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, United Kingdom*
(Received 17 April 2002; published 24 September 2002)

The performance of ''typical set (pairs) decoding'' for ensembles of Gallager's linear code is investigated using statistical physics. In this decoding method, errors occur, either when the information transmission is corrupted by atypical noise, or when multiple typical sequences satisfy the parity check equation as provided by the received corrupted codeword. We show that the average error rate for the second type of error over a given code ensemble can be accurately evaluated using the replica method, including the sensitivity to message length. Our approach generally improves the existing analysis known in the information theory community, which was recently reintroduced in IEEE Trans. Inf. Theory **45**, 399 (1999), and is believed to be the most accurate to date.

DOI: 10.1103/PhysRevE.66.036125 PACS number(s): 89.90.+n, 02.50.−r, 05.50.+q, 75.10.Hk

Promoted by active investigations on error correcting codes in both the information theory (IT) and statistical physics (SP) communities [1–8], there is growing interest in the relationship between IT and SP. Since it has turned out that the two different frameworks have investigated similar subjects, it is natural to expect that standard techniques known in one framework might bring about developments in the other, and vice versa.

The purpose of this paper is to present such an example. More specifically, we show that a method to evaluate the performance of error correcting codes established in the IT community [1,5,9] can be generally improved by introducing the replica method used in SP. This provides an answer to the question among IT researchers as to why the methods from physics generally provide more optimistic evaluations than those known in the IT literature. In our formulation, the IT method is naturally linked to the existing SP analysis, being parametrized by the number of replicas $\rho>0$, which clearly shows how the IT and SP methods are related.

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 via a noisy channel, which is taken here to be a binary symmetric channel (BSC) characterized by a 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 structured codeword redundancy.

The error correcting code that we focus on here is Gallager's linear code [10]. This code was originally introduced by Gallager about 40 years ago but was almost forgotten soon after its proposal due to the technological limitations of the time. However, since its recent rediscovery by MacKay and Neal [4], it is now recognized as one of the best codes developed to date.

A code of this type is characterized by a randomly generated $(M-N)\times M$ Boolean sparse parity check matrix H, composed of K and $C(\geqslant 3)$ nonzero (unit) elements per row and column, respectively. Encoding of the message vector $\boldsymbol{x}$ is carried out using the $M\times N$ generating matrix G^T, satisfying the condition $HG^T=0$, where $\boldsymbol{y}^0=G^T\boldsymbol{x} \pmod 2$. The M-bit codeword $\boldsymbol{y}^0$ is transmitted via a noisy channel, a BSC in the current analysis, and the corrupted vector $\boldsymbol{y}=\boldsymbol{y}^0+\boldsymbol{n}^0 \pmod 2$ 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 $\boldsymbol{z}=H\boldsymbol{y}=H(G^T\boldsymbol{x}+\boldsymbol{n}^0)=H\boldsymbol{n}^0 \pmod 2$, and finding a solution to the parity check equation

$$H\boldsymbol{n}=\boldsymbol{z} \pmod 2, \tag{1}$$

which estimates the true noise vector $\boldsymbol{n}^0$. One retrieves $\boldsymbol{x}$, an estimate of the original message, using the equation $G^T\boldsymbol{x}=\boldsymbol{y}-\boldsymbol{n} \pmod 2$.

Several schemes can be employed for solving Eq. (1). In recent years, the maximum *a posteriori* and the maximizer of posterior marginal decodings, which correspond to zero and the Nishimori temperatures, respectively, have been widely investigated [3,8,11,12]. However, we will here evaluate the performance of another scheme termed *typical set (pairs) decoding*, which was pioneered by Shannon [9], and reintroduced by MacKay [5] for analyzing Gallager-type codes. Although this decoding method is slightly weaker in reducing the block or bit error rates, a rigorous analysis is easier than for the above two methods, and it is therefore becoming popular in the IT community [1,5,13].

In order to discuss the 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 a condition

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

with a high probability for large M and a positive number $\epsilon_M\sim\mathcal{O}(M^{-\gamma})$ $(0<\gamma<1/2)$. We define as typical any vector

*Electronic address: kaba@dis.titech.ac.jp
†Electronic address: knakamur@fe.dis.titech.ac.jp
‡Electronic address: vanmourj@aston.ac.uk

$\boldsymbol{n}$ for which this condition is satisfied. We also call the set of all typical vectors the typical set.

Now, we can define 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 $\boldsymbol{n}^0$. For this scheme, two types of decoding error can occur; the first possibility, referred to as a type I error, occurs when the true noise $\boldsymbol{n}^0$ is not typical, while the other possibility, referred to as a type II error, is declared when the true noise $\boldsymbol{n}^0$ is typical, and there are multiple typical vectors that satisfy Eq. (1) [5]. Since it can be shown that the probability of type I errors occurring, P_I, vanishes in the limit $M\to\infty$, we will focus on the evaluation of the probability for type II errors, P_{II}.

To proceed, it is convenient to employ a binary expression for bit sequences rather than a Boolean one. This can be done by mapping the field $\{0,1,+(\mathrm{mod}\ 2)\}$ onto $\{+1,-1,\times\}$, which makes it possible to introduce the *error indicator* function, which becomes 1 when an error occurs and zero otherwise, as

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

where

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

where $\mathbf{1}$ denotes the M-dimensional vector all the elements of which are 1. The field $F=(1/2)\ln[(1-p)/p]$ represents the level of the channel noise, and $\mathcal{L}(\mu)$ is the set of indices that have nonzero elements in the μth row in the parity check matrix H. In the second line of Eq. (4), we have introduced the gauge transformation $n_l\to n_l^0n_l$ 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 of a type II error for a given matrix H is given by $P_{II}(H)=\langle\Delta(\boldsymbol{n}^0,H)\delta(\Sigma_{l=1}^{M}n_l^0-M\tanh F)\rangle_{\boldsymbol{n}^0}$, where $\langle\cdots\rangle_{\boldsymbol{n}^0}=\mathrm{Tr}_{\boldsymbol{n}^0}(\cdots)\exp[F\Sigma_{l=1}^{M}n_l^0]/(2\cosh F)^M$. 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 for given parameters K and C as a performance measure for the code ensemble. Employing Eq. (3), the average is given as $\overline{P_{II}}=\lim_{\rho\to+0}\exp[-M\mathcal{E}(\rho)]$, where

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

for large M. Here, $\langle\cdots\rangle_H$ represents an average over the uniform distribution of the parity check matrix for a given choice of parameters K and C.

Before proceeding, it is worth mentioning the general properties of the exponent $\mathcal{E}(\rho)$. First, $\overline{P_{II}}$ is expected to vanish in the limit $M\to\infty$ for a sufficiently small noise p. This happens when $\mathcal{E}(0)\equiv\lim_{\rho\to+0}\mathcal{E}(\rho)>0$. The highest noise level p_c for this is called the *error threshold* [1]. The value of $\mathcal{E}(0)$ (>0) represents the sensitivity of $\overline{P_{II}}$ to the message length and serves as a performance measure of the code ensemble when M is finite. Next, since the number of wrong vectors $\mathcal{V}_{NF}(\boldsymbol{n}^0,H)$ can only take a non-negative integer value $0,1,2,\ldots,\mathcal{V}_{NF}^{\rho}(\boldsymbol{n}^0,H)$ should increase with respect to ρ (>0), and therefore the exponent $\mathcal{E}(\rho)$ must be a nonincreasing function of ρ (>0). This is linked to the inequality

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

where $\mathcal{S}_{NF}(\boldsymbol{n}^0,H)=\ln\mathcal{V}_{NF}(\boldsymbol{n}^0,H)$ is the entropy representing the number of wrong solutions for Eq. (1) belonging to the typical set. One can also show that $\partial^2\mathcal{E}(\rho)/\partial\rho^2\leqslant 0$, which implies that $\mathcal{E}(\rho)$ should be a convex function of ρ.

We are now ready to connect the discussion above to the existing analysis of typical set decoding [1,5,9]. Since $\mathcal{E}(\rho)$ is a decreasing function of ρ, we have that $\mathcal{E}(0)\geqslant\mathcal{E}(1)$. This means that we can obtain a *lower* bound of p_c from the condition $\mathcal{E}(1)=0$. For $\rho=1$ in Eq. (5), it is convenient to insert an identity $1=\int Md\omega\,\delta(\Sigma_{l=1}^{M}n_l-M\omega)$ in the final form of Eq. (4). Then, for a sequence $\boldsymbol{n}$ that satisfies $(1/M)\Sigma_{l=1}^{M}n_l=\omega$, one obtains

$$\begin{aligned}&\langle\delta(\Sigma_{l=1}^{M}n_l^0n_l-M\tanh F)\,\delta(\Sigma_{l=1}^{M}n_l^0-M\tanh F)\rangle_{\boldsymbol{n}^0}\\&\quad\sim\exp[-M\mathcal{K}(\omega,F)],\end{aligned}$$

where

$$\mathcal{K}(\omega,F)=[(1-\omega)/2]H[2\tanh F/(1-\omega)] -[(1+\omega)/2]\ln 2+H(\tanh F)$$

and

$$H(x)=-[(1+x)/2]\ln[(1+x)/2]-[(1-x)/2]\ln[(1-x)/2].$$

The remaining average required in Eq. (5) can be evaluated as $\langle \mathrm{Tr}_{\boldsymbol{n}}\delta(\Sigma_{l=1}n_l-M\omega)\Pi_{\mu=1}^{M-N}\delta(1;\Pi_{l\in\mathcal{L}(\mu)}n_l)\rangle_H \sim\exp[M\mathcal{R}(\omega)]$. The exponent $\mathcal{R}(\omega)$ is the so-called *weight enumerator* [1,5], which in the current context [14] 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 [15]. One obtains $\mathcal{E}(1)=\mathrm{Ext}_{\omega\neq 1}\{\mathcal{K}(\omega,F)-\mathcal{R}(\omega)\}$, where $\mathrm{Ext}_{\{\cdots\}}$ denotes an extremization. This corresponds to Eq. (4.7) in [1].

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

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 following order parameters and their conjugate variables: $q_{\alpha,\beta,\ldots,\gamma}=q\int dx\,\pi(x)x^l, \hat{q}_{\alpha,\beta,\ldots,\gamma}=\hat{q}\int d\hat{x}\,\hat{\pi}(\hat{x})\hat{x}^l$, where l denotes the number of replica indices, and q and $\hat{q}$ are normalization variables for defining $\pi(\cdot)$ and $\hat{\pi}(\cdot)$ as distributions. Unspecified integrations are carried out over the interval $[-1,1]$. One can find details of a similar calculation in [3].

Originally, the summation $\mathrm{Tr}_{\boldsymbol{n}\neq\boldsymbol{1}}(\cdot)$ excluded the case of $\boldsymbol{n}=\boldsymbol{1}$; but one can show that for $M\to\infty$ this becomes identical to the full summation in the nonferromagnetic phase, where $\pi(x)\neq\delta(x-1)$ and $\hat{\pi}(x)\neq\delta(\hat{x}-1)$. In addition, we employ Morita's scheme [16], which in this case converts the restricted annealed average with respect to $\boldsymbol{n}^0$ to a quenched one,

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

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

$$\mathcal{E}(\rho)=\mathrm{Ext}^{*}_{\{q,\hat{q},\pi(\cdot),\hat{\pi}(\cdot),G\}}\left\{-\frac{Cq^K}{K}\int\prod_{i=1}^{K}dx_i\pi(x_i)\left(\frac{1+\prod_{i=1}^{K}x_i}{2}\right)^{\rho}-\left\langle\ln\left[\int\prod_{\mu=1}^{C}d\hat{x}_{\mu}\hat{\pi}(\hat{x}_{\mu})\right.\right.\right.$$
$$\left.\left.\left.\times\left(\mathrm{Tr}_{n=\pm1}e^{Gn^0n}\prod_{\mu=1}^{C}\left(\frac{1+\hat{x}_{\mu}n}{2}\right)\right)^{\rho}\right]\right\rangle_{n^0}-C\ln\hat{q}+Cq\hat{q}\int dx\,d\hat{x}\,\pi(x)\hat{\pi}(\hat{x})\left(\frac{1+x\hat{x}}{2}\right)^{\rho}+\left(\frac{C}{K}-C\right)+\rho G\tanh F\right\}, \tag{8}$$

where $\langle(\cdots)\rangle_{n^0}=\mathrm{Tr}_{n^0=\pm1}(\cdots)\exp[Fn^0]/(2\cosh F)$ and $\mathrm{Ext}^{*}_{\{\cdots\}}$ denotes the functional extremization excluding the possibility of $\pi(x)=\delta(x-1)$ and $\hat{\pi}(\hat{x})=\delta(\hat{x}-1)$, as is introduced in [17].

Two analytical solutions of $\pi(x)$ and $\hat{\pi}(\hat{x})$ can be obtained in the limit $K,C\to\infty$, keeping the code rate $R=N/M=1-C/K$ finite: (1) $\pi(x)=\frac{1}{2}[(1+\tanh F)\delta(x-\tanh F)+(1-\tanh F)\delta(x+\tanh F)]$, $\hat{\pi}(\hat{x})=\delta(\hat{x})$; and, (2) $\pi(x)=\frac{1}{2}[\delta(x-1)+\delta(x+1)]$, $\hat{\pi}(\hat{x})=\frac{1}{2}[\delta(\hat{x}-1)+\delta(\hat{x}+1)]$. One can show that both of these are locally stable against perturbations to the RS solutions, and they provide $\mathcal{E}(\rho)=\rho[H(\tanh F)-(1-R)\ln 2]$ and $\mathcal{E}(\rho)=H(\tanh F)-(1-R)\ln 2$, respectively, for any positive integer number $\rho=1,2,3,\ldots$.

In order to take the limit $\rho\to+0$, one has to select the relevant branch of the two solutions. Since the replica method is a strategy in which one has to perform an analytic continuation of the expressions obtained for positive integer ρ [for which the saddle point problem (8) is well defined] to those for any real numbers, the branch that is dominant (i.e., yields the lower exponent) for positive integer ρ should be selected [18]. As a result, we obtain for the exponent

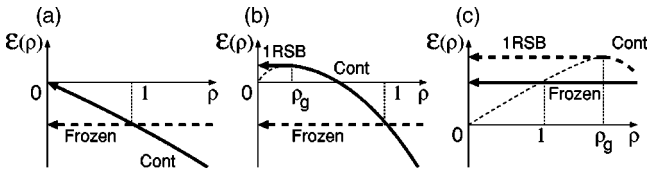

FIG. 1. Appropriate limits for $\lim_{\rho\to+0}\mathcal{E}(\rho)$ in the case of finite K and C. The solution that has the lower exponent for $\rho\geqslant 1$ should be selected as the relevant branch (see text), which is drawn as a thick curve or line in each case. For $p\geqslant p_c$ (a), the continuous 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 $p_b\leqslant p<p_c$ (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.

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

where $R_c=1+p\log_2 p+(1-p)\log_2(1-p)$ corresponds to Shannon's limit [19]. It is worth noticing that the expression (9) is identical to the lower bound of the exponent that is believed to be accurate in the information theory literature [1].

Note that in the vicinity of $R=R_c$ this exponent can exceed the upper bound on reliability functions that represent a vanishing rate of the decoding error probability for the best code [17,20,21]. However, this does not imply a contradiction, because the current analysis is only 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 can obtain $\mathcal{E}(\rho)$ via numerical methods. Similar to the case of $K,C\to\infty$, there generally appear two branches of solutions: (1) Continuous distributions for $\pi(x)$ and $\hat{\pi}(\hat{x})$, for which $\lim_{\rho\to+0}\mathcal{E}(\rho)=0$; and, (2) ρ independent frozen distributions $\pi(x)=\frac{1}{2}[(1+b)\delta(x-1)+(1-b)\delta(x+1)]$, $\hat{\pi}(\hat{x})=\frac{1}{2}[(1+\hat{b})\delta(\hat{x}-1)+(1-\hat{b})\delta(\hat{x}+1)]$. The parameters b and $\hat{b}$ are determined from the extremization problem [see Eq. (8)] by setting $\rho=1$, which reduces the functional extremization with respect to $\pi(\cdot)$ and $\hat{\pi}(\cdot)$ to that with respect to the first moments $b=\int dx\,x\pi(x)$ and $\hat{b}=\int d\hat{x}\,\hat{x}\hat{\pi}(\hat{x})$. The exponent of this branch is completely frozen to that for $\rho=1$ as $\mathcal{E}(\rho)=\mathcal{E}(1)$ for $\forall\rho\geqslant 0$. Although the distributions of the two branches look quite different, their exponents coincide at $\rho=1$ in any situation. It should be emphasized here that the $\mathcal{E}(1)$ can be accurately evaluated without use of the replica method. We will show later that this value, together with the inequality (6), plays an important role in the determination of the relevant branch for the analytic continuation $\rho\to+0$ when the channel noise p is sufficiently low.

Note that the frozen branch corresponds to the conventional IT analysis [1,5], and would provide the correct estimate in the 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 positive integer ρ [18] among the existing solutions, and the frozen branch does not necessarily provide the correct exponent for $\rho\to+0$. Our analysis supports this statement as seen in Fig. 1.

When the channel noise p is sufficiently high [Fig. 1(a)], the exponent for the continuous branch monotonically decreases with respect to ρ, which implies that this is the dominant branch for positive integer ρ. This provides $\lim_{\rho\to+0}\mathcal{E}(\rho)=0$. However, for lower values of p, $\mathcal{E}(\rho)$ of the continuous branch maximizes to a positive value at ρ_g [Fig. 1(b)]. In this situation, the continuous branch solution for $0<\rho<\rho_g$ is physically wrong because the inequality (6) does not hold. However, a frozen replica symmetry breaking (RSB) ansatz [22] [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] obtains a consistent solution. Employing this 1RSB solution, we find $\mathcal{E}(\rho)=\mathcal{E}(\rho_g)$ for $0<\rho<\rho_g$, which implies $\lim_{\rho\to+0}\mathcal{E}(\rho)=\mathcal{E}(\rho_g)>0$, indicating a vanishing behavior for $\overline{P_{II}}\sim\exp[-M\mathcal{E}(\rho_g)]$. This implies that the critical condition determining the error threshold p_c is given by $\partial\mathcal{E}(\rho)/\partial\rho|_{\rho\to+0}=0$, computed for the continuous solution. Employing the gauge transformation [11], one can show that the variational parameter G in Eq. (8) that is introduced to enforce the condition $\Sigma_{l=1}^{M}n_l^0n_l=M\tanh F$ coincides with F in this limit. The critical condition can now be summarized as

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

which is identical to what has been obtained for the phase boundary of the ferro-paramagnetic transition along Nishimori's temperature predicted by the existing replica analysis [3,17].

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. In principle, this might cause a serious problem for the selection of the relevant branch for the analytic continuation $\rho\to+0$, since the branches of frozen and continuous RS solutions intersect at a certain value of $\rho>1$, which seems to imply that the dominant branch of solutions for positive integer ρ is not unambiguously defined. This ambiguity is lifted, however, because in this case the selection of the frozen RS solutions as the relevant branch is the only possible option. This is because for $\rho<\rho_g$ it is impossible to construct any physically consistent solution that both satisfies the inequality (6) and reproduces the correct value of $\mathcal{E}(1)$, by extending the continuous RS solutions. This implies that the criterion for selection of the relevant branch for the analytic continuation $\rho\to+0$ can be conveniently summarized as selection of that branch that is dominant in the vicinity of $\rho\geqslant 1$. Thus, below p_b the limit $\rho\to+0$ is governed by the frozen (RS) solutions, identical to the result from conventional IT analysis [Fig. 1(c)]. However, this situation is realized only significantly below the threshold and the solution is therefore of no use for the direct evaluation of p_c although it does provide a lower bound.

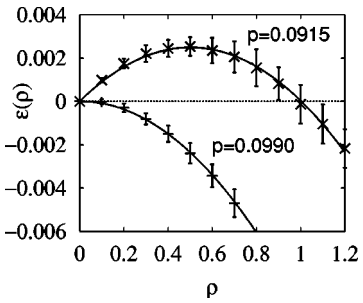

FIG. 2. Numerically computed $\mathcal{E}(\rho)$ of the continuous branch for $p=0.0915,0.0990$ for $K=6$ and $C=3$ $(R=1/2)$. Symbols and error bars are obtained from 50 numerical solutions. Curves are computed via a quadratic fit. For $p=0.0915$, $\mathcal{E}(\rho)$ is maximized to a positive value $\mathcal{E}(\rho_g)\simeq 2.5\times 10^{-3}$ 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.

As two types of frozen solution are introduced in the analysis above, one might be interested in their physical interpretation. It is a significant property of the frozen RS solutions that their exponents are independent of ρ. From Eq. (6), this implies that these solutions express a situation that at most a subexponential number of vectors contribute to $\mathcal{V}_{NF}$ (their entropy being 0). In the information theory literature [20], it is known that the average error rate for the low noise region is mostly due to a small fraction of atypical codes that have large error rates because they allow a small number of vectors close to the true noise $\boldsymbol{n}^0$ to satisfy the parity check equation (1). The frozen RS solutions may correspond to this contribution.

On the other hand, the frozen 1RSB solutions only appear below the critical parameter ρ_g, having originated from the continuous RS solutions. A transition of this type can occur if $\mathcal{V}_{NF}$ becomes an exponentially large number with an exponentially small probability while vanishing in most cases. Such a scenario quite naturally describes the situation just below the critical noise level p_c, as the transition to the ferromagnetic phase is of the first order [3,17] and, therefore, the suboptimal nonferromagnetic state (which has finite entropy) is still locally stable, and can emerge with an exponentially small probability even after the transition.

The probability of having an exponentially large $\mathcal{V}_{NF}$ in the ferromagnetic phase could become larger when the true noise $\boldsymbol{n}^0$ is atypical. This implies that the restriction to typical $\boldsymbol{n}^0$ in order to evaluate the type II error rate, as in the current analysis, should reduce the contribution of the frozen 1RSB solutions compared to that in other evaluations [17,20,21]. This speculation certainly holds in the case of $K,C\to\infty$ for which no 1RSB solution is found at all. However, for finite K and C, it is impossible to completely remove the possibility of having an exponentially large $\mathcal{V}_{NF}$ just by excluding atypical $\boldsymbol{n}^0$, and therefore the critical noise level p_c is accompanied by the emergence of 1RSB solutions.

TABLE I. 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.

(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

Finally, we have examined the case of $K=6$ and $C=3$ to demonstrate the accuracy of the estimated threshold. We have numerically evaluated $\mathcal{E}(\rho)$ of the continuous branch for $p=0.0915$, a 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 [17,23]. The numerical results are obtained by approximating $\pi(\cdot)$ and $\hat{\pi}(\cdot)$ using 10^6-dimensional vectors and iterating the saddle point equations until convergence. The results, shown in Fig. 2, indicate $\max_\rho \mathcal{E}(\rho)\simeq 2.5\times 10^{-3}$ 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. Comparisons for other parameter choices are also summarized in Table I.

In summary, we have investigated the performance of the typical set decoding for ensembles of Gallager's codes. We have shown that direct evaluation of the average type II error probability over the ensemble is possible by 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 in determining the error threshold in the current analysis, it still provides useful insight about the relationship among different decoding schemes. Its analysis from the viewpoint of statistical physics is given in [24].

We acknowledge support from Grants-in-Aid of the MEXT Nos. 13780208 and 14084206, the Japan-Anglo Collaboration Program of the JSPS (Y.K.), EPSRC (Grant No. GR/N00562), and The Royal Society (J.v.M.). David Saad and David J. C. MacKay are acknowledged for useful comments and discussions.

[1] S. Aji, H. Jin, A. Khandekar, D.J.C. MacKay and R.J. McEliece, in *Codes, Systems, and Graphical Models*, edited by B. Marcus and J. Rosenthal (Springer-Verlag, New York, 2001), p. 195.

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

[3] 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).

[4] D.J.C. MacKay and R.M. Neal, Electron. Lett. **33**, 457 (1997).

[5] D.J.C. MacKay, IEEE Trans. Inf. Theory **45**, 399 (1999).
[6] H. Nishimori and K.Y.M. Wong, Phys. Rev. E **60**, 132 (1999).
[7] T. Richardson, A. Shokrollahi, and R. Urbanke, IEEE Trans. Inf. Theory **47**, 619 (2001).
[8] N. Sourlas, Nature (London) **339**, 693 (1989); Europhys. Lett. **25**, 159 (1994).
[9] C.E. Shannon, *The Mathematical Theory of Communication* (University of Illinois Press, Urbana, IL, 1998).
[10] R.G. Gallager, IRE Trans. Inf. Theory **IT-8**, 21 (1962).
[11] H. Nishimori, J. Phys. Soc. Jpn. **62**, 2973 (1993).
[12] P. Ruján, Phys. Rev. Lett. **70**, 2968 (1993).
[13] T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[14] The weight enumerator is usually introduced for the distance between codewords [1,5,15]. However, since $\boldsymbol{y}^0-\boldsymbol{y}^1=\boldsymbol{n}^0-\boldsymbol{n}^1(\mathrm{mod}\ 2)$ holds for two sets of Boolean vectors $(\boldsymbol{y}^0,\boldsymbol{n}^0)$ and $(\boldsymbol{y}^1,\boldsymbol{n}^1)$ that satisfy $\boldsymbol{y}=\boldsymbol{y}^0+\boldsymbol{n}^0=\boldsymbol{y}^1+\boldsymbol{n}^1(\mathrm{mod}\ 2)$, the distance between the noise vectors $\boldsymbol{n}^0$ and $\boldsymbol{n}^1$ is identical to that between the codewords $\boldsymbol{y}^0$ and $\boldsymbol{y}^1$.
[15] R.J. McEliece, *The Theory of Information and Coding* (Addison-Wesley, Reading, MA, 1977).
[16] T. Morita, J. Math. Phys. **5**, 1401 (1964); R. Kühn, Z. Phys. B: Condens. Matter **100**, 231 (1996).
[17] Y. Kabashima, N. Sazuka, K. Nakamura, and D. Saad, Phys. Rev. E **64**, 046113 (2001).
[18] J.L. van Hemmen and R.G. Palmer, J. Phys. A **12**, 563 (1979).
[19] C.E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948); **27**, 623 (1948).
[20] R.G. Gallager, *Information Theory and Reliable Communication* (John Wiley & Sons, New York, 1968).
[21] R.J. McEliece and J. Omura, IEEE Trans. Inf. Theory **23**, 611 (1977).
[22] D.J. Gross and M. Mézard, Nucl. Phys. B **240**, 431 (1984).
[23] K. Nakamura, Y. Kabashima, and D. Saad, Europhys. Lett. **56**, 610 (2001).
[24] J. van Mourik, D. Saad, and Y. Kabashima, e-print cond-mat/0110023; e-print cond-mat/0203159.