EUROPHYSICS LETTERS

Europhys. Lett., (), pp. ()

Statistical mechanics of typical set decoding

YOSHIYUKI KABASHIMA[1](*), KAZUTAKA NAKAMURA[1](**) AND JORT VAN MOURIK[2](***)

[1] *Department of Computational Intelligence and Systems Science, Tokyo Institute of Technology, Yokohama 2268502, Japan.*
[2] *The Neural Computing Research Group, Aston University, Birmingham B4 7ET, UK.*

(received ; accepted)

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. – The performance of "typical set (pairs) decoding" for ensembles of Gallager's linear code is investigated using statistical physics. In this decoding scheme, an error occurs when the information transmission is corrupted by an untypical noise, or when two or more typical sequence/noise combinations satisfy the parity check equations provided by the received codeword. We show that the average error rate for the latter case over a given code ensemble can be tightly evaluated using the replica method, including the sensitivity to the message length. Our approach generally improves the existing analysis known in information theory community as reintroduced by MacKay (1999), which is believed to be the most accurate to date.

Triggered by active investigations on error correcting codes in both information theory (IT) and statistical physics (SP) communities [9, 17, 1, 6, 7, 21, 16], there is growing interest in the relationship between IT and SP. As it has turned out that both frameworks can be employed to investigate similar subjects, it is natural to expect that standard techniques known in one framework bring about novel developments in the other, and vice versa.

The purpose of this Letter is to present such an example. More specifically, we will show that a method to evaluate the performance of well established error correcting codes in IT community [1, 9, 20] can be generally improved by introducing the replica method. This serves as a direct answer to the question from IT researchers why the methods from physics generally seem to provide more optimistic bounds than those known in the IT literature. As will become clear in our formulation, the IT method is naturally linked to the SP analysis through the number of replicas $\rho \geq 0$. In a general scenario, the N dimensional Boolean message $\boldsymbol{x} \in \{0,1\}^N$ is encoded to the $M(> N)$ dimensional Boolean vector $\boldsymbol{y}^0$, and transmitted

(*) kaba@dis.titech.ac.jp
(**) knakamur@fe.dis.titech.ac.jp
(***) vanmourj@aston.ac.uk

via a noisy channel. Although here we have opted for a Binary Symmetric Channel (BSC) characterized by an independent flip probability p per bit, other transmission channels may also be examined within a similar framework. At the other end of the channel the corrupted codeword is decoded using the structured codeword redundancy.

The error correcting code that we focus on here, is Gallager's linear code [3]. This code was originally introduced by Gallager about forty years ago but was forgotten soon after the proposal due to the technological limitations in those days. However, since the recent rediscovery by MacKay and Neal [9], it is now recognized as one of the best codes to date.

A Gallager code is characterized by a randomly generated $(M$–$N) \times M$ Boolean sparse parity check matrix H, with K and $C(\geq 3)$ non-zero (unit) elements per row and column, respectively. Encoding the message vector $\boldsymbol{x}$ is carried out using the $M \times N$ generating matrix G^T satisfying the condition $HG^T = 0$, where $\boldsymbol{y}^0 = G^T\boldsymbol{x}$ (mod 2). The M bit codeword $\boldsymbol{y}^0$ is transmitted via a noisy channel (BSC); the corrupted vector $\boldsymbol{y} = \boldsymbol{y}^0 + \boldsymbol{n}^0$ (mod 2) is received at the other end, where $\boldsymbol{n}^0 \in \{0,1\}^M$ represents a noise vector with an independent probability p per bit of having a value 1. Decoding is carried out by multiplying $\boldsymbol{y}$ by the parity check matrix H, to obtain the syndrome vector $\boldsymbol{z} = H\boldsymbol{y} = H(G^T\boldsymbol{x} + \boldsymbol{n}^0) = H\boldsymbol{n}^0$ (mod 2), and to find a solution to the parity check equation

$$H\boldsymbol{n} = \boldsymbol{z} \ (\text{mod } 2) \ , \tag{1}$$

for estimating the true noise vector $\boldsymbol{n}^0$. The estimate $\boldsymbol{x}$ for the original message is then obtained from the equation $G^T\boldsymbol{x} = \boldsymbol{y}$–$\boldsymbol{n}$ (mod 2).

Several schemes can be employed for solving Eq. (1). In recent years, maximum a posteriori (MAP) decoding and the maximizer of posterior marginal (MPM) decoding have been widely investigated [21, 15, 18, 7], which correspond to decoding at zero and at Nishimori's temperature, respectively. Here, we will evaluate the performance of a scheme called *typical set (pairs) decoding*, which was pioneered by Shannon [20], and reintroduced by MacKay [9] for analyzing the Gallager-type codes. Although this decoding method is slightly weaker in reducing the block and/or bit error rates, it is now becoming popular in IT community [1, 2, 9] since a rigorous analysis is easier than for the two decoding schemes mentioned above.

In order to explain typical set decoding, we must first introduce the definition of being *typical*. Due to the law of large numbers, a noise vector $\boldsymbol{n}$ generated by the BSC satisfies the condition

$$\left| \frac{1}{M} \sum_{l=1}^{M} n_l - p \right| \leq \epsilon_M \, , \tag{2}$$

with a high probability for large M and any sequence of positive number $\epsilon_M \sim \mathcal{O}(M^{-\gamma})$ $(0 < \gamma < 1/2)$. A vector $\boldsymbol{n}$ is classified as *typical* when this condition is satisfied, and the *typical set* is the set of all typical vectors.

Then, one can define the typical set decoding as a scheme to select a vector $\boldsymbol{n}$ that belongs to the typical set and satisfies Eq. (1), as an estimate of the true noise $\boldsymbol{n}^0$. In the case that two or more typical vectors satisfy Eq. (1), an error is automatically declared [9]. For this scheme, two types of decoding error can happen: the first possibility, referred to as a type I error here, happens when the true noise $\boldsymbol{n}^0$ is not typical, while the other one, referred to as a type II error, happens when there are two or more typical vectors that satisfy Eq. (1) while the true noise $\boldsymbol{n}^0$ is typical. It can be shown that the probability for the type I error, P_I, vanishes in the limit $M \to \infty$. Therefore, we will here focus on the evaluation of the probability for a type II error, P_{II}.

In what follows, we replace the Boolean notation by a binary one through the mapping $\{0, 1, +\} \to \{+1, -1, \times\}$. We can now introduce the *error indicator* function that takes the

value 1 when an error occurs and 0 otherwise:

$$\Delta\left(\boldsymbol{n}^0, H\right) = \lim_{\rho \to +0} \mathcal{V}_{NF}^{\rho}(\boldsymbol{n}^0, H), \tag{3}$$

with

$$\begin{aligned} \mathcal{V}_{NF}(\boldsymbol{n}^0, H) &\equiv \operatorname*{Tr}_{\boldsymbol{n} \neq \boldsymbol{n}^0} \prod_{\mu=1}^{M-N} \delta\left(\prod_{l \in \mathcal{L}(\mu)} n_l^0, \prod_{l \in \mathcal{L}(\mu)} n_l \right) \delta\left(\sum_{l=1}^{M} n_l - M(1-2p) \right) \\ &= \operatorname*{Tr}_{\boldsymbol{n} \neq \mathbf{1}} \prod_{\mu=1}^{M-N} \delta\left(1; \prod_{l \in \mathcal{L}(\mu)} n_l \right) \delta\left(\sum_{l=1}^{M} n_l^0 n_l - M(1-2p) \right), \end{aligned} \tag{4}$$

where $\mathbf{1}$ denotes the M dimensional vector with all elements 1, and where $\mathcal{L}(\mu)$ is the set of indices that have non-zero elements in the μ th row in the parity check matrix H. In the second line of Eq. (4), we have introduced the gauge transform $n_l \to n_l^0 n_l$ for further convenience. The quantity $\mathcal{V}_{NF}(\boldsymbol{n}^0, H)$ is the number of vectors that differ from $\boldsymbol{n}^0$ in the intersection of the typical set and the solution space of Eq. (1).

From the definition, the probability for a type II error for a given matrix H is given by $P_{II}(H) = \left\langle \Delta(\boldsymbol{n}^0, H) \delta\left(\sum_{l=1}^{M} n_l^0 - M(1-2p) \right) \right\rangle_{\boldsymbol{n}^0}$, where $\langle \cdots \rangle_{\boldsymbol{n}^0} = \operatorname{Tr}_{\boldsymbol{n}^0} (\cdots) \exp[F \sum_{l=1}^{M} n_l^0] / (2\cosh F)^M$ with $F = \frac{1}{2} \ln[(1-p)/p]$. Since the parity check matrix H is generated somewhat randomly, it is natural to evaluate the average of $P_{II}(H)$ over an ensemble of codes with given K and C as a performance measure for the code ensemble.In the large M limit, this average is given by $\overline{P_{II}} = \lim_{\rho \to +0} \exp\left[-M \mathcal{E}(\rho)\right]$, with

$$\mathcal{E}(\rho) \equiv -\frac{1}{M} \ln \left\langle \left\langle \mathcal{V}_{NF}^{\rho}(\boldsymbol{n}^0, H) \delta\left(\sum_{l=1}^{M} n_l^0 - M(1-2p) \right) \right\rangle_{\boldsymbol{n}^0} \right\rangle_H, \tag{5}$$

where $\langle \cdots \rangle_H$ is the uniform average over the parity check matrices with given K and C.

At this point, it is worth mentioning some general properties of the exponent $\mathcal{E}(\rho)$:
- In the $M \to \infty$ limit, for a sufficiently small noise p, $\overline{P_{II}}$ is expected to vanish, corresponding to $\mathcal{E}(0) = \lim_{\rho \to +0} \mathcal{E}(\rho) > 0$. The highest noise level p_c with $\mathcal{E}(0) > 0$ is the so-called *error threshold* [1]. Furthermore, the value of $\mathcal{E}(0) (> 0)$ gives the sensitivity of $\overline{P_{II}}$ with respect to the message length and is a performance measure of the code ensemble for when M is finite.
- Since $\mathcal{V}_{NF}(\boldsymbol{n}^0, H)$ takes the values $0, 1, 2, \ldots$, $\mathcal{V}_{NF}^{\rho}(\boldsymbol{n}^0, H)$ must increase with $\rho (> 0)$, and hence $\mathcal{E}(\rho)$ must be a decreasing function of $\rho (> 0)$. We have that

$$\frac{\partial \mathcal{E}(\rho)}{\partial \rho} = -\frac{1}{M} \frac{\left\langle \left\langle \mathcal{S}_{NF}(\boldsymbol{n}^0, H)\ \mathcal{V}_{NF}^{\rho}(\boldsymbol{n}^0, H)\ \delta\left(\sum_{l=1}^{M} n_l^0 - M(1-2p) \right) \right\rangle_{\boldsymbol{n}^0} \right\rangle_H}{\left\langle \left\langle \mathcal{V}_{NF}^{\rho}(\boldsymbol{n}^0, H)\ \delta\left(\sum_{l=1}^{M} n_l^0 - M(1-2p) \right) \right\rangle_{\boldsymbol{n}^0} \right\rangle_H} < 0, \tag{6}$$

where $\mathcal{S}_{NF}(\boldsymbol{n}^0, H) = \ln \mathcal{V}_{NF}(\boldsymbol{n}^0, H)$, i.e. the entropy of the solutions ($\neq \boldsymbol{n}^0$) of Eq. (1) in the typical set. Furthermore, we have that $\partial^2 \mathcal{E}(\rho) / \partial \rho^2 < 0$, such that $\mathcal{E}(\rho)$ is a convex function.

We are now ready to connect the current argument to the existing analysis of the typical set decoding [20, 9, 1]. Since $\mathcal{E}(0) \geq \mathcal{E}(1)$, the condition $\mathcal{E}(1) = 0$ yields a *lower* bound for p_c. For $\rho = 1$ in Eq. (5), it is convenient to insert the identity $1 = \int M d\omega\ \delta\left(\sum_{l=1}^{M} n_l - M\omega \right)$ in the final form of Eq. (4). Then, for a sequence $\boldsymbol{n}$ that satisfies $(1/M) \sum_{l=1}^{M} n_l = \omega$, one obtains $\left\langle \operatorname{Tr}_{\boldsymbol{n}} \delta\left(\sum_{l=1}^{M} n_l^0 n_l - M(1-2p) \right) \delta\left(\sum_{l=1}^{M} n_l^0 - M(1-2p) \right) \right\rangle_{\boldsymbol{n}^0} \sim \exp\left[-M \mathcal{K}(\omega, p)\right]$, where $\mathcal{K}(\omega, p) = \left(\frac{1+\omega}{2}\right) H\left(\frac{2(1-2p)}{1+\omega}\right) + \left(\frac{1-\omega}{2}\right) \ln 2 - H(1-2p)$ and $H(x) = -\frac{(1+x)}{2} \ln \frac{(1+x)}{2} - \frac{(1-x)}{2} \ln \frac{(1-x)}{2}$.

The remaining average required in Eq. (5) is now evaluated as $\langle \mathrm{Tr}_{\boldsymbol{n}}\, \delta\left(\sum_{l=1} n_l - M\omega\right) \prod_{\mu=1}^{M-N} \delta\left(1; \prod_{l\in\mathcal{L}(\mu)} n_l\right)\rangle_H \sim \exp\left[M\mathcal{R}\left(\omega\right)\right]$. The exponent $\mathcal{R}\left(\omega\right)$ is the so-called *weight enumerator* [1, 9], which in the current context([1]), provides an averaged distribution of the distances between the true noise $\boldsymbol{n}^0$ and other vectors that satisfy Eq. (1), and plays an important role in the evaluation of the performance of codes in conventional coding theory [10]. One obtains $\mathcal{E}(1) = \mathrm{Ext}_{\omega(\neq 1)}\left\{\mathcal{K}(\omega, p) - \mathcal{R}(\omega)\right\}$, corresponding to Eq. (4.7) in [1].

However, it should be emphasized here that the calculation above (for $\rho = 1$) generally overestimates the decoding error probability. This is because for $\rho = 1$, $\Delta\left(\boldsymbol{n}^0, H\right)$, which should be one when a type II error occurs is replaced by the number of wrong vectors $\mathcal{V}_{NF}$ which can be exponentially large in M, and therefore contributes too much for counting one error. To obtain an accurate (exact) estimate suppressing such an overestimation, one has to introduce a positive exponent ρ in the calculation and take a limit $\rho \to +0$ as is shown in Eq. (3). This can be done by means of the replica method, where ρ becomes the number of replicas. This procedure gives rise to a set of order parameters $q_{\alpha,\beta,\ldots,\gamma} = (1/M)\sum_{l=1}^{M} Z_l n_l^{\alpha} n_l^{\beta} \ldots n_l^{\gamma}$, where $\alpha, \beta, \ldots$ represent replica indices and where the variables $Z_l,\ l = 1, \ldots, M$ arrise from enforcing the restriction that there are C connections per index l (see [7] for details).

To proceed with the calculation one requires a certain ansatz about the symmetry of the order parameters. As a first approximation we assume replica symmetry (RS) in the order parameters $q_{\alpha,\beta,\ldots,\gamma} = q\int dx\ \pi(x)\ x^l$, and their conjugate variables $\widehat{q}_{\alpha,\beta,\ldots,\gamma} = \widehat{q}\int d\widehat{x}\ \widehat{\pi}\ (\widehat{x})\widehat{x}^l$, where l denotes the number of replica indices, q and $\widehat{q}$ are normalization variables for defining $\pi(\cdot)$ and $\widehat{\pi}(\cdot)$ as distributions. Unspecified integrals are carried out over the interval $[-1, 1]$. Details of a similar calculation can be found in [7].

Originally, the summation $\mathrm{Tr}_{\boldsymbol{n}\neq\boldsymbol{1}}(\cdot)$ excludes the case $\boldsymbol{n} = \boldsymbol{1}$, but one can show that in the large M limit, this becomes identical to the full summation in the non-ferromagnetic phase, where $\pi(x) \neq \delta(x-1)$ and $\widehat{\pi}(x) \neq \delta(\widehat{x}-1)$. In addition, we employ Morita's scheme [12] which in this case converts the restricted annealed average with respect to $\boldsymbol{n}^0$ to a quenched one:

$$\frac{1}{M}\ln\left\langle (\cdots) \times \delta\left(\sum_{l=1}^{M} n_l^0 - M(1-2p)\right)\right\rangle_{\boldsymbol{n}^0} = \frac{1}{M}\left\langle \ln(\cdots)\right\rangle_{\boldsymbol{n}^0}, \tag{7}$$

to simplify the calculation of the average over $\boldsymbol{n}^0$ in Eq. (5) considerably. We obtain

$$\begin{aligned}
\mathcal{E}(\rho) \;=\; & \underset{\{q,\widehat{q},\pi(\cdot),\widehat{\pi}(\cdot),G\}}{\mathrm{Ext}^{*}} \left\{ -\frac{C\ q^K}{K}\int\prod_{i=1}^{K} dx_i \pi(x_i)\left(\frac{1+\prod_{i=1}^{K} x_i}{2}\right)^{\rho}\right. \\
- \; & \left\langle \ln\left[\int\prod_{\mu=1}^{C} d\widehat{x}_{\mu}\ \widehat{\pi}(\widehat{x}_{\mu})\left(\underset{n=\pm 1}{\mathrm{Tr}}\, e^{Gn^0 n}\prod_{\mu=1}^{C}\left(\frac{1+\widehat{x}_{\mu}\ n}{2}\right)\right)^{\rho}\right]\right\rangle_{n^0} \\
- \; & \left. C\ln\widehat{q} + Cq\widehat{q}\int dx\ d\widehat{x}\ \pi(x)\ \widehat{\pi}(\widehat{x})\left(\frac{1+x\widehat{x}}{2}\right)^{\rho} + \left(\frac{C}{K} - C\right) + \rho\, G(1-2p)\right\},
\end{aligned} \tag{8}$$

where $\langle(\cdots)\rangle_{n^0} = \mathrm{Tr}_{n^0=\pm 1}(\cdots)\exp\left[Fn^0\right]/2\cosh F$ and $\mathrm{Ext}^{*}_{\{\ldots\}}$ denotes the functional extremization excluding the possibility of $\pi(x) = \delta(x\text{–}1)$ and $\widehat{\pi}(\widehat{x}) = \delta(\widehat{x}\text{–}1)$ as is introduced in [8].

-In the limit $K, C \to \infty$ (keeping the code rate $R = N/M = 1 - C/K$ finite), we find two analytical solutions for $\pi(x)$ and $\widehat{\pi}(\widehat{x})$:

([1]) The weight enumerator is usually introduced for the distance between codewords [1, 9, 10]. However, since $\boldsymbol{y}^0 - \boldsymbol{y}^1 = \boldsymbol{n}^0 - \boldsymbol{n}^1$ (mod 2) holds for two sets of Boolean vectors $(\boldsymbol{y}^0, \boldsymbol{n}^0)$ and $(\boldsymbol{y}^1, \boldsymbol{n}^1)$ that satisfy $\boldsymbol{y} = \boldsymbol{y}^0 + \boldsymbol{n}^0 = \boldsymbol{y}^1 + \boldsymbol{n}^1$ (mod 2), the distance between the noise vectors $\boldsymbol{n}^0$ and $\boldsymbol{n}^1$ is identical to that for the codewords $\boldsymbol{y}^0$ and $\boldsymbol{y}^1$.

1. $\pi(x) = \frac{1}{2}[(1 + (1\text{–}2p))\delta(x - (1\text{–}2p)) + (1 - (1\text{–}2p))\delta(x + (1\text{–}2p))]$, $\widehat{\pi}(\widehat{x}) = \delta(\widehat{x})$
2. $\pi(x) = \frac{1}{2}[\delta(x-1) + \delta(x+1)]$, $\widehat{\pi}(\widehat{x}) = \frac{1}{2}[\delta(\widehat{x}-1) + \delta(\widehat{x}+1)]$.

providing $\mathcal{E}(\rho) = \rho\ [H((1-2p)) - (1-R)\ln 2]$ and $\mathcal{E}(\rho) = H((1-2p))$–$(1\text{–}R)\ln 2$, respectively. One can show that both solutions are locally stable against replica symmetry breaking perturbations. Selecting the relevant branch, i.e. the one with the lower exponent for $\rho \geq 1$, and taking the limit $\rho \to 0$ [5], one obtains the exponent as

$$\mathcal{E}(0) = \lim_{\rho \to +0} \mathcal{E}(\rho) = \begin{cases} (R_c - R)\ln 2, & R < R_c, \\ 0, & R > R_c, \end{cases} \tag{9}$$

where $R_c = 1 + p\log_2 p + (1\text{–}p)\log_2(1\text{–}p)$ corresponds to Shannon's limit [19].

Note that in the vicinity of $R \sim R_c$, this exponent exceeds the upper bound for the possible reliability function that represents the vanishing rate of the decoding error probability for the best code [11, 8]. However, this does not imply a contradiction because the current analysis is just for $\overline{P_{II}}$ while the convergence rate of P_I is slower than that of the reliability function.

-For finite K and C, one has to obtain $\mathcal{E}(\rho)$ via numerical methods. Like in the case of $K, C \to \infty$, generally two branches of solutions appear:

1. continuous distributions for $\pi(x)$ and $\widehat{\pi}(\widehat{x})$, for which $\lim_{\rho \to +0} \mathcal{E}(\rho) = 0$.
2. ρ independent frozen distributions $\pi(x) = \frac{1}{2}[(1+b)\ \delta(x-1) + (1-b)\ \delta(x+1)]$, $\widehat{\pi}(\widehat{x}) = \frac{1}{2}[(1+\widehat{b})\ \delta(\widehat{x}-1) + (1-\widehat{b})\ \delta(\widehat{x}+1)]$.

The parameters b and $\widehat{b}$ are determined from the extremization problem (8) by setting $\rho = 1$, the functional extremization with respect to $\pi(\cdot)$ and $\widehat{\pi}(\cdot)$ is then reduced to that of the first moments $b = \int dx x \pi(x)$ and $\widehat{b} = \int d\widehat{x}\widehat{x}\widehat{\pi}(\widehat{x})$. The exponent of this branch is completely frozen to that for $\rho = 1$ as $\mathcal{E}(\rho) = \mathcal{E}(1)$ for $\forall \rho > 0$. Although the distributions of the two branches look quite different, their exponents coincide at $\rho = 1$ in any situation.

Note that the frozen branch corresponds to the conventional IT analysis [1, 9], and would provide the exact estimate in absence of other solutions. However, in order to take an appropriate limit $\lim_{\rho \to +0} \mathcal{E}(\rho)$, one has to select the dominant branch for $\rho \geq 1$ [5] among the existing solutions, and our analysis indicates that the frozen branch does not necessarily provide the correct exponent for $\rho \to +0$ (Fig. 1).

When the channel noise p is sufficiently high (Fig. 1 (a)), the exponent for the continuous branch is monotonically decreasing with respect to ρ which implies this is the dominant branch for $\rho \geq 1$. This provides $\lim_{\rho \to +0} \mathcal{E}(\rho) = 0$. However, for lower p, $\mathcal{E}(\rho)$ of the continuous branch is maximized to a positive value at a certain value ρ_g(Fig. 1 (b)). In this situation, the solution for $0 < \rho < \rho_g$ is physically wrong because inequality (6) does not hold. This implies that the RS ansatz is no longer valid, and the frozen replica symmetry breaking (RSB) solution [4] (a one step RSB ansatz under the constraint $(1/M)\boldsymbol{n}^a \cdot \boldsymbol{n}^b = 1$ for replica indices a and b in the same subgroup) is a suitable scheme for obtaining a consistent solution. Employing this 1RSB solution, one finds $\mathcal{E}(\rho) = \mathcal{E}(\rho_g)$ for $0 < \rho < \rho_g$, which implies $\lim_{\rho \to +0} \mathcal{E}(\rho) = \mathcal{E}(\rho_g) > 0$ indicating a vanishing behaviour of $\overline{P_{II}} \sim \exp[-M\mathcal{E}(\rho_g)]$. Hence, the critical condition for determining the error threshold p_c is given by $\partial \mathcal{E}(\rho)/\partial\rho|_{\rho \to +0} = 0$, as computed from the continuous solution. Employing the gauge transform [15], one can show that the variational parameter G in Eq. (8) enforcing $\sum_{l=1}^{M} n_l^0 n_l = M(1-2p)$ coincides with F in this limit. The critical condition can now be summarized as

$$F(1-2p) - \frac{1}{M}\left\langle\left\langle \ln\left[\operatorname*{Tr}_{\boldsymbol{n}\neq\boldsymbol{1}} \prod_{\mu=1}^{M-N} \delta\left(1; \prod_{l\in\mathcal{L}(\mu)} n_l\right) e^{F\sum_{l=1}^{M} n_l^0 n_l}\right]\right\rangle_H\right\rangle_{n^0} = 0, \tag{10}$$

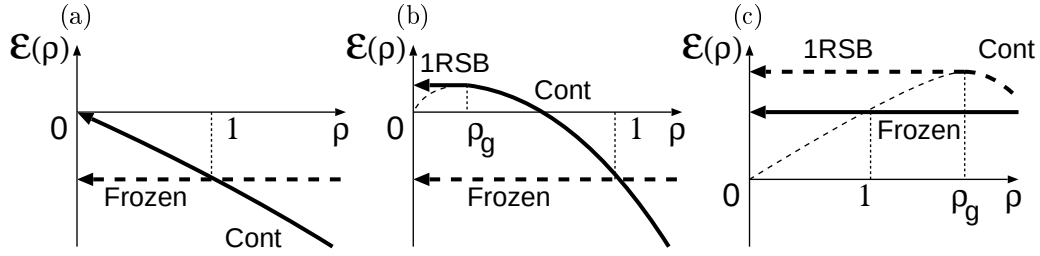
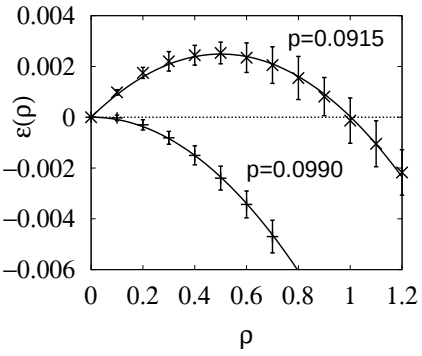


Fig. 1. – Appropriate limits for $\lim_{\rho\to+0}\mathcal{E}(\rho)$ in the case of finite K and C. The solution that has the lower exponent for $\rho \geq 1$ should be selected as the relevant branch [5], which is drawn as a thick curve or line in each case. For $p \geq p_c$ (a), the continuous solution is relevant while the 1(frozen)RSB solution which emerges from this solution at $\rho = \rho_g$ provides an appropriate exponent $\mathcal{E}(\rho_g)$ for $p_b \leq p < p_c$ (b). For $0 < p < p_b$ (c), the frozen (RS) solution is relevant. In the limit $K,\ C \to \infty$, the situation (b) does not appear.

(a)



(b)

(K, C)	$(6,3)$	$(5,3)$	$(6,4)$	$(4,3)$
Code rate	$1/2$	$2/5$	$1/3$	$1/4$
IT	0.0915	0.129	0.170	0.205
Current Method	0.0990	0.136	0.173	0.209
Shannon's limit	0.109	0.145	0.174	0.214

Fig. 2. – (a): Numerically computed $\mathcal{E}(\rho)$ of the continuous branch for $p = 0.0915,\ 0.0990$ for $K = 6$ and $C = 3$ $(R = 1/2)$. Symbols and error bars are obtained from 50 numerical solutions. Curves are computed via a quadratic fit. For $p = 0.0915$, $\mathcal{E}(\rho)$ is maximized to a positive value $\mathcal{E}(\rho_g) \simeq 2.5 \times 10^{-3}$ for $\rho_g \simeq 0.5$ while it vanishes at $\rho \simeq 1$ as is suggested in the IT literature [1]. On the other hand, for $p = 0.0990$, our predicted threshold, it is maximized to zero at $\rho \simeq 0$, which implies that this is the correct threshold. (b): Comparison of the estimates of p_c between the IT and the current methods is summarized in a table. The estimates for the IT method are taken from [1]. The numerical precision is up to the last digit for the current method. Shannon's limit denotes the highest possible p_c for a given code rate.

which is identical to what has been obtained for the phase boundary of the ferro-paramagnetic transition along the Nishimori's temperature predicted by the existing replica analysis [7, 8].

As p is reduced further, the position of the maximum ρ_g moves to the right and exceeds $\rho = 1$ at another critical noise rate p_b. This implies that below p_b the limit $\rho \to +0$ is governed by the frozen (RS) solution which is identical to what is given by the conventional IT analysis (Fig. 1(c)). Since this situation is realized only sufficiently below the threshold, the solution is of no use for direct evaluation of p_c, although it provides a lower bound.

Finally, we examined the case of $K = 6$ and $C = 3$ to demonstrate the accuracy of the estimated threshold. We numerically evaluated $\mathcal{E}(\rho)$ of the continuous branch for $p = 0.0915$, a recent highly accurate estimate of the error threshold for this parameter choice [1] and for $p = 0.0990$, which is the threshold predicted by the replica method [14, 8]. The numerical results are obtained by approximating $\pi(\cdot)$ and $\widehat{\pi}(\cdot)$ using 10^6 dimensional vectors and iterating the saddle point equations until convergence. The obtained results are shown in Fig. 2 (a); it

indicates $\max_\rho \mathcal{E}(\rho) \simeq 2.5 \times 10^{-3}$ for $p = 0.0915$ while $\mathcal{E}(\rho)$ is maximized (to zero) at $\rho \simeq 0$ for $p = 0.0990$, suggesting a tighter estimate for the error threshold than those reported so far. A comparison between the critical noise levels as obtained our current method and those with the IT method, for other parameter choices is summarized in Fig. 2 (b).

In summary, we have investigated the performance of the typical set decoding for ensembles of Gallager's codes. We have shown that the direct evaluation of the average type II error probability over the ensemble becomes possible employing the replica method. The link to the existing IT analysis which is based on the weight enumerator is also clarified. Although the weight enumerator does not play a crucial role for determination of the error threshold in the current analysis, it still remains a key factor for the error rate in low R regions. Its analysis from a view point of statistical physics is under way [13].

***

We acknowledge support from the Grants-in-Aid of the MEXT, Japan, Nos. 13680400, the Japan-Anglo Collaboration Programme of the JSPS (YK), EPSRC (GR/N00562) and The Royal Society (JVM). David Saad is acknowledged for useful comments and discussions.

REFERENCES

[1] S. Aji, H. Jin, A. Khandekar, D.J.C. MacKay and R.J. McEliece, BSC Thresholds for Code Ensembles Based on "Typical Pairs" Decoding, preprint, (1999).

[2] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, Wiley (New York), (1991).

[3] R.G. Gallager, *IRE Trans. Info. Theory*, **IT-8**, 21 (1962).

[4] D.J. Gross and M. Mézard, *Nucl. Phys.* , **B240**, 431 (1984).

[5] J.L. van Hemmen and R.G. Palmer, *J. Phys. A: Math. and Gen.*, **12**, 563 (1979).

[6] Y. Kabashima and D. Saad, *Europhys. Lett.*, **44**, 668 (1998); **45**, 97 (1999).

[7] Y. Kabashima, T. Murayama and D. Saad, *Phys.Rev.Lett.*, **84**, 1355 (2000); T. Murayama, Y. Kabashima, D. Saad and R. Vicente, *Phys. Rev. E*, **62**, 1577 (2000).

[8] Y. Kabashima, N. Sazuka, K. Nakamura and D. Saad, cond-mat/0010173 (2000).

[9] D.J.C. MacKay, *IEEE Trans. on Info. Theor*, **45**, 399 (1999); D.J.C. MacKay and R.M. Neal, *Electronic Lett.*, **33**, 457 (1997).

[10] R.J. McEliece, *The Theory of Information and Coding*, Addison-Wesley (Reading, MA), (1977).

[11] R.J. McEliece and J. Omura, *IEEE Trans. on Infor. Theor*, **23**, 611 (1977).

[12] T. Morita, *Math. Phys.* **5**, 1401, (1964); R. Kühn, *Z. Phys. B* **100**, 231 (1996).

[13] J. van Mourik, D. Saad and Y. Kabashima, preprint (2001).

[14] K. Nakamura, Y. Kabashima and D. Saad, cond-mat/0010073 (2000).

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

[16] H. Nishimori and K.Y.M. Wong, *Phys. Rev. E*, **60**, 132 (1999).

[17] T. Richardson, A. Shokrollahi and R. Urbanke, Design of provably good low-density parity check codes, preprint (1999)

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

[19] C.E. Shannon, *Bell Sys. Tech. J.*, **27**, 379 (1948); **27**, 623 (1948).

[20] C.E. Shannon, *The Mathematical Theory of Information*, University of Illinois Press (Urbana, IL), (1949); reprinted (1998).

[21] N. Sourlas, *Nature*, **339**, 693 (1989); *Euro.Phys.Lett.*, **25**, 159 (1994).