

# フーリエ変換によるあみだくじの解析

中村 彰吾                      武井 由智  
Shogo Nakamura              Yoshinori Takei  
長岡技術科学大学  
Nagaoka University of Technology

## 1 はじめに

### 1.1 背景と目的

離散的対象の順列を定義域とする関数に対して、対象へのラベル付けによってどの程度その関数が左右されるかという尺度、ラベル依存度が 2012 年に小川 [4] によって対称群上のフーリエ解析を用いて定義されている。置換群上の関数のラベル依存度は、元の関数のラベル不変な関数の空間への正射影を元の関数から引きさった成分が、元の関数をどれだけ占めているかで定義される。擬似ランダム置換の発生法を評価する上で、ラベル依存度をはじめとするフーリエ解析に基づくデータは有用な情報を含むと考えられる。たとえば、1988 年に Diaconis [5] はカードシャッフルのモデルとしてランダムな互換の繰り返しを考え、結果の確率分布と一様分布との距離の上界を与えているが、そこでは対称群上のフーリエ解析が重要な手法として応用されている。

そこで本論文では隣接互換の繰り返しによる擬似ランダム置換(あみだくじ)に注目し、その確率分布関数と一様分布との距離がフーリエ係数行列の固有値と隣接互換の繰り返し回数によって上から抑えられることを示す(定理 3)。とくに置換される対象の数  $n = 4$  のとき(あみだくじの縦棒が 4 本のとき)の具体的な上界を導出する(定理 3 系 1)。さらに、この場合において、あみだくじを環状とする(1 と  $n = 4$  の互換を許す)ことが、一様分布との距離およびラベル依存度を減少させることを示す。

### 1.2 本論文の構成

第 2 節では本論文で扱う対称群やその上の関数のフーリエ解析、ラベル依存度について述べる。第 3 節では隣接互換の繰り返しによる確率分布関数と一様

分布の距離が、フーリエ係数行列によって、繰り返し回数で抑えられることを示す。また、4 次の置換における具体的な計算結果を示す。第 4 節ではまとめを述べる。

## 2 準備

本節では対称群の表現、フーリエ変換、ラベル依存度の定義、及び擬似ランダム置換の発生方法の定義について述べる。ここでの記述は [1, 2, 3, 5] を参考としている。

### 2.1 置換と対称群

$n$  個の対象の集合を、 $[n] := \{1, 2, \dots, n-1, n\}$  とすると、 $n$  個の対象の置換の集合は、

$$S_n := \{\sigma : [n] \rightarrow [n] \mid \text{全単射}\}$$

で定義される。 $S_n$  は、写像の結合を演算として群をなし、 $n$  次対称群と呼ばれる。

$S_n$  のサイズは、 $|S_n| = n!$  である。 $S_n$  の要素  $\sigma$  は、これが  $\sigma(j) = i_j (j = 1, \dots, n)$  を満たすとき、

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \quad (1)$$

のように表記され、たとえば  $\sigma(1) = 5, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 3, \sigma(5) = 2$ , なる置換  $\sigma$  は、

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}. \quad (2)$$

の様に表記される. 任意の置換は,

$$\pi(s_i) = \begin{cases} s_{i+1} & 1 \leq i < k \\ s_1 & i = k \\ s_i & k < i \leq n \end{cases}$$

という巡回置換 (cycle)  $\pi = (s_1, s_2, \dots, s_k)$  の組み合わせで表すことが出来る. 式 (2) を巡回置換表記 (cycle notation) で書くと,

$$\sigma = (152)(34)$$

となる. 置換を構成する巡回置換の長さを巡回置換型 (cycle-type), あるいは単に型 (type) と呼ぶ.  $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ ,  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$ ,  $\sum_{i=1}^k \lambda_i = n$  を  $n$  の分割と呼び  $\lambda \vdash n$  と書く.

任意の巡回置換  $(s_1, s_2, \dots, s_k)$  は互換の積,  $(s_1, s_2) \cdot (s_2, s_3) \cdot \dots \cdot (s_{k-1}, s_k)$  で表すことが出来る. したがって, 互換の集合は対称群全体を生成する. さらに任意の互換  $(i, j)$  は次のように隣接互換  $\tau_k = (k, k+1)$  の積で表すことが出来る.

$$(i, j) = \tau_{j-1} \dots \tau_{i+1} \tau_i \tau_{i+1} \dots \tau_{j-1}$$

ここで,  $i, j$  は一般性を失わずに  $i < j$  である. 故に,  $S_n$  全体が隣接互換のみの積で生成することが出来ることが分かる.

### 2.2 共役とラベルの貼り替え

置換  $\sigma_1, \sigma_2 \in S_5$  に対し, 置換される  $1, 2, 3, 4, 5$  にそれぞれ  $5, 1, 2, 3, 4$  というラベルを貼ると

$$\{\sigma_1, \sigma_2\} = \{(123)(45), (12)(3)(45)\}$$

は

$$\{\pi_1, \pi_2\} = \{(512)(34), (51)(2)(34)\}$$

のように見える. その様子を図 1 に示す. ラベルの張り替えは

$$\pi_i = \tau \sigma_i \tau^{-1}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \quad i = 1, 2$$

と表現できる.

また,  $\sigma, \pi \in S_n$  で  $\exists \tau, \pi = \tau \sigma \tau^{-1}$  のとき  $\pi$  と  $\sigma$  は共役と呼び  $\pi_1, \pi_2 \in S_n$  に対し “ $\pi_1$  と  $\pi_2$  は共役” なる関係は  $S_n$  上の同値関係となる. この関係に関する同値類を共役類と呼ぶ. また,  $\forall \tau, \sigma \in S_n, f(\sigma) = f(\tau \sigma \tau^{-1})$  が成り立つ関数を類関数と呼ぶ.

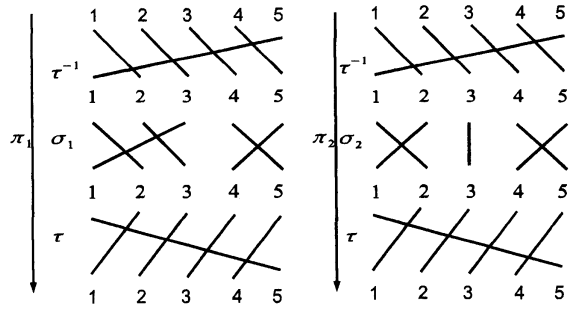


図 1: ラベルを貼り替えた置換の例

### 2.3 Young 直交表現 [3]

整数  $n$  の分割  $\lambda \vdash n$  を  $\lambda_1, \lambda_2, \dots, \lambda_k$  個のタイルの並びで図的に表現したものを Ferrers 図形と呼ぶ.

例えば  $n = 4$  のとき  $(2, 1, 1) = \begin{matrix} \square & \square \\ \square & \\ \square & \end{matrix}, (2, 2) = \begin{matrix} \square & \square \\ \square & \square \end{matrix}, \dots$  となる. Ferrers 図形に数字  $1, 2, \dots, n$  を過不足なく割り当てたものをヤング盤と呼ぶ. 例えば  $n = 4$  のとき  $\lambda = \begin{matrix} \square & \square \\ \square & \\ \square & \end{matrix}$  に対して,

$$t = \begin{matrix} 1 & 2 \\ 3 \\ 4 \end{matrix}$$

のようなものをいう. 特に各行と列について数が昇順に並んでいるものを標準ヤング盤と呼ぶ.  $\lambda$  に対する標準ヤング盤の数はフック長  $l_x$  を用いて,

$$d_\lambda = \frac{n!}{\prod_x l_x} \tag{3}$$

で表される. フック長とは Ferrers 図形の位置  $x$  のタイルに関して, より右側, より下側につづくタイルの数に 1 を加えた数である.

群  $G$  の表現は,  $\rho: G \rightarrow \mathbb{C}^{d \times d}$  であって,  $x, y \in G$  に対して,

$$\rho(xy) = \rho(x)\rho(y), \rho(x^{-1}) = \rho(x)^{-1}$$

を満たすもの (すなわち,  $\rho$  から  $d$  次正則行列への準同型写像) をいう. また, この式から単位元  $e \in S_n$  に対し  $\rho(e) = I$  が得られる. 表現  $\rho, \rho_1, \rho_2$  が与えられた場合にある正則行列  $A$  に対し,

$$\rho(x) = A \begin{bmatrix} \rho_1(x) & 0 \\ 0 & \rho_2(x) \end{bmatrix} A^{-1} \quad (x \in G)$$

と書けるとき  $\rho$  は  $\rho_1, \rho_2$  の直和であるといい、 $\rho \cong \rho_1 \oplus \rho_2$  と書く。このとき  $\rho$  は可約であるという。 $\rho$  が表現の直和で書けないとき、既約であるといい、 $\rho$  を既約表現と呼ぶ。対称群の場合、既約表現としてヤング直交表現 (YOR) がよく用いられる。YOR は整数  $n$  の分割  $\lambda \vdash n$  ごとに定義された既約表現  $\rho_\lambda : S_n \rightarrow \mathbb{R}^{d_\lambda \times d_\lambda}$  であり、次数  $d_\lambda$  は式 3 で与えられる。 $[\rho_\lambda(\tau_k)]^{d_\lambda \times d_\lambda}$  の要素は標準ヤング盤  $t$  でインデックスされ、対角成分は

$$[\rho_\lambda(\tau_k)]_{t,t} = 1/d_t(k, k+1) \quad (4)$$

となる。また、 $\tau_k(t)$  も標準ヤング盤の場合、(4) に加えて非対角要素

$$[\rho_\lambda(\tau_k)]_{t,\tau_k(t)} = \sqrt{1 - 1/d_t(k, k+1)^2} \quad (5)$$

があらわれる。他のすべての行列要素はゼロである。ここで  $d_t(i, j) = c(j) - c(i)$ ,  $c(x)$  は  $x$  の content と呼ばれる量であり、ヤング盤の中に置かれた  $x$  の列インデックスと行インデックスの差で定義される。すべての置換は隣接互換の積で表されることから、式 (4), (5) によって  $\forall \sigma \in S_n$  の表現が定義できる。以上のように定義した  $\rho_\lambda$  は、 $\rho_\lambda(\sigma)^{-1} = \rho_\lambda(\sigma)^T$  を満たす。すなわち、 $\rho_\lambda(\sigma)$  は直交行列である。

例として、 $n = 4, \lambda = (2, 2)$  のとき  $d_\lambda = 2$  で、 $\rho_\lambda$  の  $\sigma = (123)(4)$  における値は

$$\rho_{(2,2)}((123)(4)) = \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} \quad \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

となる。

また、 $\rho_\lambda$  に対し、指標と呼ばれる関数  $\chi_\lambda$  が

$$\chi_\lambda(\sigma) := \text{tr}[\rho_\lambda(\sigma)]$$

で定義される。 $\chi_\lambda$  は共役に対して不変な関数 (類関数) である。

## 2.4 対称群上のフーリエ解析

$f, g : S_n \rightarrow \mathbb{R}$  に対し、これらの内積を

$$\langle f | g \rangle = \frac{1}{n!} \sum_{\sigma \in S_n} f(\sigma)g(\sigma)$$

で定義する。 $\rho_\lambda$  の  $(i, j)$  成分と  $\rho_{\lambda'}$  の  $(k, l)$  成分は  $\lambda = \lambda'$  かつ  $(i, j) = (k, l)$  のときを除き直交する。

$\lambda = \lambda'$  かつ  $(i, j) = (k, l)$  のときは  $1/d_\lambda$  である。すなわち、

$$\langle \rho_{\lambda,(i,j)} | \rho_{\lambda',(k,l)} \rangle = \frac{1}{d_\lambda} \delta_{\lambda\lambda'} \delta_{ik} \delta_{jl}$$

が成立する。 $S_n$  上の関数  $f : S_n \rightarrow \mathbb{R}$  の既約表現  $\rho_\lambda : S_n \rightarrow \mathbb{R}^{d_\lambda \times d_\lambda}$  に対し、 $\lambda \vdash n$  における関数  $f$  のフーリエ変換は

$$\hat{f}(\lambda) = \sum_{\sigma \in S_n} f(\sigma) \rho_\lambda(\sigma) \quad (6)$$

で定義される。これに対しフーリエ逆変換

$$f(\sigma) = \frac{1}{n!} \sum_{\lambda \vdash n} d_\lambda \text{tr}[\hat{f}(\lambda) \rho_\lambda(\sigma)^T] \quad (7)$$

が成り立つ。

**補題 1.** 関数  $p : S_n \rightarrow \mathbb{R}$  が  $p(\pi_i) = p(\pi_i^{-1})$  を満たすとき、

$$\hat{p}(\lambda) = \hat{p}(\lambda)^T$$

である。

**証明.**  $p(\pi_i) = p(\pi_i^{-1})$  がみたまされるため、

$$\begin{aligned} \hat{p}(\lambda) &= \sum_{\sigma \in S_n} p(\sigma) \rho_\lambda(\sigma) \\ &= \sum_{\sigma \in S_n} p(\sigma^{-1}) \rho_\lambda(\sigma) \\ &= \sum_{\sigma \in S_n} p(\sigma) \rho_\lambda(\sigma^{-1}) \end{aligned}$$

だが、 $\rho_\lambda$  は表現なので  $\rho_\lambda(\sigma^{-1}) = \rho_\lambda(\sigma)^{-1}$  が成立し、さらに、 $\rho_\lambda$  は直交行列なので  $\rho_\lambda(\sigma)^{-1} = \rho_\lambda(\sigma)^T$  である。よって、

$$\hat{p}(\lambda) = \sum_{\sigma \in S_n} p(\sigma) \rho_\lambda(\sigma)^T = \left( \sum_{\sigma \in S_n} p(\sigma) \rho_\lambda(\sigma) \right)^T = \hat{p}(\lambda)^T$$

となり、 $\hat{p}(\lambda)$  は対称行列である。□

また、指標  $\chi_\lambda$  は次を満たす：

$$\langle \chi_\lambda | \chi_{\lambda'} \rangle = \delta_{\lambda\lambda'}. \quad (8)$$

類関数の空間は  $\{\chi_\lambda\}_{\lambda \vdash n}$  で張られることが知られており、式 (8) とあわせて、 $\{\chi_\lambda\}_{\lambda \vdash n}$  は類関数の空間の正規直交基底をなす。さらに、指標の 2 乗和と共役類の関係として下が成立する。

**定理 1.** [1]  $\pi, \pi' \in \mathbb{S}_n$  に対して,  $c(\pi)$  を  $\pi$  の共役類のサイズとするととき次が成立する.

$$\frac{1}{n!} \sum_{\lambda \vdash n} \chi_\lambda(\pi) \chi_\lambda(\pi') = \begin{cases} \frac{1}{c(\pi)} & (\pi \text{ と } \pi' \text{ が共役}) \\ 0 & (\text{その他}) \end{cases} \quad (9)$$

また, 内積  $\langle f|g \rangle$  を周波数領域のそれに結びつける, パーセバルの定理が成立する.

**定理 2** (パーセバルの定理). [2] 関数  $f(\sigma), g(\sigma) (\sigma \in \mathbb{S}_n)$  に対して

$$\sum_{\sigma \in \mathbb{S}_n} f(\sigma) g(\sigma) = \left(\frac{1}{n!}\right)^2 \sum_{\lambda \vdash n} d_\lambda \text{tr}[\hat{f}(\lambda)^\top \hat{g}(\lambda)].$$

## 2.5 畳み込み

関数  $f, g: \mathbb{S}_n \rightarrow \mathbb{R}$  はそれぞれランダム置換  $\sigma, \tau$  の確率分布関数とする. つまり  $f(\sigma) = \text{Pr}[\sigma], g(\tau) = \text{Pr}[\tau]$  とする. 2つのランダム置換  $\sigma, \tau$  が独立であるとき, 2つの合成  $\pi = \sigma\tau$  ( $\tau$  が先,  $\sigma$  が後に作用する) がいかなる確率分布に従うかを考える.  $h(\pi) = \text{Pr}[\pi]$  とおくと, [A] で事象  $A$  のインジケータ変数 ( $A$  が真のとき 1, 偽のとき 0) で表せば

$$\begin{aligned} h(\pi) &= \sum_{\sigma, \tau \in \mathbb{S}_n} f(\sigma) g(\tau) [\pi = \sigma\tau] \\ &= \sum_{\tau \in \mathbb{S}_n} f(\pi\tau^{-1}) g(\tau) \\ &= f * g(\pi). \end{aligned} \quad (10)$$

すなわち,  $h$  は畳み込み  $f * g$  となる. 一般に  $f * g$  について, そのフーリエ変換は簡明な性質をもつ, つまり, 畳み込み定理

$$\widehat{f * g}(\lambda) = \hat{f}(\lambda) \cdot \hat{g}(\lambda) \quad (11)$$

が成立する. この式の右辺はフーリエ係数行列の積である.

## 2.6 擬似ランダム置換の生成法

本論文で考察する擬似ランダム置換生成法はランダムな隣接互換の繰り返しによるものを考える. より正確には次の通り定義する.

**定義 1** (あみだくじ). 次の方式で得られるランダム置換  $\pi$  を  $k$  段あみだくじと呼ぶ.

1. 等確率で  $l$  を  $k, k+1$  から選ぶ.

2. 各  $1 \leq i \leq l$  に対して  $\pi_i$  を隣接互換の集合  $\{(j, j+1) | 1 \leq j \leq n-1\} \subseteq \mathbb{S}_n$  から, 一様ランダムに抽出する.

3.  $\pi = \pi_l \cdots \pi_2 \pi_1$  とする. □

繰り返し回数  $k$  に対する性質を考察するとき,  $k$  を固定すると, ランダム置換の出力が  $k$  の偶奇に応じて, 偶置換または奇置換に偏る不都合が生じる. そこで定義 1 では  $k$  段のあみだくじと言った場合, 確率  $1/2$  で  $k$  段または  $k+1$  段のあみだくじがそれぞれ選ばれるモデルを考えている.

この擬似ランダム置換は図 2 のようなあみだくじと考えられる. 要素数  $n$  が縦棒の数で, 隣接互換の回数が横棒の本数に対応している. 一回隣接互換による置換  $\pi_i$  は, 点線で挟まれた横棒一本のあみだくじに対応し, その  $\mathbb{S}_n$  上の確率分布を  $p$  と置くと

$$p(\pi_i) = \begin{cases} \frac{1}{n-1} & (\pi_i \text{ が一回隣接互換}) \\ 0 & (\text{それ以外}) \end{cases}$$

となる.  $p(\pi_i) = p(\pi_i^{-1})$  であることに注意する.  $k$  回隣接互換による確率分布を  $g_k$  とすると  $g_k$  は  $p$  を  $k$  段積み重ねたものなので, 式 (10) より,  $g_k = p * \cdots * p$  (右辺は  $k$  回畳み込み) であり, この関係を式 (11) を用いてフーリエ係数で表現すると

$$\hat{g}_k = \hat{p}^k.$$

定義 1 の  $k$  段あみだくじでは,  $f_k = \frac{1}{2}(p^{(*)k} + p^{(*)k+1})$  であるため,

$$\hat{f}_k = \frac{\hat{p}^k + \hat{p}^{k+1}}{2} \quad (12)$$

が成立する.

次に隣接互換の他に 1 と  $n$  の互換を認めた, 環状のあみだくじを定義する.

**定義 2** (環状あみだくじ). 次の方式で得られるランダム置換  $\pi$  を環状あみだくじと呼ぶ.

1. 等確率で  $l$  を  $k, k+1$  から選ぶ.

2. 各  $1 \leq i \leq l$  に対して  $\pi_i$  を 1 と  $n$  の互換と隣接互換の集合  $\{(j, j+1) | 1 \leq j \leq n-1\} \cup \{(1, n)\} \subseteq \mathbb{S}_n$  から, 一様ランダムに抽出する.

3.  $\pi = \pi_l \cdots \pi_2 \pi_1$  とする. □

これは図 2 のあみだくじにおいて 1 と  $n$  ( $= 5$ ) の間にも横棒が発生するモデルである.

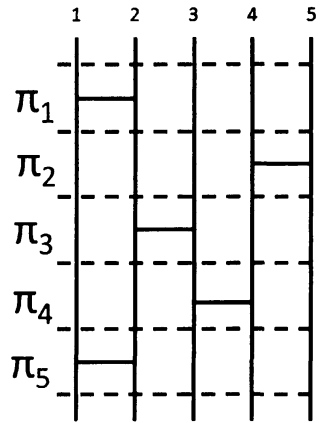


図 2: 隣接互換の繰り返しに基づく置換

## 2.7 対称行列と固有値

実行列  $A$  のフロベニウスノルムは

$$\|A\|_F = \sqrt{\text{tr}[A^T A]}$$

と定義する.  $\text{tr}[A^T A]$  が  $A$  の成分の 2 乗和であることに注意する.  $A$  が  $d$  次対称行列であるとき直交行列  $U$  で対角化でき,  $A$  の固有値を  $\mu_1, \dots, \mu_d$  とすると

$$\text{tr}[A^k A^T k] = \sum_{i=1}^n \mu_i^{2k} \quad (13)$$

となり, 実対称行列の  $k$  乗のフロベニウスノルムが固有値の  $2k$  乗和で表現できる.

## 2.8 ラベル依存度の定義 [4]

関数  $f$  のラベル非依存成分  $P(f)$  として

$$(P(f))(\sigma) = \sum_{\lambda \vdash n} \langle f | \chi_\lambda \rangle \chi_\lambda(\sigma) \quad (14)$$

のような関数が考えられる. これは 2.4 節で述べたように,  $\{\chi_\lambda\}_{\lambda \vdash n}$  が類関数の空間の正規直交基底であるから  $P$  は  $\mathbb{R}^{S_n}$  から類関数空間への直射影とみなせる. 関数  $f$  からラベル非依存成分  $P(f)$  を引くとラベル依存成分が得られる. 一般に  $f, g \in \mathbb{R}^{S_n}$  に対し

$$\begin{aligned} \langle P(f) | g \rangle &= \sum_{\lambda \vdash n} \langle f | \chi_\lambda \rangle \langle \chi_\lambda | g \rangle \\ &= \langle f | P(g) \rangle \end{aligned} \quad (15)$$

で, 式 (8) から

$$\begin{aligned} P(P(f)) &= \sum_{\lambda' \vdash n} \sum_{\lambda \vdash n} \langle f | \chi_\lambda \rangle \langle \chi_\lambda | \chi_{\lambda'} \rangle \chi_{\lambda'} \\ &= \sum_{\lambda \vdash n} \langle f | \chi_\lambda \rangle \chi_\lambda \\ &= P(f) \end{aligned} \quad (16)$$

であるから

$$\begin{aligned} \langle f | P(f) \rangle &= \langle f | P(P(f)) \rangle \\ &= \langle P(f) | P(f) \rangle \end{aligned} \quad (17)$$

である.

関数  $f$  のラベルの貼り換えに対する関数  $f$  の安定性の尺度がラベル依存成分  $f - P(f)$  と  $f$  のそれぞれの 2-ノルムの 2 乗の比として,

$$LD(f) = \frac{\langle f - P(f) | f - P(f) \rangle}{\langle f | f \rangle} \quad (18)$$

で定義される. この式は

$$\begin{aligned} \langle f - P(f) | f - P(f) \rangle &= \langle f | f \rangle - 2\langle f | P(f) \rangle + \langle P(f) | P(f) \rangle \\ &= \langle f | f \rangle - \langle P(f) | P(f) \rangle \end{aligned}$$

であることから,

$$\begin{aligned} LD(f) &= \frac{\langle f | f \rangle - \langle P(f) | P(f) \rangle}{\langle f | f \rangle} \\ &= 1 - \frac{\langle P(f) | P(f) \rangle}{\langle f | f \rangle} \end{aligned} \quad (19)$$

と書くことができる.

## 3 擬似ランダム置換の解析

Diaconis [5] は一般の互換  $(i, j) (1 \leq i < j \leq n)$  の繰り返しに基づく確率分布の一様分布との距離の上界を示した. そこではフーリエ解析, 特にパーセバルの定理が重要な役割を果たしている. この節では定義 2 で与えたような隣接互換の繰り返しによる確率分布にフーリエ解析を適用して解析を行う.

まず, 確率分布関数  $f$  と一様分布との距離を  $f$  のフーリエ係数を用いて表現することで, フーリエ係数行列の固有値によって, 確率分布  $f$  と一様分布  $u$  の距離が繰り返し回数で抑えられることを示す. また, 実際に隣接互換の繰り返しによって確率分布  $f$  と一様分布  $u$  の距離がどの程度近づくかを示す. また,  $n = 4$  の場合に実際に計算を行いその結果を示す.

### 3.1 一様分布との距離 [2, Chap.17, The Upper Bound Lemma]

任意の確率分布  $f$  と一様分布  $u$  の 2-ノルムに基づく距離について考える. 関数  $f$  と一様分布の距離の 2 乗が

$$\|f - u\|_2^2 = \sum_{\sigma \in \mathbb{S}_n} |f(\sigma) - u(\sigma)|^2$$

であり, 定理 2 (パーセバルの定理) より

$$\sum_{\sigma \in \mathbb{S}_n} |f(\sigma) - u(\sigma)|^2 = \frac{1}{n!} \sum_{\lambda \vdash n} d_\lambda \|\hat{f}(\lambda) - \hat{u}(\lambda)\|_2^2 \quad (20)$$

とフーリエ係数で表せる. ここで確率分布関数  $f$  については, その自明表現  $\rho_{(n)}$  に対するフーリエ係数が

$$\hat{f}((n)) = \sum_{\sigma \in \mathbb{S}_n} f(\sigma) \rho_{(n)}(\sigma) = \sum_{\sigma \in \mathbb{S}_n} f(\sigma) \cdot 1 = 1$$

である. また確率分布関数  $f$  が定義 1 の  $k$  段あみだくじの場合,  $f = f_k$  とすると,

$$\begin{aligned} \hat{f}_k(1^n) &= \frac{\hat{p}((1^n))^k + \hat{p}((1^n))^{k+1}}{2} \\ &= \frac{(-1)^k + (-1)^{k+1}}{2} = 0 \end{aligned}$$

である. よって,  $\hat{f}_k$  と  $\hat{u}$  の直流成分 ( $\lambda = (n)$ ) に対するフーリエ係数は 1 である. また,  $\hat{u}$  の直流成分以外 ( $\lambda \neq (n)$ ) のフーリエ係数行列が 0 行列であることから

$$\begin{aligned} \frac{1}{n!} \sum_{\lambda \vdash n} d_\lambda \|\hat{f}_k(\lambda) - \hat{u}(\lambda)\|_2^2 \\ = \frac{1}{n!} \sum_{\lambda \vdash n, \lambda \neq (n), \lambda \neq (1^n)} d_\lambda \|\hat{f}_k(\lambda)\|_2^2 \quad (21) \end{aligned}$$

となり, 関数  $f_k$  のフーリエ係数行列で表すことができる. 関数  $f_k$  が  $k \rightarrow \infty$  で一様分布に近づくとき  $\|f_k - u\|_2^2 \rightarrow 0$  であり, 式 (20) の右辺も 0 に向かう. つまり  $\|\hat{f}_k(\lambda)\|_2 \rightarrow 0$  ( $\lambda \neq (n)$ ) であり, これは関数  $f_k$  の直流成分を除いたフーリエ係数行列が 0 行列に向かうことを意味する.

### 3.2 繰り返し回数とフーリエ係数行列の固有値の関係

確率分布  $f_k$  が段数  $k$  によってどの程度一様分布  $u$  に近づくかを示す. ここで  $f_k$  が定義 1 の  $k$  段あみだ

くじ (横棒  $k, k+1$  本が確率  $1/2$  で選ばれる) の場合を考えると式 (12) より  $\hat{f}_k = \frac{\hat{p}^k + \hat{p}^{k+1}}{2}$  であった. また補題 1 より  $\hat{p}(\lambda)$  は対称行列である. その  $k$  乗である  $\hat{p}^k$  は対称で, このことから  $\hat{f}_k$  は対称である. よって, 式 (21) について  $\hat{f}_k(\lambda)$  は実数値対称行列であることから, 式 (21) の値は

$$\begin{aligned} \frac{1}{n!} \sum_{(n) \neq \lambda \vdash n} d_\lambda \|\hat{f}_k(\lambda)\|_2^2 \\ = \frac{1}{n!} \sum_{(n) \neq \lambda \vdash n} d_\lambda \text{tr}[\hat{f}_k(\lambda) \hat{f}_k(\lambda)^\top]. \end{aligned}$$

右辺を変形すると

$$\begin{aligned} \frac{1}{n!} \sum_{\lambda \vdash n, \lambda \neq (n), \lambda \neq (1^n)} d_\lambda \text{tr} \left[ \left( \frac{\hat{p}(\lambda)^k + \hat{p}(\lambda)^{k+1}}{2} \right) \left( \frac{\hat{p}(\lambda)^k + \hat{p}(\lambda)^{k+1}}{2} \right)^\top \right] \\ = \frac{1}{4n!} \sum_{\lambda \vdash n, \lambda \neq (n), \lambda \neq (1^n)} d_\lambda \text{tr} [(\hat{p}(\lambda)^k + \hat{p}(\lambda)^{k+1}) (\hat{p}(\lambda)^k + \hat{p}(\lambda)^{k+1})^\top]. \quad (22) \end{aligned}$$

補題 1 より  $\hat{p}(\lambda) = \hat{p}(\lambda)^\top$  であるため, この式の値は

$$\begin{aligned} \frac{1}{4n!} \sum_{\lambda \vdash n, \lambda \neq (n), \lambda \neq (1^n)} d_\lambda \text{tr} [(\hat{p}(\lambda)^k + \hat{p}(\lambda)^{k+1}) (\hat{p}(\lambda)^k + \hat{p}(\lambda)^{k+1})] \\ = \frac{1}{4n!} \sum_{\lambda \vdash n, \lambda \neq (n), \lambda \neq (1^n)} d_\lambda \text{tr} [(\hat{p}(\lambda))^{2k} (\hat{p}(\lambda) + I)^2]. \quad (23) \end{aligned}$$

ここで  $\hat{p}$  の固有値を  $\mu_{(\lambda)1}, \dots, \mu_{(\lambda)d_\lambda}$  とし,  $\lambda \vdash n$ ,  $\lambda \neq (n), (1^n)$  の範囲での絶対値における最大固有値を

$$\mu_{\max} = \max_{\lambda \vdash n, \lambda \neq (n), \lambda \neq (1^n), 1 \leq i \leq d_\lambda} (|\mu_{(\lambda)i}|) \quad (24)$$

と定義する. もし  $\mu_{\max} < 1$  なら, 和の下に trace について不等式

$$\begin{aligned} \text{tr} [(\hat{p}(\lambda))^{2k} ((\hat{p}(\lambda) + I)^2)] \\ \leq \mu_{\max}^{2k} (\mu_{\max} + 1) (\text{tr}[(\hat{p}(\lambda))] + \text{tr}[I]) \quad (25) \end{aligned}$$

(証明は付録 A 参照) を適用して

$$\begin{aligned} \|f_k - u\|_2^2 \\ \leq \frac{1}{4n!} \sum_{\lambda \vdash n} d_\lambda \mu_{\max}^{2k} (\mu_{\max} + 1) (\text{tr}[\hat{p}(\lambda)] + \text{tr}[I]). \end{aligned}$$

$\mu_{\max}$  は  $\lambda$  に依らないので前に出すと、右辺は次のように変形できる

$$\begin{aligned} & \frac{1}{4n!} \sum_{\lambda \vdash n} d_\lambda \mu_{\max}^{2k} (\mu_{\max} + 1) (\text{tr}[\hat{p}(\lambda)] + \text{tr}[I]) \\ &= \frac{\mu_{\max}^{2k} (\mu_{\max} + 1)}{4n!} \sum_{\lambda \vdash n} d_\lambda (\text{tr}[\hat{p}(\lambda)] + \text{tr}[I]). \end{aligned}$$

ここで  $\frac{1}{n!} \sum_{\lambda \vdash n} d_\lambda \text{tr}[\hat{p}(\lambda)] = \frac{1}{n!} \sum_{\lambda \vdash n} d_\lambda \text{tr}[\hat{p}(\lambda) \rho_\lambda(e)^T]$  が式 (7) のフーリエ逆変換による単位元での  $p$  の値  $p(e) = 0$  であることおよび  $\sum_{\lambda \vdash n} d_\lambda^2 = n!$  に注意すると  $\sum_{\lambda \vdash n} d_\lambda (\text{tr}[\hat{p}(\lambda)] + \text{tr}[I]) = n!$  である。したがって

$$\begin{aligned} & \frac{\mu_{\max}^{2k} (\mu_{\max} + 1)}{4n!} \sum_{\lambda \vdash n} d_\lambda (\text{tr}[\hat{p}(\lambda)] + \text{tr}[I]) \\ &= \frac{\mu_{\max}^{2k} (\mu_{\max} + 1)}{4} \end{aligned}$$

以上をまとめて次の定理を得る。

**定理 3.** 1 段のあみだくじの確率分布を  $p: S_n$ ,  $k$  段あみだくじの確率分布を  $f_k = \frac{p^{(*)k} + p^{(*)k+1}}{2}$  とする。 $\mu_{\max}$  を式 (24) で定義した  $f_k$  の固有値の最大絶対値とし、 $\mu_{\max} \leq 1$  とする。このとき  $f_k$  と一様分布  $u$  の 2 乗距離の 2 乗は上界

$$\|f_k - u\|_2^2 \leq \frac{1}{4} \mu_{\max}^{2k} (\mu_{\max} + 1)$$

をもつ。

これは  $p(\lambda)$  の固有値の  $\lambda \neq (n), (1^n)$  での絶対値における最大値が 1 未満であれば、 $f_k = \frac{p^{(*)k} + p^{(*)k+1}}{2}$  が、2 乗ノルムにおいて一様分布に収束することを示す。また、 $k$  に対する一様分布との距離の上界が最大固有値で評価できる。

さらに、次節で調査する  $n = 4$  に対する  $k$  段あみだくじのフーリエ解析から次の具体的結果が得られる。

**系 1** (定理 3 に対する).  $n = 4$  に対する  $S_n$  上の一様分布を  $u$ ,  $k$  段あみだくじから生じる  $S_n$  上の分布を  $f_k$  とすると

$$\begin{aligned} \|f_k - u\|_2^2 &\leq \frac{1}{4} \left( \frac{1 + \sqrt{2}}{3} \right)^{2k} \left( \frac{1 + \sqrt{2}}{3} + 1 \right) \\ &\leq 0.451(0.805)^{2k}. \end{aligned}$$

### 3.3 固有値、一様分布との距離の計算

以下では、 $n = 4$  に限定して具体的な数値による計算を行う。隣接置換を一回行った置換の確率分布  $p_1$  とおき、 $n = 4$  としたときの各  $\lambda \vdash 4$  に対する  $p_1$  のフーリエ係数行列とその固有値を示す。行列のインデックスとなる標準ヤング盤を行および列に添え書きしてある。

$$\begin{aligned} \hat{p}_{1(4)} &= \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline \end{array} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \hat{p}_{1(3,1)} &= \begin{array}{|c|c|c|} \hline 1 & 3 & 4 \\ \hline 2 \\ \hline 1 & 2 & 4 \\ \hline 3 \\ \hline 1 & 2 & 3 \\ \hline 4 \end{array} \begin{pmatrix} \frac{1}{6} & \frac{\sqrt{3}}{6} & 0 \\ \frac{\sqrt{3}}{6} & \frac{5}{9} & \frac{2\sqrt{2}}{9} \\ 0 & \frac{2\sqrt{2}}{9} & \frac{5}{9} \end{pmatrix} \\ \hat{p}_{1(2,2)} &= \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline 1 & 2 \\ \hline 3 & 4 \end{array} \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{6} \\ \frac{\sqrt{3}}{6} & \frac{1}{2} \end{pmatrix} \\ \hat{p}_{1(2,1,1)} &= \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 \\ \hline 1 & 3 \\ \hline 2 \\ \hline 1 & 2 \\ \hline 3 \\ \hline 4 \end{array} \begin{pmatrix} -\frac{5}{9} & \frac{2\sqrt{2}}{9} & 0 \\ \frac{2\sqrt{2}}{9} & -\frac{5}{18} & \frac{\sqrt{3}}{6} \\ 0 & \frac{\sqrt{3}}{6} & -\frac{1}{6} \end{pmatrix} \\ \hat{p}_{1(1,1,1,1)} &= \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \end{array} \begin{pmatrix} -1 \end{pmatrix} \end{aligned}$$

次に隣接互換の他に 1 と  $n$  の互換を認めた、環状のあみだくじ (定義 2) を考える。この環状のあみだくじの 1 段、つまり一回置換の確率分布を  $p_2$  とおき、フーリエ係数行列とその固有値を示す。

$$\begin{aligned} \hat{p}_{2(4)} &= \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline \end{array} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \hat{p}_{2(3,1)} &= \begin{array}{|c|c|c|} \hline 1 & 3 & 4 \\ \hline 2 \\ \hline 1 & 2 & 4 \\ \hline 3 \\ \hline 1 & 2 & 3 \\ \hline 4 \end{array} \begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{12} & -\frac{\sqrt{6}}{12} \\ \frac{\sqrt{3}}{12} & \frac{5}{12} & \frac{\sqrt{2}}{12} \\ -\frac{\sqrt{6}}{12} & \frac{\sqrt{2}}{12} & \frac{1}{3} \end{pmatrix} \\ \hat{p}_{2(2,2)} &= \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline 1 & 2 \\ \hline 3 & 4 \end{array} \begin{pmatrix} -\frac{1}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix} \end{aligned}$$

$$\hat{p}_{2(2,1,1)} = \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 3 & 2 \\ 1 & 3 \\ 2 & 2 \\ 4 & 1 \\ 1 & 2 \\ 3 & 4 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 3 & 2 \\ 1 & 3 \\ 2 & 2 \\ 4 & 1 \\ 1 & 2 \\ 3 & 4 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \\ 3 & 2 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 4 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} -\frac{1}{3} & \frac{\sqrt{2}}{12} & \frac{\sqrt{6}}{12} \\ \frac{\sqrt{2}}{12} & -\frac{5}{12} & \frac{\sqrt{3}}{12} \\ \frac{\sqrt{6}}{12} & \frac{\sqrt{3}}{12} & -\frac{1}{4} \end{pmatrix}$$

$$\hat{p}_{2(1,1,1,1)} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \begin{pmatrix} -1 \end{pmatrix}$$

表 1: フーリエ係数行列の固有値

確率分布	(4) 固有値		(3, 1) 固有値		
$p_1$	1	$\frac{1}{3}$	$\frac{1-\sqrt{2}}{3}$	$\frac{1+\sqrt{2}}{3}$	$\frac{1+\sqrt{2}}{3}$
$p_2$	1	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
確率分布	(2, 2) 固有値		(2, 1, 1) 固有値		
$p_1$	$\frac{\sqrt{3}}{3}$	$-\frac{\sqrt{3}}{3}$	$-\frac{1}{3}$	$-\frac{1-\sqrt{2}}{3}$	$-\frac{1+\sqrt{2}}{3}$
$p_2$	$\frac{1}{2}$	$-\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{1}{2}$
確率分布	(1, 1, 1, 1) 固有値				
$p_1$	-1				
$p_2$	-1				

表 1 より, (4) 固有値と (1, 1, 1, 1) 固有値以外の最大固有値から, 繰り返し回数  $k$  に対する確率分布の一樣分布との距離の上界が分かる. 定理 3 系 1 と同様に  $k$  段環状あみだくじの一樣分布からの距離の 2 乗は  $\frac{3}{8}(\frac{1}{2})^{2k}$  を上界にもつ.  $p_1, p_2$  の繰り返し回数に対する, 一樣分布との距離のグラフを図 3 に示す. この図から, 環状あみだくじが通常あみだくじより少ない段数で一樣分布に近づくことが分かる. また, それぞれの上界においても環状あみだくじが通常あみだくじより少ない段数で一樣分布に近づいている.

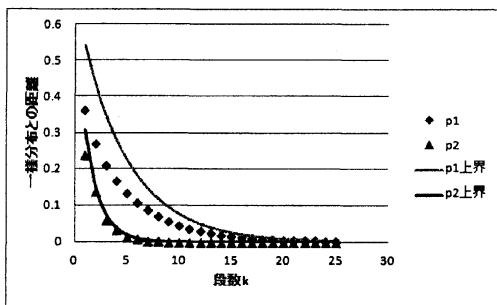


図 3: 段数  $k$  に対する  $p_1, p_2$  の一樣分布との距離

### 3.4 ラベル依存度の実験的計算

通常あみだくじの一回置換の確率分布  $p_1$  と, 環状あみだくじの一回置換の確率分布  $p_2$  の繰り返し回数に対するラベル依存度のグラフを図 4 に示す.

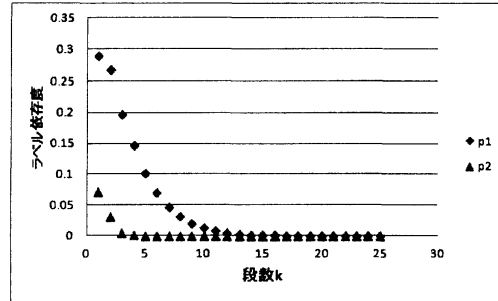


図 4: 段数  $k$  に対する  $p_1, p_2$  のラベル依存度

疑似ランダム置換として縦線が  $n$  本の  $3n$  段あみだくじによる確率分布を考え, 実験的に  $|S_n| \times 10$  回あみだくじを発生させて得られる  $\sigma \in S_n$  の分布を  $f_1(\sigma)$  とする. 次に 1 本目と  $n$  本目を繋ぐことのできる環状あみだくじ ( $f_2$ ) と環状あみだくじに 2 つ隣の縦棒に繋がられる条件を追加したあみだくじ ( $f_3$ ), さらにすべての縦線の間横棒を引くことを許したあみだくじ ( $f_4$ ) のラベル依存度を計算した.  $n = 4$  から 11 までの結果を表 2 に示す.

表 2: あみだくじのラベル依存度

$n$	$LD(f_1)$	$LD(f_2)$	$LD(f_3)$	$LD(f_4)$
4	0.06	0.06	0.06	0.05
5	0.19	0.09	0.08	0.08
6	0.38	0.09	0.09	0.09
7	0.58	0.14	0.09	0.09
8	0.74	0.29	0.09	0.09
9	0.84	0.54	0.10	0.09
10	0.91	0.75	0.13	0.09
11	0.95	0.88	0.20	0.09

## 4 まとめ

隣接置換の繰り返しによる疑似ランダム置換 (あみだくじ) に注目し, その確率分布の性質を対称群上



のフーリエ解析に基づいて調査した。その結果確率分布関数と一様分布との距離がフーリエ係数行列の固有値とあみだくじの段数によって上から抑えられることを示した (定理 3)。さらに、置換される対象の数  $n = 4$  のとき (あみだくじの縦棒が 4 本) のあみだくじ (定義 1) の具体的な上界を導出した (定理 3 系 1)。また  $n = 4$  のとき、あみだくじと環状あみだくじ (定義 2) を比較し、後者の確率分布関数と一様分布との距離およびラベル依存度が前者のそれより減少することを示した。

## 謝辞

トレースの不等式についてご教示頂いた和田州平氏に感謝いたします。

## 参考文献

- [1] J.-P. セール. 有限群の線形表現. 岩波書店. 1974.
- [2] Audrey Terras: *Fourier Analysis on Finite Groups and Applications* London Math. Soc. Student Texts 43, 1999
- [3] Risi Kondor. Group theoretical methods in machine learning. Ph.D. thesis, Columbia University, 2008.
- [4] 小川 浩明, 武井 由智. “対称群上の未知関数のラベル依存度の抽出”, 平成 24 年度 電子情報通信学会信越支部大会 講演論文集, 2C-2, Oct. 2012.
- [5] Persi Diaconis: *Group Representations in Probability and Statistics*. IMS. 1988.

## 付録 A トレーズの不等式 (25) の証明

**補題 2.** 実数  $x(-1 < -\alpha < x < \alpha < 1)$  に対して

$$x^{2k}(x+1)^2 \leq \alpha^{2k}(\alpha+1)(x+1).$$

**証明.** 関数  $f(x) := x^{2k}(1+x)$  を考える.  $x \geq 0$  において  $f(x)$  は増加である. よって

$$0 \leq x \leq \alpha \Rightarrow f(x) \leq f(\alpha). \quad (26)$$

$x < 0$  に対して,  $\xi = -x = |x| > 0$  とおくと

$$f(x) = f(-\xi) = \xi^{2k}(1-\xi) < \xi^{2k}(1+\xi) = f(\xi).$$

よって, 式 (26) で  $x = \xi$  としたのから

$$0 \leq |x| \leq \alpha \Rightarrow f(x) \leq f(\alpha).$$

つまり  $|x| \leq \alpha$  なら  $x^{2k}(1+x) \leq \alpha^{2k}(1+\alpha)$ . さらに  $\alpha \leq 1$  なら  $1+x \geq 0$  から  $x^{2k}(1+x)^2 \leq \alpha^{2k}(1+\alpha)(1+x)$ .  $\square$

**命題 1.** 実対称行列  $A$  に対し, その絶対値における最大固有値を  $\alpha$  とするとき,  $\alpha \leq 1$  なら

$$\text{tr}[A^{2k}(A+I)^2] \leq \alpha^{2k}(\alpha+1)(\text{tr}[A+I]).$$

**証明.**  $A$  の固有値を  $\mu_1, \dots, \mu_d$  とする. 補題 2 の  $x$  を  $\mu_i$  として足し合わせ,

$$\sum_{i=1}^d \mu_i^{2k}(\mu_i+1)^2 \leq \alpha^{2k}(\alpha+1) \sum_{i=1}^d (\mu_i+1) \quad (27)$$

$D = UAU^{-1} = \begin{pmatrix} \mu_1 & & 0 \\ & \ddots & \\ 0 & & \mu_d \end{pmatrix}$  とするとき, 左辺は

$\text{tr}[D^{2k}(D+I)^2]$  であり, これは

$$\begin{aligned} & \text{tr}[U^{-1}(D^{2k}(D+I)^2)U] \\ &= \text{tr}[U^{-1}D^{2k}UU^{-1}(D+I)^2U] \\ &= \text{tr}[A^{2k}(A+I)^2] \end{aligned}$$

に等しい. また, 式 (27) の右辺は

$$\alpha^{2k}(\alpha+1)(\text{tr}[A] + \text{tr}[I])$$

である.  $\square$