK) and by EPSRC grant GR/L19232 (DS).

REFERENCES

- [1] SHANNON C. E., *Bell Sys. Tech. J.*, **27** (1948) 379; 623.
- [2] SOURLAS N., *Nature*, **339** (1989) 693.
- [3] SOURLAS N., *Europhys. Lett.*, **25** (1994) 159.
- [4] SHERRINGTON D. and KIRKPATRICK S., *Phys. Rev. Lett.*, **35** (1975) 1792.
- [5] DERRIDA B., *Phys. Rev. B*, **24** (1981) 2613.
- [6] WONG K. Y. M. and SHERRINGTON D., *J. Phys. A*, **20** L793 (1987); SHERRINGTON D. and WONG K. Y. M., *J. Phys. A*, **20** (1987) L785.
- [7] KABASHIMA Y. and SAAD D., to be published in *Europhys. Lett.* (1998).
- [8] DE DOMINICIS C. and MOTTISHAW P., *J. Phys. A*, **20** (1987) L1267.
- [9] GROSS D. J. and MEZARD M., *Nucl. Phys. B*, **240** (1984) 431.
- [10] NISHIMORI H., *J. Phys. C* **13**, (1980) 4071.
- [11] NISHIMORI H., *J. Phys. Soc. Jpn.*, **62** (1993) 2973.
- [12] RUJÁN P., *Phys. Rev. Lett.*, **70** (1993) 2968.
- [13] GALLAGER R. G., *IRE Trans. Info. Theory*, **IT-8** (1962) 21.
- [14] MACKAY D. J. C. and NEAL R. M., *Electronic Lett.*, **33** (1997) 457.