(オンライン)ISSN 2432-1036
(冊子版)ISSN 0286-116X

都城工業高等専門学校

研　究　報　告

第 57 号

令和 5 (2023)年 1 月

目　　次

研究論文編

****

研　究　論　文　編

On p-adic Dedekind-Rademacher sums attached to Dirichlet characters

KOZUKA Kazuhito[1]

(Accepted September 30, 2022)

Abstract The purpose of this paper is to generalize the author's preceding work on the construction of a p-adic analytic function interpolating the Dedekind sums attached to Dirichlet characters and the calculation of the radius of convergence of the function We define the generalized Dedekind-Rademacher sums by making use of Dirichlet characters and deduce an expression of the sums by the generalized Euler numbers. Applying the expression, we construct a p-adic analytic function interpolating the generalized Dedekind-Rademacher sums. The function is expressed as a linear combination of some p-adic functions interpolating the Euler numbers. The main result is the explicit expression of the radius of convergence of the function. Except for some special cases, the result is an analogue to the one for the Kubota-Leopoldt p-adic L-function, which interpolates the generalized Bernoulli numbers p-adically and plays an important role in the Iwasawa theory for cyclotomic fields.

Keywords [p-adic interpolation, Dedekind sums, Dirichlet character]

1 Introduction

For any real number x, we denote by $[x]$ the greatest integer not exceeding x, put $\{x\} = x - [x]$ and define

$$((x)) = \begin{cases} \{x\} - \frac{1}{2} & \text{if } x \text{ is not an integer.} \\ 0 & \text{if } x \text{ is an integer.} \end{cases}$$

For positive integers h and k, the classical Dedekind sum $s(h,k)$ is defined by

$$s(h,k) = \sum_{\lambda \bmod k} \left(\left(\frac{\lambda}{k}\right)\right)\left(\left(\frac{h\lambda}{k}\right)\right). \tag{1}$$

The sum first appeared in Dedekind's study on the transformation properties of the η-function ($\eta(z) = e^{\pi iz/12}\prod_{n\geq 1}(1-e^{2\pi inz})$) under the modular group and in the case of $\gcd\{h,k\} = 1$ Dedekind showed the following reciprocity formula[1)]:

$$12hk\{s(h,k) + s(k,h)\} = h^2 - 3hk + k^2 + 1. \tag{2}$$

Generalizations of Dedekind sums and their reciprocity formulas have been studied extensively with many methods.

For each non-negative integer n, let B_n and $B_n(X)$ be the nth Bernoulli number and polynomial respectively, and define

$$\tilde{B}_n(x) = B_n(\{x\}).$$

1 Department of General Education, National Institute of Technology(KOSEN), Miyakonojo College

As a generalization of $s(h,k)$, Apostol defined the nth higher-order Dedekind sum as

$$s_n(h,k)=\sum_{\lambda \bmod k}\tilde{B}_1\Big(\frac{\lambda}{k}\Big)\tilde{B}_n\Big(\frac{h\lambda}{k}\Big) \tag{3}$$

and he generalized the formula (2) as

$$(n+1)\left(hk^n s_n(h,k)+h^n k s_n(k,h)\right)=nB_{n+1}+\sum_{j=0}^{n+1}\binom{n+1}{j}(-k)^{n+1-j}h^j B_{n+1-j}B_j \tag{4}$$

for positive integers h and k with $\gcd\{h,\,k\}=1$ and odd n.

As a natural generalization of (3), we can define

$$s_{m,n}(h,k)=\sum_{\lambda \bmod k}\tilde{B}_m\Big(\frac{\lambda}{k}\Big)\tilde{B}_n\Big(\frac{h\lambda}{k}\Big) \tag{5}$$

for non-negative integers m and n. Further for real numbers α and β, we extend the sum (5) as

$$S_{m,n}\begin{pmatrix}h & k\\ \alpha & \beta\end{pmatrix}=\sum_{\lambda \bmod k}\tilde{B}_m\left(\frac{\lambda+\beta}{k}\right)\tilde{B}_n\left(\frac{h(\lambda+\beta)}{k}-\alpha\right), \tag{6}$$

which is often called the Dedekind-Rademacher sum. The reciprocity formula for (6) is studied by Rademacher and Carlitz[3~5].

In addition to the reciprocity formulas, Rosen and Snyder constructed a p-adic interpolating function for the sums (3)[6]. The function is an analogue of the well known Kubota-Leopoldt p-adic L-function which interpolates the generalized Bernoulli numbers and plays an important role in the Iwasawa theory for cyclotomic fields. Later, Snyder generalized the construction slightly and deduced a p-adic version of the reciprocity formula (4)[7]. Further Kudo constructed a p-adic interpolating function for the sums (5) and deduced many properties[8,9]. For the p-adic function constructed by Kudo, the author studied the explicit value of the radius of convergence [10]. Besides, by generalizing the sums (5) by means of Dirichlet characters, the author constructed a p-adic interpolating function for the sums and deduced the value of the radius of convergence[11].

The purpose of this paper is to extend the study of the paper[11]. We generalize the sums (6) by Dirichlet characters, construct a p-adic interpolating function and deduce the value of the radius of convergence.

Throughout the paper, we denote by $\mathbf{Q}$, $\mathbf{Z}$ and $\mathbf{N}$, the rational number field, the ring of integers of $\mathbf{Q}$ and the set of positive integers, respectively as usual, and denote the set of non-negative integers by $\bar{\mathbf{N}}$.

2 Definition of Dedekind sums attached to Dirichlet characters

As in the introduction, let B_n and $B_n(X)$ be the nth Bernoulli numbers and polynomial, respectively, defined by

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}B_n\frac{t^n}{n!}\ \text{ and }\ \frac{te^{tX}}{e^t-1}=\sum_{n=0}^{\infty}B_n(X)\frac{t^n}{n!}$$

and define $\tilde{B}_n(x)=B_n(\{x\})$.

For any primitive Dirichlet character χ, we denote by f_χ the conductor of χ and denote by I_χ the ring of rational numbers of which the denominators are relatively prime to f_χ. For any $x\in I_\chi$ we can define the value $\chi(x)$ by multiplicativity. We define the twisted Bernoulli function $\tilde{B}_{n,\chi}(x)$ attached to χ by

$$\sum_{\rho=0}^{f_\chi-1}\frac{\chi(\{x\}+\rho)te^{(\{x\}+\rho)t}}{e^{f_\chi t}-1}=\sum_{n=0}^{\infty}\tilde{B}_{n,\chi}(x)\frac{t^n}{n!}$$

or equivalently

$$\tilde{B}_{n,\chi}(x) = f_\chi^{n-1} \sum_{\rho \bmod f_\chi} \chi(x+\rho)\tilde{B}_n\left(\frac{x+\rho}{f_\chi}\right).$$

Let χ and ψ be primitive Dirichlet characters, $m, n \in \bar{\mathbf{N}}$, $h, k \in \mathbf{N}$ and $\alpha, \beta \in I_\chi \cap I_\psi$. We define the generalized Dedekind sums attached to χ and ψ by

$$S_{(m,\chi),(n,\psi)}\begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix} = \sum_{\lambda \bmod k} \tilde{B}_{m,\chi}\left(\frac{\lambda+\beta}{k}\right)\tilde{B}_{n,\psi}\left(\frac{h(\lambda+\beta)}{k} - \alpha\right). \tag{7}$$

3 Expression by Euler numbers

For a parameter u, we define the n th modified Euler numbers $E_n(u)$ for $n \in \mathbf{Z}$ with $n \geq -1$ by[9)]

$$\frac{u}{e^t - u} = \frac{E_{-1}(u)}{t} + \sum_{n=0}^{\infty} E_n(u)\frac{t^n}{n!}.$$

Note that $E_{-1}(u) \neq 0$ only if $u = 1$. We put $\tilde{n} = \max\{n, 1\}$ for $n \in \bar{\mathbf{N}}$. Then we have $\tilde{n}E_{n-1}(1) = B_n$ for $n \in \bar{\mathbf{N}}$. It is known that for any $\lambda \in \mathbf{Z}, c, k, n \in \mathbf{N}$ and for any kth root of unity ξ, we have[12)]

$$k^n\tilde{B}_n\left(\frac{\lambda}{k}\right) = \tilde{n}\sum_{\zeta^k=1} E_{n-1}(\zeta)\zeta^\lambda, \tag{8}$$

$$\tilde{n}E_{n-1}(\xi) = k^{n-1}\sum_{j \bmod k} \tilde{B}_n\left(\frac{j}{k}\right)\xi^{-j} \tag{9}$$

and

$$\sum_{\eta^c=1} E_n(u\eta) = c^{n+1}E_n(u^c). \tag{10}$$

For a primitive Dirichlet character χ, we define the numbers $E_{n,\chi}(u)$ (a modification of the generalized Euler number[13)]) by

$$\sum_{\rho=0}^{f_\chi-1} \frac{\chi(\rho)u^{f_\chi-\rho}e^{\rho t}}{e^{f_\chi t} - u^{f_\chi}} = \frac{E_{-1,\chi}(u)}{t} + \sum_{n=0}^{\infty} E_{n,\chi}(u)\frac{t^n}{n!}.$$

Note that $E_{-1,\chi}(u) \neq 0$ only if u is a primitive f_χth root of unity. Note also that $\tilde{n}E_{n-1,\chi}(1) = B_{n,\chi}$ for $n \in \bar{\mathbf{N}}$. Let ζ_χ be an arbitrarily chosen primitive f_χth root of unity and put $\tau(\chi, \zeta_\chi) = \sum_{\rho=0}^{f_\chi-1} \chi(\rho){\zeta_\chi}^\rho$, the Gauss sum attached to χ and ζ_χ. Then

$$\sum_{\rho=0}^{f_\chi-1} \frac{\chi(\rho)u^{f_\chi-\rho}e^{it}}{e^{f_\chi t} - u^{f_\chi}} = \frac{\tau(\chi, \zeta_\chi)}{f_\chi}\sum_{\rho=0}^{f_\chi-1} \frac{\chi^{-1}(\rho){\zeta_\chi}^\rho u}{e^t - {\zeta_\chi}^\rho u},$$

which implies,

$$E_{n,\chi}(u) = \frac{\tau(\chi, \zeta_\chi)}{f_\chi}\sum_{\rho \bmod f_\chi} \chi^{-1}(\rho)E_n\big({\zeta_\chi}^\rho u\big). \tag{11}$$

Hence if $\gcd\{k, f_\chi\} = 1$, as generalizations of (8), (9) and (10), we deduce that

$$\chi(k)k^n\tilde{B}_{n,\chi}\left(\frac{\lambda}{k}\right) = \tilde{n}\sum_{\zeta^k=1} E_{n-1,\chi}(\zeta)\zeta^\lambda, \tag{12}$$

$$\tilde{n}E_{n-1,\chi}(\xi) = \chi(k)k^{n-1}\sum_{j \bmod k} \tilde{B}_{n,\chi}\left(\frac{j}{k}\right)\xi^{-j} \tag{13}$$

and

$$\sum_{\eta^c=1} E_{n,\chi}(u\eta) = \chi(c)c^{n+1}E_{n,\chi}(u^c). \tag{14}$$

For $g \in \mathbf{N}$, let $J(g)$ denote an arbitrarily fixed complete set of representatives of the residue class group $\mathbf{Z}/g\mathbf{Z}$. For $g_1, \cdots g_m$, we put $J(g_1, \cdots, g_m) = J(g_1) \times \cdots \times J(g_m)$. For $c \in \mathbf{N}$ with $c > 1$, we denote by $\mathcal{V}_c$ the set of non-trivial cth roots of unity. As for the expression of the sums (7) by the Euler numbers, we have the following.

Proposition 3.1. *Let χ and ψ be primitive Dirichlet characters and let $h, k \in \mathbf{N}$. Let $\alpha, \beta \in I_\chi \cap I_\psi$ and express $\alpha = a/d$ and $\beta = b/d$ with $d \in \mathbf{N}, a, b \in \mathbf{Z}$. We suppose that $\gcd\{h, k\} = \gcd\{kd, f_\chi f_\psi\} = 1$. Let ζ_{kd} denote an arbitrarily chosen primitive kdth root of unity and put $\zeta_k = \zeta_{kd}^d$ and $\zeta_d = \zeta_{kd}^k$. Then we have*

$$(\chi\psi)(kd)(kd)^{m+n}S_{(m,\chi),(n,\psi)}\begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix} = \tilde{m}\tilde{n}\frac{\tau(\psi,\zeta_\psi)}{f_\psi} \times \sum_{(i,j_1,j_2,\rho)\in J(k,d,d,f_\psi)} \psi^{-1}(\rho)E_{m-1,\chi}(\zeta_{kd}^{-hi+kj_1})E_{n-1}(\zeta_\psi^\rho\zeta_{kd}^{i+kj_2})\zeta_{kd}^{bj_1-ai+j_2(hb-ka)}. \tag{15}$$

Further if $c \in \mathbf{N}$ with $c \equiv 1 \pmod{f_\psi kd}$ and $c > 1$, then

$$(c^n-1)(\chi\psi)(kd)(kd)^{m+n}S_{(m,\chi),(n,\psi)}\begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix} = \tilde{m}\tilde{n}\frac{\tau(\psi,\zeta_\psi)}{f_\psi} \times \sum_{(i,j_1,j_2,\rho)\in J(k,d,d,f_\psi)}\sum_{\eta\in\mathcal{V}_c} \psi^{-1}(\rho)E_{m-1,\chi}(\zeta_{kd}^{-hi+kj_1})E_{n-1}(\zeta_\psi^\rho\zeta_{kd}^{i+kj_2}\eta)\zeta_{kd}^{bj_1-ai+j_2(hb-ka)}. \tag{16}$$

Proof. We see from (12) that

$$\begin{aligned}\chi(kd)(kd)^m\tilde{B}_{m,\chi}\left(\frac{\lambda+\beta}{k}\right) &= \chi(kd)(kd)^m\tilde{B}_{m,\chi}\left(\frac{\lambda d+b}{kd}\right)\\ &= \tilde{m}\sum_{(i_1,j_1)\in J(k,d)} E_{m-1,\chi}(\zeta_{kd}^{-hi_1+kj_1})\zeta_{kd}^{(-hi_1+kj_1)(\lambda d+k)}\end{aligned}$$

and

$$\begin{aligned}\psi(kd)(kd)^n\tilde{B}_{m,\psi}\left(\frac{h(\lambda+\beta)}{k}-\alpha\right) &= \psi(kd)(kd)^n\tilde{B}_{n,\psi}\left(\frac{h\lambda d+hb-ka}{kd}\right)\\ &= \tilde{n}\sum_{(i_2,j_2)\in J(k,d)} E_{n-1,\psi}(\zeta_{kd}^{i_2+kj_2})\zeta_{kd}^{(i_2+kj_2)(h(\lambda d+b)-ka)}.\end{aligned}$$

Note that for $i_1, i_2 \in J(k)$ we have $\sum_{\lambda\in J(k)}\zeta_{kd}^{h(-i_1+i_2)(\lambda d+b)} = k$ or 0 according as $i_1 = i_2$ or $i_1 \neq i_2$. Hence by (7) and (11), we obtain (15). In addition, applying (14), we also obtain (16).

4 p-adic interpolation

Let p be a prime number. If $p \geq 3$, we put $e_o = p-1$ and $q = p$. If $p = 2$, we put $e_0 = 2$ and $q = 4$. In this section we construct a p-adic interpolating function for the sums (7).

As usual, we denote by $\mathbf{Q}_p$, $\mathbf{Z}_p$ and $\mathbf{C}_p$ the rational p-adic number field, the ring of integers of $\mathbf{Q}_p$ and the completion of the algebraic closure of $\mathbf{Q}_p$, respectively. Let $|\ \ |_p$ denote the p-adic valuation of $\mathbf{C}_p$ normalized by $|p|_p = 1/p$. For any $u \in {\mathbf{C}_p}^\times$ with $|1-u^p|_p \geq 1$, the Koblitz measure $\mathcal{M}_u$ on $\mathbf{Z}_p$ is defined by

$$\mathcal{M}_u\big(\nu + p^n\mathbf{Z}_p\big) = \frac{u^{p^n-\nu}}{1-u^{p^n}}$$

for any $n, \nu \in \bar{\mathbf{N}}$ with $0 \le \nu \le p^n - 1$ and we have

$$\int_{\mathbf{Z}_p} x^n \, d\mathcal{M}_u(x) = E_n(u) \quad \text{and} \quad \int_{\mathbf{Z}_p^\times} x^n \, d\mathcal{M}_u(x) = E_n(u) - p^n E_n(u^p).$$

Let ω_p denote the Teichmüller character for p and put $\langle x \rangle = x/\omega_p(x)$ for $x \in \mathbf{Z}_p^\times$. We put

$$G_p(s,u) = \int_{\mathbf{Z}_p^\times} \langle x \rangle^s d\mathcal{M}_u(x) \ \text{ for } \ s \in \mathbf{Z}_p, \tag{17}$$

which is the p-adic Γ-transform for the measure $\mathcal{M}_u$ and satisfies an interpolating property such as

$$G_p(n,u) = E_{n,\omega_p^{-n}}(u) - p^n E_{n,\omega_p^{-n}}(u^p) \tag{18}$$

for $n \in \bar{\mathbf{N}}$.

As in Proposition 3.1, let χ and ψ be primitive Dirichlet characters and let $h, k \in \mathbf{N}$. Let $\alpha, \beta \in I_\chi \cap I_\psi$ and express $\alpha = a/d$ and $\beta = b/d$ with $d \in \mathbf{N}, a, b \in \mathbf{Z}$. We suppose that $\gcd\{h,k\} = \gcd\{kd, f_\chi f_\psi\} = \gcd\{p, kdf_\chi f_\psi\} = 1$. In addition, we choose and fix integers $c, p' \in \mathbf{N}$ with $c \equiv 1 \pmod{qkdf_\psi}$, $c > 1$ and $pp' \equiv 1 \pmod{kdf_\psi}$. For each $m \in \bar{\mathbf{N}}$, we set

$$T_{p,m}^c\left(s,\chi,\psi : \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right) = \tilde{m}k\frac{\tau(\psi,\zeta_\psi)}{f_\psi} \times \sum_{(i,j_1,j_2)\in J(k,d,d)} \sum_{\eta\in\mathcal{V}_c} E_{m-1,\chi}(\zeta_{kd}^{-h_i+kj_1})\zeta_d^{bj_1-ai+j_2(hb-ka)} G_p(s, \zeta_{kd}^{i+kj_2}\eta). \tag{19}$$

Then by Proposition 3.1 and (18), we deduce that

$$T_{p,m}^c\left(n-1,\chi,\psi : \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right) = \tilde{m}\tilde{n}k(c^n-1)(\chi\psi)(kd)(kd)^{m+n} \times \left(S_{(m,\chi),(n,\psi)}\begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix} - \psi^{-1}p^n S_{(m,\chi),(n,\psi)}\begin{pmatrix} p'h & k \\ p'\alpha & \beta \end{pmatrix}\right)$$

for any $n \in \mathbf{N}$ with $n \equiv 1 \pmod{e_0}$. Now we define

$$S_{p,m}\left(s,\chi,\psi : \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right) = \frac{1}{\tilde{m}k(c^s-1)(\chi\psi)(kd)(kd)^m d^{<d>^s}} T_{p,m}^c\left(s,\chi,\psi : \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right), \tag{20}$$

which is independent of the choice of c. Then we obtain the following.

THEOREM 4.1. *We have the interpolating property such as*

$$S_{p,m}\left(n-1,\chi,\psi : \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right) = \tilde{n}k^n\left(S_{(m,\chi),(n,\psi)}\begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix} - \psi^{-1}(p)p^n S_{(m,\chi),(n,\psi)}\begin{pmatrix} p'h & k \\ p'\alpha & \beta \end{pmatrix}\right)$$

for any $n \in \mathbf{N}$ with $n \equiv 1 \pmod{e_0}$.

5 Radius of convergence

By (17), the function $G_p(s,u)$ is expanded at any $s_0 \in \mathbf{Z}_p$ as

$$G_p(s,u) = \sum_{n=0}^{\infty} c_{n,u,s_0}(s-s_0)^n \tag{21}$$

with

$$c_{n,u,s_0} = \frac{1}{n!}\int_{\mathbf{Z}_p^\times} (\log_p < x >)^n < x >^{s_0} \, d\mathcal{M}_u(x).$$

Hence we can enlarge the domain of definition of the function $G_p(s,u)$ from $\mathbf{Z}_p$ to the set of $s \in \mathbf{C}_p$ for which the right-hand side of (21) converges. For the same reason, the domain of definition of the function $S_{p,m}\left(s,\chi,\psi : \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right)$ can be enlarged. Let $r_m(\chi,\psi,h,k,\alpha,\beta : s_0)$ denote the radius of convergence of the expansion of $S_{p,m}\left(s,\chi,\psi : \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right)$ at $s_0 \in \mathbf{Z}_p$. In order to study the value, we first recall the main result of Section 3 of the paper[10].

Let $\mathcal{I}$ be a finite set and consider functions

$$U : \mathcal{I} \to \mathbf{C}_p^\times \text{ and } \mathcal{A} : \mathcal{I} \to \mathbf{C}_p^\times.$$

For each $i \in \mathcal{I}$, put $U(i) = u_i$ and $\mathcal{A}(i) = \alpha_i$ and suppose that $|1 - u_i^p|_p \geq 1$ for all $i \in \mathcal{I}$. We put

$$G_p(s : U, \mathcal{A}) = \sum_{i \in I} \alpha_i G_p(s, u_i)$$

and denote by $r(U, \mathcal{A} : s_0)$ the radius of convergence of $G_p(s : U, \mathcal{A})$ at $s_0 \in \mathbf{Z}_p$. Let $\mathcal{I}_+ = \{i \in \mathcal{I} | |u_i|_p < 1\}$, $\mathcal{I}_- = \{i \in \mathcal{I} | |u_i|_p > 1\}$ and $\mathcal{I}_0 = \{i \in \mathcal{I} | |u_i|_p = 1\}$. For each $n \in \mathbf{N}$, we put

$$\mathcal{N}_n = \{\mu \in \mathbf{N} | \gcd\{\mu, p\} = 1, | < \mu > -1|_p = |q|_p |p|_p^{n-1}\}.$$

If there exists an integer $n \in \mathbf{N}$ such that either

$$\sum_{i \in \mathcal{I}_+} \alpha_i u_i^\mu - \sum_{i \in \mathcal{I}_-} \alpha_i u_i^{-\mu} \neq 0 \text{ or } \sum_{i \in \mathcal{I}_0} \alpha_i (u_i^\mu - u_i^{-|\mu}) \neq 0$$

holds for some $\mu \in \mathcal{N}_n$, we denote the minimum of such n by $n(U, \mathcal{A})$. Otherwise we put $n(U, \mathcal{A}) = \infty$. Then we have[10]

$$r(U, \mathcal{A} : s_0) = \begin{cases} |p|_p^{\frac{1}{p-1} - n(U,\mathcal{A}) + 1} |q|_p^{-1} & \text{if } n(U, \mathcal{A}) \neq \infty. \\ \infty & \text{if } n(U, \mathcal{A}) = \infty. \end{cases} \tag{22}$$

Now we put $r\left(S_{p,m}\left(s;\chi,\psi\begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right) : s_0\right) = r_m(\chi,\psi,h,k,\alpha,\beta : s_0)$ for $s_0 \in \mathbf{Z}_p$. Further, we introduce following subsets of $\mathbf{Q}$:

$$\mathcal{B}_{m,\chi} = \{x \in \mathbf{Q} | \tilde{B}_{m,\chi}(x) = 0\} \text{ and } \mathcal{C}_{m,\chi}(\varepsilon, A) = \{x \in \mathbf{Q} | \tilde{B}_{m,\chi}(A + x) - \varepsilon \tilde{B}_{m,\chi}(A - x) = 0\} \text{ for } A \in \mathbf{Q}.$$

The main result is the following.

THEOREM 5.1. *Let $h' \in \mathbf{Z}$ be an arbitrary integer such that $hh' \equiv 1 \pmod{k}$.*
(1) *If $2(h\beta - k\alpha) \notin \mathbf{Z}$, then*

$$r_m(\chi,\psi,h,k,\alpha,\beta : s_0) = \begin{cases} |p|_p^{\frac{1}{p-1}} |q|_p^{-1} & \text{if } \dfrac{\lambda + \beta}{k} \notin \mathcal{B}_{n,\chi} \text{ for some } \lambda \in \mathbf{Z}. \\ \infty & \text{otherwise.} \end{cases}$$

(2) If $2(h\beta - k\alpha) \in \mathbf{Z}$, then

$$r_m(\chi,\psi,h,k,\alpha,\beta : s_0) = \begin{cases} |p|_p^{\frac{1}{p-1}} |q|_p^{-1} & \text{if } \dfrac{-h'(h\beta - k\alpha) + \lambda}{k} \notin \mathcal{C}_{n,\chi}\left(\psi(-1), \dfrac{\beta - h'(h\beta - k\alpha)}{k}\right) \text{ for some } \lambda \in \mathbf{Z}. \\ \infty & \text{otherwise.} \end{cases}$$

Proof. By (19) and (20), it is sufficient to prove the assertion for $T^c_{p,m}\left(s,\chi,\psi:\begin{pmatrix}h & k\\ \alpha & \beta\end{pmatrix}\right)$ instead of $S_{p,m}\left(s,\chi,\psi:\begin{pmatrix}h & k\\ \alpha & \beta\end{pmatrix}\right)$. We put $\mathcal{I}=J(f_\psi)\times J(k)\times J(d)\times\mathcal{V}_c$. For each $(\rho,i,j_2,\eta)\in\mathcal{I}$, we put

$$u(\rho,i,j_2,\eta)=\zeta_\psi^\rho\zeta_{kd}^{i+kj_2}\eta \text{ and } \alpha(\rho,i,j_2,\eta)=\sum_{j_1\in J(d)}\psi^{-1}(\rho)E_{m-1,\chi}(\zeta_{kd}^{-hi+kj_1})\zeta_d^{bj_1-ai+j_2(hb-ka)}.$$

Then by (19), we see that

$$T^c_{p,m}\left(s;\chi,\psi\begin{pmatrix}h & k\\ \alpha & \beta\end{pmatrix}\right)=\sum_{(\rho,i,j_2,\eta)\in I}\alpha(\rho,i,j_2,\eta)G_p(s,u(\rho,i,j_2,\eta)).$$

Note that $|u(\rho,i,j_2,\eta)|_p=1$ for all $(\rho,i,j_2,\eta)\in\mathcal{I}$. For $\mu\in\mathbf{N}$, we put

$$\begin{aligned}\mathcal{F}(\mu) &= \sum_{(\rho,i,j_2,\eta)\in\mathcal{I}}\alpha(\rho,i,j_2,\eta)(u(\rho,i,j_2,\eta)^\mu-u(\rho,i,j_2,\eta)^{-\mu})\\ &= \sum_{(\rho,i,j_2,\eta)\in\mathcal{I}}\sum_{j_1\in J(d)}\psi^{-1}(\rho)E_{m-1,\chi}(\zeta_{kd}^{-hi+kd})\zeta_d^{bj_1-ai+j_2(hb-ka)}\\ &\qquad\times((\zeta_\psi^\rho\zeta_{kd}^{i+kj_2}\eta)^\mu-(\zeta_\psi^\rho\zeta_{kd}^{i+kj_2}\eta)^{-\mu}).\end{aligned}$$

Note that $\sum_{\rho\in J(f_\psi)}\psi^{-1}(\rho)\zeta_\psi^{\pm\rho\mu}=\psi(\pm\mu)\tau(\psi^{-1},\zeta_\psi)$. For any $x\in\mathbf{Q}$, put $\Phi(x)=1$ or $\Phi(x)=0$ according as $x\in\mathbf{Z}$ or $x\notin\mathbf{Z}$. Then

$$\sum_{\eta\in\mathcal{J}_c}\eta^{\pm\mu}=\Phi\left(\frac{\mu}{c}\right)c-1 \text{ and } \sum_{j_2\in J(d)}\zeta_d^{j_2(hb-ka)}\zeta_{kd}^{\pm kj_2\mu}=\Phi\left(\frac{hb-ka\pm\mu}{d}\right)d.$$

Further for any $r_1,r_2\in\mathbf{C}_p$, let us write $r_1\sim r_2$ if $r_1=r_2r$ for some $r\in\mathbf{C}_p^\times$. Then we can express

$$\begin{aligned}\mathcal{F}(\mu)\sim\psi(\mu)\sum_{(i,j_1)\in J(k)\times J(d)}&E_{m-1,\chi}(\zeta_{kd}^{-hi+kj_1})\\ &\times\zeta_d^{bj_1-ai}\left(\zeta_{kd}^{i\mu}\Phi\left(\frac{hb-ka+\mu}{d}\right)-\psi(-1)\zeta_{kd}^{-i\mu}\Phi\left(\frac{hb-ka-\mu}{d}\right)\right).\end{aligned}$$

Applying (13) we also deduce that

$$\begin{aligned}\mathcal{F}(\mu)\sim\psi(\mu)\sum_{(i,j_1)\in J(k)\times J(d)}\sum_{\tau\in J(kd)}&\tilde{B}_{m,\chi}\left(\frac{\tau}{kd}\right)\zeta_{kd}^{(hi-kj_1)\tau}\\ &\times\zeta_d^{bj_1-ai}\left(\zeta_{kd}^{i\mu}\Phi\left(\frac{hb-ka+\mu}{d}\right)-\psi(-1)\zeta_{kd}^{-i\mu}\Phi\left(\frac{hb-ka-\mu}{d}\right)\right).\end{aligned}$$

Note that $\sum_{j_1\in J(d)}\zeta_{kd}^{-kj_1\tau}\zeta_d^{bj_1}=\sum_{j_1\in J(d)}\zeta_d^{(b-\tau)j_1}=\Phi((b-d)/\tau)d$. Hence

$$\begin{aligned}\mathcal{F}(\mu)\sim\psi(\mu)\sum_{i\in J(k)}\sum_{\tau\in J(k)}&\tilde{B}_{m,\chi}\left(\frac{b+\tau d}{kd}\right)\\ &\times\left(\zeta_{kd}^{(hb-ka+\mu+h\tau d)i}\Phi\left(\frac{hb-ka+\mu}{d}\right)-\psi(-1)\zeta_{kd}^{(hb-ka-\mu+h\tau d)i}\Phi\left(\frac{hb-ka-\mu}{d}\right)\right).\end{aligned}$$

If $hb-ka\pm\mu\not\equiv 0 \pmod d$, then $\mathcal{F}(\mu)=0$. If $hb-ka+\mu\equiv 0 \pmod d$, we can express $hb-ka+\mu=\tau_1 d$ for some $\tau_1\in\mathbf{Z}$. In addition, if $2(hb-ka)\not\equiv 0 \pmod d$, then $hb-ka-\mu=2(hb-ka)-\tau_1 d\not\equiv 0 \pmod d$ and we see that

$$\mathcal{F}(\mu)\sim\psi(\mu)\sum_{i\in J(k)}\sum_{\tau\in J(k)}\tilde{B}_{m,\chi}\left(\frac{b+\tau d}{kd}\right)\zeta_k^{(\tau_1+h\tau)i}\sim\psi(\mu)\tilde{B}_{m,\chi}\left(\frac{\beta-h'\tau_1}{k}\right).$$

If $(\lambda_1+\beta)/k\notin\mathcal{B}_{m,\chi}$ for some $\lambda_1\in\mathbf{Z}$, then by the assumption $\gcd\{f_\psi p, kd\}=1$ there is an integer $\mu_1\in\mathcal{N}_1$ satisfying $\mu_1\equiv -h\lambda_1 d-hk+ka \pmod{kd}$ and $\gcd\{\mu_1,f_\psi\}=1$. For such μ_1, we have

$$\mathcal{F}(\mu_1)\sim\ \tilde{B}_{m,\chi}\left(\frac{\lambda_1+\beta}{k}\right).$$

This implies $\mathcal{F}(\mu_1)\neq 0$ and by (22), we conclude that $r_m(\chi,\psi,h,k,\alpha,\beta:s_0)=|p|_p^{\frac{1}{p-1}}|q|_p^{-1}$. On the other hand if $(\lambda+\beta)/k\in\mathcal{B}_{m,\chi}$ for all $\lambda\in\mathbf{Z}$, considering the case of $hb-ka-\mu\equiv 0 \pmod d$ in the same way, we see that $\mathcal{F}(\mu)=0$ for all $\mu\in\mathbf{N}$. Hence we conclude that $r_m(\chi,\psi,h,k,\alpha,\beta:s_0)=\infty$.

Finally let us consider the case of $2(hb-ka)\equiv 0 \pmod d$. In this case if $hb-ka+\mu\equiv 0 \pmod d$, we can express $hb-ka+\mu=\tau_1 d$ and $hb-ka-\mu=2(hb-ka)-\tau_1 d$ for some $\tau_1\in\mathbf{Z}$ and

$$\begin{aligned}\mathcal{F}(\mu)\ &\sim\ \psi(\mu)\left(\tilde{B}_{m,\chi}\left(\frac{\beta-h'\tau_1}{k}\right)-\psi(-1)\tilde{B}_{m,\chi}\left(\frac{\beta-2h'(h\beta-k\alpha)+h'\tau_1}{k}\right)\right)\\ &\sim\ \psi(\mu)\Bigg(\tilde{B}_{m,\chi}\left(\frac{\beta-h'(h\beta-k\alpha)}{k}+\frac{-h'(h\beta-k\alpha)+h'\tau_1}{k}\right)\\ &\qquad -\psi(-1)\tilde{B}_{m,\chi}\left(\frac{\beta-h'(h\beta-k\alpha)}{k}-\frac{-h'(h\beta-k\alpha)+h'\tau_1}{k}\right)\Bigg).\end{aligned}$$

Hence in the similar way as in the case of $2(hb-ka)\not\equiv 0 \pmod d$, we obtain our assertion. This completes the proof.

If χ is trivial, making use of some fundamental properties of Bernoulli numbers and polynomials, we can deduce more explicit results as the following.

Corollary 5.2. *If χ is trivial. we have*

$$r_m(\chi,\psi,h,k,\alpha,\beta:s_0)=|p|_p^{\frac{1}{p-1}}|q|_p^{-1}$$

except for the following cases :

Case 1: $2(h\beta-k\alpha)\notin\mathbf{Z}$, $m\equiv 1 \pmod 2$, $k=1$, $\beta\in\frac{1}{2}+\mathbf{Z}$.
Case 2: $2(h\beta-k\alpha)\notin\mathbf{Z}$, $m\equiv 1 \pmod 2$ with $m\geq 3$, $k\leq 2$, $\beta\in\mathbf{Z}$.
Case 3: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=1$, $k=1$.
Case 4: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=1$, $k=2$, $m\geq 2$, $h\beta-k\alpha\in\mathbf{Z}$.
Case 5: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=1$, $k=2$, $m\geq 2$, $h\beta-k\alpha,\beta\in\frac{1}{2}+\mathbf{Z}$.
Case 6: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=1$, $k=2$, $m\equiv 1 \pmod 2$ with $m\geq 3$, $\beta\in\mathbf{Z}$.
Case 7: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=1$, $k\geq 3$, $m\equiv 0 \pmod 2$, $2\alpha,2\beta\in\mathbf{Z}$.
Case 8: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=-1$, $k=1$, $m=1$, $\beta\in\frac{1}{2}+\mathbf{Z}$.
Case 9: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=-1$, $k=1$, $m\equiv 1 \pmod 2$ with $m\geq 3$, $2\beta\in\mathbf{Z}$.
Case 10: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=-1$, $k=2$, $m=1$, $2\alpha\in\mathbf{Z}$, $\beta\in\frac{1}{2}+\mathbf{Z}$.
Case 11: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=-1$, $k=2$, $m\equiv 1 \pmod 2$ with $m\geq 3$, $2\alpha,2\beta\in\mathbf{Z}$.
Case 12: $2(h\beta-k\alpha)\in\mathbf{Z}$, $\psi(-1)=-1$, $k=2$, $m\equiv 1 \pmod 2$ with $m\geq 3$, $2\alpha\in\frac{1}{2}+\mathbf{Z}$, $\beta\in\mathbf{Z}$.

Case 13: $2(h\beta - k\alpha) \in \mathbf{Z}$, $\psi(-1) = -1$, $k \geq 3$, $m = 1$, $2\alpha, 2\beta \in \mathbf{Z}$.
Case 14: $2(h\beta - k\alpha) \in \mathbf{Z}$, $\psi(-1) = -1$, $k \geq 3$, $m \equiv 1 \pmod 2$ with $m \geq 3$, $2\alpha, \beta \in \mathbf{Z}$.

In these exceptional cases, we have

$$S_{p,m}\left(s; \chi, \psi \begin{pmatrix} h & k \\ \alpha & \beta \end{pmatrix}\right) = 0 \quad (\textit{identically}).$$

References

1) R.Dedekind; "Erläuterungen zu zwei Fragmenten von Riemann," Gesammelte Math. Werke, 1, 159-173 (1930)
2) T.M.Apostol; "Generalized Dedekind sums and transformation formulae of certain Lambert series," Duke Math.J., 17 no.2, 147-157 (1950)
3) H.Rademacher; "Some remarks on certain generalized Dedekind sums," Acta Arith., 9, 97-105 (1964)
4) L.Carlitz; "Generalized Dedekind sums," Math.Zeit., 85, 83-90 (1964)
5) L.Carlitz; "A theorem on generalized Dedekind sums," Acta Arith., 11, 253-260 (1965)
6) K.Rosen, W.Snyder; "p-adic Dedekind sums," J.Reine Angew. Math., 361, 23-26 (1985)
7) C.Snyder; "p-adic interpolation of Dedekind sums," Bull. Austral. Math. Soc., 38, 293-301 (1988)
8) A.Kudo; "On p-adic Dedekind sums," Nagoya Math. J., 144, 155-170 (1996)
9) A.Kudo; "On p-adic Dedekind sums (II)," Mem. Fac. Sci. Kyushu Univ., 45, 245-284 (1991)
10) K.Kozuka; "On linear combinations of p-adic interpolating functions for the Euler numbers," Kyusyu J. Math., 54, 403-421 (2000)
11) K.Kozuka; "On a generalization of the higher-order p-adic Dedekind sums," Research Report of Miyakonojo National College of Technology, 34, 15-21 (2000)
12) L.Carlitz; "Some theorems on generalized Dedekind sums," Pacific J. Math., 3, 513-522 (1953)
13) H.Tsumura; "On a p-adic interpolation of the generalized Euler numbers and its applications," Tokyo J. Math., 10, 281-293 (1987)
14) K.Shiratani, S.Yamamoto; "On a p-adic interpolating function for the Euler numbers and its derivatives," Mem. Fac. Sci. Kyushu Univ., 39, 113-125 (1985)

大規模MIMOにおけるBP信号検出に対応したカオス暗号へのテント写像の適用

迫田和之[1]・谷口莉菜

Application of Tent Map to Chaotic Encryption in Massive MIMO Using BP Decoding

SAKODA Kazuyuki[1] and TANIGUCHI Rina

(Accepted September 29, 2022)

Abstract　In wireless communications, chaotic encryptions at the physical layer provide enhanced security. Recent study has reported that the chaotic encryption works within a massive MIMO (Multiple-Input Multiple-Output) using Belief-Propagation decoding. However, it is pointed out that the chaos equation used in the previous method is a logistic map, which can be easily incorporated, but is not suitable for an encryption due to the biased distribution of pseudorandom numbers. A chaotic map that can be easily introduced into the previous method is the tent map. The tent map is considered suitable for cryptography because the distribution of pseudorandom numbers is uniform distribution. In this study, we propose a method to introduce a tent map to chaotic encryption. We numerically evaluate decoding accuracy, secrecy capacity and computation time of the proposed method. The results suggest that the proposed method performs as well as or better than the previous method.

Keywords　[Chaos, Encryption, Massive MIMO, BP decoding]

1　序論

近年、PCだけでなく身近な家電もネットワークに繋がることが珍しくなくなっている。それらは無線での接続が主流となりつつあり、無線通信容量の需要は年々拡大している。その傾向に対応した第5世代無線通信サービスにより、莫大な通信量の需要を賄っている。第5世代以降の移動無線通信は、大容量かつ多接続を可能とする大規模MIMO（Multiple Input Multiple Output)が中核技術である[1~4]。大規模MIMOは、第4世代で用いられている複数の送受信アンテナで構成されたMIMOのアンテナ数を、数十～数百本程度まで増やした通信システムである。送受信アンテナ数を増加させることで、多接続と大容量の通信容量を可能とする。しかしながら、アンテナ数を増加させると、受信側での信号検出（受信信号から送信信号を推定する技術）における計算量が増加する。特に、MIMOで用いられる一般的な信号検出である最尤推定法（Maximum Likelihood Detection, MLD）は、アンテナ数に対し指数関数的に計算量が増加し、現実的な計算時間での信号検出が困難である[5,6]。この問題を解決する信号検出法としてBP（Belief Propagation)法を用いた信号検出、BP信号検出がある[7~12]。BP信号検出は、少ない計算量と符号化を施さなくても低い誤り率（BER, Bit Error Rate）であるため、大規模MIMO

1 都城工業高等専門学校電気情報工学科（現 鹿屋体育大学スポーツ情報センター） Department of Electrical and Computer Engineering, National Institute of Technology(KOSEN), Miyakonojo College (Present address: Information Technology Center for Sports Sciences, National Institute of Fitness and Sports in Kanoya)

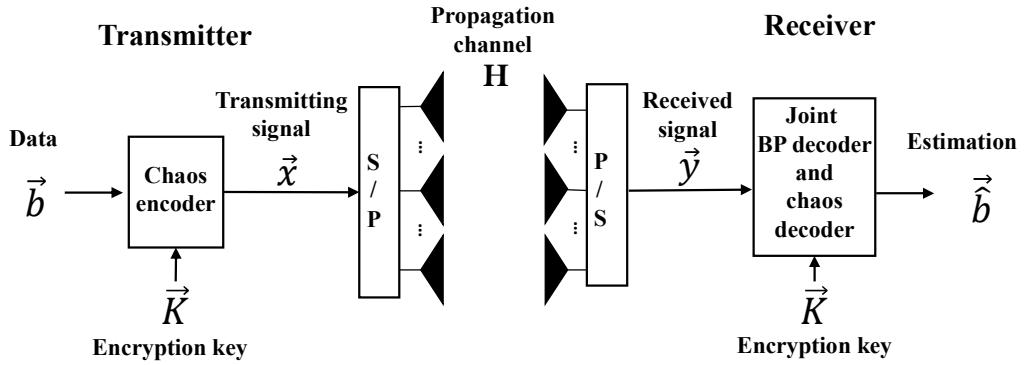

Fig.1 Chaotic encryption and BP decoding applied to massive MIMO

の信号検出として注目されている。

一方、様々なものがネットワークにつながることで、通信容量の課題とは別に、セキュリティの向上も求められている。無線通信でセキュリティを向上させるための暗号技術として、上位レイヤを対象とした AES (Advanced Encryption Standard)などが多いが、近年では下位レイヤである物理レイヤで、暗号化を追加する技術が提案されている [13,14]。物理レイヤでの暗号化は、情報を伝搬する電磁波に指向性を持たせ正規の受信者に電磁波が漏れないようにするビームフォーミング技術や電磁波の位相を乱雑に置き換えて情報を秘匿する技術がある。特に、電磁波の位相をカオス写像により乱雑に置き換えるカオス暗号は、比較的簡易な回路で構築でき、導入への障壁が小さい [15]。カオス暗号を MIMO に適応したカオス MIMO は、復号における精度の高さとセキュリティの高さで注目されている [16,17]。しかしながら、カオス MIMO を大規模 MIMO 化すると、復号に MLD を用いているため、計算量爆発を起こし、現実的な計算量での復号が困難である。そこで、カオス MIMO に BP 信号検出を用い大規模 MIMO 化を可能とする手法（Fig.1）が報告されている [18,19]。これにより、大規模 MIMO の物理レイヤに暗号化を導入でき、セキュリティの向上が見込める。このカオス暗号で用いられるカオス写像は、ロジスティック写像である。ロジスティック写像は、カオスの特性により、疑似乱数を発生させることができるが、その値がとる頻度分布に偏りが存在する（Fig. 2-1）。その偏りにより、暗号化された信号も偏りのある信号となる。暗号化された信号を盗聴者が解読を試みる場合、一般的には疑似乱数に偏りがないため全てのパターンを探索する必要があり、解読が困難となる。信号に偏りが存在すると、発生頻度の高い値から探索することで解読にかかる時間を短縮しうる可能性がある。そのためロジスティック写像は暗号に適していないという指摘がなされている [19]。

そこで本研究では、カオス暗号に、疑似乱数の頻度分布に偏りのないテント写像（Fig. 2-2）を導入する手法を提案し、その性能を数値実験により評価する。2 章では無線通信のシステムモデルと前手法を紹介する。3 章では提案手法を述べる。4 章では提案手法の数値実験結果、5 章では考察とまとめを述べる。

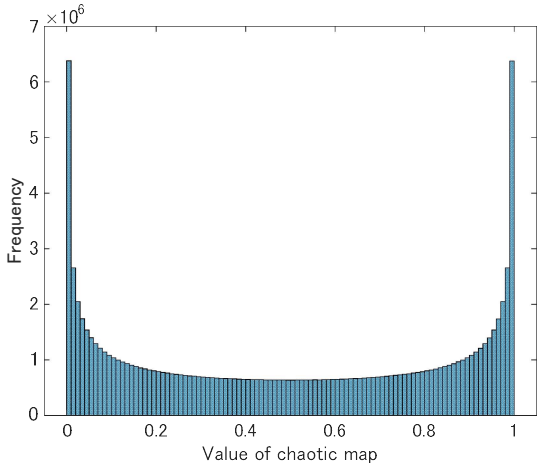

Fig. 2-1 Frequency distribution of the logistic map

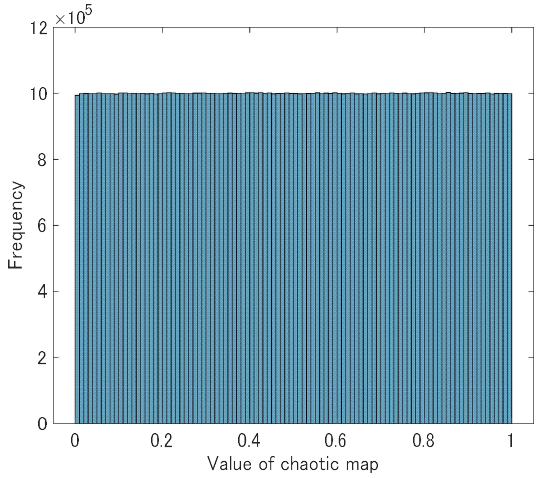

Fig. 2-2 Frequency distribution of the tent map

2　システムモデルと前手法

ここではシステムモデルであるカオス暗号及び BP 信号検出を用いた大規模 MIMO のシステムモデルと前手法でのカオス暗号化の手順を紹介する。

2．1　システムモデル

システムモデルは、送信アンテナ数 N_t、受信アンテナ数 N_r の大規模 MIMO 通信方式を考える。送信機は、カオス暗号器、直並列変換器（Serial Parallel Conversion, S/P）と送信アンテナで構成され、受信機は、受信アンテナ、並直列変換器 (Parallel Serial Conversion, P/S)と BP 信号検出器で構成される(Fig. 1)。この通信システムは共通鍵暗号方式であり、送信側と受信側で M 個の要素を持つ共通暗号鍵

$$\vec{K} = (K_1, K_2, \dots, K_M) \tag{1}$$

を持つ。この鍵を用いて、送信側は暗号化し、受信側は暗号化された信号を復号する。暗号鍵を持っていない第三者は受信信号を傍受しても復号が困難であるため秘匿通信となる。送信データは、N_t 個の送信ビット

$$\vec{b} = \left(b_1, b_2, \dots, b_{N_t}\right), \quad b_i \in \{0,1\} \text{ for } i = 1,2,\cdots,N_t \tag{2}$$

で、カオス暗号器により、送信信号 $\vec{x}$ は、

$$\vec{x} = \left(x_1, x_2, \cdots, x_{N_t}\right), \quad x_i = x_i\left(b_i, \vec{K}\right), \quad i = 1,2,\cdots,N_t \tag{3}$$

となる。前手法での暗号化の詳細は 2.2 節、提案手法での暗号化の詳細は 3 章で述べる。x_i を送信シンボルと呼び、送信アンテナに 1 つずつ割り当てられ、同時刻同周波数で受信アンテナに送信される。電磁波が通る空間中の経路はマルチパスチャネルと呼ばれ、N_r 行 N_t 列の通信路行列 $\mathbf{H}$ で表される。受信信号 $\vec{y}$ は

$$\vec{y} = \mathbf{H}\vec{x} + \vec{n} \tag{4}$$

と表せる。ここで $\vec{n}$ は平均 0 で分散 σ_n^2 の白色雑音である。

受信機では、受信信号 $\vec{y}$ から送信データ $\vec{b}$ を BP 信号検出で推定する。従って、推定データ $\vec{\hat{b}}$ は、$\mathbf{H}$ を既知として、$\vec{y}$、$\mathbf{H}$ と $\vec{K}$ の関数

$$\vec{\hat{b}} = \vec{\hat{b}}\left(\vec{y}, \mathbf{H}, \vec{K}\right) \tag{5}$$

と書ける。なお、ここでの BP 信号検出は前手法 [19] にあるカオス暗号に適したものである。

2．2　前手法でのカオス暗号

ここでは筆者らの先行研究である前手法 [19] での BP 信号検出に適合したカオス暗号について説明する。前手法でのカオス暗号は、カオス MIMO での暗号化を基に、BP 信号検出できるように再構築されている。その詳細については文献 19)を参照されたい。まず、送信側では暗号鍵の要素 K_m を初期値とし、カオス写像であるロジスティック写像で $i \times l$ 回写像することで、複素変数

$$k_{mi} = f^{i\times l}(\mathrm{Re}[K_m]) + jf^{i\times l}(\mathrm{Im}[K_m]) \tag{6}$$

を得る。ここで、$f(\cdot)$はロジスティック写像

$$f(z) = 3.91z(1-z) \tag{7}$$

であり、lは写像回数を決めるパラメータである。さらに、生成された M 個の要素を

$$s_i = \frac{1}{M}\sum_{m=1}^{M}(\mathrm{Re}[k_{mi}] + \mathrm{Im}[k_{mi}]) \cdot \exp[8\pi j(\mathrm{Re}[k_{mi}] - \mathrm{Im}[k_{mi}])] \tag{8}$$

のように加算平均する。最終的に暗号化した送信シンボルは、

$$x_i = \begin{cases} \exp\left[2j\tan^{-1}\dfrac{\mathrm{Im}[s_i]}{\mathrm{Re}[s_i]}\right], & b_i = 1 \\ \exp\left[2j\left(\tan^{-1}\dfrac{\mathrm{Im}[s_i]}{\mathrm{Re}[s_i]} + \pi\right)\right], & b_i = 0 \end{cases} \tag{9}$$

である。

3　提案手法

ここでは、前手法のロジスティック写像をテント写像に置き換えた提案手法でのカオス暗号について述べる。

3．1　提案手法

提案手法でのカオス暗号は、前手法の式(7)をテント写像

Table 1 Simulation condition

	提案手法	前手法	参考手法 1	参考手法 2
Modulation method	Choatic encryption			BPSK
Chaotic map	tent	Logistic	Henon	−
Num. of chaotic map iteration	$l = 10$			−
Size of encryption key	$M = 10$			−
Num. of antennas	$N_{\mathrm{t}} = N_{\mathrm{r}} = 12$			
Channel	i.i.d. Rayleigh fading			
Receive channel state information	Perfect			
Decoding method	BP decoding			
Num. of BP iteration	$N_{\mathrm{iter}} = 20$			

$$g(z) = \begin{cases} 2z, & z < \frac{1}{2} \\ 2(1-z), & z \geq \frac{1}{2} \end{cases} \tag{10}$$

に置き換える。提案手法は、これを用いたカオス暗号をBP信号検出を用いた大規模MIMOに導入したものである。

4　数値実験による評価

提案手法の性能を評価するため、信号検出にかかる計算時間、誤り率とセキュリティ性能について数値実験を行い、前手法、参考手法1、2と比較する。
参考手法 1 はカオス写像にエノン写像を用いたもの、参考手法 2 はカオス暗号を行わず、無線通信で一般的な変調方法の BPSK（Binary Phase Shift Keying）を用いたものである。なお、エノン写像は後述する式(11)で表され、生成される疑似乱数に偏りがない。それらに共通する諸元は Table 1 の通りとした。送信データの要素は等確率で 0 または 1 をとるとし、無作為に生成した。チャネル行列の要素は平均 0、分散 1 の複素ガウス分布$\mathcal{CN}(0,1)$に従う乱数とした。受信信号に含まれる雑音は白色雑音と仮定し、複素ガウス分布$\mathcal{CN}(0,\sigma_{\mathrm{n}}^2)$に従う乱数とした。雑音の分散は信号電力と雑音電力の比である SN 比（SNR, Signal to Noise Ratio）を用いて、$\sigma_{\mathrm{n}}^2 = 10^{-\mathrm{SN}/}$ とした。全ての乱数は互いに独立に生成した。これらの数値実験は MATLAB®で行った。

4．1　計算時間

4 つの手法での BP 信号検出と暗号の復号にかかる計算時間を比較した結果を Table 2 に示す。それぞれの値は、10^3回試行にかかった計算時間を$N_{\mathrm{t}} = 2$の参考手法 2 で規格化したものである。N_{t}が増えるとどの手法も計算時間が増加する。提案手法と参考手法 1 を比較すると、参考手法 1 の計算時間が長くなった。エノン写像は、

$$\begin{cases} x_{n+1} = 1 - 1.4x_n^2 + z_n \\ z_{n+1} = 0.3x_n \end{cases} \tag{11}$$

で表される 2 変数連立写像であるため、1 変数写像である提案手法よりも計算時間が長くなったと考えられる。提案手法と前手法を比較すると、わずかながら提案手法の計算時間が短くなった。テント写像とロジスティック写像のどちらも 1 変数写像であるが、テント写像では計算に必要な項の数が平均的に少なくなることが要因であると考えられる。暗号化を行う 3 手法の中では、提案手法の計算時間が一番短いことがわかった。なお、暗号化を行わない参考手法 2 の計算時間が一番短くなることは自明である。

Table 2 Computation time for decoding

N_{t}	2	4	5	8	12	16	24	32	64
Proposed method	1.06	1.15	1.22	1.54	2.07	3.22	5.10	7.46	22.75
Previous method	1.16	1.29	1.38	1.74	2.36	3.62	5.65	8.21	23.81
Method 1(Henon)	2.22	2.44	2.62	3.38	4.75	7.23	11.05	16.14	47.27
Method 2(BPSK)	1	1.01	1.04	1.20	1.52	2.45	3.95	5.89	19.63

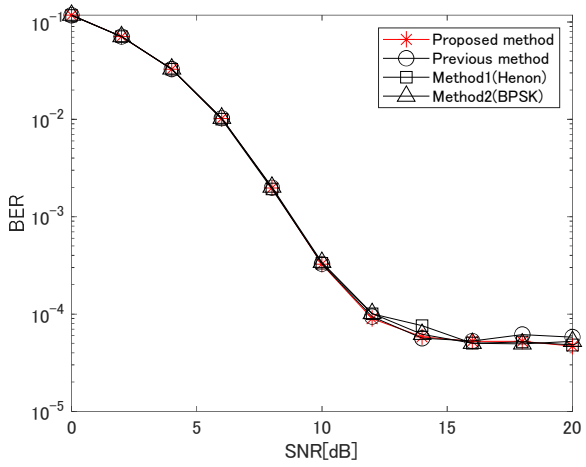

Fig. 3 BERs in massive MIMO for proposed method, previous method, method 1 and 2

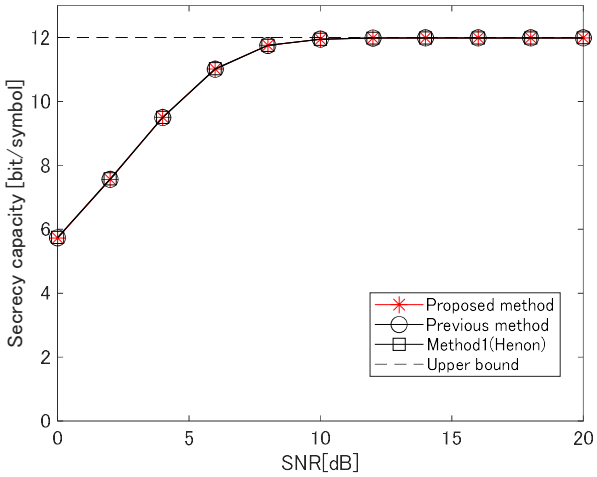

Fig. 4 Secrecy capacity in proposed method and previous method

4．2　誤り率

ここではBit Error Rate(BER)を用いて誤り率（1ビット当りの推定結果が誤る確率）の評価を行う。提案手法、前手法と参考手法1、2のBERを比較した結果がFig.3である。縦軸をBER、横軸をSNRとし、提案手法をアスタリスク、前手法を円、参考手法1を四角、参考手法2を三角で表示した。BERは10^5試行の平均値とした。全ての手法でSNRが大きくなると、BERは徐々に低下しある値に漸近した。BERがある値に漸近する理由は、BP信号検出特有のものであり、その詳細は文献19)を参照されたい。BERの特性は手法間で差がなかった。テント写像を用いることによるBERの増加は起きないことが示唆された。

4．3　セキュリティ性能

セキュリティ性能を示す一般的な指標である秘匿容量を用いて提案手法とその他の手法を比較し評価した。秘匿容量は、

$$C_{\mathrm{S}} = C_{\mathrm{R}} - C_{\mathrm{E}} \tag{12}$$

で与えられる。ここで、C_{R}は正規受信者のチャネル容量で、C_{E}は盗聴者のチャネル容量であり、

$$C_{\mathrm{R}} = qN_{\mathrm{t}}[1 + P_{\mathrm{R}}\log_2 P_{\mathrm{R}} + (1-P_{\mathrm{R}})\log_2(1-P_{\mathrm{R}})], \tag{13}$$
$$C_{\mathrm{E}} = qN_{\mathrm{t}}[1 + P_{\mathrm{E}}\log_2 P_{\mathrm{E}} + (1-P_{\mathrm{E}})\log_2(1-P_{\mathrm{E}})] \tag{14}$$

で表される。P_{R}とP_{E}はそれぞれ正規受信者と盗聴者のBERで、qは変調多値数であり、本研究では$q=1$である。チャネル容量は、その値が上限値に近いほど正確に情報が伝わる。つまり、秘匿容量は、正規受信者に正確に情報を伝達し盗聴者に情報が洩れない場合に上限値に近くなり、セキュリティ性能を示す指標となる。しかしながら、カオス写像での疑似乱数の偏りを起因とするセキュリティ性能の優劣をこの指標で示すことができないことに注意されたい。

提案手法と前手法の秘匿容量を比較した結果がFig.4である。縦軸を秘匿容量、横軸をSNRとし、提案手法をアスタリスク、前手法を円、参考手法1を四角、秘匿容量の上限を破線で表示した。秘匿容量は10^5試行の平均値とした。全ての手法で、SNRが大きくなると、秘匿容量が増加し上限値に漸近した。SNR≥10では、正規受信者に正確に情報を伝達でき、盗聴者には情報が洩れていないことを示しており、秘匿通信が成り立っていると示唆される。一方SNR<10では、上限値に届いていないが、盗聴者に情報が漏れているのではなく、ノイズにより正規受信者が正確に信号検出できていないためである。秘匿容量の特性は手法間で差がなかった。そのためテント写像を用いることによる秘匿容量の低下は起きないことが示唆された。

5　まとめ

本研究では、カオス暗号に、疑似乱数の頻度分布に偏りのないテント写像を導入する手法を提案した。そのカオス暗号を大規模MIMOに適用して提案手法とし、数値実験により計算時間、誤り率と秘匿容量を評価した。その結果、提案手法の誤り率と秘匿容量は、前手法と比べ、ほとんど差がないことが確かめられた。計算時間では、わずかながら提案手法の計算時間が短いことが確かめられた。これらの点から、提案手法が、前手法の欠点であるロジスティック写像による疑似乱数の偏りを回避し、前手法と同等以上の性能を持つことを示すことができた。今後の課題として、本研究

ではセキュリティ性能の評価を秘匿容量のみで行ったため、盗聴者の持つ鍵と正規の鍵との近さに対するセキュリティ性能の依存性についても調査し、評価したいと考えている。

参考文献

1) T. L. Marzetta : Noncooperative Cellular Wireless with Unlimited Numbers of Base Station Antennas, IEEE Trans. Wireless Commun., Vol.9, pp.3590-3600, 2010
2) F. Rusek, D. Persson, B. K. Lau, et al. : Scaling Up MIMO Opportunities and Challenges with Very Large Arrays, IEEE Signal Process. Mag., Vol.30, pp.40-60, 2013
3) E. Telatar : Capacity of Multi-antenna Gaussian Channels, European Transactions on Telecommunications, Vol.10, pp.585-595, 1999
4) L. Lu, G. Y. Li, A. L. Swindlehurst, et al. : An Overview of Massive MIMO: Benefits and Challenges, IEEE J. Sel. Topics Signal Process., 8, pp.742-758, 2014
5) S. Yang, L. Hanzo : Fifty Years of MIMO Detection the Road to Large-scale MIMOs, IEEE Commun. Surveys Tuts., 17, pp.1941-1988, 2015
6) D. Araújo, T. Maksymyuk, A. L. F. Almeida, et al. : Massive MIMO: Survey and Future Research Topics, IET Commun., 10, pp.1938-1946, 2016
7) J. Yang, C. Zhang, X. Liang, et al. : Improved Symbol-based Belief Propagation Detection for Large-scale MIMO, Proc. IEEE Workshop on Signal Processing Systems, pp.1-6, 2015
8) W. Fukuda, T. Abiko, T. Nishimura, et al. : Low-complexity Detection Based on Belief Propagation in a Massive MIMO System, Proc. IEEE Vehicular Technology Conf., pp.1-5, 2013
9) T. Takahashi, S. Ibi, S. Sanpei, et al. : On Normalization of Matched Filter Belief in GaBP for Large MIMO detection, Proc. IEEE Vehicular Technology Conf., pp.1-6, 2016
10) P. Som, T. Datta, A. Chockalingam, B. S. Rajan, et al. : Improved large-MIMO Detection Based on Damped Belief Propagation, Proc. IEEE Trans. inf. Theory, pp.1-5, 2010
11) J. Yang, W. Song, S. Zhang, et al. : Low-Complexity Belief Propagation Detection for Correlated Large-Scale MIMO Systems, J Sign. Process. Syst., 90, pp.585-599, 2018
12) K. Sakoda, H. Hata and S. Hata : Residue Effect of Parallel Interference Canceller in Belief Propagation Decoding in Massive MIMO Systems, International Journal of Electrical and Electronic Engineering & Telecommunications, Vol.9, pp.13-17, No.1, 2020
13) M. Bloch and J. Barros : Physical-Layer Security, Cambridge University Press, Cambridge, 2011
14) L. Dong, Z. Han, A. P. Petropulu and H. V. Poor : Improving Wireless Physical Layer Security via Cooperating Relays, IEEE Trans. Signal Processing, Vol.58, No.3, pp.1875-1888, 2010
15) Y. Shiu, S. Y. Chang, H. Wu, S. C. Huang and H. Chen : Physical Layer Security in Wireless Networks: a Tutorial, IEEE Wireless Commun., Vol.18, No.2, pp.66–74, 2011
16) E. Okamoto : A Chaos MIMO Transmission Scheme for Channel Coding and Physical-layer Security, IEICE Trans. Commun., Vol.E95-B, No.4, pp.1384-1392, 2012
17) E. Okamoto and Y. Inaba : Multilevel Modulated Chaos MIMO Transmission Scheme with Physical Layer Security, NOLTA IEICE, Vol.5, No.2, pp.140-156, 2014
18) K. Sakoda, H. Hata and S. Hata : Chaotic Encryption for Belief Propagation Decoding in Massive MIMO Systems, Journal of Communications Technology and Electronics, Vol.65, No.2, pp.172-178, 2020
19) K. Sakoda, H. Hata and S. Hata : Chaotic Encryption for Massive MIMO using BP decoding, IEICE Trans. Commum., Vol.J105-B, No.7, pp.535-542, 2022

多値変調に対応する大規模 MIMO における BP 信号検出の検討

迫田和之 [1]・湯之前翔大 [2]

Study on Belief Propagation Decoding for Multivalued Modulation in Massive MIMO

SAKODA Kazuyuki[1] and YUNOMAE Shota [2]

(Accepted September 27, 2022)

Abstract　A Massive MIMO (Multiple Input Multiple Output) is expected to become the core of technology for future large-capacity wireless communication. However, massive MIMO systems generally experience the explosive increase of the computation time required for decoding. BP decoding is attracting attention as decoding method in a massive MIMO because of practical computation time. There are several types of BP decoding that will be used for a decoding in a massive MIMO. The BP decoding (previous method) proposed in our laboratory shows high performance, but does not support multivalued modulation. Support for multivalued modulation is essential for large-capacity wireless communication.　In this study, we propose a new BP decoding to adapt multivalued modulation. We numerically evaluate decoding accuracy and channel capacity of the proposed method. The results suggest that the proposed method achieves the standard criteria for establishing wireless communication in bit error ratio and increases channel capacity.

Keywords　[Massive MIMO, BP decoding, Multivalued modulation]

1 序論

近年、高速・大容量無線移動通信規格である第 5 世代（5G）サービスが提供され、無線移動通信の大容量化が進んだ。今後は移動通信の主要端末である携帯電話だけに留まらず、家電、自動車や工場の自動操作等といった様々なものがインターネットに接続可能になる Internet Of Things(IoT)の発展は必至である。それらの機器は無線で接続されることが想定されるため、今後の無線通信は大容量かつ多接続可能な移動通信が条件となる。その条件を満たす中核技術は大規模 Multiple Input Multiple Output(MIMO)である[1,2]。大規模 MIMO は、これまで数本程度であった MIMO 送受信アンテナを数十～数百本程度に増やすことで、チャネル容量の大容量化を実現するものである[3,4]。しかしながら、送信アンテナ数の増加に比例して送信信号数も増加し、それにより受信側での信号検出（受信信号から送信信号を推定する技術）における計算量が指数関数的に増加するという課題がある[5,6]。この問題を解決するため、MIMO の一般的な信号検出手法である

1 都城工業高等専門学校電気情報工学科(現 鹿屋体育大学スポーツ情報センター) Department of Electrical and Computer Engineering, National Institute of Technology(KOSEN), Miyakonojo College (Present address: Information Technology Center for Sports Sciences, National Institute of Fitness and Sports in Kanoya)
2 富士アイティ株式会社情報制御システム本部産業ソリューション事業部環境ソリューション部計測システム課 Instruments Control System Section, Industry Solution Division, Environment Solution Department, Fuji IT Co. Ltd.

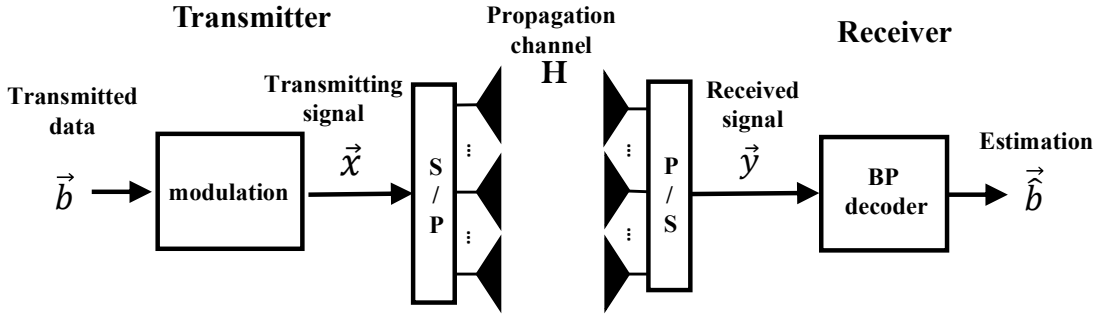

Fig. 1 Massive MIMO overview

最尤推定法（Maximum Likelihood Detection, MLD）の計算量を削減する手法や繰り返し計算を用いた手法等が提案されている[7,8]。中でも、確率伝播法（Belief Propagation, BP）を用いた繰り返し計算手法、以下 BP 信号検出は、高い推定精度と少ない計算量により、注目を集めている[9~13]。BP 信号検出には大きく分けて 2 種類あり、1 つは信号検出に BP 法を適用した最初の手法であり、通信容量を増加させる多値変調への適応[14]や推定精度を向上させる改良[11,12]が行われ、5G の信号検出の主流となりつつあるものである[9~14]。もう 1 つは、当研究室で考案された手法で（以下、前手法）[15]、今後の改良が期待されるものである。この 2 つの大きな違いは、繰り返し計算の際に算出する残留干渉成分と呼ばれるものの分散の計算方法である。この違いにより、繰り返し計算途中の推定値の振る舞いが大きく変わることが報告されている。両手法の振る舞いに大きな違いはあるが、推定精度と計算量は同程度である。しかしながら、前手法は、多値変調への対応や推定精度を向上させる改良は未だ行われていない。特に、必要な通信容量は年を追う毎に増加する一方であるため、通信容量の増加が見込める多値変調への対応は急務である。そこで本研究では、2 値変調(Binary Phase Shift Keying, BPSK)の信号検出にしか対応していない前手法を、多値変調の 1 つである Quadrate Phase Shift Keying(QPSK)の信号検出に対応できる手法に改良し提案する。その提案手法の誤り率と通信容量を数値実験により評価する。2 章では、無線通信のシステムモデルと前手法を紹介する。3 章では、提案手法を述べる。4 章では提案手法の数値実験結果、5 章では考察とまとめを述べる。

2　システムモデルと前手法

ここでは本研究および前手法でのシステムモデルである大規模 MIMO 通信方式と前手法である BPSK に対応した BP 信号検出を紹介する。

2．1　システムモデル

システムモデルは、送信アンテナ数N_{t}、受信アンテナ数N_{r}の大規模 MIMO 通信方式を考える。送信ビットは BPSK を用いて電磁波で送りやすい形式に変換され、直並列変換器（Serial Parallel Conversion, S/P）を経て，送信アンテナから受信アンテナに向けて送信される。受信機では、受信アンテナで得られた受信信号を並直列変換器（Parallel Serial Conversion, P/S）に通し、BP 信号検出により送信ビットを推定する（Fig. 1）。

送信データは、N_{t}個の送信ビット

$$\vec{b} = \left(b_1, b_2, \ldots, b_{N_{\mathrm{t}}}\right), \quad b_i \in \{0,1\} \text{ for } i = 1,2,\cdots,N_{\mathrm{t}} \tag{1}$$

で、送信信号$\vec{x}$は、送信データを BPSK で変調し、

$$\vec{x} = \left(x_1, x_2, \cdots, x_{N_{\mathrm{t}}}\right), \quad x_i = \begin{cases} 1 & (b_i = 1) \\ -1 & (b_i = 0) \end{cases} \text{ for } i = 1,2,\cdots,N_{\mathrm{t}} \tag{2}$$

となる。x_iは送信シンボルといい、送信信号の 1 要素である。BPSK は位相変調の最も基礎的な手法であり、電磁波の位相を Fig. 2(a)のように 180° ずらすことで$b_i \in \{0,1\}$を表すことができ、1 送信シンボルに 1 ビットの情報を含む。$\vec{x}$の各要素は、送信アンテナに 1 つずつ割り当てられ、同時刻同周波数で受信アンテナに向けて送信される。電磁波が通る空間中の経路はマルチパスチャネルと呼ばれ、N_{r}行N_{t}列の通信路行列$\mathbf{H}$で表される。受信信号$\vec{y}$は

$$\vec{y} = \mathbf{H}\vec{x} + \vec{n} \tag{3}$$

と表せる。ここで$\vec{n}$は平均 0 で分散σ_n^2の白色雑音である。

受信機では、受信信号$\vec{y}$から送信データ$\vec{b}$を BP 信号検出を用いて推定する。従って、推定データ$\hat{\vec{b}}$は、$\mathbf{H}$を既知として、$\vec{y}$と$\mathbf{H}$の関数

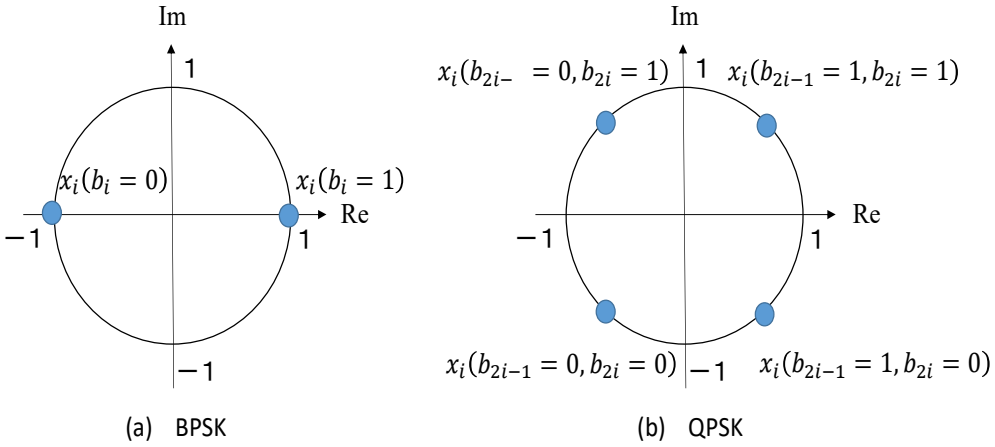

Fig. 2 Constellation points of BPSK and QPSK

$$\vec{\hat{b}} = \vec{\hat{b}}(\vec{y}, \mathbf{H}) \tag{4}$$

と書ける。BPSK に対応した BP 信号検出の詳細は次節で述べる。

２．２　BPSK に対応した BP 信号検出

BP 信号検出は並列干渉除去（Parallel Interference Cancellation, PIC）を用い、繰り返し計算により送信データを推定する。PIC により不必要な送信信号を除去することで、MIMO を Single Input Multiple Output (SIMO) として見なし、送信データの各ビットを推定可能とする。推定された各ビットの尤度を次の繰り返し計算で PIC に用いることで、徐々に推定された送信データの精度が向上する。以下に BPSK に対応した BP 信号検出である前手法 [15]の手順を述べる。

２．２．１　並列干渉除去

ここでは受信機で受け取った受信信号に PIC を行い SIMO 化する手順を述べる。受信信号の要素であるy_jのx_k以外の送信信号を PIC で除去したものを

$$\tilde{y}_{jk}^{(l)} = y_j - \sum_{i=1, i\neq k}^{N_t} h_{ji}\tilde{x}_{ji}^{(l)}, \tag{5}$$

$$\tilde{x}_{ji}^{(l)} = \tanh\left(\frac{\beta_{ji}^{(l)}}{2}\right) \tag{6}$$

とする。ここで、$\tilde{x}_{ji}^{(l)}$はレプリカ信号であり、$l = 1,2,\cdots$は繰り返し回数である。$\beta_{ji}^{(l)}$（式（14））については後述する。レプリカ信号は$-1 \leq \tilde{x}_{ji}^{(l)} \leq 1$ の範囲の連続値であり、BP の繰り返し回数が増えると 1 もしくは-1 に収束することが期待される。式(5)は、

$$\tilde{y}_{jk}^{(l)} = h_{jk}x_k + n_j + R_{jk}^{(l)}, \tag{7}$$

$$R_{jk}^{(l)} = \sum_{i=1, i\neq k}^{N_t} h_{ji}\left(x_i - \tilde{x}_{ji}^{(l)}\right) \tag{8}$$

と書き直すことができる。式(7)はx_kに着目し、それ以外の送信信号はレプリカ信号により BP の繰り返し毎に徐々に除去されることを期待する。ここで、$R_{jk}^{(l)}$は残留干渉成分と呼ばれ、レプリカ信号で除去しきれなかった成分である。

２．２．２　LLR

ここでは PIC により着目した送信信号が 1 か-1 であるかを評価する対数尤度比(Log Likelihood Ratio, LLR）について述べる。$R_{jk}^{(l)}$を雑音と見なすと、x_kの尤度関数は、

$$\Pr\left(\tilde{y}_{jk}^{(l)} \middle| x_k(b_k)\right) = CN\left(\tilde{y}_{jk}^{(l)} \middle| h_{jk}x_k + \mu_{jk}^{(l)}, \sigma_{jk}^{(l)2} + \sigma_n^2\right) \tag{9}$$

で与えられる。ここで$CN(* \,|\mu, \sigma^2)$は平均μで分散σ^2の複素ガウス分布である。式(9)の$\mu_{jk}^{(l)}$と$\sigma_{jk}^{(l)2}$は残留干渉成分の分散と平均で

$$\mu_{jk}^{(l)} = 0, \tag{10}$$

$$\sigma_{jk}^{(l)2} = \sum_{i=1,i\neq k}^{N_t} |h_{ji}|^2 \left(x_i - \tilde{x}_{ji}^{(l)}\right)^2 \quad (11)$$

である。式(9)の尤度関数を用いて、対数尤度比(LLR)

$$\alpha_{jk}^{(l)} = \log \frac{\Pr\left(\tilde{y}_{jk}^{(l)} \middle| x_k(b_k = 1)\right)}{\Pr\left(\tilde{y}_{jk}^{(l)} \middle| x_k(b_k = 0)\right)} \quad (12)$$

を算出することで、j番目の受信アンテナで得られた受信信号y_jでのk番目の送信信号x_kを評価することができる。$\alpha_{jk}^{(l)}$が正であればx_k =1、つまりb_k =1 である確率が高く、負であればx_k =−1、つまりb_k =0 である確率が高い。この LLR の情報を次の BP 繰り返しに引き継ぐため

$$\gamma_k^{(l)} = \sum_{j=1}^{N_t} \alpha_{jk}^{(l)}, \quad (13)$$

$$\beta_{jk}^{(l+1)} = \gamma_k^{(l)} - \alpha_{jk}^{(l)} \quad (14)$$

を算出する。式(13)は送信信号x_kを評価する LLR を加算したものである。式(14)は次の BP 繰り返しで式(5)に用いる。

２．２．３　BP 繰り返し処理と推定値

PIC を元に式(5)−(12)により LLR を得られる。LLR から構成される$\beta_{jk}^{(l)}$を生成することで次の BP 繰り返し処理へ移る。繰り返し処理により、$\alpha_{jk}^{(l)}$、$\beta_{jk}^{(l)}$と$\tilde{x}_{jk}^{(l)}$が更新され、BP 繰り返しの規定回数N_{iter}に到達した際に、送信ビットの推定を

$$\hat{b}_k = \begin{cases} 1, & \gamma_k^{(N_{\mathrm{iter}})} \geq 0 \\ 0, & \gamma_k^{(N_{\mathrm{iter}})} < 0 \end{cases} \quad (15)$$

とする。

２．２．４　残留干渉成分の分散の取り扱い

尤度関数に式(11)で表される残留干渉成分の分散を導入する必要があるが、その中には真の送信信号x_iが含まれている。これは受信側では知りえない情報であるため、疑似残留干渉成分の分散を他の方法で残留干渉成分の分散を見積もる必要がある。疑似残留干渉成分の分散を

$$\tilde{\sigma}_{jk}^{(l)2} = \sum_{i=1,i\neq k}^{N_t} |h_{ji}|^2 \left(\tilde{x}_{ji}^{(l-1)} - \tilde{x}_{ji}^{(l)}\right)^2 \quad (16)$$

と設定し，残留干渉成分の分散の代わりに用いる。また、BP 繰り返しの初回において$\tilde{x}_{ji}^{(1)}$ =0 とし、$\tilde{x}_{ji}^{(0)}$は 1 と−1 が等確率と仮定し、その疑似残留干渉成分の分散を

$$\tilde{\sigma}_{jk}^{(0)2} = \sum_{i=1,i\neq k}^{N_t} |h_{ji}|^2 \quad (17)$$

と設定する。

３　提案手法

ここでは、多値変調として QPSK の概要とそれに対応した BP 信号検出、以下、提案手法を述べる。

３．１　QPSK

QPSK は、送信シンボルx_iに 2 ビットの情報を含む変調方式である。Fig. 2(b)のように、電磁波の位相 90°をずらして、2 ビットの情報を表す。その時の送信データ$\vec{b}$は、

$$\vec{b} = (b_1, b_2, \ldots, b_{2N_t}), \quad b_i \in \{0,1\}, \quad i = 1,2,\cdots,2N_t \quad (18)$$

で、送信信号$\vec{x}$は、

$$\vec{x} = (x_1, x_2, \cdots, x_{N_t}),$$
$$x_i = \begin{cases} \exp\left(i\pi/4\right) & (b_{2i-1} = 1, b_{2i} = 1) \\ \exp\left(3i\pi/4\right) & (b_{2i-1} = 0, b_{2i} = 1) \\ \exp\left(5i\pi/4\right) & (b_{2i-1} = 0, b_{2i} = 0) \\ \exp\left(7i\pi/4\right) & (b_{2i-1} = 1, b_{2i} = 0) \end{cases}, \quad i = 1,2,\cdots,N_t \quad (19)$$

である。BPSK と比べ、1 送信シンボルで送れるビット数が 2 倍になる。

３．２　提案手法

提案手法は、前手法の LLR やレプリカ信号の生成方法を QPSK に対応させるものである。ここでは、その方法を述べる。

Table 1 Simulation condition

	Proposed method	Previous method
Modulation	QPSK	BPSK
Num. of antennas	$N_{\mathrm{t}} = N_{\mathrm{r}} = 100$	
Channel	i.i.d. Rayleigh fading	
Receive channel state information	Perfect	
Decoding method	BP decoding	
Num. of BP iteration	$N_{\mathrm{iter}} = 20$	

まず、送信シンボルに含まれる第 1 ビットと第 2 ビットのそれぞれの LLR を

$$\alpha_{jk,1}^{(l)} = \log \frac{\Pr\left(\tilde{y}_{jk}^{(l)} \middle| \mathrm{Re}[x_k(b_{2k-1}=1)]\right)}{\Pr\left(\tilde{y}_{jk}^{(l)} \middle| \mathrm{Re}[x_k(b_{2k-1}=0)]\right)}, \tag{20}$$

$$\alpha_{jk,2}^{(l)} = \log \frac{\Pr\left(\tilde{y}_{jk}^{(l)} \middle| \mathrm{Im}[x_k(b_{2k}=1)]\right)}{\Pr\left(\tilde{y}_{jk}^{(l)} \middle| \mathrm{Im}[x_k(b_{2k}=0)]\right)} \tag{21}$$

とする。これにより、式(13)、(14)は、

$$\gamma_{k,1}^{(l)} = \sum_{j=1}^{N_{\mathrm{t}}} \alpha_{jk,1}^{(l)}, \quad \gamma_{k,2}^{(l)} = \sum_{j=1}^{N_{\mathrm{t}}} \alpha_{jk,2}^{(l)}, \tag{22}$$

$$\beta_{jk,1}^{(l+1)} = \gamma_{k,1}^{(l)} - \alpha_{jk,1}^{(l)}, \ \beta_{jk,2}^{(l+1)} = \gamma_{k,2}^{(l)} - \alpha_{jk,2}^{(l)} \tag{23}$$

となる。$\beta_{jk,1}^{(l+1)}$、$\beta_{jk,2}^{(l+1)}$から生成されるレプリカ信号は、

$$\tilde{x}_{ji}^{(l)} = \frac{1}{\sqrt{2}} \tanh\left(\frac{\beta_{ji,1}^{(l)}}{2}\right) + \frac{i}{\sqrt{2}} \tanh\left(\frac{\beta_{ji,2}^{(l)}}{2}\right) \tag{24}$$

とする。$|\beta_{jk,1}^{(l)}|$と$|\beta_{jk,2}^{(l)}|$が大きくなると、レプリカ信号が QPSK の送信信号に近づくことがわかる。前手法は送信シンボル毎に評価していたが、提案手法では送信ビット毎に評価することで、QPSK に対応することが可能である。提案手法は、前手法の式(6)を式(24)に、式(12)を式(20)と(21)に、式(13)と(14)を式(22)と(23)に変更する。

4 数値実験による評価

提案手法の性能を評価するため、誤り率と通信容量について数値実験を行った。それらに共通する諸元は Table 1 の通りとした。送信データの要素は等確率で 0 または 1 をとるとし、無作為に生成した。チャネル行列の要素は平均 0、分散 1 の複素ガウス分布$\mathcal{CN}(0,1)$に従う乱数とした。受信信号に含まれる雑音は白色雑音と仮定し、複素ガウス分布$\mathcal{CN}(0,\sigma_{\mathrm{n}}^2)$に従う乱数とした。雑音の分散は 1 ビットあたりの信号電力と雑音電力の比である Eb/No を用いて、$\sigma_{\mathrm{n}}^2 = 10^{-\mathrm{Eb/No}}$とした。全ての乱数は互いに独立に生成した。これらの数値実験は MATLAB® で行った。

4.1 提案手法の誤り率

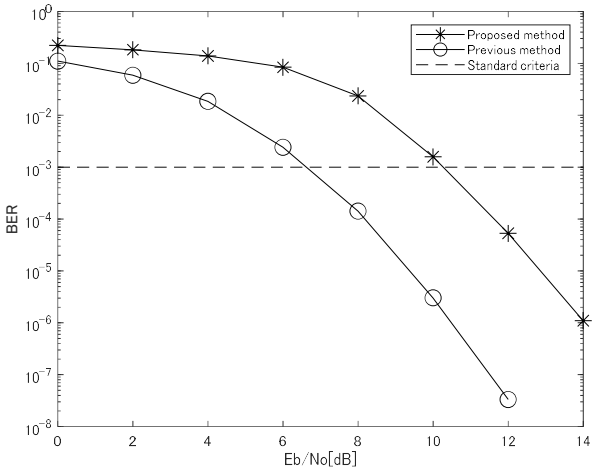

Fig. 3 BERs in massive MIMO for proposed method and previous method

本研究では Bit Error Rate(BER)を用いて誤り率の評価を行う。提案手法と前手法の BER を比較した結果が Fig. 3 である。誤り率を縦軸 BER、横軸 Eb/No とし、提案手法をアスタリスク、前手法を円で無線通信の誤り率の基準値を破線で表示した。提案手法と前手法を比較すると、Eb/No が大きくなるとどちらも BER は低下するが、全ての Eb/No で前手法の BER が低くなった。しかしながら、提案手法の BER は、無線通信の誤り率基準値である BER<10^{-3}を Eb/No<20 で達成しているため、実用上の問題はないと考えられる。提案手法の BER が増加する原因は、Fig. 2 で表される信号点

間の距離が前手法に比べ短くなり、ノイズの影響を受けやすくなったためと考えられる。

４．２　提案手法の通信容量

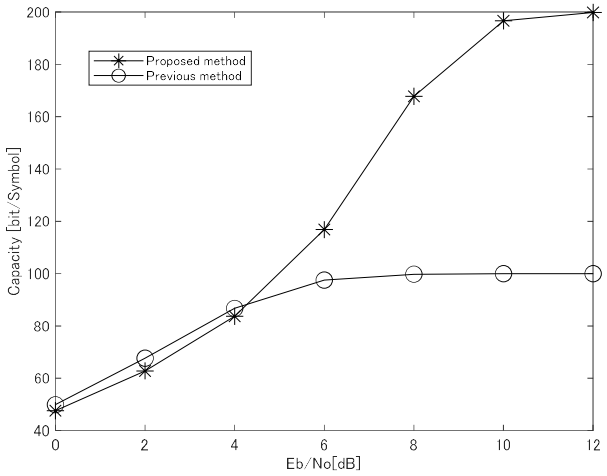

Fig. 4 Channel capacity in proposed method and previous method

提案手法の通信容量を前手法と比較し評価した。通信容量は、

$$C = qN_t[1 + P_R\log_2 P_R + (1 - P_R)\log_2(1 - P_R)] \quad (25)$$

で与えられる。ここで、qは変調多値数であり BPSK ではq =1、QPSK ではq =2 である。P_Rは BER である。

提案手法と前手法の通信容量を比較した結果が Fig. 4 である。縦軸を通信容量、横軸を Eb/No とし、提案手法をアスタリスクで表し、前手法を円で表した。どちらの手法も Eb/No が大きくなると通信容量が大きくなった。小さい Eb/No の範囲では提案手法よりも前手法の方は通信容量が僅かながら大きいが、Eb/No≥6 で提案手法の通信容量が大きくなった。提案手法と前手法の通信容量の上限は、式(24)によるとP_R =0、つまり１つも誤らなかった場合、それぞれ 200[bit/symbol]と 100[bit/symbol]である。数値実験の結果、Eb/No が大きくなると通信容量は上限に漸近した。Eb/No が十分に大きい環境で、提案手法は前手法に比べ通信容量の面で大きな性能改善が可能であることがわかった。

５　まとめ

本研究では、BPSK の信号検出にしか対応していない前手法を、多値変調の 1 つである QPSK の信号検出に対応できる手法に改良し提案した。その提案手法の誤り率と通信容量を数値実験により評価した。その結果、誤り率において、無線通信の基準値を達成すること、通信容量において、前手法よりも優れていることを示すことができた。これらの結果から、提案手法が多値変調を基本とする大規模 MIMO での信号検出で有効であるということが示唆された。

今後の課題として、提案手法を QPSK よりもさらに多値変調となる 8 Phase Shift Keying(8PSK)や 16 Quadrature Amplitude Modulation(16QAM)への拡張を考えている。

参考文献

1) T. L. Marzetta : Noncooperative Cellular Wireless with Unlimited Numbers of Base Station Antennas, IEEE Trans. Wireless Commun., Vol.9, pp.3590-3600, 2010

2) F. Rusek, D. Persson, B. K. Lau, et al. : Scaling Up MIMO Opportunities and Challenges with Very Large Arrays, IEEE Signal Process. Mag., Vol.30, pp.40-60, 2013

3) E. Telatar : Capacity of Multi-antenna Gaussian Channels, European Transactions on Telecommunications, Vol.10, pp.585-595, 1999

4) L. Lu, G. Y. Li, A. L. Swindlehurst, et al. : An Overview of Massive MIMO: Benefits and Challenges, IEEE J. Sel. Topics Signal Process., 8, pp.742-758, 2014

5) S. Yang, L. Hanzo : Fifty Years of MIMO Detection the Road to Large-scale MIMOs, IEEE Commun. Surveys Tuts., 17, pp.1941-1988, 2015

6) D. Araújo, T. Maksymyuk, A. L. F. Almeida, et al. : Massive MIMO: Survey and Future Research Topics, IET Commun., 10, pp.1938-1946, 2016

7) T. H. Im, J. Kim and Y. S. Cho : A Low Complexity QRM-MLD for MIMO Systems, Proc. IEEE Vehicular Technology Conf., pp.2243-2247, 2007

8) H. Kawai, K. Higuchi, N. Maeda, et al. : Likelihood Function for QRM-MLD Suitable for Soft-decision Turbo Decoding and its Performance for OFDM MIMO Multiplexing in Multipath Fading Channel, IEICE Trans. Commun., E88-B, pp.47-57, 2005

9) J. Yang, C. Zhang, X. Liang, et al. : Improved Symbol-based Belief Propagation Detection for Large-scale MIMO, Proc. IEEE Workshop on Signal Processing Systems, pp.1-6, 2015

10) W. Fukuda, T. Abiko, T. Nishimura, et al. : Low-complexity Detection Based on Belief Propagation in a Massive MIMO System, Proc. IEEE Vehicular Technology Conf., pp.1-5, 2013

11)T. Takahashi, S. Ibi, S. Sanpei, et al. : On Normalization of Matched Filter Belief in GaBP for Large MIMO detection, Proc. IEEE Vehicular Technology Conf., pp.1-6, 2016

12)P. Som, T. Datta, A. Chockalingam, B. S. Rajan, et al. : Improved large-MIMO Detection Based on Damped Belief Propagation, Proc. IEEE Trans. inf. Theory, pp.1-5, 2010

13)J. Yang, W. Song, S. Zhang, et al. : Low-Complexity Belief Propagation Detection for Correlated Large-Scale MIMO Systems, J Sign. Process. Syst., 90, pp.585-599, 2018

14)T. Watabe, T. Nishimura, T. Ohgane, et al. : Superposed 16-QAM Signal Detection Using GaBP in a Massive MIMO System, Proc. APSIPA Annual Summit and Conf., pp.1416-1420, 2018

15)K. Sakoda, H. Hata and S. Hata : Residue Effect of Parallel Interference Canceller in Belief Propagation Decoding in Massive MIMO Systems, International Journal of Electrical and Electronic Engineering & Telecommunications, Vol.9, pp.13-17, No.1, 2020

都城工業高等専門学校
研究報告第 57 号

令和 5 年 1 月印刷
令和 5 年 1 月発行

編集兼発行者：独立行政法人国立高等専門学校機構
都城工業高等専門学校
郵便番号：885-8567
所 在 地：宮崎県都城市吉尾町 473 番地の 1
National Institute of Technology(KOSEN), Miyakonojo College
ADDRESS:473-1 Yoshio-cho, Miyakonojo City,
Miyazaki Prefecture, Japan 885-8567
TEL(0986)47-1109
FAX(0986)47-1111

Research Report
of
National Institute of Technology(KOSEN), Miyakonojo College

No.57

2023

Contents

Research Papers;

****