A Statistical-Mechanics Approach to Large-System Analysis of CDMA Multiuser Detectors

Toshiyuki Tanaka, *Member, IEEE*

***Abstract*—We present a theory, based on statistical mechanics, to evaluate analytically the performance of uncoded, fully synchronous, randomly spread code-division multiple-access (CDMA) multiuser detectors with additive white Gaussian noise (AWGN) channel, under perfect power control, and in the large-system limit. Application of the replica method, a tool developed in the literature of statistical mechanics, allows us to derive analytical expressions for the bit-error rate, as well as the multiuser efficiency, of the individually optimum (IO) and jointly optimum (JO) multiuser detectors over the whole range of noise levels. The information-theoretic capacity of randomly spread CDMA channel and the performance of decorrelating and linear minimum mean-square error (MMSE) detectors are also derived in the same replica formulation, thereby demonstrating validity of the statistical-mechanical approach.**

***Index Terms*—Code-division multiple access (CDMA), large-system analysis, multiuser detection, optimum multiuser detector, replica method, statistical mechanics.**

I. Introduction

We evaluate analytically the performance of a class of code-division multiple-access (CDMA) multiuser detectors in the large-system limit. We adopt the Bayesian framework and consider a class of multiuser detectors which we call the *Marginal-Posterior-Mode (MPM) detectors*. It has its root in the Bayesian image analysis [1], [2], and includes the jointly optimum (JO) and individually optimum (IO) multiuser detectors as special cases. It has been recognized recently that fluctuations of macroscopic properties of detectors, due to randomness in the systems (e.g., random choice of signatures), vanish in the large-system limit [3]–[7]. Such deterministic results have been obtained by analytical arguments for some cases. Results for the decorrelating detector and the linear minimum mean-squared error (MMSE) detector can be found in [8]. Tse and Verdú [7] have analyzed the performance of the JO multiuser detector in the high signal-to-noise ratio (SNR) limit. We believe our result to be the first analytical result applicable not only for the zero-noise limit, but also over the whole range of noise levels.

Manuscript received April 3, 2001; revised May 27, 2002. This work was supported in part by the Grant-in-Aid for Scientific Research (11780287), Japan Society for the Promotion of Science, Japan. The material in this paper was presented in part at the Fourteenth Annual Conference on Neural Information Processing Systems (NIPS*2000), Denver, CO, November 2000; the IEEE International Symposium on Information Theory, Washington, DC, June 2001; and published in part as "Statistical mechanics of CDMA multiuser demodulation," *Europhys. Lett.*, vol. 54, no. 4, pp. 540–546, 2001.

The author is with the Department of Electronics and Information Engineering, Tokyo Metropolitan University, Tokyo, 192-0397, Japan (e-mail: tanaka@eei.metro-u.ac.jp).

Communicated by V. V. Veeravalli, Associate Editor for Detection and Estimation.

Digital Object Identifier 10.1109/TIT.2002.804053.

The key idea of our analysis is to apply new tools and notions developed in statistical mechanics. The motivation behind this idea is as follows. Since the ultimate goal of statistical mechanics is to understand macroscopic properties of physical systems in the large-system (thermodynamic) limit, it is natural to expect that the application of statistical-mechanical tools to the large-system analysis of multiuser detectors will help understand their macroscopic properties as well. We specifically make use of the *replica method*, developed in the field of spin-glasses (magnetic materials characterized by random spin–spin interactions) [9], [10]: Although a mathematically rigorous justification of the replica method is still missing, it has recently been applied extensively to the analysis of problems in the field of information processing, such as neural networks [11], [12], learning from examples [13]–[16], statistical image restoration based on Markov random fields [17], and error-control codes including Gallager and turbo codes [18]–[23]. The results obtained by the replica method are mostly nontrivial, and when applied to problems with known solutions, it successfully reproduces existing results. They include the following.

- Capacity of a linear classifier: The result by the replica analysis [13] on the maximum number of randomly-generated data separable by a linear classifier reproduces Cover's result [24] as a special case.
- Reliability function: Recently, Kabashima *et al.* [23] have successfully evaluated the random coding exponent and the expurgated exponent for an ensemble of Gallager codes (*not* the ensemble of whole random codes as treated in Gallager's argument on the reliability function [25], but a smaller subset), basically following Gallager's formalism, while using the replica method instead of Jensen's inequality. They have reproduced the respective results on the two exponents by Gallager for the random-code ensemble, which means that the ensemble of Gallager codes is *typical* among the ensemble of random codes in terms of asymptotic performance.

We demonstrate that the statistical-mechanical approach is also applicable to the multiuser detection problem, and that it yields novel results on optimum multiuser detectors, while successfully reproducing some of the existing results.

We restrict ourselves to the analysis of cases with various simplifying assumptions, including full synchronization, random spreading, additive white Gaussian noise (AWGN) channel, no fading, and perfect power control. This restriction allows straightforward application of the replica method. In spite of these simplifying assumptions, however, we think that our results are of significance as benchmarking results, providing a prerequisite for understanding the multiuser detectors in more practical situations. (See also a recent paper by Guo

0018-9448/02$17.00 © 2002 IEEE

and Verdú [26] which extends the analysis presented here to the unequal-power case.) Preliminary presentation of some of the results of this paper are available in [27]–[29].

II. System Model

We consider the basic fully synchronous K-user CDMA channel with perfect power control

$$r^\mu = \frac{1}{\sqrt{N}} \sum_{k=1}^{K} s_k^\mu x_k + \sigma_0 n^\mu \tag{1}$$

where $x_k \in \{-1, 1\}$ is the information bit (symbol) of user k, and where $\{s_k^\mu;\, \mu = 1, \ldots, N\}$ is the spreading sequence of user k, within the information-bit interval. We assume the AWGN channel: $n^\mu \sim N(0, 1)$, and σ_0 is the amplitude of the noise. We also assume the random spreading model, in which $\{s_k^\mu; \mu = 1, \ldots, N; k = 1, \ldots, K\}$ are assumed to be realizations of independent and identically distributed (i.i.d.) random variables following a given symmetric distribution with zero mean and unit variance. The scaling factor $1/\sqrt{N}$ is introduced so that the total energy of the spreading sequence for the information-bit interval is normalized to 1. Let us define

$$\begin{aligned} \boldsymbol{r} &\equiv [r^1, \ldots, r^N]^T \\ \boldsymbol{s}_k &\equiv \left[s_k^1, \ldots, s_k^N\right]^T, \qquad k = 1, \ldots, K \\ \boldsymbol{n} &\equiv \left[n^1, \ldots, n^N\right]^T \\ \boldsymbol{x} &\equiv [x_1, \ldots, x_K]^T. \end{aligned} \tag{2}$$

Then the communication model (1) is written as

$$\boldsymbol{r} = \frac{1}{\sqrt{N}}\, S\boldsymbol{x} + \sigma_0 \boldsymbol{n} \tag{3}$$

where $S \equiv [\boldsymbol{s}_1, \ldots, \boldsymbol{s}_K]$.

The characteristics of the channel noise can also be described by the conditional distribution of the received data $\boldsymbol{r}$, conditioned on the information bits $\boldsymbol{x}$ given the spreading sequences S. It is given by

$$p_0(\boldsymbol{r}|\boldsymbol{x}, S) = (2\pi\sigma_0^2)^{-N/2} \exp\left(-\frac{1}{2\sigma_0^2}\, \|\boldsymbol{r} - N^{-1/2} S\boldsymbol{x}\|^2\right). \tag{4}$$

We analyze the multiuser detection problem in the *large-system limit* where $K, N \to \infty$, while the ratio of K to N is kept fixed to

$$\frac{K}{N} = \beta. \tag{5}$$

The basic quantity for analyzing the multiuser detection problem is the posterior distribution $p(\boldsymbol{x}|\boldsymbol{r}, S)$, i.e., the distribution of $\boldsymbol{x}$ conditioned on received data $\boldsymbol{r}$ given S. We assume that the detectors do not know the true level of the channel noise, so that we can use σ as a control parameter in place of the true noise level parameter σ_0. Under this assumption, the posterior distribution is given by

$$\begin{aligned} &p(\boldsymbol{x}|\boldsymbol{r}, S) \\ &\quad = [Z(\boldsymbol{r}, S)]^{-1} p(\boldsymbol{x}) \exp\left(-\frac{1}{2\sigma^2}\, \|\boldsymbol{r} - N^{-1/2} S\boldsymbol{x}\|^2\right) \end{aligned} \tag{6}$$

where

$$Z(\boldsymbol{r}, S) = \sum_{\boldsymbol{x}} p(\boldsymbol{x}) \exp\left(-\frac{1}{2\sigma^2}\, \|\boldsymbol{r} - N^{-1/2} S\boldsymbol{x}\|^2\right) \tag{7}$$

is the normalizing coefficient, called the partition function. The quantity $p(\boldsymbol{x})$ is the prior distribution for the information bits. Throughout this paper, unless otherwise stated, we assume the uniform prior, i.e., $p(\boldsymbol{x}) = 2^{-K}$ for all $\boldsymbol{x}$. Since $p(\boldsymbol{x})$ is now a constant, we could drop it from mathematical expressions in the following. But we prefer to keep $p(\boldsymbol{x})$ until we perform detailed calculations, in order to make its appearance explicit.

We now define a one-parameter family of multiuser detectors the analysis of which is the main objective of this paper.

Definition 1: The Marginal-Posterior-Mode (MPM) detector with control parameter σ is defined by

$$\hat{x}_k^{(\mathrm{MPM})} = \arg\max_{x_k} \sum_{\boldsymbol{x}\backslash x_k} p(\boldsymbol{x}|\boldsymbol{r}, S), \qquad k = 1, \ldots, K \tag{8}$$

where the summation over $\boldsymbol{x}\backslash x_k$ means that we marginalize the posterior distribution over all $x_j,\, j \neq k$.

Equivalently, we can define the MPM detector as

$$\hat{x}_k^{(\mathrm{MPM})} = \operatorname{sign}\left(\langle x_k \rangle_\sigma\right), \qquad k = 1, \ldots, K, \tag{9}$$

where $\langle \cdot \rangle_\sigma$ denotes the expectation with respect to the posterior distribution (6). In the limit $\sigma \to 0$, the MPM detector corresponds to the JO multiuser detector [8],

$$\hat{\boldsymbol{x}}^{(\mathrm{JO})} = \arg\max_{\boldsymbol{x}} p(\boldsymbol{x}|\boldsymbol{r}, S), \tag{10}$$

and in the case where the control parameter is set to the true noise level, i.e., $\sigma = \sigma_0$, it gives the IO multiuser detector

$$\hat{x}_k^{(\mathrm{IO})} = \arg\max_{x_k} \sum_{\boldsymbol{x}\backslash x_k} p(\boldsymbol{x}|\boldsymbol{r}, S)|_{\sigma=\sigma_0}, \quad k = 1, \ldots, K. \tag{11}$$

These facts mean that the MPM detector is a one-parameter extension of the JO and IO multiuser detectors.

A common performance measure for multiuser detectors is the bit-error rate P_b. Let $\boldsymbol{x}_0$ be the true information-bit vector. The proportion of the bit error of a detector which outputs $\hat{\boldsymbol{x}}$ as an estimate to $\boldsymbol{x}_0$ is given by $(1-d)/2$, where

$$d \equiv \frac{1}{K} \sum_{k=1}^{K} x_{0k} \hat{x}_k = \frac{1}{K}\, \boldsymbol{x}_0 \cdot \hat{\boldsymbol{x}}. \tag{12}$$

We call d the *correlation* of the detector output. By taking into account the fact that all users are statistically equivalent in the system model treated in this paper, the bit-error rate P_b for a particular user is the same for all users, and it is given by the average of $(1-d)/2$. As is well known, the IO multiuser detector is optimum in the sense that it achieves minimum bit-error rate.

One of the basic assumptions of the statistical-mechanics approach is that the *free energy* per user $\mathcal{F}_K(\boldsymbol{r}, S)$, defined by

$$\mathcal{F}_K(\boldsymbol{r}, S) = K^{-1} \log Z(\boldsymbol{r}, S) \tag{13}$$

is *self-averaging* in the $K \to \infty$ limit with respect to the randomness of the spreading sequences and the noise. (Here, and hereafter, logarithms are taken to base e.) It is stated formally as follows.

Assumption 1: The limit $\mathcal{F} \equiv \lim_{K\to\infty} \mathcal{F}_K(\boldsymbol{r}, S)$ exists and it is equal to its average for almost all realizations of the spreading sequences and the noise.

From this assumption, we have

$$\mathcal{F} = \lim_{K\to\infty} K^{-1} \int_{\mathbb{R}^N} \overline{p_0(\boldsymbol{r}|S) \log Z(\boldsymbol{r}, S)}\, d\boldsymbol{r}. \tag{14}$$

(Here, and hereafter, $d\boldsymbol{r}$ stands for $\prod_{\mu=1}^{N} dr^{\mu}$.) The overbar denotes the average over the randomness of the spreading sequences, and $p_0(\boldsymbol{r}|S)$ is the probability of observing $\boldsymbol{r}$ as the output of the true channel, for the given spreading sequences S. We have

$$p_0(\boldsymbol{r}|S) = \sum_{\boldsymbol{x}_0} p(\boldsymbol{x}_0) p_0(\boldsymbol{r}|\boldsymbol{x}_0, S) = Z_0(\boldsymbol{r}, S)/C \tag{15}$$

where we let

$$Z_0(\boldsymbol{r}, S) = \sum_{\boldsymbol{x}_0} p(\boldsymbol{x}_0) \exp\left(-\frac{1}{2\sigma_0^2} \|\boldsymbol{r} - N^{-1/2} S\boldsymbol{x}_0\|^2\right). \tag{16}$$

The normalization coefficient

$$C = \int_{\mathbb{R}^N} Z_0(\boldsymbol{r}, S)\, d\boldsymbol{r} = (2\pi\sigma_0^2)^{N/2} \tag{17}$$

is independent of the spreading sequences.

The free energy $\mathcal{F}_K(\boldsymbol{r}, S)$ is nothing but the *cumulant generating function* [30], which carries all information about the statistics of the system. Therefore, assuming the self-averaging property of the free energy corresponds to assuming that the fluctuations of macroscopic quantities, due to the randomness of the spreading sequences and the noise, vanish in the large-system limit. The self-averaging property has been proved for the AWGN CDMA channel capacity [3], [4], performance of the linear MMSE and decorrelating detectors, including the unequal-power case [5], [6], and performance of the optimum detector in the zero-noise limit [7]. Although the self-averaging property for the MPM detector has not yet been proved, and is still an assumption, results for models such as those mentioned earlier strongly suggest that it also holds for the MPM detector. Even if the self-averaging property does not hold for the MPM detector, the main results to be obtained in this paper still provide possible approximation to the performance of the MPM detector, as well as a lower bound on the best possible performance, provided that other technical assumptions are valid.

III. Replica Analysis for MPM Detectors

A. Evaluation of Free Energy

In order to evaluate the free energy, we make use of the *replica method* (following basically the style of [31]) by which we have

$$\mathcal{F} = \lim_{K\to\infty} \left(\lim_{n\to 0} \frac{\partial}{\partial n} K^{-1} \log \Xi_n \right) \tag{18}$$

where

$$\Xi_n = C^{-1} \int_{\mathbb{R}^N} \overline{Z_0(\boldsymbol{r}, S)[Z(\boldsymbol{r}, S)]^n}\, d\boldsymbol{r}. \tag{19}$$

It should be noted that, for finite K, Ξ_n is well-defined for real n. It is straightforward to see that (18) holds by exchanging the order of the averaging and the differentiation with respect to n, and by noting that $\lim_{n\to 0} \Xi_n = 1$. In the replica method, however, we will evaluate Ξ_n only for positive integers n, and then the result is applied to real n. We *assume*, without rigorous justification, that this procedure is valid [9]. Formally, the assumption is as follows.

Assumption 2: Ξ_n for real n is given, at least in the vicinity of $n = 0$, by plugging the value of n into the expression of Ξ_n, obtained by evaluating it only for positive integers n.

For a brief introduction of the replica method and its application to large-system analysis in a general setting, see Appendix I. For more extensive reviews on the replica method in the statistical mechanics literature, see, e.g., [32], [10], [16]

Since $[Z(\boldsymbol{r}, S)]^n$ for integer n is nothing but the normalizing coefficient for a system consisting of n replicas of the posterior probability (6) sharing the same $\boldsymbol{r}$ and S, we can write down Ξ_n explicitly as shown in (20) at the bottom of the page, where we have introduced replicated random variables

$$\boldsymbol{x}_a \equiv [x_{a1}, \ldots, x_{aK}]^T \in \{-1, 1\}^K, \qquad a = 1, \ldots, n$$

to represent the random variables of the replicated posterior probabilities. The integrand depends on $\boldsymbol{x}$ only through

$$v_0 = \frac{1}{\sqrt{K}} \sum_{k=1}^{K} s_k x_{0k}$$

and

$$v_a = \frac{1}{\sqrt{K}} \sum_{k=1}^{K} s_k x_{ak}, \qquad a = 1, \ldots, n.$$

Under mild additional conditions on the statistics of S, these quantities can be regarded, in the $K \to \infty$ limit, as joint Gaussian random variables with means 0 and covariances $Q_{ab} \equiv \overline{v_a v_b} = K^{-1} \boldsymbol{x}_a \cdot \boldsymbol{x}_b$. (See Appendix II for the justification of this step.) Based on this observation, we decompose

$$\Xi_n = \sum_{\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n} \prod_{a=0}^{n} p(\boldsymbol{x}_a) \times \left\{ \frac{1}{\sqrt{2\pi\sigma_0^2}} \int_{\mathbb{R}} \overline{\exp\left[-\frac{1}{2\sigma_0^2}\left(r - \frac{1}{\sqrt{N}} \sum_{k=1}^{K} s_k x_{0k}\right)^2\right] \prod_{a=1}^{n} \exp\left[-\frac{1}{2\sigma^2}\left(r - \frac{1}{\sqrt{N}} \sum_{k=1}^{K} s_k x_{ak}\right)^2\right]}\, dr \right\}^N \tag{20}$$

the summation over $\{\boldsymbol{x}_a\}$ into two steps. First we perform the summation over a single subshell of the form

$$S\{Q\} \equiv \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n | \boldsymbol{x}_a \cdot \boldsymbol{x}_b = KQ_{ab}\} \tag{21}$$

and then integrate the result over all subshells. Thus, we have

$$\Xi_n = \int_{[-1,1]^{n(n+1)/2}} \exp(K\beta^{-1}\mathcal{G}\{Q\})\mu_K\{Q\} \prod_{a<b} dQ_{ab} \tag{22}$$

where

$$\mu_K\{Q\} = \sum_{\boldsymbol{x}_0,\ldots,\boldsymbol{x}_n} \prod_{a=0}^{n} p(\boldsymbol{x}_a) \prod_{a<b} \delta(\boldsymbol{x}_a \cdot \boldsymbol{x}_b - KQ_{ab}) \tag{23}$$

is the probability weight of the subshell $S\{Q\}$, and

$$e^{\mathcal{G}\{Q\}} = \frac{1}{\sqrt{2\pi\sigma_0^2}} \int_{\mathbb{R}} \overline{\exp\left[-\frac{\beta}{2\sigma_0^2}\left(\frac{r}{\sqrt{\beta}} - v_0\{Q\}\right)^2\right]} \overline{\times \prod_{a=1}^{n} \exp\left[-\frac{\beta}{2\sigma^2}\left(\frac{r}{\sqrt{\beta}} - v_a\{Q\}\right)^2\right]} dr + \mathcal{O}(K^{-1}) \tag{24}$$

is equal to the integral in (20) within the subshell $S\{Q\}$, where the bar denotes averaging over the Gaussian variables $v_a\{Q\}$. The covariance Q_{ab} satisfies $-1 \le Q_{ab} \le 1$, so that the integration by Q_{ab} should be taken over the interval $[-1, 1]$.

The outline of the calculation is as follows (see also [33]). We first assume the following.

Assumption 3: The order of the two limits $K \to \infty$ and $n \to 0$ in (18) can be interchanged without affecting the final result.

Based on the assumption, we have

$$\mathcal{F} = \lim_{n\to 0} \frac{\partial}{\partial n} \left(\lim_{K\to\infty} K^{-1} \log \Xi_n\right) \tag{25}$$

so that as the next step we evaluate $\lim_{K\to\infty} K^{-1}\log\Xi_n$. From the theory of large deviations [30], [34], we know from Cramér's theorem that the probability measure $\mu_K\{Q\}$ of the empirical means

$$Q_{ab} = K^{-1} \sum_{k=1}^{K} x_{ak} x_{bk}$$

satisfies, as $K \to \infty$, the large deviation property with a rate function $\mathcal{I}\{Q\}$. Then, applying Varadhan's theorem [30], [34] (also known as Laplace's method and the saddle-point method) to (22) yields

$$\lim_{K\to\infty} K^{-1} \log \Xi_n = \sup_{\{Q\}} (\beta^{-1}\mathcal{G}\{Q\} - \mathcal{I}\{Q\}). \tag{26}$$

Taking the derivative with respect to n and then the limit $n \to 0$, we will obtain the final result.

First, we work with $e^{\mathcal{G}\{Q\}}$. An implication of the application of Varadhan's theorem to (22) is that only a single subshell will contribute to the integral in the limit $K \to \infty$. One can then regard that the dominant subshell contains typical configurations with respect to the posterior distribution. For the sake of analytical tractability, we restrict ourselves to searching for the dominant subshell only within those which induce highly symmetric covariance structure. Specifically, we adopt the following assumption of the *replica symmetry* (RS).

Assumption 4: The dominant subshell is invariant under exchange of any two replica indexes a and b, where $a, b \neq 0$.

The validity of the RS assumption is checked in Section III-D. Under the RS assumption, we can let $Q_{0a} = m$ for $a \neq 0$ and $Q_{ab} = q$ for $a \neq b$, $a, b \neq 0$. We can then construct explicitly the Gaussian random variables possessing the assumed covariance structure, by

$$\begin{aligned} v_0 &= u\left(1 - \frac{m^2}{q}\right)^{1/2} - t\,\frac{m}{\sqrt{q}} \\ v_a &= z_a(1-q)^{1/2} - t\sqrt{q}, \qquad a = 1, \ldots, n \end{aligned} \tag{27}$$

where u, t, and z_a are independent Gaussian random variables with mean 0 and variance 1. Neglecting terms with vanishing orders of K, (24) becomes

$$\begin{aligned} e^{\mathcal{G}(m,q)} &= \frac{1}{\sqrt{2\pi\sigma_0^2}} \int_{\mathbb{R}^2} \int_{\mathbb{R}} \\ &\times \exp\left\{-\frac{B_0}{2}\left[u\left(1-\frac{m^2}{q}\right)^{1/2} - t\,\frac{m}{\sqrt{q}} - \frac{r}{\sqrt{\beta}}\right]^2\right\} Du \\ &\times \left\{\int_{\mathbb{R}} \exp\left[-\frac{B}{2}\left[z(1-q)^{1/2} - t\sqrt{q} - \frac{r}{\sqrt{\beta}}\right]^2\right] Dz\right\}^n \\ &\times Dt\, dr \end{aligned} \tag{28}$$

where $B \equiv \beta/\sigma^2$, $B_0 \equiv \beta/\sigma_0^2$, and $Dt = (e^{-t^2/2}/\sqrt{2\pi})\, dt$ is the Gaussian measure.

We can perform the Gaussian average explicitly, which yields (29) shown at the top of the following page.

Now we turn to the evaluation of $\mathcal{I}\{Q\}$. From Cramér's theorem of the theory of large deviations [30], [34], the rate function $\mathcal{I}\{Q\}$ of $\mu_K\{Q\}$, as $K \to \infty$, is given as the Fenchel–Legendre transform of the cumulant generating function, i.e.,

$$\mathcal{I}\{Q\} \equiv \sup_{\{\tilde{Q}\}} \left(\sum_{a<b} \tilde{Q}_{ab} Q_{ab} - \log M\{\tilde{Q}\}\right) \tag{30}$$

where

$$M\{\tilde{Q}\} \equiv \sum_{\{x_a\}} 2^{-(n+1)} \exp\left(\sum_{a<b} \tilde{Q}_{ab} x_a x_b\right) \tag{31}$$

is the moment-generating function of $\{x_a x_b\}$ with x_a's following the uniform measure on $\{-1, 1\}$. Under the RS assumption, we can let $\tilde{Q}_{0a} \equiv E$ and $\tilde{Q}_{ab} \equiv F$ for $a \neq b$, $a, b \neq 0$. Then $M\{\tilde{Q}\} = M(E, F)$ is calculated explicitly as

$$\begin{aligned} M(E,F) &= \sum_{\{x_a,\, a=1,\ldots,n\}} 2^{-(n+1)} \left\{\exp\left[E\sum_{a=1}^{n} x_a + \frac{F}{2}\left(\sum_{a=1}^{n} x_a\right)^2\right]\right. \\ &\left. + \exp\left[-E\sum_{a=1}^{n} x_a + \frac{F}{2}\left(\sum_{a=1}^{n} x_a\right)^2\right]\right\} \cdot e^{-nF/2} \\ &= \int_{\mathbb{R}} \sum_{\{x_a,\, a=1,\ldots,n\}} 2^{-(n+1)} \left\{\exp\left[\left(\sqrt{F}\,z + E\right)\sum_{a=1}^{n} x_a\right]\right. \end{aligned}$$

$$
\begin{aligned}
e^{\mathcal{G}(m,q)} &= \left[1+B_0\left(1-\frac{m^2}{q}\right)\right]^{-1/2}[1+B(1-q)]^{-n/2}\times\frac{1}{\sqrt{2\pi\sigma_0^2}}\int_{\mathbb{R}^2}\\
&\quad\times\exp\left[-\frac{B_0}{2\left[1+B_0(1-m^2/q)\right]}\left(t\frac{m}{\sqrt{q}}+\frac{r}{\sqrt{\beta}}\right)^2\right]\times\exp\left[-\frac{nB}{2[1+B(1-q)]}\left(t\sqrt{q}+\frac{r}{\sqrt{\beta}}\right)^2\right]Dt\,dr\\
&=[1+B(1-q)]^{-(n-1)/2}\left\{(1+B_0)[1+B(1-q)]+nBq\left[1+B_0\left(1-\frac{m^2}{q}\right)\right]\right\}^{-1/2}\\
&\quad\times\frac{1}{\sqrt{2\pi\sigma_0^2}}\int_{\mathbb{R}}\exp\left[-\frac{r^2}{2\beta}\,\frac{B_0\left[1+B(1-q)\right]+nB\left[1+B_0(1-2m+q)\right]}{(1+B_0)\left[1+B(1-q)\right]+nBq\left[1+B_0(1-m^2/q)\right]}\right]dr\\
&=[1+B(1-q)]^{-(n-1)/2}\left\{[1+B(1-q)]+nB(B_0^{-1}+1-2m+q)\right\}^{-1/2}. \qquad (29)
\end{aligned}
$$

$$
\begin{aligned}
&+\exp\left[-\left(\sqrt{F}\,z+E\right)\sum_{a=1}^{n}x_a\right]\Bigg\}\,Dz\cdot e^{-nF/2}\\
&=\int_{\mathbb{R}}\cosh^n\left(\sqrt{F}\,z+E\right)Dz\cdot e^{-nF/2} \qquad (32)
\end{aligned}
$$

where we used the Hubbard–Stratonovich transform

$$e^{FS^2/2}=\int_{\mathbb{R}}e^{\sqrt{F}\,zS}\,Dz \qquad (33)$$

to linearize the exponents. The rate function, under the RS assumption, is thus given by

$$
\begin{aligned}
\mathcal{I}(m,q)=\sup_{E,F}\Bigg[&nEm+\frac{n}{2}F+\frac{n(n-1)}{2}Fq\\
&-\log\int_{\mathbb{R}}\cosh^n\left(\sqrt{F}\,z+E\right)Dz\Bigg]. \qquad (34)
\end{aligned}
$$

The supremum with respect to E and F is achieved when E and F satisfy

$$m=\frac{\int_{\mathbb{R}}\cosh^{n-1}\left(\sqrt{F}\,z+E\right)\sinh\left(\sqrt{F}\,z+E\right)Dz}{\int_{\mathbb{R}}\cosh^{n}\left(\sqrt{F}\,z+E\right)Dz} \qquad (35)$$

$$q=\frac{\int_{\mathbb{R}}\cosh^{n-2}\left(\sqrt{F}\,z+E\right)\sinh^2\left(\sqrt{F}\,z+E\right)Dz}{\int_{\mathbb{R}}\cosh^{n}\left(\sqrt{F}\,z+E\right)Dz}. \qquad (36)$$

We apply Varadhan's theorem to evaluate the integral in (22) asymptotically in the limit $K\to\infty$. Under the RS assumption we have

$$\lim_{K\to\infty}K^{-1}\log\Xi_n=\sup_{m,q}\left[\beta^{-1}\mathcal{G}(m,q)-\mathcal{I}(m,q)\right]. \qquad (37)$$

A supremum point with respect to m and q satisfies the extremum condition derived from (29) and (34), which is given by

$$E=\frac{\beta^{-1}B}{[1+B(1-q)]+nB(B_0^{-1}+1-2m+q)}, \qquad (38)$$

and

$$F=\frac{\beta^{-1}B^2(B_0^{-1}+1-2m+q)}{\left\{[1+B(1-q)]+nB(B_0^{-1}+1-2m+q)\right\}[1+B(1-q)]}. \qquad (39)$$

Collecting these results, we obtain the following formula for the replica-symmetric free energy $\mathcal{F}^{\mathrm{RS}}$:

$$\mathcal{F}^{\mathrm{RS}}=\lim_{n\to0}\frac{\partial}{\partial n}\sup_{m,q}\inf_{E,F}f^{\mathrm{RS}} \qquad (40)$$

where

$$
\begin{aligned}
f^{\mathrm{RS}}=\log&\int_{\mathbb{R}}\cosh^n\left(\sqrt{F}\,z+E\right)Dz\\
&-nEm-\frac{n}{2}F-\frac{n(n-1)}{2}Fq\\
&-\frac{1}{2\beta}\left\{(n-1)\log[1+B(1-q)]\right.\\
&\left.+\log[1+B(1-q)+nB(B_0^{-1}+1-2m+q)]\right\}. \qquad (41)
\end{aligned}
$$

We can exchange the order of taking derivative with respect to n and the extremizations, by noting that $f^{\mathrm{RS}}\to0$ in the limit $n\to0$. We finally arrive at the following proposition.

Proposition 1:

a) Let Assumptions 2–4 hold, then the average free energy $\mathcal{F}$ is given, in the limit $K\to\infty$, by the replica-symmetric free energy

$$
\begin{aligned}
\mathcal{F}^{\mathrm{RS}}=&\int_{\mathbb{R}}\log\left[\cosh\left(\sqrt{F}\,z+E\right)\right]Dz-Em-\tfrac{1}{2}F(1-q)\\
&-\frac{1}{2\beta}\left\{\log[1+B(1-q)]+\frac{B[B_0^{-1}+1-2m+q]}{1+B(1-q)}\right\} \qquad (42)
\end{aligned}
$$

where the macroscopic parameters $\{m,q,E,F\}$ are to be determined by the saddle-point equations

$$
\begin{aligned}
m&=\int_{\mathbb{R}}\tanh\left(\sqrt{F}\,z+E\right)Dz\\
q&=\int_{\mathbb{R}}\tanh^2\left(\sqrt{F}\,z+E\right)Dz\\
E&=\frac{\beta^{-1}B}{1+B(1-q)}\\
F&=\frac{\beta^{-1}B^2(B_0^{-1}+1-2m+q)}{[1+B(1-q)]^2}. \qquad (43)
\end{aligned}
$$

b) Let Assumption 1 also hold, then the free energy per user $\mathcal{F}_K(\boldsymbol{r},S)$ converges with probability one to $\mathcal{F}^{\mathrm{RS}}$ in the limit $K\to\infty$.

The saddle-point equations (43) are derived by taking the $n \to 0$ limit of the respective extremum conditions (35), (36), (38), and (39). The mathematically true solution to the extremization problem of (40) is such that E and F minimize $f^{\rm RS}(m, q, E, F)$ globally, and that m and q maximize $f^{\rm RS}(m, q, E(m, q), F(m, q))$ globally. The globally extremizing solution is called the stable state in statistical mechanics. We call it the globally stable state. However, solutions yielding only local extrema, which are called the metastable states, have some significance, as discussed in Section V-A. We will, therefore, deal with such locally extremal saddle-point solutions, or metastable states, as well as with the globally stable state.

B. Expression for Correlation

We derive the expression for the correlation d between the estimation result $\hat{\boldsymbol{x}}^{\rm (MPM)}$ by MPM detector and the original information bits $\boldsymbol{x}_0$. The correlation d depends on the realizations of random quantities such as spreading sequences and noise, and therefore it is a fluctuating quantity itself. Nevertheless, we expect that the fluctuations of d will vanish in the large-system limit $K \to \infty$ due to the self-averaging property. Hence, we evaluate the average of the correlation d over all realizations of the spreading sequences and the noise. For MPM detector, we have

$$d = \lim_{n\to 0}\lim_{K\to\infty}\left\langle\!\!\left\langle \frac{1}{K}\sum_{k=1}^{K} \text{sign}\,(x_{0k}\langle x_k\rangle_\sigma)\right\rangle\!\!\right\rangle \tag{44}$$

where $\langle\cdot\rangle_\sigma$ and $\langle\langle\cdot\rangle\rangle$ denote the average with respect to the posterior distribution (6) and the average over the spreading sequences and the noise, respectively.

In this subsection, we derive, under the RS assumption, the following proposition.

Proposition 2: Let Assumptions 1–4 hold, then the correlation d for the MPM detector is self-averaging, and is given by

$$d = \int_{\mathbb{R}} \text{sign}\,\left(\sqrt{F}\,z + E\right)\,Dz \tag{45}$$

where F and E are to be determined by the saddle-point equations (43).

The proof basically follows the argument in Nishimori [35, Sec. 5.4.4]. From this equality, it immediately follows that the bit-error rate is given by

$$P_b = Q\left(\frac{E}{\sqrt{F}}\right) \tag{46}$$

where $Q(z) \equiv \int_z^\infty Dt$ is the error function, hence allowing us to evaluate the bit-error rate P_b from the saddle-point solution. Propositions 1 and 2 are the main results of this paper.

The key ingredient to deriving (45) is Lemma 1 given later. Once we admit its validity, we have for any analytic function F that

$$\lim_{n\to 0}\lim_{K\to\infty}\left\langle\!\!\left\langle \frac{1}{K}\sum_{k=1}^{K} F[x_{0k}\langle x_k\rangle_\sigma]\right\rangle\!\!\right\rangle = \int_{\mathbb{R}} F\left[\tanh\left(\sqrt{F}\,z + E\right)\right]\,Dz \tag{47}$$

and then (45) immediately follows by considering a series of analytic functions converging to $\text{sign}\,(\cdot)$ [35].

Lemma 1: Let Assumptions 1–4 hold, then we have

$$\lim_{n\to\infty}\lim_{K\to\infty}\left\langle\!\!\left\langle \frac{1}{K}\sum_{k=1}^{K} (x_{0k}\langle x_k\rangle_\sigma)^j\right\rangle\!\!\right\rangle = \int_{\mathbb{R}} \tanh^j\left(\sqrt{F}\,z + E\right)\,Dz, \qquad j = 0, 1, \ldots. \tag{48}$$

Proof: Let $1 \le a_1 < a_2 < \cdots < a_j \le n$ be j replica indexes. Since we are working with the RS assumption (Assumption 4), all the replicated systems should have the same statistical properties, so that we have

$$\left\langle\!\!\left\langle \frac{1}{K}\sum_{k=1}^{K}\prod_{m=1}^{j} (x_{0k}\langle x_{a_m k}\rangle_\sigma)\right\rangle\!\!\right\rangle = \left\langle\!\!\left\langle \frac{1}{K}\sum_{k=1}^{K} (x_{0k}\langle x_k\rangle_\sigma)^j\right\rangle\!\!\right\rangle. \tag{49}$$

The left-hand side of (49) can be handled by considering the moment-generating function of the random variable

$$\sum_{k=1}^{K}\prod_{m=1}^{j} (x_{0k}x_{a_m k}) \tag{50}$$

with respect to the (unnormalized) measure

$$\prod_{a=1}^{n} p(\boldsymbol{r}|\boldsymbol{x}_a, S)p(\boldsymbol{x}_a).$$

The moment-generating function $\mathcal{M}_n(h; \boldsymbol{r}, S)$ is

$$\begin{aligned}\mathcal{M}_n(h; \boldsymbol{r}, S) = &\sum_{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n}\prod_{a=1}^{n} p(\boldsymbol{x}_a)\\ &\times \exp\left[h\sum_{k=1}^{K}\left(\prod_{m=1}^{j} x_{0k}x_{a_m k}\right)\right]\\ &\times \prod_{a=1}^{n}\exp\left(-\frac{1}{2\sigma^2}\,\|\boldsymbol{r} - N^{-1/2}S\boldsymbol{x}_a\|^2\right)\end{aligned} \tag{51}$$

where h is the auxiliary variable introduced to define the moment-generating function. We consider a free-energy-like quantity $\tilde{\mathcal{F}}$ defined by

$$\tilde{\mathcal{F}} \equiv \lim_{K\to\infty} K^{-1}\log\tilde{\Xi}_n \tag{52}$$

where

$$\begin{aligned}\tilde{\Xi}_n &\equiv \langle\langle\mathcal{M}_n(h; \boldsymbol{r}, S)\rangle\rangle\\ &= C^{-1}\int_{\mathbb{R}^N} \overline{Z_0(\boldsymbol{r}, S)\mathcal{M}_n(h; \boldsymbol{r}, S)}\,d\boldsymbol{r}\end{aligned} \tag{53}$$

is an averaged moment-generating function. The quantity $\tilde{\mathcal{F}}$ can thus be regarded as a rescaled version of the cumulant generating function for the random variable of (50). Taking the derivative of $\tilde{\mathcal{F}}$ with respect to h, and letting h go to 0, provides us with information of the averaged first-order moment, that is,

$$\left.\frac{\partial\tilde{\mathcal{F}}}{\partial h}\right|_{h=0} = \lim_{K\to\infty}\Xi_n^{-1}\left\langle\!\!\left\langle \frac{1}{K}\sum_{k=1}^{K}\prod_{m=1}^{j} (x_{0k}\langle x_{a_m k}\rangle_\sigma)\right\rangle\!\!\right\rangle. \tag{54}$$

Taking the limit $n \to 0$ of (54) gives the desired quantity. We therefore concentrate on the quantity $\tilde{\Xi}_n$.

Thanks to the formal similarity between $\tilde{\Xi}_n$ and Ξ_n (see (53) and (19)), we can proceed basically by following the replica calculation in the preceding section to evaluate $\tilde{\Xi}_n$. Specifically, we only have to reevaluate the rate function $\tilde{\mathcal{I}}\{Q\}$ of the measure

$$\tilde{\mu}_K\{Q\} = \sum_{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n} \prod_{a=0}^{n} p(\boldsymbol{x}_a) \times \prod_{a<b} \delta(\boldsymbol{x}_a \cdot \boldsymbol{x}_b - KQ_{ab}) \times \exp\left[h \sum_{k=1}^{K} \prod_{m=1}^{j} (x_{0k} x_{a_m k})\right]. \tag{55}$$

The remaining part of the calculation is not affected. We have

$$\tilde{\mathcal{I}}\{Q\} = \sup_{\{\tilde{Q}\}} \left[\sum_{a<b} \tilde{Q}_{ab} Q_{ab} - \log \tilde{M}(\{\tilde{Q}\}, h)\right] \tag{56}$$

where

$$\tilde{M}\left(\{\tilde{Q}\}, h\right) \equiv \sum_{\{x_a\}} 2^{-(n+1)} \cdot \exp\left[\sum_{a<b} \tilde{Q}_{ab} x_a x_b + h \prod_{m=1}^{j} (x_0 x_{a_m})\right]. \tag{57}$$

h does not appear anywhere else. Therefore, by exchanging the order of the two limits $n \to 0$ and $K \to \infty$ (Assumption 3), we obtain, under the RS assumption

$$\begin{aligned} \left.\frac{\partial \tilde{\mathcal{F}}}{\partial h}\right|_{h=0} &= \frac{\partial}{\partial h}\left.\left(\lim_{K\to\infty} K^{-1} \log \tilde{\Xi}_n\right)\right|_{h=0} \\ &= \frac{\partial}{\partial h} \log \tilde{M}\left.\left(\{\tilde{Q}\}, h\right)\right|_{h=0} \\ &= \frac{\int_{\mathbb{R}} \cosh^{n-j}\left(\sqrt{F}\, z + E\right) \sinh^{j}\left(\sqrt{F}\, z + E\right) Dz}{\int_{\mathbb{R}} \cosh^{n}\left(\sqrt{F}\, z + E\right) Dz} \\ &\xrightarrow{n\to 0} \int_{\mathbb{R}} \tanh^{j}\left(\sqrt{F}\, z + E\right) Dz \end{aligned} \tag{58}$$

which proves (48). □

The proof of Lemma 1 explains, as a by-product, that the macroscopic parameters m and q have the following meaning:

$$m = \lim_{K\to\infty} \left\langle\!\!\left\langle \frac{1}{K} \sum_{k=1}^{K} x_{0k} \langle x_k \rangle_\sigma \right\rangle\!\!\right\rangle \tag{59}$$

$$q = \lim_{K\to\infty} \left\langle\!\!\left\langle \frac{1}{K} \sum_{k=1}^{K} (x_{0k} \langle x_k \rangle_\sigma)^2 \right\rangle\!\!\right\rangle. \tag{60}$$

Furthermore, the form of (46) suggests that the quantity E^2/F serves as the signal-to-interference ratio SIR.

C. Solving Numerically the Saddle-Point Equations

One has to solve the saddle-point equations (43) numerically in order to evaluate the performance of the MPM multiuser detector. The approach we have taken is as follows. We consider the problem of evaluating B_0 which gives a prescribed value of the bit-error rate $0 < P_b < 1/2$, for a given β. From (46) we calculate $A \equiv Q^{-1}(P_b)$ $(0 < A < \infty)$. Since $A^2 = E^2/F$ at the saddle-point solution, the first three equations of (43) can be rewritten as

$$m = \int_{\mathbb{R}} \tanh \sqrt{F}\, (z + A)\, Dz \tag{61}$$

$$q = \int_{\mathbb{R}} \tanh^2 \sqrt{F}\, (z + A)\, Dz \tag{62}$$

$$A\sqrt{F} = \frac{\beta^{-1} B}{1 + B(1 - q)}. \tag{63}$$

By eliminating q from (62) and (63), we obtain a one-dimensional problem

$$A\sqrt{F} = \frac{\beta^{-1} B}{1 + B\,(1 - F_A[F])} \tag{64}$$

where $0 < F < \infty$, and where

$$F_A[F] \equiv \int_{\mathbb{R}} \tanh^2 \sqrt{F}\, (z + A)\, Dz. \tag{65}$$

The saddle-point solution F (i.e., the fixed point of (64)) subsequently determines $m(F)$ and $q(F)$ via (61) and (62), respectively, and then B_0 via the last equation of (43).

D. Assumptions Made in Replica Analysis

We list the technical assumptions made in the course of the replica analysis.

- The free energy $\mathcal{F}_K(\boldsymbol{r}, S)$ has the self-averaging property in $K \to \infty$ limit (Assumption 1).
- Analytic continuation of Ξ_n to real n is valid (Assumption 2).
- The order of the limits $n \to 0$ and $K \to \infty$ can be exchanged (Assumption 3).
- The RS assumption does not exclude the true solution (Assumption 4).
- The relevant subshell $S\{Q\}$ contains an exponentially large number of possible $\boldsymbol{x}$ values.

In order to check the validity of the replica method, we have to consider these factors in more depth.

Assumption 1, the self-averaging property, has already been discussed at the end of Section II. Assumption 2, the analytic continuation to real n from the expression obtained by evaluating the relevant quantity only for positive integers n, is the central assumption of the replica method. Providing mathematical justification to this procedure is a great challenge, and is beyond the scope of this paper.

Assumption 3 is about the validity of exchanging the order of the two limits $n \to 0$ and $K \to \infty$, which has been utilized to evaluate relevant integrals by invoking Varadhan's theorem *before* taking the $n \to 0$ limit. It can be shown for one of the standard models in statistical mechanics, called the Sherrington–Kirkpatrick model [36], and possibly for our model as well, that the exchange of the order of the limits is justified [37], although we have at present no rigorous result regarding this point.

Assumption 4, the RS assumption, may seem a quite natural assumption, since there seems to be no *a priori* reason to consider broken symmetry between the replicas. Nevertheless, it is in principle still possible that the true extremum of

$$f \equiv \log M\{\tilde{Q}\} - \sum_{a<b} \tilde{Q}_{ab} Q_{ab} + \beta^{-1} \mathcal{G}\{Q\} \tag{66}$$

does not have the RS. Therefore, the validity of the RS assumption should be checked.

We probe the so-called de Almeida–Thouless (AT) stability [38], which refers to the local stability of the RS saddle-point solution against replica-symmetry-breaking (RSB) perturbations. The procedure is briefly described as follows: we evaluate the Hessian of f with respect to the macroscopic parameters $\{Q_{ab}, \tilde{Q}_{ab}\}$ at the RS saddle-point solution, and then derive the stability condition, the condition under which f is maximized and minimized with respect to $\{Q\}$ and $\{\tilde{Q}\}$, respectively. The result is summarized in the following proposition as the AT line, which marks the boundary between two regions in the parameter space, one in which the RS saddle-point solution is stable against RSB and thus the RS assumption is valid, and another in which the RS saddle-point solution is unstable against RSB, and consequently, the RS assumption is no longer valid.

Proposition 3: Let Assumptions 1–3 hold, then the AT line is given by

$$1 - \beta E^2 \int_{\mathbb{R}} \operatorname{sech}^4\left(\sqrt{F}\, z + E\right) Dz = 0. \tag{67}$$

The RS saddle-point solution is valid as long as the left-hand side of (67) is positive.

Details of the derivation of (67) are given in Appendix III.

The last assumption has not been stated explicitly so far. However, it is certainly one of the necessary conditions for the final result to be valid because, for the summation over the dominant subshell to have the proper meaning, the dominant subshell has to contain an exponentially large number of $\boldsymbol{x}$ values. Under the RS assumption, we can evaluate the volume of the dominant subshell $S\{E, F\}$, specified by E and F, as given by the saddle-point solution. The number $N\{E, F\}$ of possible microscopic configurations $\{\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ within the subshell $S\{E, F\}$ is given by

$$N\{E, F\} = \mu_K\{Q\}\, 2^{K(n+1)}. \tag{68}$$

In order for the evaluation of probability weight over the subshell to be valid, $N\{E, F\}$ should be exponentially large in K. This leads, in the $n \to 0$ limit, to the condition

$$\Psi \equiv \int_{\mathbb{R}} \log\left[\cosh\left(\sqrt{F}\, z + E\right)\right] Dz - Em - \frac{1}{2} F(1-q) + \log 2 > 0. \tag{69}$$

The condition $\Psi = 0$ defines the so-called *freezing point*, at which the system loses its microscopic degrees of freedom.

E. IO Multiuser Detector

If we put the control parameter σ of the MPM detector to be equal to the true channel noise level σ_0, we are given the IO multiuser detector. In this case, the true channel characteristics, and its model used in designing the detector, enter the replica calculation in a completely symmetric way. Thus, the true channel (see (15)) can be regarded as the 0th replica, and all $n+1$ replicas can be treated in a symmetric manner [31]. This symmetry allows us to prove some interesting properties of the IO multiuser detector. One such result is summarized in the following proposition.

Proposition 4: For the case of the IO multiuser detector, the RS assumption is valid for the stable saddle-point solution.

Proof: The proposition is proved by first deriving the stability condition of the RS saddle-point solution for the IO multiuser detector, and then showing that it is equivalent to the AT stability condition (see (67)). Because of the symmetry between the $n+1$ replicas, we can assert, under the RS assumption, that $E = F$ and $q = m$ hold. The function f^{RS} becomes

$$f^{\mathrm{RS}} = \log \int_{\mathbb{R}} \cosh^n\left(\sqrt{E}\, z + E\right) Dz - \frac{n}{2} E[1 + (n+1)q] - \frac{1}{2\beta} \times \{n \log[1 + B(1-q)] + \log(n+1)\} \tag{70}$$

from which the RS free energy $\mathcal{F}^{\mathrm{RS}}$ follows as

$$\mathcal{F}^{\mathrm{RS}} = \int_{\mathbb{R}} \log\left[\cosh\left(\sqrt{E}\, z + E\right)\right] Dz - \frac{1}{2} E(1+q) - \frac{1}{2\beta} \{\log[1 + B(1-q)] + 1\} \tag{71}$$

where the saddle-point equations determining $\{q, E\}$ are given by

$$q = \int_{\mathbb{R}} \tanh\left(\sqrt{E} z + E\right) Dz = \int_{\mathbb{R}} \tanh^2\left(\sqrt{E}\, z + E\right) Dz$$
$$E = \frac{\beta^{-1} B}{1 + B(1-q)}. \tag{72}$$

Imposing the second equality of (72) on (71) yields

$$\mathcal{F}^{\mathrm{RS}} = \int_{\mathbb{R}} \log\left[\cosh\left(\sqrt{E}\, z + E\right)\right] Dz - \frac{1}{2}(2 + B^{-1})E - \frac{1}{2\beta} \log \frac{B}{\beta E} \tag{73}$$

in which $E = E(q) = \beta^{-1} B / (1 + B(1-q))$. As the condition under which q, as given by the saddle-point solution, maximizes f^{RS} at the saddle point, we have

$$\frac{d^2 f^{\mathrm{RS}}}{dq^2} = \left(\frac{dE(q)}{dq}\right)^2 \frac{\partial^2 f^{\mathrm{RS}}}{\partial E^2} \xrightarrow{n \to 0} (\beta E^2)^2 \left[\int_{\mathbb{R}} \operatorname{sech}^4\left(\sqrt{E} z + E\right) Dz - \frac{1}{\beta E^2}\right] < 0. \tag{74}$$

This is identical with the AT stability condition (see (67)), thus proving the proposition. □

It should be noted that, by the same $(n+1)$-replica argument, the signal-to-interference ratio for the IO multiuser detector is straightforwardly given by $\mathsf{SIR} = E^2/F = E$. The stability result of Proposition 4 can also be derived without using the replica method. Nishimori [39] applied a gauge theory to the analysis of the IO multiuser detector, to obtain a result extending Proposition 4, also proving the identity $q = m$ as a corollary.

IV. Derivation of Existing Results by Replica Method

A. Capacity of CDMA Channels

The statistical mechanics approach is also useful in deriving the information-theoretic capacity of CDMA channels. In the following analysis, we assume that the information rate is the same for all users, i.e., $R_k = R$ for $k = 1, \ldots, K$. By the canonical argument for the capacity region [40], we have the following inequality for the sum rate:

$$\sum_{k=1}^{K} R_k = KR \le I(X_1, \ldots, X_K; Y) \tag{75}$$

where X_k, $k = 1, \ldots, K$, and Y denote the random variables corresponding to the information x_k and the received data $\boldsymbol{r}$, respectively. We define the capacity C of a CDMA channel as the maximum rate (rather than the maximum sum rate in the literature), which is given by

$$\mathsf{C} = K^{-1} I(X_1, \ldots, X_K; Y). \tag{76}$$

In this subsection, we evaluate the capacity C in the large-system limit $K \to \infty$.

The mutual information in the right-hand side of (76) is given in terms of differential entropies as

$$I(X_1, \ldots, X_K; Y) = h(Y) - h(Y|X_1, \ldots, X_K). \tag{77}$$

The conditional information $h(Y|X_1, \ldots, X_K)$ is equal to the differential entropy of the channel noise, because the noise is assumed to be independent of the information X_k. It is given by

$$h(Y|X_1, \ldots, X_K) = \frac{N}{2}\left(1 + \log 2\pi\sigma_0^2\right) = \frac{N}{2} + \log C. \tag{78}$$

(Note that the base of the logarithm is e so that the unit of information here is *nats*.) By definition, for $h(Y)$ we have

$$\begin{aligned} h(Y) &= -\int_{\mathbb{R}^N} p_0(\boldsymbol{r}|S) \log p_0(\boldsymbol{r}|S)\, d\boldsymbol{r} \\ &= -C^{-1} \int_{\mathbb{R}^N} Z_0(\boldsymbol{r}, S) \log Z_0(\boldsymbol{r}, S)\, d\boldsymbol{r} + \log C. \end{aligned} \tag{79}$$

The self-averaging property in this case means that, in the large-system limit, the differential entropy normalized by the number of users $K^{-1}h(Y)$ is equal to its average

$$\begin{aligned} &\lim_{K\to\infty} K^{-1} h(Y) \\ &= \lim_{K\to\infty} \left[-(KC)^{-1} \int_{\mathbb{R}^N} \overline{Z_0(\boldsymbol{r}, S) \log Z_0(\boldsymbol{r}, S)}\, d\boldsymbol{r} \right. \\ &\qquad \left. + K^{-1} \log C \right] \end{aligned} \tag{80}$$

for almost all realizations of the spreading sequences. It should be noted that the first term in the right-hand side of (80) is nothing but the free energy (see (14))

$$\mathcal{F}_0 \equiv \mathcal{F}|_{\sigma=\sigma_0}. \tag{81}$$

Using this fact, from (77), (78), and (80), we have the following proposition.

Proposition 5: The capacity C of the CDMA channel is given, in the large-system limit, by

$$\mathsf{C} = \lim_{K\to\infty} K^{-1} I(X_1, \ldots, X_K; Y) = -\left(\mathcal{F}_0 + \frac{1}{2\beta}\right) \tag{82}$$

where $\mathcal{F}_0$ is defined by (81).

This means that, if we can evaluate the free energy $\mathcal{F}_0$ analytically, we can obtain an analytical expression for the maximum information rate and, in turn, for the capacity.

In this paper, we address the capacity of the AWGN CDMA channel, and of the binary-input AWGN (BIAWGN) CDMA channel. We first discuss the AWGN CDMA case, in which the inputs can take continuous values. The Gaussian prior is known to give the maximum of the differential entropy $h(Y)$ in this case, and, therefore, the maximum of the common information-theoretic capacity of the CDMA channel, under power constraint. Verdú and Shamai [4] have reported an analytical result in the large-system limit, on the capacity, and on the optimum spectral efficiency of the CDMA channel, based on the asymptotic empirical spectral distribution (ESD) of random cross-correlation matrices [41]. Our objective here is to demonstrate that the replica analysis does reproduce their result, thereby providing supporting evidence for the validity of our approach.

We assume the unit-variance Gaussian prior

$$p(x_k) = \frac{1}{\sqrt{2\pi}}\, e^{-x_k^2/2} \tag{83}$$

and perform the replica calculation again. We start with the probability measure $\mu_K^G\{Q\}$ of $\{Q\}$, given by

$$\mu_K^G\{Q\} = \int_{\mathbb{R}^{K(n+1)}} \prod_{a\le b} \delta(\boldsymbol{x}_a \cdot \boldsymbol{x}_b - KQ_{ab}) \prod_{a=0}^{n} [p(\boldsymbol{x}_a)\, d\boldsymbol{x}_a], \tag{84}$$

where $d\boldsymbol{x}_a \equiv \prod_{k=1}^{K} dx_{ak}$. It should be noted that now we have Q_{aa}, $a = 0, 1, \ldots, n$, as variables as well. This is because x_k may take any real values under the Gaussian prior, so that we have to take into account the possibility that $Q_{aa} = K^{-1}\|\boldsymbol{x}_a\|^2$ at the saddle-point solution may be different from 1. From Cramér's theorem, the probability measure $\mu_K^G\{Q\}$ satisfies the large deviation property with rate function

$$\mathcal{I}^G\{Q\} \equiv \sup_{\{\tilde{Q}\}} \left(\sum_{a\le b} \tilde{Q}_{ab} Q_{ab} - \log M^G\{\tilde{Q}\} \right) \tag{85}$$

where

$$M^G\{\tilde{Q}\} \equiv \int_{\mathbb{R}^{n+1}} \exp\left(\sum_{a\le b} \tilde{Q}_{ab} x_a x_b \right) \prod_{a=0}^{n} Dx_a. \tag{86}$$

We proceed with the RS assumption, and let $Q_{00} \equiv p_0$, $Q_{aa} \equiv p$, $\tilde{Q}_{00} \equiv G_0/2$, and $\tilde{Q}_{aa} \equiv G/2$, $a = 1, \ldots, n$. Then we have

$$\begin{aligned} M^G\{\tilde{Q}\} &= (1 - G_0)^{-1/2} (1 + F - G)^{-(n-1)/2} \\ &\quad \times \left[1 + F - G - n\left(\frac{E^2}{1 - G_0} + F \right) \right]^{-1/2}. \end{aligned} \tag{87}$$

Calculation of $\mathcal{G}$ under the RS assumption can be done in the same way as before, by letting

$$v_0 = u\left(p_0 - \frac{m^2}{q}\right)^{1/2} - t\,\frac{m}{\sqrt{q}}$$
$$v_a = z_a(p-q)^{1/2} - t\sqrt{q}, \qquad a = 1, \ldots, n. \tag{88}$$

After some algebra we obtain that $p_0 = 1$ and $G_0 = 0$ at the RS saddle point, and the RS free energy becomes

$$\mathcal{F}^{\rm RS} = -\frac{1}{2}\left[\log(1+F-G) - \frac{E^2+F}{1+F-G}\right] - Em + \frac{1}{2}Fq - \frac{1}{2}Gp - \frac{1}{2\beta} \times\left\{\log[1+B(p-q)] + \frac{B(B_0^{-1}+1-2m+q)}{1+B(p-q)}\right\} \tag{89}$$

where $\{m, q, p, E, F, G\}$ are to be determined from the following saddle-point equations:

$$m = \frac{E}{1+F-G}, \qquad q = \frac{E^2+F}{(1+F-G)^2}$$
$$p = \frac{E^2+2F+1-G}{(1+F-G)^2}, \qquad E = \frac{\beta^{-1}B}{1+B(p-q)}$$
$$F = \frac{\beta^{-1}B^2(B_0^{-1}+1-2m+q)}{[1+B(p-q)]^2}, \qquad G = F - E. \tag{90}$$

Here, we only need to evaluate the free energy for $\sigma = \sigma_0$ in order to discuss the capacity (see (81)). In this case, we can eliminate the variables m, F, p, and G using the relations $m = q$, $F = E$, $p = 1$, and $G = 0$, which immediately follow from the $(n+1)$-replica argument (like in the replica analysis of the IO multiuser detector). The free energy $\mathcal{F}_0 = \mathcal{F}|_{\sigma=\sigma_0}$ and the corresponding capacity C become

$$\mathcal{F}_0 = -\frac{1}{2}\left[\log(1+E) - E(1-q) + \beta^{-1} \times\{\log[1+B_0(1-q)]+1\}\right] \tag{91}$$

and

$$\beta\mathsf{C} = \frac{\beta}{2}\log(1+E) + \frac{1}{2}\log[1+B_0(1-q)] - \frac{\beta}{2}E(1-q) \tag{92}$$

where the saddle-point equations determining $\{q, E\}$ are

$$q = \frac{E}{1+E}, \qquad E = \frac{\beta^{-1}B_0}{1+B_0(1-q)}. \tag{93}$$

With a modest amount of foresight we let

$$\tau \equiv B_0 q \tag{94}$$

and solve the saddle-point equations (93) in terms of τ, to obtain

$$\tau = \tfrac{1}{4}\,\mathcal{F}(\mathsf{SNR}, \beta), \qquad E = \mathsf{SNR} - \tau \tag{95}$$

where

$$\mathcal{F}(x, z) \equiv \left(\sqrt{x\left(1+\sqrt{z}\right)^2+1} - \sqrt{x\left(1-\sqrt{z}\right)^2+1}\right)^2$$

(not to be confused with the free energy), and where $\mathsf{SNR} \equiv 1/\sigma_0^2$ is the ratio of the energy per N chips and the Gaussian noise spectral density. The capacity, evaluated at the saddle point, is

$$\beta\mathsf{C} = \frac{\beta}{2}\log(1+\mathsf{SNR}-\tau) + \frac{1}{2}\log(1+\mathsf{SNR}\beta-\tau) - \frac{\tau}{2\mathsf{SNR}} \tag{96}$$

which is exactly the same result as the one reported by Verdú and Shamai [4].

Next, we consider the case of the BIAWGN CDMA channel, in which the input is constrained to be binary, i.e., $x_k = \pm 1$. If we assume (as it should be) that $h(Y)$ is maximized for the uniform prior $p(\boldsymbol{x}) = 2^{-K}$, then we already have the analytical expression of the free energy (Proposition 1) for this case, and the capacity can be obtained using (82).

B. Decorrelating and Linear MMSE Detectors

In this subsection, we show the derivation and the results for the decorrelating and the linear MMSE detectors by the replica analysis, in order to compare them with the results so far reported in the literature. In the Bayes framework, it is not unusual to assume models of the source and the channel with different characteristics from those of the true source and channel, for the detector. We have already seen such an example in the MPM detector, where the detector assumes the noise level σ, which may be different from the true noise level σ_0. Here, we consider the case in which the detector assumes the unit-variance Gaussian prior (see (83)), whereas the true prior is binary, i.e., $p(\boldsymbol{x}_0) = 2^{-K}$ for all $\boldsymbol{x}_0$. Under this assumption, we can consider, just like for the MPM detector, a general class of *linear multiuser detectors*, defined as follows.

Definition 2: The linear multiuser detector with control parameter σ is defined by

$$\hat{x}_k^{(l)} = \arg\max_{x_k} \int_{\mathbb{R}^{K-1}} p^{(l)}(\boldsymbol{x}|\boldsymbol{r}, S) \prod_{j\neq k} dx_j \tag{97}$$

where

$$p^{(l)}(\boldsymbol{x}|\boldsymbol{r}, S) = [Z^{(l)}(\boldsymbol{r}, S)]^{-1}p^{(l)}(\boldsymbol{x}) \times\exp\left(-\frac{1}{2\sigma^2}\|\boldsymbol{r} - N^{-1/2}S\boldsymbol{x}\|^2\right) \tag{98}$$

is the posterior distribution for the unit-variance Gaussian prior

$$p^{(l)}(\boldsymbol{x}) \equiv (2\pi)^{-K/2}\exp\left(-\frac{\|\boldsymbol{x}\|^2}{2}\right) \tag{99}$$

with

$$Z^{(l)}(\boldsymbol{r}, S) = \int_{\mathbb{R}^K}\exp\left(-\frac{1}{2\sigma^2}\|\boldsymbol{r} - N^{-1/2}S\boldsymbol{x}\|^2\right) D\boldsymbol{x} \tag{100}$$

where $D\boldsymbol{x} \equiv \prod_{k=1}^K Dx_k$.

This appears to be different from the conventional definition of the linear multiuser detector, because we have made no explicit reference to the linearity. However, the posterior, appearing in the definition of the linear multiuser detector, becomes Gaussian because both the prior and the noise distributions are Gaussian. Hence, the detection (see (97)) can be done simply by a linear transformation on the received signals, and therefore this definition does specify a family of linear multiuser detectors. Moreover, as is well known, for the linear model treated in this paper (see (1)), considering the MMSE detector within the restricted set of linear transformations, is equivalent to the assumption that the prior is Gaussian. As in the case of the MPM detector, the linear multiuser detector uses the control parameter σ to represent the detector's assumption about the noise level. As can be confirmed by simple algebra, in the limit $\sigma \to 0$ our linear multiuser detector corresponds to the decorrelating detector [42], [43], and if we can set the true control parameter $\sigma = \sigma_0$, then we have the linear MMSE detector [43]–[45].

The replica calculation for the linear multiuser detector is essentially the same as those for the MPM detector and for the capacity. We only have to re-evaluate $\mathcal{I}\{Q\}$ using the Gaussian prior for $a = 1, \ldots n$ and the binary one for $a = 0$. We have

$$\mathcal{I}\{Q\} = \sup_{\{\tilde{Q}\}} \left({\sum_{a \le b}}' \tilde{Q}_{ab} Q_{ab} - \log \overline{M}\{\tilde{Q}\} \right) \tag{101}$$

where

$$\overline{M}\{\tilde{Q}\} \equiv \sum_{x_0 = \pm 1} \frac{1}{2} \int_{\mathbb{R}^n} \exp\left({\sum_{a \le b}}' \tilde{Q}_{ab} x_a x_b \right) \prod_{a=1}^{n} Dx_a. \tag{102}$$

The symbols $\sum'$ and $\prod'$ mean that the term with $(a, b) = (0, 0)$ should be excluded from the summation and the multiplication, respectively. This exclusion is due to the binary nature of x_0, which yields $x_{0k}^2 = 1$ and thus makes introduction of Q_{00} and $\tilde{Q}_{00}$ unnecessary. Under the RS assumption we have, by a similar calculation

$$\begin{aligned} \overline{M}\{\tilde{Q}\} = &(1 + F - G)^{-(n-1)/2} \\ &\times (1 + F - G - nF)^{-1/2} \\ &\times e^{nE^2/2(1+F-G-nF)} \end{aligned} \tag{103}$$

from which we eventually obtain the same free energy as (89), and the same saddle-point equations determining $\{m, q, p, E, F, G\}$ as (90). The correlation d and the bit-error rate P_b are evaluated from the saddle-point solution in the same way as the case of the MPM detector, using (45) and (46), respectively. This also means that the signal-to-interference ratio SIR in this case is given by E^2/F, like in the case of the MPM detector. The AT line turns out to be

$$1 - \beta m^2 = 0. \tag{104}$$

The RS saddle-point solution is stable against RSB if the left-hand side of (104) is positive. Due to the continuous nature of the configuration space, the freezing point is not defined for the linear multiuser detector.

Letting $\sigma = \sigma_0$ yields the result for the linear MMSE detector. From the saddle-point equations (90), $m = q$ and $F = E$ hold for the linear MMSE detector. It should be noted that these are *not* the consequence of the $(n+1)$-replica argument. In the case of the linear MMSE detector, the 0th replica and each of n replicas are not equivalent because the Gaussian prior assumed by the latter is different from the binary one of the former. The values of the macroscopic parameters are to be determined from (93), from which the bit-error rate is evaluated via (46). This result is the same as the one derived by applying a general result by Tse and Hanly [5] for the case in which power distribution approaches a given limiting distribution in the large-system limit, to the equal-power case. The replica approach can also be applied to the unequal-power case, in which the general result of Tse and Hanly [5] is reproduced for the linear MMSE detector.

Taking the limit $\sigma \to 0$, we obtain the result for the decorrelating detector. For $\beta < 1$, we have $m = 1$, E, $F \to +\infty$, and

$$\mathsf{SIR} = \frac{1-\beta}{\sigma_0^2}. \tag{105}$$

On the other hand, for $\beta \ge 1$, we have $m = \beta^{-1}$, $E = (\beta - 1)^{-1}$, and

$$\mathsf{SIR} = 0. \tag{106}$$

This is again in agreement with the literature [8], [5].

V. Results and Discussion

A. Bit-Error Rate

Fig. 1 shows how the bit-error rate P_b of the JO and IO multiuser detectors, as evaluated from the RS saddle-point solution, depends on the ratio E_b/N_0, i.e., the energy per bit E_b divided by noise spectral density N_0. Since we consider uncoded systems here, $E_b/N_0 = 1/2\sigma_0^2$ holds. When the number of users is relatively small, both the JO and the IO multiuser detectors have almost the same performance as in the single-user case, as shown in Fig. 1(a).

An interesting property observed in these results is that the bit-error rate P_b shows anomalous, nonmonotonic dependence on the ratio E_b/N_0, as β becomes larger ($\beta > 1.49$ for IO and $\beta > 1.08$ for JO). The S-shaped performance curves in Fig. 1(c) and (d) mean that under some conditions more than one solution coexists: one with the bit-error rate almost as small as in the single-user case, which we call the *good* solution, and another with larger bit-error rate, which we call the *bad* solution (the third solution on the intermediate branch is physically unstable and therefore irrelevant). The coexistence of more than one solution is essentially the same as the coexistence of *phases* in physical systems (such as water and ice at 0 °C), and such a phenomenon is called phase coexistence in statistical mechanics. Curves in the parameter space which mark the boundary between the regions with and without such coexistence are called *spinodal lines*. Fig. 2 shows the spinodal lines (solid curves) for the JO and IO multiuser detectors. The upper and lower branches represent the bifurcation points at which the good and bad solutions disappear, respectively. It can be seen that the bad solution disappears at a finite E_b/N_0 for $1.49 < \beta < 2.09$ for IO and $1.08 < \beta < 1.51$ for JO.

As discussed at the end of Section III-A, one may argue that the true procedure of evaluating the free energy (see (40)), in the information-theoretic sense, should be such that one picks up the globally stable state, i.e., the saddle-point solution giving the global extremization of f^{RS}. In the region of the phase coexistence, the globally stable state may be given by either the good or the bad solution, depending on their free energy values, and thus a boundary is defined at which the globally stable state switches between these solutions. In statistical mechanics, this kind of switching is called a thermodynamic transition, and the

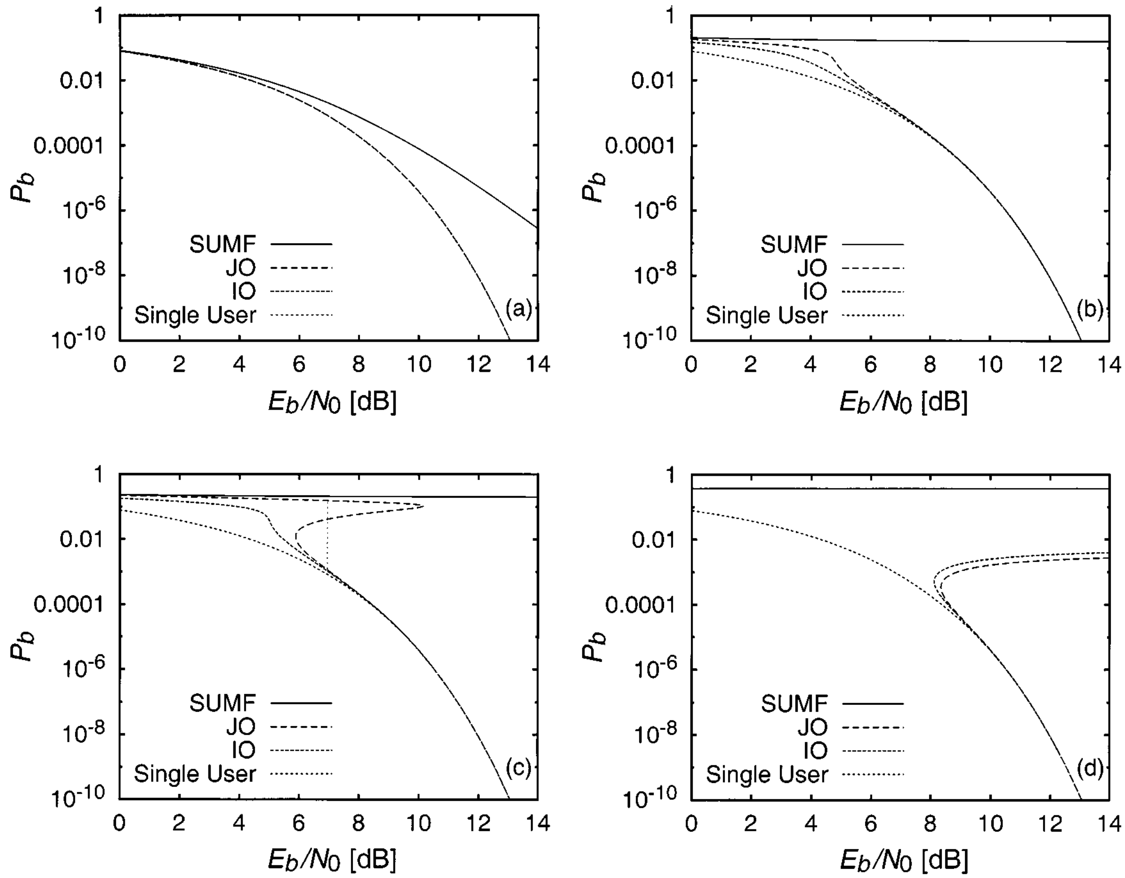

Fig. 1. Bit-error rate of single-user matched filter (SUMF), JO multiuser detector (JO), and IO multiuser detector (IO). Bit-error rate for the single-user case is also shown for comparison. (a) $\beta = 0.02$, (b) $\beta = 1$, (c) $\beta = 1.4$, and (d) $\beta = 10$. The vertical dotted line in (c) shows the thermodynamic transition for JO multiuser detector.

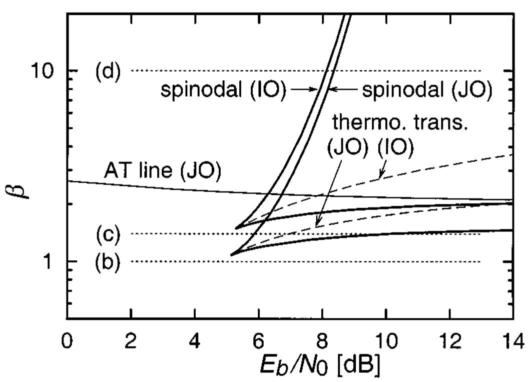

Fig. 2. Spinodal lines (solid) and thermodynamic transition lines (dashed) for JO and IO multiuser detectors. Dotted lines show the parameter values for which bit-error rate is shown in Fig. 1.

boundary in the parameter space signaling the thermodynamic transition is called the thermodynamic transition line. Fig. 2 also shows the thermodynamic transition lines (dashed curves) for the JO and IO multiuser detectors. The bad solution is the globally stable state at the upper-left side of the thermodynamic transition lines in Fig. 2, and it becomes a metastable state at the other side of the lines, where the good solution is the globally stable state. One important consequence of the thermodynamic transition is that the bit-error rate becomes discontinuous at the thermodynamic transition point. Shown in Fig. 1(c) by a vertical dotted line is the thermodynamic transition for the JO multiuser detector, at which the bit-error rate changes discontinuously. In Fig. 1(d), the thermodynamic transition occurs where E_b/N_0 is much larger than the range of the figure, hence the good solution is only metastable over the range of E_b/N_0 values shown in the figure.

We now discuss the significance of the phase coexistence and the thermodynamic transition. Most decision-driven multiuser detectors implementing suboptimal multiuser detectors can be regarded as searching for the best possible solution based on locally available information about the posterior distribution $p(\boldsymbol{x}|\boldsymbol{r}, S)$. When the phase coexistence occurs, such detectors may get trapped in the bad solution, despite the fact that the good solution exists. Moreover, we have to assume that these detectors almost certainly get trapped in the bad solution, and accordingly, will return the corresponding bad detection result. An intuitive explanation is as follows. Initialization of a multiuser detector can be done either with a random configuration or with the output of the single-user matched filters, but in any case, the initial state is as bad as the bad solution of the multiuser detectors, as can be seen in Fig. 1(c) and (d). The good solution is therefore distant from the initial state compared with the bad one, so that any algorithm based on locally available information should traverse many more subshells with bad quality (i.e., with extremely small values of the posterior $p(\boldsymbol{x}|\boldsymbol{r}, S)$) in order to arrive at the good solution, which is computationally infeasible in practice. It should be noted that this is a direct consequence of the system's loss of ergodicity, which will be discussed in more detail in Section V-B, and that this is *not* the property of any particular detection algorithm, but the property of the multiuser detection problem itself.

We can also predict that, if the phase coexistence occurs, the waterfalling phenomenon will be observed in the vicinity of the bifurcation point of the bad solution, the waterfalling phenomenon will be observed in experimentally obtained performance curves of detectors based on locally available information (in a fashion similar to turbo decoding [46], [47]). When β becomes larger than 2.09 for IO and 1.51 for JO, the bad solution persists for arbitrarily large values of E_b/N_0. Under such conditions, one cannot find the good solution, even if it exists and is globally stable so that it is the true solution in the information-theoretic sense, by any practical detection algorithms (i.e., detectors based on locally available information). This will limit the practical efficiency of the IO and JO multiuser detectors, although heuristics such as annealing [48] may help to escape the bad solution to a certain degree.

Another prediction, although of a completely theoretical nature and of no practical significance, is the following. Consider again a decision-driven multiuser detection algorithm based on locally available information. Let us assume that the algorithm *knew* the true information vector. Then one can initialize the algorithm with the true information vector, and have it run. Because the initial state of the algorithm is the true detection result, P_b is initially zero. The bit-error rate P_b then gradually increases as the algorithm proceeds, until convergence is achieved. Our prediction, based on the same argument as that which has been shown earlier, is that the equilibrium value of P_b is likely to be close to the good solution, even if it is not globally stable but only metastable. (In this case, the performance of the detector may exceed Shannon's limit, but this does not contradict the Shannon theory, because we now assume that the detector knows the true information vector.) If one decreases the SNR, the equilibrium value will change abruptly toward the bad solution, at the spinodal point where the good solution disappears. This phenomenon will show the significance of the phase coexistence and the spinodal point clearer.

To summarize the discussion so far, our statements about the relevance of the good solution are as follows.

- The good solution is relevant in the information-theoretic sense only for those values of E_b/N_0 above the thermodynamic transition.
- The good solution is relevant in the computational sense only for those values of E_b/N_0 above the spinodal point at which the bad solution disappears.

Here, the relevance in the computational sense is the relevance assuming any detection algorithm based on locally available information. For example, Fig. 1(d) shows the existence of the good solutions for the IO and JO multiuser detectors, but since they are both below the thermodynamic transition, they are not relevant either theoretically or computationally. On the other hand, the good solution for the JO multiuser detector found in Fig. 1(c) at 7 dB $< E_b/N_0 <$ 10 is relevant only theoretically but not from the computational viewpoint. It should also be noted that the phase coexistence does not occur for $\beta < 1$ for the cases investigated in this paper, therefore, it has no practical relevance, unless one considers an overloaded system (a system with $\beta > 1$). However, at present we can only say that this observation is valid for the cases investigated. Whether the phase coexistence is relevant for systems with more practical settings including, for example, systems with unequal-power users, detectors with finite $\sigma^2 \neq \sigma_0^2$, and so on, is an open problem.

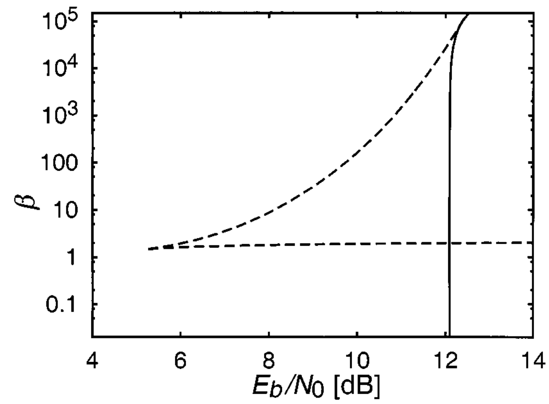

Fig. 3. Freezing line (solid curve) for IO multiuser detector. Spinodal line for IO multiuser detector (cf. Fig. 2) is also shown (dashed curve).

Fig. 2 also shows the AT line for the JO multiuser detector. The bad solution for the parameter values above the AT line is stable against RSB. The good solution was found to be AT unstable. This means that the good solution of the JO multiuser detector, as predicted by the replica analysis, may be approximately true but not exact. It also means that the free-energy landscape is rather rough around the good solution [15], suggesting that any practical local-search-based algorithms implementing the JO multiuser detector will converge very slowly, hence limiting their practical efficiency. As we have shown in Section III-E, the stable solutions of the IO multiuser detector are also stable against RSB, so that the IO multiuser detector is free from such a difficulty.

We also checked the freezing condition $\Psi = 0$ for the IO multiuser detector, which defines the freezing line in the E_b/N_0–β parameter space. For β not too large, the freezing line lies at $E_b/N_0 = 12.09$ dB, as shown in Fig. 3. The system freezes at the larger E_b/N_0 side of the freezing line. One can see from Fig. 1 that the frozen region $E_b/N_0 >$ 12.09 dB approximately corresponds to a bit-error rate of $P_b < 10^{-8}$. The significance of freezing is that results of numerical experiments will fluctuate in the frozen region, no matter how large we set the system size, due to the discreteness of the configuration space $\{-1, 1\}^K$. The freezing line moves toward the larger E_b/N_0 direction when $\beta > 10^4$. This is caused by the spinodal line approaching the freezing line, as can be seen in Fig. 3. Since $\beta > 10^4$ is too large in practice, we can safely assume that the freezing line lies at $E_b/N_0 = 12.09$ dB for any practical values of β.

B. Multiuser Efficiency

The *effective energy* e is defined as the energy per bit required to achieve a bit-error rate equal to P_b in a single-user Gaussian

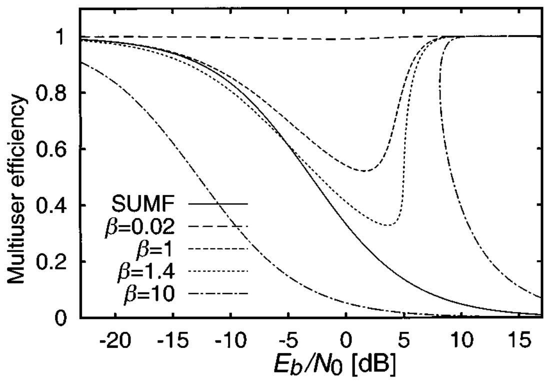

Fig. 4. Multiuser efficiency for IO multiuser detector.

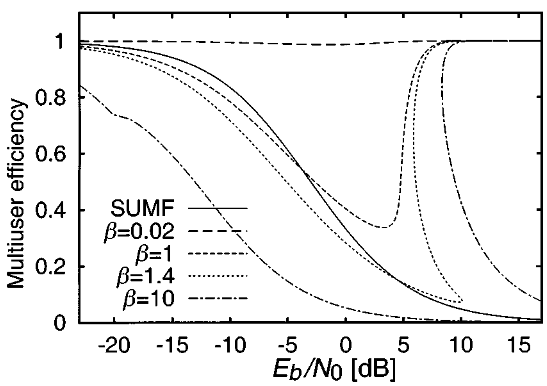

Fig. 5. Multiuser efficiency for JO multiuser detector.

channel with the same spreading factor N and noise level σ_0^2 [8]. Specifically,

$$P_b = Q\left(\frac{\sqrt{e}}{\sigma_0}\right). \tag{107}$$

For the MPM detector, from (46) we have that

$$e = \frac{\sigma_0^2 E^2}{F} = \frac{1}{1+\beta(1-2m+q)/\sigma_0^2}. \tag{108}$$

Since we have assumed that the signal from each user has a unit amplitude, the *multiuser efficiency* [8] is equal to the effective energy e. The multiuser efficiency for the single-user matched filter is given by $e^{(\mathrm{SUMF})} = (1+\beta/\sigma_0^2)^{-1}$.

Figs. 4 and 5 show the multiuser efficiency for the IO and JO multiuser detectors versus E_b/N_0, respectively. The multiuser efficiency for the single-user matched filter for $\beta = 1$ (SUMF) is also shown for comparison. For both of the IO and JO multiuser detectors, the multiuser efficiency is almost 1 over the whole range of SNR E_b/N_0 when β is small enough. As β becomes larger, the multiuser efficiency gets smaller in the lower SNR region. As the phase coexistence occurs, the curve intrudes into higher signal-to-noise region. The multiuser efficiency of the good solution remains almost equal to 1, whereas that of the bad solution decreases toward 0.

C. Remark on the Asymptotic Multiuser Efficiency

Tse and Verdú [7] have studied the asymptotic behavior of the multiuser efficiency of the optimum multiuser detector. They have discussed the asymptotic multiuser efficiency by taking the zero-noise limit $\sigma_0 \to 0$ first, and then the large-system limit $K \to \infty$. They have reported that the asymptotic multiuser efficiency converges to 1 almost surely. They have questioned as to whether these two limits commute. Our answer to this question is rather complicated. Based on the analogy with statistical mechanics, we can say that the problem is essentially the same as that of ergodicity breaking, which we may encounter by taking the thermodynamic limit of a physical model system. To be more precise, the zero-noise limit and the large-system limit can be compared to the zero-temperature and thermodynamic limits, respectively, and the above-mentioned problem can be regarded as the question as to whether these two limits commute in physical model systems. The answer to the latter question is, in general, negative. One simple and well-known example is that of a ferromagnet. The equilibrium distribution of microscopic configurations is ergodic at finite temperature when the system size is finite, so that the spontaneous magnetization vanishes when the system is in thermal equilibrium. However, as we take the thermodynamic limit, the thermal equilibrium distribution becomes nonergodic at low temperature (i.e., below the *Curie temperature*), and we will observe a spontaneous magnetization since the microscopic configuration will get trapped in one ergodic component. This spontaneous magnetization persists in the zero-temperature limit. On the other hand, if we first take the temperature of a finite-size system to zero, we will not observe any spontaneous magnetization even in the zero-temperature limit, because the system remains ergodic as long as the temperature is positive, even if it is small. The spontaneous magnetization will remain zero if we take the thermodynamic limit thereafter.

The multiuser detection problem shares essentially the same property as the ferromagnet. It should be noted that taking the limit $K \to \infty$ first, and $\sigma_0 \to 0$ afterwards, corresponds to considering the zero-noise limit properties of our result. When the phase coexistence occurs, the system as a whole becomes nonergodic in the large-system limit, and each solution corresponds to one ergodic component. The nonergodicity persists even if we consider the zero-noise limit, provided that the phase coexistence is maintained. Hence, although the multiuser efficiency of the good solution approaches 1 in the zero-noise limit, the multiuser efficiency of the bad solution approaches 0, as can be observed in Figs. 4 and 5. For the IO multiuser detector, we observe numerically that, in the zero-noise limit, the good solution for finite β is the globally stable state and is therefore relevant in the information-theoretic sense. This means that the result by Tse and Verdú still holds for the IO multiuser detector even when the order of the two limits is exchanged, although the efficient communication predicted by the solution is computationally infeasible if the bad solution coexists. As for the JO multiuser detector within the RS assumption, we can draw the same conclusion as in the case of the IO multiuser detector, but one may have to take RSB into account for more definite statements. The complication in our answer to the question posed by Tse and Verdú, compared with their result, is a consequence of the ergodicity breaking, which arises in turn from the exchange of the order of taking the two limits.

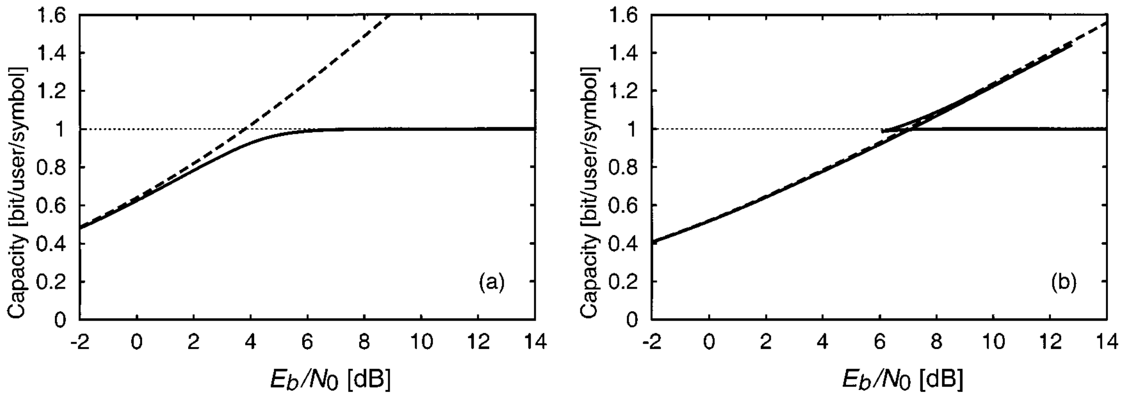

Fig. 6. Information-theoretic capacity of BIAWGN CDMA channel (solid) and AWGN CDMA channel (dashed). (a) $\beta = 1$ and (b) $\beta = 2$.

D. Capacity

Fig. 6 shows the information-theoretic capacity of the BIAWGN CDMA channel and the AWGN CDMA channel. When E_b/N_0 is small, the channel capacity is limited mainly by the channel noise, so that the capacity is almost the same, irrespective of whether the source is binary or Gaussian. Because the capacity for the BIAWGN CDMA case should not exceed 1, it saturates as E_b/N_0 becomes larger. As an overall tendency, the capacity becomes smaller as β increases. For the BIAWGN CDMA case, phase coexistence occurs when $\beta > 1.49$. Correspondingly, more than one value is obtained for the capacity (see Fig. 6(b)). We should take the lowest branch as the true capacity. Since we are evaluating the differential entropy $h(Y)$ using (80) via the application of Varadhan's theorem, the contribution from each of the metastable states to the integral in (80) vanishes in the large-system limit, compared to the contribution from the globally stable state. Ignoring the contribution from metastable states corresponds to taking the lowest branch as the true information-theoretic capacity. As a result, when β is large, one observes that the capacity for the BIAWGN CDMA case is almost the same as the capacity for the AWGN CDMA case as long as the latter is less than 1. On the other hand, when the latter exceeds 1, the former saturates abruptly to remain less than 1.

E. On the ESD

Existing approaches to large-system analysis of randomly spread models generally rely on the evaluation of the ESD of large random matrices [41], [49]. Let us consider the general linear multiuser detector under the equal-power condition. The posterior distribution is

$$p^{(l)}(\boldsymbol{x}|\boldsymbol{r}, S) \propto \exp\left[-\frac{1}{2}\boldsymbol{x}^T\left(I + \frac{1}{\sigma^2}R\right)\boldsymbol{x} + \frac{1}{\sigma^2}\boldsymbol{y}^T\boldsymbol{x}\right] \quad (109)$$

where $R \equiv N^{-1}S^TS$ is the cross-correlation matrix of the spreading sequences, and where $\boldsymbol{y} \equiv N^{-1/2}S^T\boldsymbol{r}$ is the vector of the matched-filter outputs. Since the posterior distribution is jointly Gaussian, the mean of $\boldsymbol{x}$ coincides with the maximum *a posteriori* (MAP) estimate, and is given by a linear transform of the matched-filter output, as $\hat{\boldsymbol{x}} = [R + \sigma^2 I]^{-1}\boldsymbol{y}$. Because of the linear structure of the detection problem, eigenspace decomposition and evaluation of ESD of the cross-correlation matrix R provides an efficient tool for large-system analysis of the linear multiuser detector.

The detection problem for the MPM detector, however, does not possess such a linear structure due to the discreteness of the domain of $\boldsymbol{x}$, which follows from the discreteness of the prior distribution. The discreteness of the domain of $\boldsymbol{x}$ seems to prevent us from directly applying ESD results to the analysis of the MPM detector. Our analysis, as well as that of Tse and Verdú [7], successfully takes into account the discrete nature of the problem by invoking arguments based on the large-deviation theory. In our analysis, the discrete nature of $\boldsymbol{x}$ is explicitly dealt with via the rate function $\mathcal{I}\{Q\}$.

VI. Conclusion

We have studied the large-system properties of the MPM detector by means of the replica method. Based on the RS assumption we have obtained the analytical formulas that allow the evaluation of the bit-error rate for arbitrary SNR values. We have also derived, within the same replica formalism, the capacity of the randomly spread CDMA channel and the performance of the decorrelating and linear MMSE multiuser detectors, all of which have successfully reproduced the reported results in the literature, confirming the validity of the replica approach.

We have examined the bit-error rate properties of the IO and JO multiuser detectors by numerically evaluating the analytical formulas. We have found that there may be the phenomenon of phase coexistence, i.e., the coexistence of good and bad solutions, which will cause the waterfall phenomenon in the performance curve of a decision-driven multiuser detector under certain conditions, just as in turbo decoding.

The whole presentation in this paper relies on the replica method. Discussing the validity of the replica approach in the rigorous mathematical sense is beyond the scope of this paper. However, we believe that successful application of the replica method to various problems, including the one presented here, should not be regarded as incidental. Researchers in the fields of probability theory and mathematical physics has begun to work toward mathematical justification of the replica theory: For details, see [50] and references therein.

There are various interesting directions for future work. One of them is the implementation aspect of the MPM detectors, such as their computational complexity [51], which we did not address in this paper. Although the NP-hardness proved by Verdú [51] seems unavoidable, we expect that the mean-field approximation [52], a notion in statistical mechanics to systematically approximate microscopic behavior of systems, can provide practical means of implementing the MPM detectors approximately.

APPENDIX I
REPLICA METHOD

In this appendix, we provide a brief introduction of the replica method, as well as the outline of the calculation performed in a typical replica analysis.

Let us consider the abstract problem of Bayes inference to evaluate a posterior average

$$a(\boldsymbol{y},\, \boldsymbol{s}) \equiv \langle a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})\rangle = \sum_{\boldsymbol{x}} a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s}) p(\boldsymbol{x}|\boldsymbol{y},\, \boldsymbol{s}) \tag{110}$$

where $\boldsymbol{x}$ is a random vector representing configurations of the underlying probability model, $\boldsymbol{y}$ is another random vector representing observables, $\boldsymbol{s}$ is a set of parameters, $a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})$ is a function of $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{s}$, and $p(\boldsymbol{x}|\boldsymbol{y},\, \boldsymbol{s})$ is an assumed posterior distribution of $\boldsymbol{x}$ conditioned on the values of the observables $\boldsymbol{y}$ and the parameters $\boldsymbol{s}$. The posterior distribution is to be derived from Bayes theorem, with an assumed prior distribution $p(\boldsymbol{x})$ of $\boldsymbol{x}$, and an assumed conditional distribution $p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})$ of $\boldsymbol{y}$ on $\boldsymbol{x}$, parametrized by $\boldsymbol{s}$, as

$$p(\boldsymbol{x}|\boldsymbol{y},\, \boldsymbol{s}) = \frac{p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})}{\sum_{\boldsymbol{x}} p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})}. \tag{111}$$

The posterior average $a(\boldsymbol{y},\, \boldsymbol{s})$ depends on the observables $\boldsymbol{y}$ and, quite often, they are also random variables. In such cases, the quantity of interest is the average of $a(\boldsymbol{y},\, \boldsymbol{s})$ over all possible observed values, that is,

$$E_{\boldsymbol{y}}[a(\boldsymbol{y},\, \boldsymbol{s})] \tag{112}$$

where $E_{\boldsymbol{y}}[\cdot]$ denotes expectation with respect to the true distribution of $\boldsymbol{y}$, which may or may not be equal to the assumed one.

We now consider the case in which the parameters $\boldsymbol{s}$ are also random, and are assumed to be independent of $\boldsymbol{x}$. This is actually the case for the CDMA multiuser detection problem under the random spreading assumption. Let $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{s}$ be the information bit vector, the received signals, and the spreading sequences of all users, respectively. For every $\boldsymbol{s}$, one can in principle calculate the average bit-error rate. One still has to average the result over the randomness of the spreading sequences to obtain the desired result. In general, we want to evaluate quantities like

$$E_{\boldsymbol{y},\, \boldsymbol{s}}[a(\boldsymbol{y},\, \boldsymbol{s})]. \tag{113}$$

In statistical-mechanics literature, the average over $\boldsymbol{y}$ and $\boldsymbol{s}$ is called the *quenched average*. When one first takes the average with respect to the posterior distribution, one has to quench the values of $\boldsymbol{y}$ and $\boldsymbol{s}$. The result is then averaged over $\boldsymbol{y}$ and $\boldsymbol{s}$. Very often, one encounters difficulties in the evaluation of the quenched average. This becomes evident by rewriting the quenched average as

$$\begin{aligned} E_{\boldsymbol{y},\, \boldsymbol{s}}[a(\boldsymbol{y},\, \boldsymbol{s})] &= E_{\boldsymbol{y},\, \boldsymbol{s}}\left[\sum_{\boldsymbol{x}} a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})p(\boldsymbol{x}|\boldsymbol{y},\, \boldsymbol{s})\right] \\ &= E_{\boldsymbol{y},\, \boldsymbol{s}}\left[\frac{\sum_{\boldsymbol{x}} a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})}{\sum_{\boldsymbol{x}} p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})}\right]. \end{aligned} \tag{114}$$

One now has to take the expectation of a ratio of random variables $\sum_{\boldsymbol{x}} a(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{s})p(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{s})p(\boldsymbol{x})$ and $\sum_{\boldsymbol{x}} p(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{s})p(\boldsymbol{x})$, which is in general difficult. A related quantity is the *annealed average*, or the annealed approximation to the quenched average, which is given by taking the expectation for the denominator and the numerator separately, that is,

$$\frac{E_{\boldsymbol{y},\, \boldsymbol{s}}\left[\sum_{\boldsymbol{x}} a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})\right]}{E_{\boldsymbol{y},\, \boldsymbol{s}}\left[\sum_{\boldsymbol{x}} p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})\right]}. \tag{115}$$

The calculation of the annealed average is usually much simpler than that of the quenched average, so that the annealed average is often used as an approximation to the quenched average, but the final results are in general different from each other.

Let us define the moment generating function of $a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})$, or the partition function, of the (unnormalized) measure $p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})$ of $\boldsymbol{x}$, given $\boldsymbol{y}$ and $\boldsymbol{s}$, as

$$Z(h; \boldsymbol{y},\, \boldsymbol{s}) = \sum_{\boldsymbol{x}} e^{h\cdot a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})} p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x}). \tag{116}$$

(It is not necessary to include the factor $e^{h\cdot a(\boldsymbol{x},\, \boldsymbol{y},\, \boldsymbol{s})}$ explicitly if $p(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{s})p(\boldsymbol{x})$ already contains such a factor. This is usually the case in statistical mechanics because, for example, the Gibbs factor $e^{-\beta E}$ with inverse temperature β and energy functional E is usually included in $p(\boldsymbol{y}|\boldsymbol{x},\, \boldsymbol{s})p(\boldsymbol{x})$, which makes the partition function, even without the factor, the moment generating function of the energy.) If we could evaluate the average

$$E_{\boldsymbol{y},\, \boldsymbol{s}}\left[\log Z(h; \boldsymbol{y},\, \boldsymbol{s})\right] \tag{117}$$

we would obtain the desired quenched average (113) by

$$E_{\boldsymbol{y},\, \boldsymbol{s}}[a(\boldsymbol{y},\, \boldsymbol{s})] = \left.\frac{\partial}{\partial h} E_{\boldsymbol{y},\, \boldsymbol{s}}[\log Z(h; \boldsymbol{y},\, \boldsymbol{s})]\right|_{h\to 0} \tag{118}$$

by exchanging the order of the expectation and the differentiation by h. Of course, this simple manipulation does not help resolve the difficulty we are faced with. The difficulty we encounter here is that the evaluation of the average (117) is often hard. Now we have to average the *logarithm* of a sum of random variables, which prevents us in most cases from evaluating it analytically. Also, it is usually computationally hard. The summation may be over a very large number of terms in large-sized problems. Again, it is generally far easier to evaluate the average instead

$$E_{\boldsymbol{y},\, \boldsymbol{s}}[Z(h; \boldsymbol{y},\, \boldsymbol{s})] \tag{119}$$

but the calculation

$$\left.\frac{\partial}{\partial h} \log E_{\boldsymbol{y},\, \boldsymbol{s}}[Z(h; \boldsymbol{y},\, \boldsymbol{s})]\right|_{h\to 0} \tag{120}$$

only yields the annealed average (115), which is, in general, the wrong answer.

The replica method is a way to evaluate (117). It makes use of the identity

$$E_{\boldsymbol{y},\boldsymbol{s}}[\log Z(h;\boldsymbol{y},\boldsymbol{s})] = \lim_{n\to 0} \frac{\partial}{\partial n} \log E_{\boldsymbol{y},\boldsymbol{s}}[\{Z(h;\boldsymbol{y},\boldsymbol{s})\}^n] \tag{121}$$

and replaces the evaluation of the average (117) with that of

$$E_{\boldsymbol{y},\boldsymbol{s}}\left[\{Z(h;\boldsymbol{y},\boldsymbol{s})\}^n\right]. \tag{122}$$

It should be noted that the quantity $[Z(h;\boldsymbol{y},\boldsymbol{s})]^n$ is well-defined for real n. In applying the replica method, however, one usually evaluates (122) for positive integer n only, by regarding $[Z(h;\boldsymbol{y},\boldsymbol{s})]^n$ as the partition function of the probability model consisting of n identical replicas of the original probability model, that is,

$$[Z(h;\boldsymbol{y},\boldsymbol{s})]^n = \sum_{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n} e^{h\cdot a(\boldsymbol{x}_1,\boldsymbol{y},\boldsymbol{s})} \prod_{i=1}^{n} [p(\boldsymbol{y}|\boldsymbol{x}_i,\boldsymbol{s})p(\boldsymbol{x}_i)]. \tag{123}$$

Since the replica method has been developed in statistical mechanics, it has been extensively applied to the analysis of models in the large-system (thermodynamic) limit (but see also [53], [54] for application of the replica method to finite-sized problems). In such cases, the replica method is used in conjunction with the saddle-point method, or Varadhan's theorem for asymptotics of integrals. Let K be a parameter representing the size of a problem, and let us further assume that $a(\boldsymbol{x},\boldsymbol{y},\boldsymbol{s})$ scales with K so that the actual quantity of interest is the asymptotic value of the quenched average of $K^{-1}a(\boldsymbol{x},\boldsymbol{y},\boldsymbol{s})$ as $K\to\infty$. In this case, we have to evaluate the *free energy* defined as

$$\mathcal{F} \equiv \lim_{K\to\infty} K^{-1} E_{\boldsymbol{y},\boldsymbol{s}}[\log Z(h;\boldsymbol{y},\boldsymbol{s})]. \tag{124}$$

The replica method replaces the right-hand side of (124) as

$$\mathcal{F} = \lim_{K\to\infty} K^{-1} \lim_{n\to 0} \frac{\partial}{\partial n} \log E_{\boldsymbol{y},\boldsymbol{s}}\left[\{Z(h;\boldsymbol{y},\boldsymbol{s})\}^n\right]. \tag{125}$$

The approach of combining the replica method with the saddle-point method is efficient if the following conditions are met.

- The two limits $K\to\infty$ and $n\to 0$ can be interchanged, so that the equality

$$\mathcal{F} = \lim_{n\to 0} \frac{\partial}{\partial n} \lim_{K\to\infty} K^{-1} \log E_{\boldsymbol{y},\boldsymbol{s}}\left[\{Z(h;\boldsymbol{y},\boldsymbol{s})\}^n\right] \tag{126}$$

holds.

- Dependence on $\boldsymbol{x}$ of the function

$$e^{h\cdot a(\boldsymbol{x}_1,\boldsymbol{y},\boldsymbol{s})} \prod_{i=1}^{n} p(\boldsymbol{y}|\boldsymbol{x}_i,\boldsymbol{s}) \tag{127}$$

is expressed in terms of a set of parameters $q = q\{\boldsymbol{x}_i\}$ (which may be functionals) and the average of the function over $\boldsymbol{y}$ and $\boldsymbol{s}$ can be performed analytically *for fixed* $\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n\}$, yielding a result of the form $\exp[Kg(q)]$, where $g(q)$ is a continuous function of q whose supremum is finite.

- The probability measure $\mu_K(q)$ of the parameters $q = q\{\boldsymbol{x}_i\}$, induced by the prior $\prod_{i=1}^{n} p(\boldsymbol{x}_i)$, has a large deviation property with a rate function $\mathcal{I}(q)$ as $K\to\infty$. This enables us to evaluate $K^{-1}E_{\boldsymbol{y},\boldsymbol{s}}[\{Z(h;\boldsymbol{y},\boldsymbol{s})\}^n]$ asymptotically using Varadhan's theorem, as

$$\begin{aligned}
&K^{-1}\log E_{\boldsymbol{y},\boldsymbol{s}}\left[\{Z(h;\boldsymbol{y},\boldsymbol{s})\}^n\right] \\
&\quad= K^{-1}\log E_{\boldsymbol{y},\boldsymbol{s}}\left[\sum_{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n} e^{h\cdot a(\boldsymbol{x}_1,\boldsymbol{y},\boldsymbol{s})} \prod_{i=1}^{n}\{p(\boldsymbol{y}|\boldsymbol{x}_i,\boldsymbol{s})p(\boldsymbol{x}_i)\}\right] \\
&\quad= K^{-1}\log \int E_{\boldsymbol{y},\boldsymbol{s}|q}\left[e^{h\cdot a(\boldsymbol{x}_1,\boldsymbol{y},\boldsymbol{s})} \prod_{i=1}^{n} p(\boldsymbol{y}|\boldsymbol{x}_i,\boldsymbol{s})\right]\mu_K(q)\,dq \\
&\quad= K^{-1}\log \int e^{Kg(q)}\mu_K(q)\,dq \\
&\quad\to \sup_q\,[g(q)-\mathcal{I}(q)], \qquad K\to\infty.
\end{aligned} \tag{128}$$

We have applied Varadhan's theorem to derive the final expression in (128).

Now we assume that $\boldsymbol{x}$ has K components, and that $p(\boldsymbol{x})$ implies that the components x_k of $\boldsymbol{x}$ are i.i.d. We furthermore assume that q consists of empirical means of K i.i.d. random variables, each of which depends on $\{x_{ik}|i=1,\ldots,n\}$. Then, we can apply Cramér's theorem to the measure $\mu_K(q)$ to prove its large deviation property, and it turns out that the rate function $\mathcal{I}(q)$ is given in terms of the Fenchel–Legendre transform as

$$\mathcal{I}(q) = \sup_{\tilde{q}}\,[\tilde{q}\cdot q - \phi(\tilde{q})] \tag{129}$$

where

$$\phi(\tilde{q}) \equiv \log \sum_{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n} e^{\tilde{q}\cdot q\{\boldsymbol{x}_i\}} \prod_{i=1}^{n} p(\boldsymbol{x}_i). \tag{130}$$

is the cumulant generating function of $q\{\boldsymbol{x}_i\}$ with respect to the prior distribution of $\{\boldsymbol{x}_i\}$. Collecting the results of (128) and (129), one obtains

$$\lim_{K\to\infty} K^{-1}\log E_{\boldsymbol{y},\boldsymbol{s}}\left[\{Z(h;\boldsymbol{y},\boldsymbol{s})\}^n\right] = \sup_q \inf_{\tilde{q}}\,[g(q) - \tilde{q}\cdot q + \phi(\tilde{q})] \tag{131}$$

where the extremization condition is given by the following saddle-point equations:

$$q = \frac{\partial\phi(\tilde{q})}{\partial\tilde{q}}, \qquad \tilde{q} = \frac{\partial g(q)}{\partial q}. \tag{132}$$

Taking derivative with respect to n and taking the limit $n\to 0$, we obtain the free energy $\mathcal{F}$.

It should be noted that, as mentioned, the true distribution $p_0(\boldsymbol{y},\boldsymbol{s})$ of $\boldsymbol{y}$ and $\boldsymbol{s}$, by which the expectation $E_{\boldsymbol{y},\boldsymbol{s}}[\cdot]$ is taken, may, in general, be different from the assumed marginal $\sum_{\boldsymbol{x}} p(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s})p(\boldsymbol{x})p(\boldsymbol{s})$. However, if $p_0(\boldsymbol{y},\boldsymbol{s})$ has a form similar to the assumed marginal, one can exploit the $(n+1)$-replica formulation, as has been done in Section III.

APPENDIX II
JOINT DISTRIBUTION OF $v_0, v_1, \ldots, v_n$

We have assumed, as far as the calculation of $\mathcal{G}\{Q\}$ is concerned, that the joint distribution of $\boldsymbol{v} \equiv (v_0, v_1, \ldots, v_n)^T$, with

$$v_0 = \frac{1}{\sqrt{K}}\,\boldsymbol{s}\cdot\boldsymbol{x}_0, \quad v_a = \frac{1}{\sqrt{K}}\,\boldsymbol{s}\cdot\boldsymbol{x}_a, \qquad a=1,\ldots,n \tag{133}$$

can be regarded, in the $K \to \infty$ limit, as the joint Gaussian distribution $N(\mathbf{0}, Q)$, where $Q \equiv (Q_{ab})$, $Q_{ab} = K^{-1}\boldsymbol{x}_a \cdot \boldsymbol{x}_b$, for *fixed* $\{\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ and where each entry of $\boldsymbol{s}$ is an i.i.d. random variable with zero mean, unit variance, and vanishing odd-order moments. To prove this, we note that the second- and fourth-order cumulants of $\boldsymbol{v}$ are given by

$$\kappa^{a,b} = Q_{ab} = K^{-1}\boldsymbol{x}_a \cdot \boldsymbol{x}_b \tag{134}$$

$$\kappa^{a,b,c,d} = \kappa_4 K^{-2} \sum_{k=1}^{K} x_{ak}x_{bk}x_{ck}x_{dk} \tag{135}$$

where κ_4 is the fourth-order cumulant of each entry of $\boldsymbol{s}$. All the odd-order cumulants vanish. Then, from the Edgeworth expansion [55] we have for the probability density $\mathcal{W}(\boldsymbol{v})$ of $\boldsymbol{v}$

$$\mathcal{W}(\boldsymbol{v}) = f_0(\boldsymbol{v}; Q) + \frac{1}{K}\Delta(\boldsymbol{v}; Q, w) + \mathcal{O}(K^{-2}) \tag{136}$$

$$\Delta(\boldsymbol{v}; Q, w) \equiv \frac{\kappa_4}{24} \sum_{a,b,c,d} w_{abcd} \frac{\partial^4 f_0(\boldsymbol{v})}{\partial v_a \partial v_b \partial v_c \partial v_d} \tag{137}$$

$$f_0(\boldsymbol{v}; Q) \equiv \frac{1}{\sqrt{(2\pi)^{n+1}\det Q}}\, e^{-(1/2)\boldsymbol{v}\cdot(Q^{-1})\boldsymbol{v}} \tag{138}$$

where

$$w_{abcd} \equiv K^{-1}\sum_{k=1}^{K} x_{ak}x_{bk}x_{ck}x_{dk} = \mathcal{O}(1).$$

It then follows that the average over $\boldsymbol{v}$ can be replaced by the average over the joint Gaussian random variables $\boldsymbol{v} \sim N(\mathbf{0}, Q)$ in the large-system limit

$$\begin{aligned}\int_{\mathbb{R}^{n+1}} [\cdots]\, \mathcal{W}(\boldsymbol{v})\, d\boldsymbol{v} &= \int_{\mathbb{R}^{n+1}} [\cdots]\, f_0(\boldsymbol{v}; Q)\, d\boldsymbol{v} \\ &\quad + \frac{1}{K}\int_{\mathbb{R}^{n+1}} [\cdots]\, \Delta(\boldsymbol{v}; Q, w)\, d\boldsymbol{v} + \mathcal{O}(K^{-2}) \\ &\approx \int_{\mathbb{R}^{n+1}} [\cdots]\, f_0(\boldsymbol{v}; Q)\, d\boldsymbol{v}, \qquad K \to \infty. \end{aligned} \tag{139}$$

APPENDIX III
DERIVATION OF AT LINE

We show the derivation of the equation for the AT line (Proposition 3; (67)), which marks the boundary between one region in the parameter space where the RS saddle-point solution is stable against RSB perturbations, and another where the RS solution is unstable against RSB. We have to evaluate the Hessian of the exponent of the integrand of the integral to which the saddle-point method is applied, with respect to the macroscopic parameters $\{Q_{ab}, \tilde{Q}_{ab}\}$ at the RS saddle-point solution, and then to derive the stability condition under which the application of the saddle-point method is justified.

Let

$$f \equiv f(\{Q\}, \{\tilde{Q}\}) = \log M\{\tilde{Q}\} - \sum_{a<b} \tilde{Q}_{ab}Q_{ab} + \beta^{-1}\mathcal{G}_1\{Q\}. \tag{140}$$

In the asymptotic evaluation of Ξ_n in the large-system limit $K \to \infty$, we have performed the extremization of f twice: first, with respect to $\{\tilde{Q}\}$, and next, with respect to $\{Q\}$, that is,

$$\lim_{K\to\infty} K^{-1}\Xi_n = \sup_{\{Q\}} \inf_{\{\tilde{Q}\}} f. \tag{141}$$

In order for a saddle-point solution to be valid, it has to satisfy the following conditions, which we refer to as the stability condition.

- f should be minimum with respect to $\{\tilde{Q}\}$ at the saddle-point solution. We call this condition type 1 stability.
- f should be maximum with respect to $\{Q\}$ at the saddle-point solution, when $\{\tilde{Q}\}$ is taken to be dependent on $\{Q\}$ in such a way that $\{\tilde{Q}\}$ minimizes f *for given* $\{Q\}$. We call this condition type 2 stability.

The requirement of the dependence of $\{\tilde{Q}\}$ on $\{Q\}$ in type 2 stability comes from the fact that the supremum with respect to $\{Q\}$ is to be evaluated *after* the first infimum evaluation, in which we have determined $\{\tilde{Q}\}$ as functions of $\{Q\}$, so as to minimize f. Hence, when we consider perturbations of $\{Q\}$, the variables $\{\tilde{Q}\}$ are no longer independent variables, and we have to take into account their dependence on $\{Q\}$.

To analyze the stability of the RS saddle-point solution against RSB, we first evaluate the Hessian of f at the RS saddle-point solution, and then probe the two types of stability. It should be noted that, to obtain the stability result of the RS saddle-point solution, we have to evaluate the stability conditions *in the limit* $n \to 0$, the same limit that we have used to derive the RS saddle-point solution.

We start with the evaluation of $\mathcal{G}$, but this time without the RS assumption. To do this, we perform the integral over the channel noise first

$$\begin{aligned} e^{\mathcal{G}} &= \frac{1}{\sqrt{2\pi\sigma_0^2}} \int \overline{\exp\left\{-\frac{1}{2}\left[B_0\left(\frac{r}{\sqrt{\beta}} - v_0\right)^2 + B\sum_{a=1}^{n}\left(\frac{r}{\sqrt{\beta}} - v_a\right)^2\right]\right\}}\, dr \\ &= \frac{1}{\sqrt{2\pi\sigma_0^2}} \int \overline{\exp\left\{-\frac{1}{2}\left[(B_0 + nB)\frac{r^2}{\beta} - 2\left(B_0 v_0 + B\sum_{a=1}^{n} v_a\right)\frac{r}{\sqrt{\beta}} + \left(B_0 v_0^2 + B\sum_{a=1}^{n} v_a^2\right)\right]\right\}}\, dr \\ &= \left(1 + \frac{nB}{B_0}\right)^{-1/2} \overline{\exp\left\{-\frac{1}{2}\left[B_0 v_0^2 + B\sum_{a=1}^{n} v_a^2 - \frac{1}{B_0 + nB}\left(B_0 v_0 + B\sum_{a=1}^{n} v_a\right)^2\right]\right\}} \\ &= \left(1 + \frac{nB}{B_0}\right)^{-1/2} \overline{\exp\left(-\frac{\rho}{2}\boldsymbol{v}^T \Sigma \boldsymbol{v}\right)} \end{aligned} \tag{142}$$

where $\boldsymbol{v} \equiv [v_0, v_1, \ldots, v_n]^T$, and where Σ is an $(n+1) \times (n+1)$ matrix defined by

$$\Sigma \equiv \left(\begin{array}{c|c} n & -\boldsymbol{e}^T \\ \hline -\boldsymbol{e} & \left(1 + \frac{nB}{B_0}\right)\boldsymbol{I} - \frac{B}{B_0}\boldsymbol{E} \end{array} \right) \tag{143}$$

$$\rho \equiv \frac{B}{1 + nB/B_0} \tag{144}$$

$\boldsymbol{e}$ is an n-dimensional vector $\boldsymbol{e} \equiv [1, \ldots, 1]^T$, $\boldsymbol{E} \equiv \boldsymbol{e}\boldsymbol{e}^T$, and $\boldsymbol{I}$ is the n-dimensional identity matrix.

For fixed $\{\boldsymbol{x}_a\}$, $\boldsymbol{v}$ can be regarded, in the large-system limit $K \to \infty$, as an $(n+1)$-dimensional Gaussian random variable with mean $\mathbf{0}$ and variance–covariance matrix Q, by following the argument of Appendix II. This means that the average over the spreading sequences can be replaced by the average over the Gaussian random variable $\boldsymbol{v} \sim N(\mathbf{0}, Q)$, which gives

$$\begin{aligned} &\overline{\exp\left(-\frac{\rho}{2}\boldsymbol{v}^T\Sigma\boldsymbol{v}\right)} \\ &\quad = \frac{1}{(2\pi)^{n+1/2}|Q|^{1/2}} \int \exp\left(-\frac{1}{2}\boldsymbol{v}^T R\boldsymbol{v}\right) d\boldsymbol{v} \\ &\quad = |QR|^{-1/2} = \exp\left[-\frac{1}{2}\log\det(QR)\right] \end{aligned} \tag{145}$$

where we let

$$R \equiv Q^{-1} + \rho\Sigma. \tag{146}$$

As a result, we have

$$\mathcal{G}\{Q\} = -\frac{1}{2}\log\det(QR) - \frac{1}{2}\log\left(1 + \frac{nB}{B_0}\right) \tag{147}$$

and, therefore,

$$\begin{aligned} f = &\log M\{\tilde{Q}\} - \sum_{a<b} \tilde{Q}_{ab}Q_{ab} \\ &- \frac{1}{2\beta}\log\det(QR) - \frac{1}{2\beta}\log\left(1 + \frac{nB}{B_0}\right). \end{aligned} \tag{148}$$

Before deriving the Hessian of f itself, we first work out the Hessian of the term $\log\det(QR)$. From the definition of R, it immediately follows that

$$QR = I + \rho Q\Sigma \tag{149}$$

where I is the $(n+1)$-dimensional identity matrix. Let E_{ab} denote the matrix whose (a, b)-element is 1 and all the remaining elements are 0. Let $S \equiv \Sigma(I + \rho Q\Sigma)^{-1}$. Using the identities [56]

$$\frac{\partial \log\det F}{\partial x} = \mathrm{tr}\left[F^{-1}\frac{\partial F}{\partial x}\right]$$

and

$$\frac{\partial F^{-1}}{\partial x} = -F^{-1}\frac{\partial F}{\partial x}F^{-1}$$

we have

$$\begin{aligned} \frac{\partial \log\det(QR)}{\partial Q_{ab}} &= \mathrm{tr}\left[(QR)^{-1}\frac{\partial QR}{\partial Q_{ab}}\right] \\ &= \rho\,\mathrm{tr}\left[(I + \rho Q\Sigma)^{-1}(E_{ab} + E_{ba})\Sigma\right] \\ &= \rho\,\mathrm{tr}\left[S(E_{ab} + E_{ba})\right] \end{aligned} \tag{150}$$

and

$$\begin{aligned} \frac{\partial^2 \log\det(QR)}{\partial Q_{ab}\partial Q_{cd}} &= -\rho\,\mathrm{tr}\left[\Sigma(I + \rho Q\Sigma)^{-1}\frac{\partial(I + \rho Q\Sigma)}{\partial Q_{ab}}\right. \\ &\qquad \left.\times(I + \rho Q\Sigma)^{-1}(E_{ab} + E_{ba})\right] \\ &= -\rho^2\,\mathrm{tr}\left[S(E_{ab} + E_{ba})S(E_{cd} + E_{dc})\right] \\ &= -2\rho^2(S_{ac}S_{bd} + S_{ad}S_{bc}). \end{aligned} \tag{151}$$

The evaluation of the matrix S should be done at the RS saddle-point solution, since we are now concerned with the stability of the RS saddle-point solution. The matrix S at the RS solution is given by

$$S = \beta\rho^{-1}\left(\begin{array}{c|c} nE & -E\boldsymbol{e}^T \\ \hline -E\boldsymbol{e} & (E + nF)\boldsymbol{I} - F\boldsymbol{E} \end{array} \right) \tag{152}$$

where the values of E and F are the ones that extremize (37), and are given by (38) and (39).

We next compute the Hessian of the term $\log M\{\tilde{Q}\}$. By the same argument as that in Section III-B, we have

$$\frac{\partial \log M\{\tilde{Q}\}}{\partial \tilde{Q}_{ab}} = [x_a x_b]_M \tag{153}$$

where the notation $[g\{x_a\}]_M$ for any function g of $\{x_a\}$ means

$$[g\{x_a\}]_M \equiv \frac{\sum_{\{x_a\}} 2^{-(n+1)} g\{x_a\} \exp\left(\sum_{a<b} \tilde{Q}_{ab}x_a x_b\right)}{M\{\tilde{Q}\}}. \tag{154}$$

In the same notation, we have

$$\frac{\partial^2 \log M\{\tilde{Q}\}}{\partial \tilde{Q}_{ab}\partial \tilde{Q}_{cd}} = [x_a x_b x_c x_d]_M - [x_a x_b]_M[x_c x_d]_M. \tag{155}$$

The Hessian of f is of dimension $n(n+1) \times n(n+1)$, and it has the structure

$$C = \begin{bmatrix} \{A^{ab,\,cd}\} & \{-\delta^{ab,\,cd}\} \\ \{-\delta^{ab,\,cd}\} & \{B^{ab,\,cd}\} \end{bmatrix} \tag{156}$$

with

$$\begin{aligned} A^{ab,\,cd} &= \beta^{-1}\rho^2(S_{ac}S_{bd} + S_{ad}S_{bc}) \\ B^{ab,\,cd} &= [x_a x_b x_c x_d]_M - [x_a x_b]_M[x_c x_d]_M \\ \delta^{ab,\,cd} &= \delta_{ac}\delta_{bd} + \delta_{ad}\delta_{bc}. \end{aligned} \tag{157}$$

At the RS saddle-point solution, the matrix A has seven different types of elements. They are

$$\begin{aligned} A^{0a,\,0a} &= \beta[E^2 + n(E^2 - EF) + n^2EF] \\ A^{0a,\,0b} &= \beta(E^2 - nEF) \\ A^{0a,\,ab} &= \beta(-E^2 + 2EF - nEF) \\ A^{0a,\,bc} &= 2\beta EF \\ A^{ab,\,ab} &= \beta(E^2 - 2EF + 2F^2 + 2nEF + n^2F^2) \\ A^{ab,\,ac} &= \beta(-EF + 2F^2 - nF^2) \\ A^{ab,\,cd} &= 2\beta F^2 \end{aligned} \tag{158}$$

where, and hereafter, a, b, c, d represent nonzero and mutually different indexes. Similarly, the elements of the matrix B can be categorized into seven different types

$$\begin{aligned} B^{0a,0a} &= 1-m^2, & B^{0a,0b} &= q-m^2 \\ B^{0a,ab} &= m(1-q), & B^{0a,bc} &= t-mq \\ B^{ab,ab} &= 1-q^2, & B^{ab,ac} &= q(1-q) \\ & & B^{ab,cd} &= r-q^2 \end{aligned} \tag{159}$$

where, by abuse of notation, we let

$$\begin{aligned} m &= [x_0x_a]_M, & q &= [x_ax_b]_M \\ t &= [x_0x_ax_bx_c]_M, & r &= [x_ax_bx_cx_d]_M. \end{aligned} \tag{160}$$

(The variable r that appears here is not to be confused with the received signal.) It should be noted that the equalities $m=[x_0x_a]_M$ and $q=[x_ax_b]_M$ actually hold *only after* we take the limit $n\to 0$, as derived in Section III-B.

The function f can be expanded to the second-order of perturbations of $\{Q\}$ and $\{\tilde{Q}\}$ around the RS saddle-point solution, as

$$f = f_0 + \frac{1}{2}(\boldsymbol{u}^T, \tilde{\boldsymbol{u}}^T)C\begin{pmatrix}\boldsymbol{u}\\ \tilde{\boldsymbol{u}}\end{pmatrix} + \mathcal{O}\left(\|\boldsymbol{u}\|^3, \|\tilde{\boldsymbol{u}}\|^3\right) \tag{161}$$

$$\boldsymbol{u} = \begin{pmatrix}\{\delta Q_{0a}\}\\ \{\delta Q_{ab}\}\end{pmatrix} \equiv \begin{pmatrix}\{\epsilon^a\}\\ \{\eta^{ab}\}\end{pmatrix} \tag{162}$$

$$\tilde{\boldsymbol{u}} = \begin{pmatrix}\{\delta \tilde{Q}_{0a}\}\\ \{\delta \tilde{Q}_{ab}\}\end{pmatrix} \equiv \begin{pmatrix}\{\tilde{\epsilon}^a\}\\ \{\tilde{\eta}^{ab}\}\end{pmatrix} \tag{163}$$

where f_0 denotes the value of f at the RS saddle-point solution, and where $\boldsymbol{u}$ and $\tilde{\boldsymbol{u}}$ are the perturbations to the RS saddle-point values of $\{Q\}$ and $\{\tilde{Q}\}$, respectively. The conditions for the two types of stability can be expressed in terms of the components of the Hessian C, as follows.

- Type 1 stability: The $[n(n+1)/2]\times[n(n+1)/2]$ matrix $\tilde{\mathcal{H}}\equiv\{B^{ab,cd}\}$ should be positive definite.
- Type 2 stability: The $[n(n+1)/2]\times[n(n+1)/2]$ matrix $\mathcal{H}\equiv\{A^{ab,cd}\}-\{\delta^{ab,cd}\}\{B^{ab,cd}\}^{-1}\{\delta^{ab,cd}\}$ should be negative definite.

It has been known in the literature of spin glasses [38] that the eigenspaces of $\mathcal{H}$ and $\tilde{\mathcal{H}}$ can be classified into three types according to their symmetry. Stability for each type of eigenspace is discussed in what follows.

We first investigate the eigenspace with full symmetry with respect to the replica indexes $a=1,\ldots,n$, that is,

$$\epsilon^a=\epsilon, \qquad \eta^{ab}=\eta, \qquad \tilde{\epsilon}^a=\tilde{\epsilon}, \qquad \tilde{\eta}^{ab}=\tilde{\eta} \tag{164}$$

or equivalently

$$\boldsymbol{u}=U_1\begin{pmatrix}\epsilon\\ \eta\end{pmatrix}, \qquad \tilde{\boldsymbol{u}}=U_1\begin{pmatrix}\tilde{\epsilon}\\ \tilde{\eta}\end{pmatrix} \tag{165}$$

where

$$U_1 = \left(\begin{array}{c|c} 1 & 0\\ \vdots & \vdots \\ 1 & 0 \\ \hline 0 & 1 \\ \vdots & \vdots \\ 0 & 1\end{array}\right) \tag{166}$$

is an $(n+n(n-1)/2)\times 2$ matrix. The representation C_1 of the restriction of C to the eigenspace with full symmetry is given by

$$C\begin{pmatrix}U_1 & O\\ O & U_1\end{pmatrix} = \begin{pmatrix}U_1 & O\\ O & U_1\end{pmatrix}C_1. \tag{167}$$

C_1 is a 4×4 matrix. Let

$$C_1 = \begin{bmatrix} A_1 & -\Delta_1 \\ -\Delta_1 & B_1\end{bmatrix} \tag{168}$$

with

$$\{A^{ab,cd}\}U_1 = U_1A_1 \tag{169}$$

$$\{\delta^{ab,cd}\}U_1 = U_1\Delta_1 \tag{170}$$

$$\{B^{ab,cd}\}U_1 = U_1B_1. \tag{171}$$

Using this representation, the two types of stability conditions are reduced as follows.

- Type 1 stability: All the eigenvalues of the matrix $\tilde{\mathcal{H}}_1\equiv B_1$ should have a positive real part.
- Type 2 stability: All the eigenvalues of the matrix $\mathcal{H}_1\equiv A_1-\Delta_1B_1^{-1}\Delta_1$ should have a negative real part.

We can define the eigenspaces of $\mathcal{H}_1$ and $\tilde{\mathcal{H}}_1$ by considering eigenvalue equations determining the values of the pairs (ϵ, η) and $(\tilde{\epsilon}, \tilde{\eta})$, respectively. The eigenspaces of $\mathcal{H}_1$ and $\tilde{\mathcal{H}}_1$ are of dimension two. Eigenvectors $\boldsymbol{v}_1$ and $\tilde{\boldsymbol{v}}_1$ belonging to these eigenspaces are called the longitudinal modes. The representation of C_1 is given by (172)–(174) shown at the top of the following page. By taking the limit $n\to 0$, the representation reduces to

$$C_1 = \begin{pmatrix} 0 & \beta E^2 & -1 & 0 \\ -2\beta E^2 & \beta(E^2+2EF) & 0 & -1 \\ -1 & 0 & 1-q & t-m \\ 0 & -1 & 2(m-t) & 1-4q+3r\end{pmatrix}. \tag{175}$$

We could derive the stability condition from the representation given above. However, perturbations within the eigenspaces keep symmetry across the replicas, and therefore the stability condition to be derived within the eigenspaces is irrelevant to RSB but only determines the stability *within* the RS assumption.

We next analyze the stability within the eigenspaces of the second type. These eigenspaces are spanned by the eigenvectors $\boldsymbol{v}_2$ and $\tilde{\boldsymbol{v}}_2$ of $\mathcal{H}$ and $\tilde{\mathcal{H}}$, respectively, which are symmetric under interchange of all of the indexes $\{1,\ldots,n\}$ except one. Let μ

$$A_1 = \begin{pmatrix} 2n\beta E^2 & \beta(1-n)E^2 \\ -2\beta E^2 & \beta(E^2+2EF+nF^2) \end{pmatrix} \tag{172}$$

$$B_1 = \begin{pmatrix} 1-q+n(q-m^2) & (1-n)\left[(t-m)-\frac{n}{2}(t-mq)\right] \\ 2(m-t)-n(t-mq) & 1-4q+3r+\frac{n}{2}\left[4q+q^2-5r+n(r-q^2)\right] \end{pmatrix} \tag{173}$$

$$\Delta_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{174}$$

be the specific index in $\{1, \ldots n\}$ which lacks the symmetry. The elements of $\boldsymbol{v}_2$ and $\tilde{\boldsymbol{v}}_2$ are

$$\begin{aligned} &\epsilon^a = \epsilon, && \tilde{\epsilon}^a = \tilde{\epsilon}, && a \neq \mu \\ &\epsilon^\mu = (1-n)\epsilon, && \tilde{\epsilon}^\mu = (1-n)\tilde{\epsilon} && \\ &\eta^{ab} = \eta, && \tilde{\eta}^{ab} = \tilde{\eta}, && a, b \neq \mu \\ &\eta^{\mu a} = \eta^{a\mu} = \tfrac{1}{2}(2-n)\eta, && \tilde{\eta}^{\mu a} = \tilde{\eta}^{a\mu} = \tfrac{1}{2}(2-n)\tilde{\eta}, && a \neq \mu. \end{aligned} \tag{176}$$

The forms of ϵ^μ, $\eta^{\mu a}$, and $\eta^{a\mu}$ are chosen in such a way that $\boldsymbol{v}_2$ is orthogonal to $\boldsymbol{v}_1$, the vectors in the eigenspace of the first type. Similarly, the orthogonality requirement yields the forms of $\tilde{\epsilon}^\mu$, $\tilde{\eta}^{\mu a}$, and $\tilde{\eta}^{a\mu}$. The eigenvectors belonging to the eigenspace of the second type are called the anomalous modes in spin glass theory. As in the analysis of the eigenspaces of the first type, (176) induces the transform U_2 from $(\epsilon, \eta, \tilde{\epsilon}, \tilde{\eta})^T$ to $(\boldsymbol{u}^T, \tilde{\boldsymbol{u}}^T)^T$, from which the representation C_2 of the restriction of C to the eigenspaces with the prescribed symmetry. C_2 is given by

$$C_2 = \begin{bmatrix} A_2 & -\Delta_2 \\ -\Delta_2 & B_2 \end{bmatrix}, \tag{177}$$

with

$$A_2 = \begin{pmatrix} n\beta E(E+nF) & \tfrac{1}{2}(2-n)\beta E(E+nF) \\ -2\beta E(E+nF) & \beta(E+2F)(E+nF) \end{pmatrix} \tag{178}$$

$$B_2 = \begin{pmatrix} 1-q & \tfrac{1}{2}(2-n)(t-m) \\ 2(m-t) & 1-4q+3r+n(q-r) \end{pmatrix} \tag{179}$$

$$\Delta_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{180}$$

The matrix C_2 reduces, in the limit $n \to 0$, to the matrix C_1 for the eigenspace of the first type (see (175)) means that the stability condition within the eigenspace of the second type is identical to that within the eigenspace of the first type, that is, the RS saddle-point solution is stable against perturbations in the direction of the anomalous mode whenever it is stable within the RS assumption.

For each choice of the specific index μ, the eigenspaces of $\tilde{\mathcal{H}}_2 \equiv B_2$ and $\mathcal{H}_2 \equiv A_2 - \Delta_2 B_2^{-1}\Delta_2$ are of dimension two. Since there are n possible choices of the index μ, the total dimensionality of each eigenspace would seem $2n$. However, the n eigenvectors corresponding to the n choices of the index μ are linearly dependent, and only $n-1$ of them are actually linearly independent, so that the degeneracy is $n-1$. Thus, the total dimensionality of the eigenspaces of the anomalous modes is $2(n-1)$.

We now probe stability within the eigenspaces of the third type. They are spanned by the eigenvectors $\boldsymbol{v}_3$ and $\tilde{\boldsymbol{v}}_3$ of $\mathcal{H}$ and $\tilde{\mathcal{H}}$, respectively. These eigenvectors are symmetric under interchange of all of the indexes $\{1, \ldots, n\}$ except two. Let μ and ν $(\mu \neq \nu)$ be the two specific indexes in $\{1, \ldots, n\}$ for which the symmetry is absent. We assume that the elements of $\boldsymbol{v}_3$ and $\tilde{\boldsymbol{v}}_3$ are of the form

$$\begin{aligned} &\epsilon_a = \epsilon, && \tilde{\epsilon}_a = \tilde{\epsilon}, && a \neq \mu, \nu \\ &\epsilon_\mu = \epsilon_\nu = \tfrac{1}{2}(2-n)\epsilon, && \tilde{\epsilon}_\mu = \tilde{\epsilon}_\nu = \tfrac{1}{2}(2-n)\tilde{\epsilon} && \\ &\eta_{ab} = \eta, && \tilde{\eta}_{ab} = \tilde{\eta}, && a, b \neq \mu, \nu \\ &\eta_{\mu a} = \eta_{\nu a} = P\eta, && \tilde{\eta}_{\mu a} = \tilde{\eta}_{\nu a} = P\tilde{\eta}, && a \neq \mu, \nu \\ &\eta_{\mu\nu} = Q\eta, && \tilde{\eta}_{\mu\nu} = Q\tilde{\eta}. && \end{aligned} \tag{181}$$

$\boldsymbol{v}_3$ and $\tilde{\boldsymbol{v}}_3$ should be orthogonal to $\boldsymbol{v}_1$ and $\tilde{\boldsymbol{v}}_1$, respectively. A sufficient condition yields the coefficient $(1/2)(2-n)$ for ϵ_μ, ϵ_ν, $\tilde{\epsilon}_\mu$, and $\tilde{\epsilon}_\nu$, and the condition

$$2(n-2)P + Q + \tfrac{1}{2}(n-2)(n-3) = 0. \tag{182}$$

$\boldsymbol{v}_3$ and $\tilde{\boldsymbol{v}}_3$ should be also orthogonal to $\boldsymbol{v}_2$ and $\tilde{\boldsymbol{v}}_2$, respectively. This requirement yields the conditions

$$\epsilon = 0, \qquad (n-2)P + Q = 0, \qquad P + \tfrac{1}{2}(n-3) = 0. \tag{183}$$

From (182) and (183), we have

$$P = \frac{1}{2}(3-n), \qquad Q = \tfrac{1}{2}(2-n)(3-n). \tag{184}$$

Thus, we analyze the stability within the eigenspaces spanned by the eigenvectors of the form

$$\begin{aligned} &\epsilon_a = 0, && \tilde{\epsilon}_a = 0 && \\ &\eta_{ab} = \eta, && \tilde{\eta}_{ab} = \tilde{\eta} && (a, b \neq \mu, \nu) \\ &\eta_{\mu a} = \eta_{\nu a} = \tfrac{1}{2}(3-n)\eta, && \tilde{\eta}_{\mu a} = \eta_{\nu a} = \tfrac{1}{2}(3-n)\tilde{\eta} && (a \neq \mu, \nu) \\ &\eta_{\mu\nu} = \tfrac{1}{2}(2-n)(3-n)\eta, && \tilde{\eta}_{\mu\nu} = \tfrac{1}{2}(2-n)(3-n)\tilde{\eta}. && \end{aligned} \tag{185}$$

Again, the transform U_3 from $(\eta, \tilde{\eta})^T$ to $(\boldsymbol{u}^T, \tilde{\boldsymbol{u}}^T)^T$ is defined, from which the representation C_3 of the restriction of C to the eigenspaces with the prescribed symmetry is determined. C_3 is a 2×2 matrix, and is given by

$$C_3 = \begin{pmatrix} \beta(E+nF)^2 & -1 \\ -1 & 1-2q+r \end{pmatrix}. \tag{186}$$

As the stability condition, we have, in the limit $n \to 0$

$$\tilde{\mathcal{H}}_3 \equiv 1-2q+r > 0 \tag{187}$$

and

$$\mathcal{H}_3 \equiv \beta E^2 - (1-2q+r)^{-1} < 0. \tag{188}$$

There are $n(n-1)/2$ choices for the indexes μ and ν. However, n of them are linearly dependent, so that the total dimension of each eigenspace in the replicon modes is $n(n-3)/2$. Together with other two types of modes, we have $n(n+1)/2$ eigenvectors for both $\mathcal{H}$ and $\tilde{\mathcal{H}}$, and have exhausted them all. We do not have to consider any other types of eigenvectors.

In the limit $n \to 0$, we have

$$1-2q+r \to \int \operatorname{sech}^4\left(\sqrt{F}\,z+E\right) Dz > 0 \tag{189}$$

so that the condition (187) is always satisfied. Therefore, it is (188) that gives the stability condition of the RS solution against RSB, which becomes

$$1-\beta E^2 \int \operatorname{sech}^4\left(\sqrt{F}\,z+E\right) Dz > 0. \tag{190}$$

This proves (67).

ACKNOWLEDGMENT

The author would like to thank Y. Kabashima, H. Nishimori, D. Saad, M. Okada, N. Skantzos, and J. van Mourik, for their helpful discussion and comments, and D. Agrawal for providing the author with [47] prior to publication. The author would also like to thank anonymous reviewers for their critical comments, which were most helpful in revising this paper.

REFERENCES

[1] J. Besag, "On the statistical analysis of dirty pictures," *J. Roy. Statist. Soc. B*, vol. 48, no. 3, pp. 259–302, 1986.

[2] G. Winkler, *Image Analysis, Random Fields and Dynamic Monte Carlo Methods*. Berlin, Heidelberg, Germany: Springer-Verlag, 1995.

[3] A. J. Grant and P. D. Alexander, "Random sequence multisets for synchronous code-division multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2832–2836, Nov. 1998.

[4] S. Verdú and S. Shamai (Shitz), "Spectral efficiency of CDMA with random spreading," *IEEE Trans. Inform. Theory*, vol. 45, pp. 622–640, Mar. 1999.

[5] D. N. C. Tse and S. V. Hanly, "Linear multiuser receivers: Effective interference, effective bandwidth and user capacity," *IEEE Trans. Inform. Theory*, vol. 45, pp. 641–657, Mar. 1999.

[6] D. N. C. Tse and O. Zeitouni, "Linear multiuser receivers in random environment," *IEEE Trans. Inform. Theory*, vol. 46, pp. 171–188, Jan. 2000.

[7] D. N. C. Tse and S. Verdú, "Optimum asymptotic multiuser efficiency of randomly spread CDMA," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2718–2722, Nov. 2000.

[8] S. Verdú, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[9] M. Mézard, G. Parisi, and M. A. Virasoro, *Spin Glass Theory and Beyond*. Singapore: World Scientific, 1987, vol. 9, World Scientific Lecture Notes in Physics.

[10] K. H. Fischer and J. A. Hertz, *Spin Glasses*. Cambridge, U.K.: Cambridge Univ. Press, 1991.

[11] D. J. Amit, H. Gutfreund, and H. Sompolinsky, "Storing infinite numbers of patterns in a spin-glass model of neural networks," *Phys. Rev. Lett.*, vol. 55, no. 14, pp. 1530–1533, 1985.

[12] J. Hertz, A. Krogh, and R. G. Palmer, *Introduction to the Theory of Neural Computation*. Reading, MA: Addison-Wesley, 1991.

[13] E. Gardner, "The space of interactions in neural network models," *J. Phys. A: Math. Gen.*, vol. 21, no. 1, pp. 257–270, 1988.

[14] E. Gardner and B. Derrida, "Optimal storage properties of neural network models," *J. Phys. A: Math. Gen.*, vol. 21, no. 1, pp. 271–284, 1988.

[15] H. S. Seung, H. Sompolinsky, and N. Tishby, "Statistical mechanics of learning from examples," *Phys. Rev. A*, vol. 45, no. 8, pp. 6056–6091, Apr. 1992.

[16] T. L. H. Watkin, A. Rau, and M. Biehl, "The statistical mechanics of learning a rule," *Rev. Mod. Phys.*, vol. 65, no. 2, pp. 499–556, Apr. 1993.

[17] H. Nishimori and K. Y. M. Wong, "Statistical mechanics of image restoration and error-correcting codes," *Phys. Rev. E*, vol. 60, no. 1, pp. 132–144, July 1999.

[18] Y. Kabashima and D. Saad, "Statistical mechanics of error-correcting codes," *Europhys. Lett.*, vol. 45, no. 1, pp. 97–103, Jan. 1999.

[19] I. Kanter and D. Saad, "Error-correcting codes that nearly saturate Shannon's bound," *Phys. Rev. Lett.*, vol. 83, no. 13, pp. 2660–2663, Sept. 1999.

[20] T. Murayama, Y. Kabashima, D. Saad, and R. Vicente, "Statistical physics of regular low-density parity-check error-correcting codes," *Phys. Rev. E*, vol. 62, no. 2, pp. 1577–1591, 2000.

[21] A. Montanari and N. Sourlas, "The statistical mechanics of turbo codes," *Eur. Phys. J. B*, vol. 18, no. 1, pp. 107–119, 2000.

[22] A. Montanari, "Turbo codes: The phase transition," *Eur. Phys. J. B*, vol. 18, no. 1, pp. 121–136, 2000.

[23] Y. Kabashima, N. Sazuka, K. Nakamura, and D. Saad, "Tighter decoding reliability bound for Gallager's error-correcting code," *Phys. Rev. E*, vol. 64, no. 4, pp. 046113-1–046113-4, 2001.

[24] T. M. Cover, "Geometrical and statistical properties of systems of linear inequalities with applications in pattern recognition," *IEEE Trans. Electron. Comput.*, vol. EC-14, pp. 326–334, 1965.

[25] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

[26] D. Guo and S. Verdú, "Multiuser detection and statistical mechanics," *Ian Blake Festschrift*, 2002, to be published.

[27] T. Tanaka, "Analysis of bit error probability of direct-sequence CDMA multiuser demodulators," in *Advances in Neural Information Processing Systems*, T. Leen, T. Dietterich, and V. Tresp, Eds. Cambridge, MA: MIT Press, 2001, vol. 13, pp. 315–321.

[28] ——, "Statistical mechanics of CDMA multiuser demodulation," *Europhys. Lett.*, vol. 54, no. 4, pp. 540–546, 2001.

[29] ——, "Average-case analysis of multiuser detectors," in *Proc. 2001 IEEE Int. Symp. Information Theory*, Washington, DC, June 2001, p. 287.

[30] R. S. Ellis, *Entropy, Large Deviations, and Statistical Mechanics (A Series of Comprehensive Studies in Mathematics)*. Berlin, Germany: Springer-Verlag, 1985, vol. 271.

[31] M. Opper and W. Kinzel, "Statistical mechanics of generalization," in *Models of Neural Networks III*, E. Domany, J. L. van Hemmen, and K. Schulten, Eds. New York: Springer-Verlag, 1996, ch. 5, pp. 151–209.

[32] K. Binder and A. P. Young, "Spin glasses: Experimental facts, theoretical concepts, and open questions," *Rev. Mod. Phys.*, vol. 58, no. 4, pp. 801–976, Oct. 1989.

[33] J. L. van Hemmen and R. Kühn, "Collective phenomena in neural networks," in *Models in Neural Networks I*, 2nd updated ed, E. Domany, J. L. van Hemmen, and K. Schulten, Eds. Berlin, Germany: Springer-Verlag, 1991, 1995, pp. 1–113.

[34] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications (Applications of Mathematics)*, 2nd ed. New York: Springer-Verlag, 1993, 1998, vol. 38.

[35] H. Nishimori, *Statistical Physics of Spin Glasses and Information Processing: An Introduction*. Oxford, U.K.: Oxford Univ. Press, 2001, Number 111 in International Series of Monographs on Physics.

[36] D. Sherrington and S. Kirkpatrick, "Solvable model of a spin-glass," *Phys. Rev. Lett.*, vol. 35, no. 26, pp. 1792–1796, Dec. 1975.

[37] J. L. van Hemmen and R. G. Palmer, "The replica method and a solvable spin glass model," *J. Phys. A: Math. Gen.*, vol. 12, no. 4, pp. 563–580, Apr. 1979.

[38] J. R. L. de Almeida and D. J. Thouless, "Stability of the Sherrington–Kirkpatrick solution of a spin glass model," *J. Phys. A: Math. Gen.*, vol. 11, no. 5, pp. 983–990, 1978.

[39] H. Nishimori, "Comment on 'Statistical mechanics of CDMA multiuser demodulation' by T. Tanaka," *Europhys. Lett.*, vol. 57, no. 2, pp. 302–303, 2002.

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

[41] Z. D. Bai and Y. Q. Yin, "Limit of the smallest eigenvalue of a large dimensional sample covariance matrix," *Ann. Probab.*, vol. 21, pp. 1275–1294, 1993.

[42] R. Lupas and S. Verdú, "Linear multiuser detectors for synchronous code-division multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 35, pp. 123–136, Jan. 1989.

[43] Z. Xie, R. T. Short, and C. K. Rushforth, "A family of suboptimum detectors for coherent multiuser communications," *IEEE J. Select. Areas Commun.*, vol. 8, pp. 683–690, May 1990.

[44] U. Madhow and M. L. Honig, "MMSE interference suppression for direct-sequence spread-spectrum CDMA," *IEEE Trans. Commun.*, vol. 42, pp. 3178–3188, Dec. 1994.

[45] H. V. Poor and S. Verdú, "Probability of error in MMSE multiuser detection," *IEEE Trans. Inform. Theory*, vol. 43, pp. 858–871, May 1997.

[46] D. Agrawal and A. Vardy, "The turbo decoding algorithm and its phase trajectories," in *Proc. 2000 IEEE Int. Symp. Information Theory*, Sorrento, Italy, 2000, p. 316.

[47] ——, "The turbo decoding algorithm and its phase trajectories," *IEEE Trans. Inform. Theory*, vol. 47, pp. 699–722, Feb. 2001.

[48] S. Kirkpatrick, C. D. Gelatt, Jr., and M. P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671–680, 1983.

[49] Z. D. Bai, "Methodologies in spectral analysis of large dimensional random matrices, a review," *Statist. Sinica*, vol. 9, no. 3, pp. 611–677, 1999.

[50] A. Bovier and P. Picco, Eds., *Mathematical Aspects of Spin Glasses and Neural Networks (Progress in Probability)*. Boston, MA: Birkhäuser, 1998, vol. 41.

[51] S. Verdú, "Computational complexity of optimum multiuser detection," *Algorithmica*, vol. 4, pp. 303–312, 1989.

[52] M. Opper and D. Saad, Eds., *Advanced Mean Field Methods: Theory and Practice*. Cambridge, MA: MIT Press, 2001.

[53] D. Malzahn and M. Opper, "Learning curves for Gaussian processes models: Fluctuations and universality," in *Artificial Neural Networks—ICANN 2001 (Lecture Notes in Computer Science)*, G. Dorffner, H. Bischof, and K. Hornik, Eds. Berlin, Germany: Springer-Verlag, 2001, vol. 2130, pp. 271–276.

[54] ——, "A variational approach to learning curves," in *Advances in Neural Information Processing Systems*, T. G. Dietterich, S. Becker, and Z. Ghahramani, Eds. Cambridge, MA: MIT Press, 2002, vol. 14.

[55] P. McCullagh, *Tensor Methods in Statistics (Monographs on Statistics and Applied Probability)*. London, U.K.: Chapman & Hall, 1987.

[56] D. A. Harville, *Matrix Algebra From a Statistician's Perspective*. Berlin, Germany: Springer-Verlag, 1997.