量子通信路研究における確率論的手法

福田　素久

2017 年 02 月 18 日

目 次

1　量子通信路と加法性の問題について

1.1 量子状態

量子状態は半正定値エルミート行列（$n \times n$）でトレースが 1 のものとする。例えば量子状態を $\rho \in M_n(\mathbb{C})$ と書くと、

- （量子）状態は離散確率分布を与える。

$$\rho \sim \mathrm{diag}(p_1, \ldots, p_n)$$

- よって、状態は Entropy を与える。

$$S(\rho) = -\sum_{i=1}^{n} p_i \log p_i$$

  - ランクが 1 の場合は特に純粋（量子）状態と呼ばれ、エントロピーは 0 になる。
  - $\rho = I/n$ のときはエントロピーは $\log n$ になる。

- 「古典情報 (対角行列) は可換で量子情報は非可換」。

1.2　量子通信路

（量子）通信路 $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ に必要な条件は?

- 正写像であること。
- トレースを保存すること。
- さらに、完全正写像であることが求められる。

初めの 2 つは状態を状態に写すことから必要。完全正写像性は他の量子システムを考えると理解できる。つまり $\sigma \in M_{nm}(\mathbb{C}) = M_n(\mathbb{C}) \otimes M_m(\mathbb{C})$ という状態を考えると、

$$\Phi \otimes \mathrm{id}_m(\sigma)$$

も半正定値にならなければならない。つまり、「$\Phi \otimes \mathrm{id}_m$ が任意の m に対して正写像になる」という完全正写像性が導き出される。

ちなみに、正写像であるが完全正写像でない例として Transpose が挙げられる。

Stinespring の方法

トレースを保存する完全正写像は Stinespring の枠組みで考えると、

$$\Phi(\rho) = \underset{\mathbb{C}^k}{\mathrm{Tr}}\left[V\rho V^*\right]$$

と書ける。ここで $V : \mathbb{C}^n \to \mathbb{C}^k \otimes \mathbb{C}^n$ は等長写像で、$\mathbb{C}^k$ は Environment とする。

ここで V を $U \in \mathcal{U}(kn)$ の最初の n 列を取ってきたものとして定義すると、$\mathcal{U}(kn)$ の Haar 測度から自然な測度が定義できる。これを持って、 ランダムな通信路を定義することができる。

この考えをもう少し推し進めると、通信路は以下のように見ることもできる。

$$\underset{\mathbb{C}^k}{\mathrm{Tr}} : L(E) \to M_n(\mathbb{C})$$

ここで、$E = \mathrm{Image}(V) \leq \mathbb{C}^k \otimes \mathbb{C}^n$ は n 次元部分空間で、 $L(E)$ はその空間に作用する行列空間。つまり、(ランダム) 通信路とは（ランダム）部分空間である。

1.3 Minimum Output Entropy とその加法性/非加法性

- Minimum Output Entropy の定義：
  通信路 Φ に対して、Minimum Output Entropy は

$$S_{\min}(\Phi) = \min_{\rho} S(\Phi(\rho))$$

  で定義される。ここで、ρ は状態。

- 加法性/非加法正の問題の定式化：２つの通信路 Φ, Ω に対して、

$$S_{\min}(\Phi \otimes \Omega) \stackrel{?}{=} S_{\min}(\Phi) + S_{\min}(\Omega)$$

$$S_{\min}(\Phi \otimes \Omega) \stackrel{?}{<} S_{\min}(\Phi) + S_{\min}(\Omega)$$

  2008 年に Hastings が非加法性を示す通信路が存在することを示すまでは一般的に加法性が成立すると信じられていた。

- 数学的な問題意識：
  任意の状態 ρ, σ に対して、

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$$

  となるため、以下は常に成立する。

$$S_{\min}(\Phi \otimes \Omega) \leq \min_{\rho \otimes \sigma} S(\Phi \otimes \Omega(\rho \otimes \sigma)) = S_{\min}(\Phi) + S_{\min}(\Omega)$$

- 情報理論的な問題意識：
  - 「Entropy $=$ 負の情報」と考えると、Entropy が小さい Output があるとよい。（本当はもっと複雑だが。。。）
  - N 回通信が行われ、各通信のノイズが独立だとすると、複数回の通信全体は $\Phi^{\otimes N}$ と表現できる。このとき、

$$S_{\min}(\Phi^{\otimes N}) \stackrel{?}{=} N \cdot S_{\min}(\Phi)$$

    が問題になる。上記の加法性の問題はこの一般型である。

- Shor が 2003 年に Minimum Output Entropy の問題と通信量の問題が全体として同値であることを示す。[1] これにより、通信量の問題が行列の固有値の問題に帰着される。

- 証明された事実：
  $1 << k << n$ のとき、上に定義したランダムな通信路を考えると、高い確率で Minimum Output Entropy の非加法性を示す（Hastings 2008）。

- 数学的深化：

  - 厳密な証明：
    F, King, Moser[2] ; Brandao, Horodecki
  - Asymptotic Geometric Analysis：
    Aubrun, Szarek, Werner; F
  - 自由確率：
    Belinschi, Collins, Nechita

[1] P. Shor, Comm. Math. Phys., 246(3):453472, (2004)
[2] M.F., C. King, D. Moser, Comm. Math. Phys., 296, 1, 111-143 (2010)

2　非加法性を示す通信路の存在

2.1 Asymptotic Geometric Analysis によるアプローチ

以下に、Aubrun, Szarek, Werner が通信路の非加法性を証明した[3] アイデアを理解する。そのために同著者が示した通信路の非乗法性[4] について解説する。

通信路の非乗法性とは $p > 1$ に対して

$$\|\Phi \otimes \Omega\|_{1\to p} > \|\Phi\|_{1\to p} \cdot \|\Omega\|_{1\to p}$$

となることである。定義にある $\|\cdot\|_{1\to p}$ は Maximum Output p-Norm と呼ばれ

$$\|\Phi\|_{1\to p} = \max_{\rho} \|\Phi(\rho)\|_p$$

のように Output の最大 Schatten Norm で定義される。ここで、ρ は状態である。

非乗法性と非加法性の関係は、Renyi Entropy の定義よりわかる：

$$\frac{1}{1-p} \log \mathrm{Tr}[\sigma^p] = \frac{p}{1-p} \log \|\sigma\|_p$$

Renyi Entropy は $p \to 1$ で Entropy に収束する。

---

[3] G. Aubrun, S. Szarek, and E. Werner, Comm. Math. Phys., 305(1):8597, (2011)
[4] G. Aubrun, S. Szarek, and E. Werner, J. Math. Phys., 51(2):022102, (2010)

Aubrun, Szarek, Werner のモデル

以下のランダムな等長写像を使って通信路 Φ を定義する:

$$V : \mathbb{C}^{d^{1+1/p}} \to \mathbb{C}^d \otimes \mathbb{C}^d$$

これに対し、その複素共役 $\bar{\Phi}$ を $\bar{V}$ で定義すれば、高い確率で

$$\|\bar{\Phi}\|_{1\to p} = \|\Phi\|_{1\to p} \sim d^{-1+1/p} \leq \|\Phi \otimes \bar{\Phi}\|_{1\to p} \tag{1}$$

となる。もちろん $p > 1$ に対して n を大きくとれば

$$\|\bar{\Phi}\|_{1\to p} \cdot \|\Phi\|_{1\to p} < \|\Phi \otimes \bar{\Phi}\|_{1\to p}$$

ここで評価 (1) において、

- 漸近的振る舞いは Dvoretzky の定理で証明できる。
- 不等式を示すには以下の性質を使う。

$$U \otimes \bar{U}|b\rangle = |b\rangle$$

Dvoretzky の定理を使って

- Dvoretzky の定理の重要な部分だけを書き抜けば以下のようになる。
  実ノルム空間 $(\mathbb{R}^n, \|\cdot\|)$ に対して、ある部分空間 E が存在して

$$(1-\epsilon)\, M\, \|x\|_2 \leq \|x\| \leq (1+\epsilon)\, M\, \|x\|_2 \qquad \forall x \in E$$

  M は S^{n-1} 上で一様にランダムな x に対しての $\|x\|$ の Median とする。

- 長さが 1 のベクトル $|x\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ に対し、

$$\left\| \operatorname*{Tr}_{\mathbb{C}^n} [|x\rangle\langle x|] \right\|_p = \|XX^*\|_p = \|X\|_{2p}^2$$

  に注意して、以下の設定で Dvoretzky の定理を適用する。

$$S^{2d^2-1} \ni x \longmapsto \|X\|_{2p} \in \mathbb{R}$$

- 通信路はテンソル積空間の部分空間なので、ある通信路 Φ が存在して、

$$\|\Phi(|x\rangle\langle x|)\|_p \sim d^{-1+\frac{1}{p}} \qquad \forall \text{ 純粋な Input } |x\rangle\langle x|$$

複素共役な通信路とのテンソル積

任意に選んだ通信路とその複素共役にたいして Input を Bell 状態とすると Output は大きな固有値を持つ。Bell 状態とはテンソル積空間上の以下のベクトルへの射影として定義される。Bra-Ket 記号を乱用すると

$$|b_l\rangle = \sum_{i=1}^{l} |i\rangle \otimes |i\rangle$$

と書くことができる。このとき、Input 空間を $\mathbb{C}^l$、 Output 空間を $\mathbb{C}^n$、また、Environment 空間を $\mathbb{C}^k$ とすると、

$$\langle b_n| \left[\Phi \otimes \bar{\Phi}(|b_l\rangle\langle b_l|)\right] |b_n\rangle \geq \frac{l}{kn}$$

が言える。Aubrun, Szarek, Werner の設定では

$$\frac{l}{kn} = d^{1+\frac{1}{p}} \cdot d^{-2} = d^{-1+\frac{1}{p}}$$

よって

$$\|\Phi \otimes \bar{\Phi}\|_{1\to p} \geq d^{-1+\frac{1}{p}}$$

となる。

Bell Input と大きい固有値を持つ Output の計算

$$
\begin{aligned}
&\langle b_n| \left[\Phi \otimes \bar{\Phi}(|b_l\rangle\langle b_l|)\right] |b_n\rangle \\
&= \langle b_n| \left[\sum_{i,j=1}^{k} (\langle i,j| \otimes I_{n^2})V \otimes \bar{V}|b_l\rangle\langle b_l|V^* \otimes V^T(|i,j\rangle \otimes I_{n^2})\right] |b_n\rangle \\
&= \sum_{i,j=1}^{k} (\langle i,j| \otimes \langle b_n|)V \otimes \bar{V}|b_l\rangle\langle b_l|V^* \otimes V^T(|i,j\rangle \otimes |b_n\rangle) \\
&= \langle b_l|V^* \otimes V^T \left(\sum_{i,j=1}^{k} |i,j\rangle\langle i,j| \otimes |b_n\rangle\langle b_n|\right) V \otimes \bar{V}|b_l\rangle \\
&\geq \langle b_l|V^* \otimes V^T \left(|b_k\rangle\langle b_k| \otimes |b_n\rangle\langle b_n|\right) V \otimes \bar{V}|b_l\rangle \\
&= \left|\langle b_l|V^* \otimes V^T \left(|b_k\rangle \otimes |b_n\rangle\right)\right|^2 = \left|\langle b_l| \frac{1}{\sqrt{kn}} \left[\sum_{i=1}^{l} |i\rangle \otimes |i\rangle\right]\right|^2 \geq \frac{l}{kn}
\end{aligned}
$$

ここで、 $V^* \otimes V^T \left(\sum_{i=1}^{kn} |i\rangle \otimes |i\rangle\right) = V^*V \otimes I_l \left(\sum_{i=1}^{l} |i\rangle \otimes |i\rangle\right)$

証明の改良

通信路の乗法性に関しては Dvoretzky の定理を直接適用して示すことができた。しかし、Entropy をノルムを使って表現することはできないため、通信路の加法性を示すには改良が必要となる。

- Dudley の不等式を使う。 (Aubrun, Szarek, Werner [5])
- Dvoretzky の定理の重要なアイデアが使えるように工夫する。(F [6])

残された問題

- 非加法性を示す通信路の具体例を見つける。
  非乗法性に関しては、$p > 2$ で具体例が見つかっている。
  (Grudka, Horodecki, Pankowski [7])
- 非加法性の程度を探る。

---

[5] G. Aubrun, S. Szarek, E. Werner, Comm. Math. Phys., 305(1):8597, (2011)
[6] M.F., Comm. Math. Phys., 332, 2, 713-728 (2014)
[7] A. Grudka, M. Horodecki, L. Pankowski, J. Phys. A, 43(42):425304, 7, (2010)

2.2　自由確率論を使ったアプローチ

Belinschi, Collins, Nechita の手法[8] を以下に説明する。

- Unitary 行列を使って等長写像を定義する。

$$UP : \mathbb{C}^{tnk} \to \mathbb{C}^n \otimes \mathbb{C}^k$$

ここで、P は射影で UP は P の Support に制限してある。Support の次元は tnk とする。($0 < t < 1$)

- この等長写像を使って通信路 Φ を定義して、その Output を知るために以下の計算を行う。

$$\mathrm{Tr}[\Phi(|x\rangle\langle x|)A] = \mathrm{Tr}\left[\underset{\mathbb{C}^n}{\mathrm{Tr}}[UP|x\rangle\langle x|PU^*]A\right] = \langle x|PU^*(I \otimes A)UP|x\rangle$$

つまり、以下の極限に興味がある。

$$\max_x \mathrm{Tr}[\Phi(|x\rangle\langle x|)A] \;=\; \|PU^*(I \otimes A)UP\|_\infty \longrightarrow \quad ?$$

ここで、 t, k は固定して、$n \to \infty$ の場合を考える。

[8] S. Belinschi, B. Collins, I. Nechita, Commun. Math. Phys., 341: 885, (2016)

- Collins, Male が証明した強収束性[9] の重要な部分は以下のように書ける。

$$\|\mathrm{Poly}(U_1, U_1^* \ldots, U_p, U_p^*, Y_1, Y_1^*, \ldots, Y_q, Y_q^*)\|_\infty$$
$$\to \|\mathrm{Poly}(u_1, u_1^* \ldots, u_p, u_p^*, y_1, y_1^*, \ldots, y_q, y_q^*)\|$$

  (ほとんど至る所の収束)。ここで、

  - U_i は Haar 測度で独立分布。
  - u_i は C^*-代数確率空間の Unitary 要素で自由独立。

- 上の結果は以下の GUE ランダム行列の半円要素 $(x_i)_{i=1}^p$ への強収束の結果の延長にある。

  - $\|\mathrm{Poly}(x_1, \ldots, x_p)\|$ への収束（Haagerup and Thorbjørnsen[10]）
  - $\|\mathrm{Poly}(x_1, \ldots, x_p, y_1, y_1^*, \ldots, y_q, y_q^*)\|$ への収束 (Male[11])

---

[9] B. Collins and C. Male, Ann. Sci. Ec. Norm. Supr. (4), 47(1):147-163, (2014)
[10] U. Haagerup and S. Thorbjørnsen, Ann. of Math. (2), 162(2):711775, (2005)
[11] C. Male, Prob. Theo. Rela. Fiel.,1-56, June (2011)

2.3　関連するもう一つの例

通信路が以下のように定義されているとする。

$$\Psi(\rho) = \frac{1}{k}\sum_{i,j=1}^{k}\left[U_i \rho U_j^*\right]|i\rangle\langle j| \qquad \left(\Omega(\rho) = \frac{1}{k}\sum_{i=1}^{k} U_i \rho U_1^* \quad \text{と関連}\right)$$

このとき、

$$\rho = |x\rangle\langle x| \in M_n(\mathbb{C}), \qquad A = |a\rangle\langle a| \in M_k(\mathbb{C})$$

として、以前の計算を行うと、

$$\max_x \mathrm{Tr}\left[\Psi(|x\rangle\langle x|)|a\rangle\langle a|\right] = \max_x \langle x| \sum_{i,j=1}^{k} \bar{a}_i a_j U_j^* U_i |x\rangle$$

$$= \left\| \sum_{i=1}^{k} \bar{a}_i U_i \right\|_\infty^2 \longrightarrow \left\| \sum_{i=1}^{k} \bar{a}_i u_i \right\|^2$$

この値は Akemann, Ostrand によって計算[12] されており、その結果:

$$\|\Omega\|_{1\to\infty} = \|\Psi\|_{1\to\infty}$$

[12] C. Akemann, P. Ostrand, Amer. J. Math., 98.4, 10151047, (1976)

3　解決すべき問題と関連問題

3.1 解決すべき問題

- 以下のように正則化された Minimum Output Entropy は $N \to \infty$ のときどのように振る舞うか?

$$\frac{1}{N} S\left(\Phi^{\otimes N}\right)$$

これは、理論的に興味深いが、現実的には以下のような意見もある。

  - 実際には無限回の通信を行うことができず、有限回の通信について研究するのが興味深い。
  - ノイズが独立でない場合は N 回の通信は $\Phi^{\otimes N}$ と表現できない。

- 通信の非加法性を示す具体例を見つける。
  - ランダムな構成法だと、高次元では典型的に非加法性を示す。
  - 最近は、Brannan, Collins が Quantum Group の表現を使って研究 [13]

- 通信路容量の問題を理解するために Output が構成する空間の構造を理解する。

[13] M. Brannan, B. Collins, arXiv:1612.09598 [math-ph]

3.2 関連する問題 - メアンダー多項式との関連

以下のランダム行列は Meander 多項式を生成する。これは、Di Francesco が発見したランダム行列モデルより簡単なものとなる。[14]

1. 単位球上で一様に分布しているランダムベクトルを考える。

$$|x\rangle \in \mathbb{C}^r \otimes \mathbb{C}^n \otimes \mathbb{C}^n$$

2. 次に $\mathbb{C}^r$ 上で $|x\rangle\langle x|$ の Trace をとる。

$$XX^* \in M_{n^2}(\mathbb{C})$$

3. 最後に 2 つの $\mathbb{C}^n$ のうち 1 つで Transpose をとる。

$$[XX^*]^\Gamma \in M_{n^2}(\mathbb{C})$$

---

[14] P. Di Francesco, Rand. matr. mode. appl., volume 40 of Math. Sci. Res. Inst. Publ., pages 111-170. CUP, (2001)

- このランダム行列 $[XX^*]^\Gamma$ の $2n$ 次 Moment を計算すると、Meander 多項式が出てくる。[15]

$$\sum_{k=1}^{n} r^k M_n^{(k)}$$

- $M_n^{(k)}$ は 「無限に長い川に橋が $2n$ 個架かっていて、どの橋も一度だけ渡り、k 個のループができるような歩く道のパターン数」。折れ曲がる閉じた高分子と同一視できる。

- この考えを進めて、Meander 多項式を自由確率論の手法を使って研究した。今のところ、Meander 多項式を生成する方法は見つかっていない。[16]

[15] F, P. Sniady, J. Math. Phys., 54, 042202 (2013)
[16] F, I. Nechita, arXiv:1609.02756 [math.CO].

4　謝辞

本日はご清聴有難うございました。

スライドに載っていた自身の結果は以下の支援を受けました。

- CHISTERA/BMBF project CQC
- John Templeton Foundation (ID#48322)
- JSPS 科研費 JP16K00005