

# Optimization of sequences in CDMA systems: a statistical-mechanics approach

Koichiro Kitagawa<sup>a</sup>, Toshiyuki Tanaka<sup>a</sup>

<sup>a</sup>*Graduate School of Informatics, Kyoto University, Japan.*

---

## Abstract

Statistical mechanics approach is useful not only in analyzing macroscopic system performance of wireless communication systems, but also in discussing design problems of wireless communication systems. In this paper, we discuss a design problem of spreading sequences in code-division multiple-access (CDMA) systems, as an example demonstrating the usefulness of statistical mechanics approach. We analyze, via replica method, the average mutual information between inputs and outputs of a randomly-spread CDMA channel, and discuss the optimization problem with the average mutual information as a measure of optimization. It has been shown that the average mutual information is maximized by orthogonally-invariant random Welch bound equality (WBE) spreading sequences.

*Key words:* code-division multiple-access (CDMA), replica method, average mutual information, large system limit

---

## 1. Introduction

In recent years, advances in information and communication technologies have been demanding high data-rate wireless communications. In order to realize high data-rate wireless communications, bandwidth of systems should be as wide as possible, which means that such systems should have a large degree of freedom. Those systems are also required to be able to operate

---

*Email addresses:* `kitagawa@sys.i.kyoto-u.ac.jp` (Koichiro Kitagawa),  
`tt@i.kyoto-u.ac.jp` (Toshiyuki Tanaka)

<sup>1</sup>Graduate School of Informatics, Kyoto University, 36-1 Yoshida Hon-machi, Sakyo-ku, Kyoto-shi, Kyoto 606-8501, Japan.

efficiently even in bad and uncertain environments. For example, in urban areas, there are many obstacles, such as buildings, cars, and people, which interact with wireless communication systems as reflecting/scattering bodies, thereby making communication environment very complex. In analyzing wireless communication systems, therefore, one has to regard them as systems with very high dimensionality and randomness. This is why statistical mechanics approach is expected to be useful in studying wireless communication systems.

In this paper, we consider a problem arising from considerations of multiple-access channels. Typically, a wireless communication system has to accommodate multiple users simultaneously. In such a system, signals coming from different users interfere with each other. How to mitigate such multiple-access interference (MAI) is one of the most important problems in wireless communications. Code-division multiple-access (CDMA) [1, 2] provides an effective scheme to mitigate MAI, and is widely used in various commercial systems. In CDMA, an information symbol of a user is modulated with a spreading sequence assigned to the user. Receiver has to estimate information symbols based on received sequences by utilizing knowledge of spreading sequences of the users.

A conventional choice to mitigate MAI is to use pseudorandom sequences as the spreading sequences. Although analysis of such randomly-spread CDMA systems was thought to be difficult, it has turned out that *replica method*, which is an analytical tool developed in the research field of statistical physics of disordered systems (spin glasses), is very useful for the analysis [3, 4]. More precisely, these studies have revealed that replica method allows us to evaluate “macroscopic” performance of CDMA systems with independent and identically-distributed (i.i.d.) random spreading sequences in the large-system limit, such as mutual information between inputs and outputs, bit error rate, and so on.

Since theoretical performance of CDMA systems is affected by choices of spreading sequences, design of spreading sequences is an important problem in CDMA. There have been several researches in which the problem of designing spreading sequences is formulated in terms of an optimization problem. For example, Rupf and Massey [5] discussed optimization of spreading sequences with the channel capacity of CDMA systems as a measure of optimization. They showed that so-called Welch bound equality (WBE) spreading sequences, which minimize the total squared correlation (TSC) of spreading sequences, achieve the channel capacity.

We restrict ourselves to considering the optimization problem of spreading sequences of CDMA systems with the mutual information between inputs and outputs as the measure of optimization. There have been several researches in which such optimization problems are discussed [5, 6, 7]. They have assumed inputs of the system to be Gaussian distributed and discussed theoretical upper bound (i.e., channel capacity) of mutual information between inputs and outputs. If one wishes to consider realistic wireless communication systems, however, it is important to study the optimization problem under the assumption of non-Gaussian inputs. The objective of this paper is therefore to discuss the optimization problem of spreading sequences of CDMA systems when one allows non-Gaussian inputs. We would like to emphasize that, unlike previous statistical-mechanics studies of CDMA systems [3, 4, 8] whose objectives are basically to analyze macroscopic system performance, we show in this paper that the statistical-mechanics approach is also useful in dealing with design problems in wireless communication, with the optimization problem of spreading sequences of CDMA systems as a demonstrative example. A digest version of this paper has been presented as a conference paper [9].

## 2. Problem

We consider the following real-valued  $K$ -user CDMA channel model,

$$y_\mu = \frac{1}{\sqrt{L}} \sum_{k=1}^K s_{\mu k} x_k + \sigma n_\mu, \quad \mu = 1, \dots, L, \quad (1)$$

where  $x_k$  is an information symbol of user  $k$ . We assume that  $\{x_k; k = 1, \dots, K\}$  are i.i.d. random variables, and let  $p(\cdot)$  be the prior probability of  $x_k$ , whose mean and variance are assumed to be zero and one, respectively.  $\{s_{\mu k}; \mu = 1, \dots, L\}$  is the spreading sequence of user  $k$  in the symbol interval of interest, and  $L$  denotes the spreading factor of the CDMA channel model. We assume that the power of the spreading sequences is normalized to one, so that  $\sum_{\mu=1}^L (s_{\mu k}/\sqrt{L})^2 = 1$  holds for  $k = 1, \dots, K$ . We assume additive white Gaussian noise (AWGN):  $n_\mu \sim \mathcal{N}(0, 1)$  so that  $\sigma^2$  is the variance of AWGN. Let us introduce the following notations:  $\mathbf{y} \equiv [y_1, \dots, y_L]^T$ ,  $\mathbf{n} \equiv [n_1, \dots, n_L]^T$ ,  $\mathbf{x} \equiv [x_1, \dots, x_K]^T$ , and  $S = (S_{\mu k})$ ,  $S_{\mu k} \equiv (1/\sqrt{L})s_{\mu k}$ ;  $k = 1, \dots, K$ ;  $\mu = 1, \dots, L$ . The system model (1) is then rewritten as

$$\mathbf{y} = S\mathbf{x} + \sigma\mathbf{n}. \quad (2)$$

One can consider a maximization problem of per user mutual information between  $\mathbf{x}$  and  $\mathbf{y}$  with respect to the spreading sequences  $S$ , with the channel input  $\mathbf{x}$  drawn from the probability distribution  $p(\mathbf{x}) = \prod_k p(x_k)$ ,

$$C_{\text{user}} = \frac{1}{K} I(\mathbf{x}; \mathbf{y})|_S, \quad (3)$$

where the notation  $I(\mathbf{x}; \mathbf{y})|_S$  denotes the mutual information between  $\mathbf{x}$  and  $\mathbf{y}$  when  $S$  is specified. When  $K \leq L$ , the mutual information  $C_{\text{user}}$  is maximized by assigning to all users orthogonal  $L$ -dimensional vectors as spreading sequences, regardless of the input distribution  $p(\cdot)$ . When  $K > L$ , on the other hand, spreading sequences maximizing the mutual information  $C_{\text{user}}$  are not trivial. When  $x_k$ ,  $k = 1, \dots, K$ , are i.i.d. standard Gaussian random variables, it is known that the WBE spreading sequences maximize the mutual information  $C_{\text{user}}$  [5]. WBE spreading sequences are characterized as [10, 11]

$$SS^T = \beta I_{L \times L}, \quad \beta \equiv \frac{K}{L} > 1, \quad (4)$$

where  $I_{L \times L}$  is an  $L$ -dimensional identity matrix.

When one assumes Gaussian inputs, spreading sequences maximizing  $C_{\text{user}}$  have been identified in more general system models than (2). For example, in a system model where one allows the power of inputs to be different, Viswanath and Anantharam [6] showed that the mutual information is maximized by assigning orthogonal spreading sequences to relatively high-power users and so-called generalized WBE spreading sequences to the remaining users, where the users are classified according to a certain criterion. Also, in a system model where the inputs may arrive asynchronously, Luo *et al.* [7] showed that the mutual information is maximized by spreading sequences which can be regarded as an extension of the ones which Viswanath and Anantharam proposed.

On the other hand, when  $x_k$ 's are drawn from a non-Gaussian distribution, to the authors' knowledge, spreading sequences maximizing the mutual information (3) have not been known. We analyze, via statistical mechanics, spreading sequences maximizing the mutual information of the system with non-Gaussian inputs. Since the case with non-Gaussian inputs is difficult to analyze analytically, we resort to making several assumptions. First, we evaluate mutual information in the large-system limit, in which the number of users  $K$  and the spreading factor  $L$  are both sent to infinity while maintaining their ratio  $\beta = K/L$  constant. Second, we assume random spreading.

More specifically, we assume that the sample correlation matrix  $R = S^T S$  of random spreading sequences  $S$  is asymptotically orthogonally invariant, that is, the probability law of  $R$  and that of an orthogonal transform  $U^T R U$  are the same for any orthogonal matrix  $U$  in the large-system limit, and that empirical eigenvalue distribution of  $R$  converges to a limiting eigenvalue distribution  $\rho(\lambda)$  with a finite support included in  $[\lambda_{\min}, \lambda_{\max}]$ , in the large-system limit. Under the assumption of random spreading, we consider the average conditional mutual information in the large-system limit,

$$C = \lim_{K \rightarrow \infty} \mathbb{E}_S \{C_{\text{user}}\} = \lim_{K \rightarrow \infty} \frac{1}{K} I(\mathbf{x}; \mathbf{y}|S), \quad (5)$$

where  $\mathbb{E}_S$  denotes expectation with respect to  $S$ , and where  $I(\mathbf{x}; \mathbf{y}|S)$  is conditional mutual information between  $\mathbf{x}$  and  $\mathbf{y}$  given  $S$ . We discuss maximization of  $C$  with respect to characteristics of the random matrix  $S$ .

### 3. Analysis

#### 3.1. Evaluation of average mutual information via replica method

The average mutual information (5) is decomposed into two terms,

$$C = \lim_{K \rightarrow \infty} \frac{1}{K} [\mathbb{E}_{\mathbf{y}, S} \{\log p(\mathbf{y}|S)\} - \mathbb{E}_{\mathbf{y}, \mathbf{x}, S} \{\log p(\mathbf{y}|\mathbf{x}, S)\}] \quad (6)$$

$$= \mathcal{F} - \frac{1}{2\beta} (1 + \log(2\pi\sigma^2)), \quad (7)$$

with

$$\mathcal{F} \equiv - \lim_{K \rightarrow \infty} \frac{1}{K} \mathbb{E}_{\mathbf{y}, S} \{\log p(\mathbf{y}|S)\}, \quad (8)$$

where  $\mathbb{E}_{\mathbf{y}, S}$  denotes expectation with respect to  $\mathbf{y}$  and  $S$ . Direct calculation of the right-hand side of (8) is in general computationally intractable. In order to evaluate (8), we invoke the replica method. Substituting the identity

$$\lim_{n \rightarrow 0} \frac{\partial}{\partial n} (p(\mathbf{y}|S))^n = \log p(\mathbf{y}|S) \quad (9)$$

to the right-hand side of (8), we obtain

$$\mathcal{F} = - \lim_{K \rightarrow \infty} \frac{1}{K} \lim_{n \rightarrow 0} \frac{\partial}{\partial n} \log \mathbb{E}_{\mathbf{y}, S} \{(p(\mathbf{y}|S))^n\}. \quad (10)$$

We assume that the limit with respect to  $K$  and the limit and the differentiation with respect to  $n$  are interchangeable without altering the final result, obtaining

$$\mathcal{F} = -\lim_{n \rightarrow 0} \frac{\partial}{\partial n} \lim_{K \rightarrow \infty} \frac{1}{K} \log \mathbb{E}_{\mathbf{y}, S} \{ (p(\mathbf{y}|S))^n \}. \quad (11)$$

The limit  $K \rightarrow \infty$  allows us to apply the saddle-point method to evaluate a relevant quantity. We apply replica trick in order to evaluate (11), in which we first evaluate  $\mathbb{E}_{\mathbf{y}, S} \{ (p(\mathbf{y}|S))^n \}$  assuming that  $n$  is a non-negative integer, and then perform the limit and the differentiation with respect to  $n$ , assuming that  $n$  is real.

Evaluation of (11) basically goes in a similar manner as [8]. Detailed analysis is described in the appendix. Here, we only show the result. The average mutual information in the large-system limit is given by

$$C = -\frac{1}{2}\theta\mathcal{E} - \frac{1}{2}G\left(-\frac{\mathcal{E}}{\sigma^2}\right) - \frac{1}{2}\log\frac{2\pi}{\theta} - \frac{1}{2} - \int p(u; \theta) \log p(u; \theta) du, \quad (12)$$

where  $\{\mathcal{E}, \theta\}$  are parameters whose values are to be determined later, and where  $p(u; \theta)$  is a probability density function of output  $u$  of a scalar AWGN channel with  $1/\theta$  the noise variance, when the channel input  $x$  is generated from the distribution  $p(x)$ . The function  $G(t)$  is defined as

$$G(t) = \int_0^t \mathbf{R}(z) dz \quad (13)$$

where  $\mathbf{R}(z)$  is the R-transform [12] of the limiting eigenvalue distribution  $\rho(\lambda)$  of the correlation matrix  $R$ , which is defined on the basis of the Hilbert transform<sup>2</sup> of  $\rho(\lambda)$ ,

$$\mathcal{C}(\gamma) = \int \frac{\rho(\lambda)}{\gamma - \lambda} d\lambda, \quad \gamma < \lambda_{\min}, \quad (14)$$

as

$$\mathcal{C}\left(\mathbf{R}(z) + \frac{1}{z}\right) = z. \quad (15)$$

---

<sup>2</sup>It should be noted that the so-called Cauchy transform is defined by the same formula as the Hilbert transform (14), but with  $\gamma$  in the upper half of complex plane.

The parameters  $\{\mathcal{E}, \theta\}$  are to be determined from the following saddle-point equations:

$$\mathcal{E} = \mathbb{E}\{(x - \langle x \rangle)^2; \theta\} \quad (16)$$

$$\theta = \frac{1}{\sigma^2} \mathbf{R} \left( -\frac{\mathcal{E}}{\sigma^2} \right) \quad (17)$$

where  $\langle x \rangle$  denotes posterior mean estimate of the channel input  $x$  of the scalar AWGN channel introduced above, defined as

$$\langle x \rangle = \frac{\int x \sqrt{\frac{\theta}{2\pi}} e^{-\theta(u-x)^2/2} p(x) dx}{\int \sqrt{\frac{\theta}{2\pi}} e^{-\theta(u-x)^2/2} p(x) dx}, \quad (18)$$

and where  $\mathbb{E}$  in (16) denotes expectation with respect to the channel input  $x$  and output  $u$  of the scalar AWGN channel.

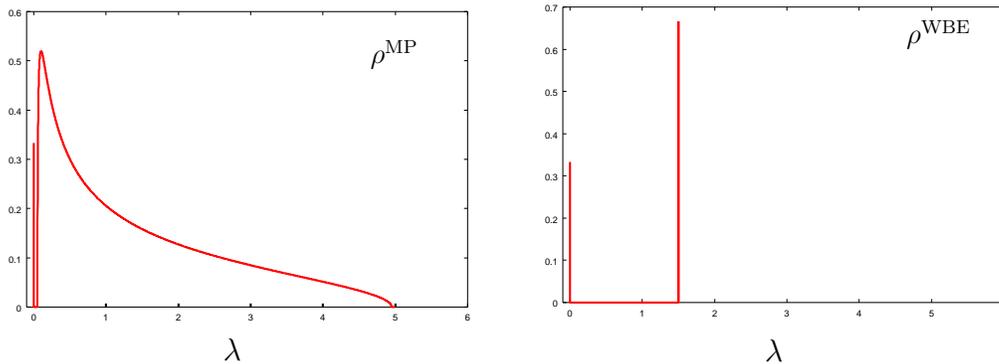


Figure 1: Eigenvalue distributions  $\rho^{\text{MP}}$ (left figure) and  $\rho^{\text{WBE}}$ (right figure) with  $\beta = 1.5$ . Both distributions have probability weight  $1 - 1/\beta$  at  $\lambda = 0$ .

The average mutual information (12) depends on the limiting eigenvalue distribution  $\rho(\lambda)$  of  $R$  as well as the prior distribution  $p(x_k)$ . When we assume that  $s_{\mu k}$  are i.i.d. random variables whose mean and variance are zero and one, respectively, our result is reduced to that obtained by Guo and Verdú [4]. In this case, the limiting eigenvalue distribution  $\rho(\lambda)$  is given by the so-called Marčenko-Pastur law [13],

$$\rho^{\text{MP}}(\lambda) = \left(1 - \frac{1}{\beta}\right)^+ \delta(\lambda) + \frac{\sqrt{(\lambda - a)^+(b - \lambda)^+}}{2\pi\beta\lambda}, \quad (19)$$

where  $(x)^+ = \max(0, x)$ , and  $a = (1 - \sqrt{\beta})^2$ ,  $b = (1 + \sqrt{\beta})^2$  (see figure 1), whose R-transform is given by

$$\mathbf{R}^{\text{MP}}(z) = \frac{1}{1 - \beta z}. \quad (20)$$

Substituting (20) to (13), one can confirm the above-mentioned fact. Our analysis also includes the case of the system with WBE spreading sequences. Since the characteristic of WBE spreading sequences is expressed as (4), the correlation matrix of WBE spreading sequences has trivial zero eigenvalue and the eigenvalue  $\lambda = \beta$ , with multiplicities  $(K - L)$  and  $L$ , respectively (see figure 1), and therefore

$$\rho^{\text{WBE}}(\lambda) = \left(1 - \frac{1}{\beta}\right) \delta(\lambda) + \frac{1}{\beta} \delta(\lambda - \beta), \quad (21)$$

whose R-transform is given by

$$\mathbf{R}^{\text{WBE}}(z) = \frac{2}{1 - \beta z + \sqrt{(\beta z - 1)^2 + 4z}}. \quad (22)$$

One can evaluate, via  $\mathbf{R}^{\text{WBE}}(z)$ , the mutual information when orthogonally-invariant random WBE spreading sequences are employed. In figure 2, we show a comparison of the mutual information when the above two spreading sequences are employed, and when probability distribution of  $\{x_k\}$  is given by  $p(x_k) = (\delta(x_k - 1) + \delta(x_k + 1))/2$ ,  $k = 1, \dots, K$ . One can confirm that WBE spreading sequences achieve higher mutual information than i.i.d. random spreading sequences do.

### 3.2. Optimizing spreading sequences

Choices of spreading sequences affect the average mutual information  $C$  through the limiting eigenvalue distribution  $\rho(\lambda)$  of the correlation matrix  $R$ . Then, we regard the average mutual information  $C$  as a functional of  $\rho(\lambda)$ , and seek the eigenvalue distribution  $\rho^*(\lambda)$  which maximizes the average mutual information  $C$ . Hereafter, we consider the case of  $\beta > 1$  since optimal spreading sequences in the case of  $\beta \leq 1$  are obviously orthogonal spreading sequences. In optimizing  $C$  with respect to  $\rho(\lambda)$ , the following two constraints should be imposed on  $\rho(\lambda)$ : First, since  $\beta > 1$ , the  $K \times K$  matrix  $R$  has trivial zero eigenvalues with multiplicity  $(K - L)$ . Second, since we have normalized

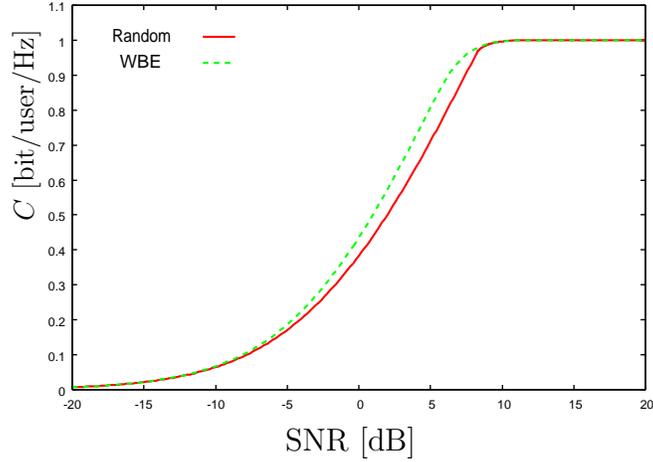


Figure 2: The average mutual information  $C$  when  $\rho^{\text{WBE}}$  (WBE) and  $\rho^{\text{MP}}$  (Random) are specified, in case of  $\beta = 1.5$ .

the power of spreading sequences as  $\sum_{\mu=1}^L (s_{\mu k}/\sqrt{L})^2 = 1, k = 1, \dots, K$ , the matrix  $S$  should satisfy

$$\text{Tr} S^T S = \sum_{k=1}^K \lambda_k = K, \quad (23)$$

where  $\{\lambda_k\}$  are the eigenvalues of  $K \times K$  matrix  $S^T S$ . In terms of  $\rho(\lambda)$ , the constraint (23) is expressed as

$$\int \lambda \rho(\lambda) d\lambda = 1. \quad (24)$$

We rewrite  $\rho(\lambda)$  in view of these constraints as

$$\rho(\lambda) = \left(1 - \frac{1}{\beta}\right) \delta(\lambda) + \frac{1}{\beta} \pi(\lambda), \quad (25)$$

where  $\pi(\lambda)$  satisfies

$$\int \pi(\lambda) d\lambda = 1, \quad (26)$$

as the normalization as a probability distribution, and

$$\int \lambda \pi(\lambda) d\lambda = \beta, \quad (27)$$

which corresponds to the normalization of the power of spreading sequences (24).

In order to discuss the extremum of  $C$  with respect to  $\rho(\lambda)$ , we consider first-order perturbations of  $C$ . Since the parameters affected by the perturbation of  $\rho(\lambda)$  are  $\{G(t), \mathcal{E}, \theta\}$ , the functional derivative of  $C$  with respect to  $\rho$  is expressed as

$$\frac{\delta C}{\delta \rho} = \frac{\delta C}{\delta G} \cdot \frac{\delta G}{\delta \rho} + \frac{\partial C}{\partial \mathcal{E}} \cdot \frac{\delta \mathcal{E}}{\delta \rho} + \frac{\partial C}{\partial \theta} \cdot \frac{\delta \theta}{\delta \rho}. \quad (28)$$

Since  $\{\mathcal{E}, \theta\}$  should satisfy the saddle-point equations (16) and (17), the derivatives of  $C$  with respect to the parameters  $\{\mathcal{E}, \theta\}$  should be zero at the saddle point. Therefore, one can safely ignore the effects of perturbations via  $\mathcal{E}$  and  $\theta$ .

Our next observation is that, if one can find an eigenvalue distribution which maximizes  $-(1/2)G(-\mathcal{E}/\sigma^2)$ , which is the only term having the first-order effect in (12), it also maximizes the average mutual information (12). We rewrite  $-G(-\mathcal{E}/\sigma^2)$  as

$$-G\left(-\frac{\mathcal{E}}{\sigma^2}\right) = -\int_0^{-\mathcal{E}/\sigma^2} \mathbf{R}(z)dz = \int_{-\mathcal{E}/\sigma^2}^0 \mathbf{R}(z)dz. \quad (29)$$

Since  $-\mathcal{E}/\sigma^2 < 0$  and  $\mathbf{R}(z) > 0$ , one can make the following statement: If there is a distribution  $\rho^*(\lambda)$  whose R-transform  $\mathbf{R}^*(z)$  satisfies

$$\mathbf{R}^*(z) \geq \mathbf{R}(z), \quad \text{for } \forall z \in (-\mathcal{E}/\sigma^2, 0), \quad (30)$$

for any R-transform  $\mathbf{R}(z)$  of the distribution  $\rho(\lambda)$  which satisfies the constraints (25)–(27),  $\rho^*(\lambda)$  also maximizes  $-G(-\mathcal{E}/\sigma^2)$ . We summarize the above arguments in the next proposition.

**Proposition 1** *If one can find an eigenvalue distribution  $\rho^*(\lambda)$  which maximizes R-transform for  $\forall z \in (-\mathcal{E}/\sigma^2, 0)$ ,  $\rho^*(\lambda)$  also maximizes the average mutual information  $C$ .*

It should be noted that the existence of  $\rho^*(\lambda)$  is not guaranteed at this stage. However, in the following, we show that there is a distribution which satisfies the condition of Proposition 1.

As a next step, we convert the optimization problem in terms of R-transform into the one in terms of Hilbert transform. Since Hilbert transform  $\mathcal{C}(\gamma)$  is a monotonically decreasing function of  $\gamma$ , and since Hilbert transform

has the relation (15) with R-transform, it follows that  $\mathbf{R}(z) + 1/z$  also decreases monotonically with respect to  $z$ . This fact leads us to the following statement: If one can find an eigenvalue distribution  $\rho^*(\lambda)$  which maximizes  $\mathcal{C}(\gamma)$  for  $\forall \gamma < \lambda_{\min}$ , and which satisfies (25)–(27),  $\rho^*(\lambda)$  also maximizes  $\mathbf{R}(z)$  for  $\forall z \in (z_{\min}, 0)$ , with

$$z_{\min} = \lim_{\gamma \rightarrow \lambda_{\min}^-} \mathcal{C}(\gamma). \quad (31)$$

Summarizing the arguments so far, we can state the next proposition.

**Proposition 2** *If one can find an eigenvalue distribution  $\rho^*(\lambda)$  whose Hilbert transform  $\mathcal{C}^*(\gamma)$  satisfies*

$$\mathcal{C}^*(\gamma) \geq \mathcal{C}(\gamma), \quad \forall \gamma < \lambda_{\min}, \quad (32)$$

*for any eigenvalue distribution  $\rho(\lambda)$  with Hilbert transform  $\mathcal{C}(\gamma)$ , which satisfies (25)–(27),  $\rho^*(\lambda)$  also maximizes the average mutual information  $C$ .*

Following the above proposition, we consider the maximization problem of the Hilbert transform for  $\gamma < \lambda_{\min}$ . Substituting (25) to (14), the Hilbert transform  $\mathcal{C}(\gamma)$  is rewritten as

$$\mathcal{C}(\gamma) = \left(1 - \frac{1}{\beta}\right) \frac{1}{\gamma} + \frac{1}{\beta} \int \frac{\pi(\lambda)}{\gamma - \lambda} d\lambda. \quad (33)$$

Since the first term, which is derived from the trivial zero eigenvalues, has no room for optimization, we maximize the second term under the constraints (26) and (27). Let us consider the following integral:

$$\int \pi(\lambda) \left( \frac{1}{\gamma - \lambda} - f(\lambda) \right) d\lambda, \quad (34)$$

where  $f(\lambda)$  is a linear function tangential to  $1/(\gamma - \lambda)$  at  $\lambda = \beta$ . Since the function  $f(\lambda)$  is a linear function, the expectation of  $f(\lambda)$  with respect to  $\pi(\lambda)$  is constant under the constraints (26) and (27). Thus, the quantities (34) and (33) are maximized by the same eigenvalue distribution. We here consider a maximization problem of the objective function (34) for  $\gamma < \lambda_{\min}$  with the constraint (26), but *without* the constraint (27). Since we have only to consider  $\lambda \in [\lambda_{\min}, \lambda_{\max}]$ , we can assume  $\lambda > \gamma$ . Since  $1/(\gamma - \lambda)$  is convex upward in  $\lambda$  for  $\lambda > \gamma$ , one has

$$\frac{1}{\gamma - \lambda} - f(\lambda) \leq 0, \quad \lambda > \gamma, \quad (35)$$

where the equality holds if and only if  $\lambda = \beta$ . Then, the objective function (34) is maximized for  $\gamma < \lambda_{\min}$  by the probability distribution

$$\pi(\lambda) = \delta(\lambda - \beta). \quad (36)$$

Since the distribution (36) incidentally satisfies the power constraint (27), the distribution (36) is also a maximizer of the objective function (34) with both of the constraints (26) and (27). Since the two functions (33) and (34) are maximized by the same probability distribution, the distribution (36) is also the optimal solution of the maximization problem of the Hilbert transform. Thus, we obtain the maximizer of the average mutual information (12). Substituting (36) to (25), one can confirm that the optimal eigenvalue distribution is the one of WBE spreading sequences  $\rho^{\text{WBE}}$ , which is given by (21).

We have so far shown that WBE spreading sequences are also asymptotically optimal in CDMA systems with a non-Gaussian input distribution in the large-system limit. This finding is an extension of the optimality result of WBE spreading sequences for Gaussian-input CDMA systems.

#### 4. Conclusion

We have demonstrated that the statistical-mechanics approach is useful not only in analyzing theoretical performance of wireless communication systems but also in providing clues to how to design them, via the problem of optimizing spreading sequences in CDMA systems. We have evaluated, via replica method, average mutual information between input and output of the system in the large-system limit, and discussed the optimization problem of the average mutual information in terms of characteristics of random spreading sequences. It has been shown that the average mutual information is maximized in the large-system limit by orthogonally-invariant random WBE spreading sequences even when the inputs are non-Gaussian. Although in this paper we have only studied a fully-synchronous CDMA model with perfect power control, one can consider the same problem in more general CDMA systems, such as the one with unequal-power users, and that is deferred to our future work.

##### A. Details of replica analysis

In this appendix, we explain how to evaluate  $\mathcal{F}$  given by (11). First, we calculate the expectation  $\mathbb{E}_{\mathbf{y}, S} \{p(\mathbf{y}|S)^n\}$  assuming that  $n$  is a non-negative

integer. Introducing replicated random vectors  $\mathbf{x}_a = [x_{a1}, \dots, x_{aK}]^T \in \mathbb{R}^K$ ,  $a = 0, \dots, n$ , which are drawn from the same probability distribution as  $\mathbf{x}$ , we rewrite  $\mathbb{E}_{\mathbf{y}, S}\{p(\mathbf{y}|S)^n\}$  as

$$\mathbb{E}_S \left\{ \int \int \prod_{a=0}^n p(\mathbf{y}|\mathbf{x}_a, S) p(\mathbf{x}_a) d\mathbf{x}_a d\mathbf{y} \right\}. \quad (37)$$

Performing the integral with respect to  $\mathbf{y}$ , we obtain

$$\begin{aligned} & \mathbb{E}_{\mathbf{y}, S}\{(p(\mathbf{y}|S))^n\} \\ &= \mathbb{E}_{\mathbf{x}_a, S} \left\{ \exp \left[ \frac{K}{2} \text{Tr} R V - \frac{L}{2} \log(n+1) - \frac{nL}{2} \log(2\pi\sigma^2) \right] \right\}. \end{aligned} \quad (38)$$

where  $K \times K$  matrix  $V$  is given by

$$V = \frac{1}{(n+1)K\sigma^2} \left( \sum_{a=0}^n \mathbf{x}_a \right) \left( \sum_{a=0}^n \mathbf{x}_a \right)^T - \frac{1}{K\sigma^2} \sum_{a=0}^n \mathbf{x}_a \mathbf{x}_a^T. \quad (39)$$

The expectation with respect to  $S$  can be performed via the so-called Itzykson-Zuber integral [14, 12] (see also [8, 15]), since  $R = S^T S$  is assumed orthogonally invariant and rank of  $V$  is at most  $(n+1)$ , as

$$\lim_{K \rightarrow \infty} \frac{1}{K} \log \mathbb{E}_S \left\{ \exp \left[ \frac{K}{2} \text{Tr} R V \right] \right\} = \frac{1}{2} \text{Tr} G(V), \quad (40)$$

where  $G(x)$  is the function defined in (13). Thus, we obtain the following equation, ignoring vanishing terms in the large-system limit,

$$\begin{aligned} & \mathbb{E}_{\mathbf{y}, S}\{(p(\mathbf{y}|S))^n\} \\ &= \mathbb{E}_{\{\mathbf{x}_a\}} \left\{ \exp \left[ \frac{K}{2} \text{Tr} G(V) - \frac{L}{2} \log(n+1) - \frac{nL}{2} \log(2\pi\sigma^2) \right] \right\}. \end{aligned} \quad (41)$$

We next take expectation of (41) with respect to  $\{\mathbf{x}_a\}$ . Since eigenvalues of the matrix  $V$  are functions of  $\{\mathbf{x}_a\}$  only through their inner products  $\mathbf{x}_a \cdot \mathbf{x}_b$ ,  $a, b = 0, \dots, n$ , we rewrite the expectation with respect to  $\{\mathbf{x}_a\}$  into the one with respect to the  $(n+1) \times (n+1)$  matrix

$$Q = (Q_{ab}), \quad Q_{ab} = \frac{1}{K} \sum_{k=1}^K x_{ak} x_{bk}, \quad (42)$$

as

$$\int \exp[K\mathcal{G}(Q)]\mu_K(Q)dQ, \quad (43)$$

where  $K\mathcal{G}(Q)$  is the exponent of (41),

$$\mathcal{G}(Q) = \left[ \frac{1}{2} \text{Tr}G(V) \right] (Q) - \frac{1}{2\beta} \log(n+1) - \frac{n}{2\beta} \log(2\pi\sigma^2), \quad (44)$$

and where  $\mu_K$  is the following measure

$$\mu_K(Q) = \mathbb{E}_{\{x_a\}} \left\{ \prod_{0 \leq a < b}^n \delta \left( \sum_{k=1}^K x_{ak}x_{bk} - KQ_{ab} \right) \right\}. \quad (45)$$

Utilizing the saddle-point method [3, 4], we evaluate (43) in the limit  $K \rightarrow \infty$  as

$$\lim_{K \rightarrow \infty} \frac{1}{K} \log \mathbb{E}\{(p(\mathbf{y}|S))^n\} = \sup_Q \{\mathcal{G}(Q) - \mathcal{I}(Q)\}, \quad (46)$$

where  $\mathcal{I}(Q)$  is the rate function of the empirical means (42), defined via a Legendre transform as

$$\mathcal{I}(Q) = \sup_{\tilde{Q}} \left[ \sum_{0 \leq a < b} Q_{ab} \tilde{Q}_{ab} - \log M(\tilde{Q}) \right], \quad (47)$$

where  $\tilde{Q} = (\tilde{Q}_{ab})$  is an  $(n+1) \times (n+1)$  symmetric matrix. The cumulant generating function  $\log M(\tilde{Q})$  of  $\{x_a\}$  is defined as

$$\log M(\tilde{Q}) = \log \mathbb{E}_{\{x_a\}} \left\{ \exp \left[ \sum_{0 \leq a < b} \tilde{Q}_{ab} x_a x_b \right] \right\}. \quad (48)$$

In order to proceed further, we assume the so-called *replica symmetry*: We assume that the extremum of (46) is invariant under exchanges of the replica indexes. Under the assumption of replica symmetry, we introduce new parameters,

$$Q_{aa} = p, \quad Q_{ab} = q, \quad a \neq b. \quad (49)$$

Using these parameters, the eigenvalues of  $V$  are expressed as

$$\lambda_1 = -\frac{p-q}{\sigma^2}, \quad (50)$$

$$\lambda_2 = 0, \quad (51)$$

whose multiplicities are  $n$  and  $(K - n)$ , respectively. Since  $G(x)$  is an analytic function and  $G(0) = 0$ , we can express  $\mathcal{G}(Q)$  as

$$\mathcal{G}(Q) = \frac{n}{2}G\left(-\frac{p-q}{\sigma^2}\right) - \frac{1}{2\beta}\log(n+1) - \frac{n}{2\beta}\log(2\pi\sigma^2). \quad (52)$$

We also apply the assumption of replica symmetry to  $\tilde{Q}$  as

$$\tilde{Q}_{aa} = c, \quad \tilde{Q}_{ab} = \theta, \quad a \neq b, \quad (53)$$

and rewrite the rate function  $\mathcal{I}(Q)$  as

$$\mathcal{I}(Q) = \sup_{\tilde{Q}} \left[ (n+1)cp + \frac{n(n+1)}{2}\theta q - \log \mathbb{E}_{\{x_a\}} \left\{ \exp \left[ c \sum_{a=0}^n x_a + \theta \sum_{0 \leq a < b} x_a x_b \right] \right\} \right]. \quad (54)$$

Deriving the extremum condition of (46) with respect to  $p$  and  $q$  in the limit  $n \rightarrow 0$ , we obtain the following saddle-point equations,

$$c = 0, \quad (55)$$

$$\theta = \frac{1}{\sigma^2} \mathbf{R}\left(-\frac{p-q}{\sigma^2}\right). \quad (56)$$

Similarly, as the extremum condition of (46), we obtain the following saddle-point equation,

$$p - q = \mathbb{E}\{(x - \langle x \rangle)^2; \theta\}, \quad (57)$$

where  $x$  follows the probability distribution  $p(x)$ , and where  $\langle x \rangle$  is the posterior mean estimate of channel input  $x$  given output  $u$  in a single-user AWGN channel whose variance is  $1/\theta$  and whose input and output are  $x$  and  $u$ , respectively. Introducing the posterior variance  $\mathcal{E} \equiv p - q$ , we obtain the saddle-point equations (16) and (17). In order to obtain  $\mathcal{F}$ , we differentiate  $\log \mathbb{E}\{(p(\mathbf{y}|S))^n\}$ , which is obtained by substituting (52) and (54) to (46), with respect to  $n$ , and then take the limit  $n \rightarrow 0$ . Finally, we obtain the representation of  $\mathcal{F}$  as

$$\mathcal{F} = -\frac{1}{2}\theta\mathcal{E} - \frac{1}{2}G\left(-\frac{\mathcal{E}}{\sigma^2}\right) - \frac{1}{2}\log\frac{2\pi}{\theta} - \frac{1}{2} - \int p(u; \theta) \log p(u; \theta) du + \frac{1}{2\beta}(1 + \log(2\pi\sigma^2)). \quad (58)$$

Substituting (58) to (7), we obtain the average mutual information (12).

### Acknowledgment

Support from the Grant-in-Aid for Scientific Research on Priority Areas, the Ministry of Education, Culture, Sports, Science and Technology, Japan (no. 18079010) is acknowledged.

### References

- [1] A. J. Viterbi, CDMA: Principles of spread spectrum communication, Addison-Wesley, 1995.
- [2] S. Verdú, Multiuser Detection, Cambridge University Press, 1998.
- [3] T. Tanaka, A statistical-mechanics approach to large-system analysis of CDMA multiuser detectors, *IEEE Trans. Info. Theory* 48 (2002) 2888–2910.
- [4] D. Guo, S. Verdú, Randomly spread CDMA: Asymptotics via statistical physics, *IEEE Trans. Info. Theory* 51 (2005) 1983–2010.
- [5] M. Rupf, J. L. Massey, Optimum sequence multisets for synchronous code-division multiple-access channels, *IEEE Trans. Info. Theory* 40 (1994) 1261–1266.
- [6] P. Viswanath, V. Anantharam, Optimal sequences and sum capacity of synchronous CDMA systems, *IEEE Trans. Info. Theory* 45 (1999) 1984–1991.
- [7] J. Luo, S. Ulukus, A. Ephremides, Optimal sequences and sum capacity of symbol asynchronous CDMA systems, *IEEE Trans. Info. Theory* 51 (2005) 2760–2769.
- [8] K. Takeda, S. Uda, Y. Kabashima, Analysis of CDMA systems that are characterized by eigenvalue spectrum, *Europhys. Lett.* 76 (2006) 1193–1199.
- [9] K. Kitagawa, T. Tanaka, Optimal spreading sequences in large CDMA systems: A statistical mechanics approach, in: *IEEE Int. Symp. Info. Theory*, Tronto, 2008, pp. 1373–1377.

- [10] J. L. Massey, T. Mittelholzer, Welch's bound and sequence sets for code-division multiple-access systems, in: R. Capocelli, A. D. Santis, U. Vaccaro (Eds.), *Sequences II*, Methods in Communication, Security, and Computer Science, Springer-Verlag, 1993, pp. 53–78.
- [11] P. Viswanath, V. Anantharam, D. N. C. Tse, Optimal sequences, power control, and user capacity of synchronous CDMA systems with linear MMSE multiuser receivers, *IEEE Trans. Info. Theory* 45 (1999) 1968–1983.
- [12] A. Guionnet, M. Maïda, A fourier view on the  $R$ -transform and related asymptotics of spherical integrals, *Journal of Functional Analysis* 222 (2005) 435–490.
- [13] A. M. Tulino, S. Verdú, *Random Matrix Theory and Wireless Communications*, now Publishers, 2004.
- [14] C. Itzykson, J.-B. Zuber, The planar approximation, II, *Journal of Mathematical Physics* 21 (3) (1980) 411–421.
- [15] T. Tanaka, Asymptotics of Harish-Chandra-Itzykson-Zuber integrals and free probability theory, *Journal of Physics: Conference Series* 95 (2008) 012002–1–9.