

Rayleigh-normal 分布の導入とその応用

熊谷 亘

神奈川大学工学部

Wataru Kumagai

Faculty of Engineering, Kanagawa University

Abstract

近年, Kumagai and Hayashi[9] は Rayleigh-normal 分布と呼ばれる新種の確率分布を導入した. Rayleigh-normal 分布族は特定のパラメータを持つ Rayleigh 分布と標準正規分布を含み, 古典情報理論における乱数変換や量子情報理論における純粋状態の LOCC 変換と密接に関連している. 本論文では Rayleigh-normal 分布の基本的な性質を紹介し, その情報理論における役割を説明する.

1 Rayleigh-Normal 分布の導入

本節では Rayleigh-normal 分布の基本的な性質を述べる. 詳しくは Kumagai and Hayashi[9] を参照せよ.

1.1 Rayleigh-Normal 分布の定義

ある特定のパラメータをもつ Rayleigh 分布と標準正規分布をつなぐ $\mathbb{R}$ 上の新種の確率分布を導入する. $\mathbb{R}$ 上の関数 Z で, 右連続, 広義単調増加であり $\lim_{x \rightarrow -\infty} Z(x) = 0$ と $\lim_{x \rightarrow \infty} Z(x) = 1$ をみたすものは一般に累積分布関数と呼ばれる. 累積分布関数 Z に対し, 累積分布が Z に一致するような確率分布が一意的に定まる. すなわち, 上記の意味での累積分布関数が与えられたとき, それは $\mathbb{R}$ 上の確率分布を一つ定めるのである. 新種の確率分布を定めるために, 本節ではその累積確率分布を与える.

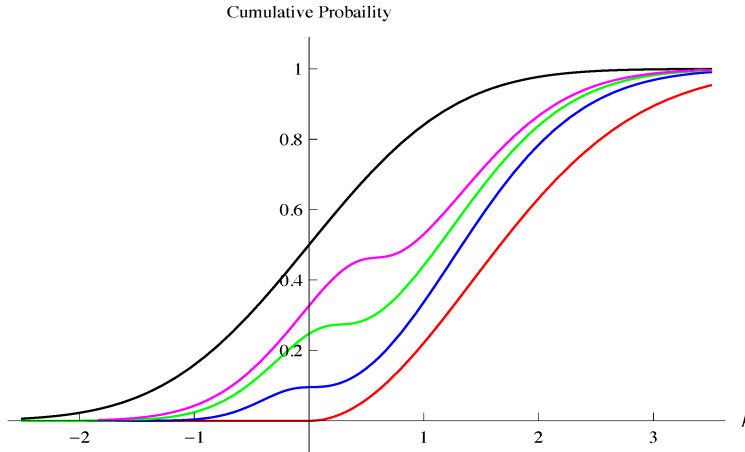


Figure 1: Rayleigh-normal 分布関数のグラフ. 黒, 紫, 緑, 青, 赤はそれぞれパラメータ $v = 0, 1/10, 1/6, 1/3, 1$ をもつ Rayleigh-normal 分布関数を表す.

以後, $\Phi_{\mu,v}$ と $N_{\mu,v}$ は平均 $\mu \in \mathbb{R}$ と分散 $v \in \mathbb{R}_+$ を持つ正規分布の累積分布関数と密度関数とする. 簡単のため $\Phi_{0,1}$ と $N_{0,1}$ を Φ と N と表す. $\mathbb{R}$ 上の連続確率分布 p と q に対し, 連続忠実度 (または Bhattacharyya 係数) を

$$\mathcal{F}(p, q) := \int_{\mathbb{R}} \sqrt{p(x)q(x)} dx \quad (1)$$

と定めるとき, 以下のように関数を定める.

Definition 1 実数 $v > 0$ に対し, $\mathbb{R}$ 上の Rayleigh-normal 分布関数 Z_v は以下のように定められる

$$Z_v(\mu) = 1 - \sup_A \mathcal{F}\left(\frac{dA}{dx}, N_{\mu,v}\right)^2, \quad (2)$$

ただし $A: \mathbb{R} \rightarrow [0, 1]$ は連続微分可能かつ単調増加であり $\Phi \leq A \leq 1$ を満たす関数を表す.

Rayleigh-normal 分布関数が累積分布関数である. すなわち, それは $\mathbb{R}$ 上の確率分布を表す. Rayleigh-normal 分布のグラフは Fig. 1 のように表される.

1.2 Rayleigh-Normal 分布の性質

始めに Rayleigh-Normal 分布族はスケールパラメータ $\sqrt{2}$ の Rayleigh 分布と標準正規分布をつなぐことを示す. Rayleigh-normal 分布関数の具体的な形を与えるために, 2つの補題を用意

する.

Lemma 1 パラメータが $v < 1$ をみたすとき, x に関する方程式

$$\frac{N(x)}{N_{\mu,v}(x)} = \frac{1 - \Phi(x)}{1 - \Phi_{\mu,v}(x)} \quad (3)$$

は $\beta_{\mu,v} < \frac{\mu}{1-v}$ を満たす一意的な解を持つ.

Lemma 2 パラメータが $v > 1$ をみたすとき, x に関する方程式

$$\frac{N(x)}{N_{\mu,v}(x)} = \frac{\Phi(x)}{\Phi_{\mu,v}(x)} \quad (4)$$

は $\alpha_{\mu,v} > \frac{\mu}{1-v}$ を満たす一意的な解を持つ.

スケールパラメータ $\sigma > 0$ をもつ Rayleigh 分布の累積分布関数を以下のように表す.

$$R_{\sigma}(x) = \begin{cases} 1 - e^{-\frac{x^2}{2\sigma^2}} & \text{if } x > 0 \\ 0 & \text{if } x \leq 0. \end{cases}$$

そのとき, Rayleigh-normal 分布関数の族は以下のように表される. 特に, その族は $v = 1$ の時にスケールパラメータ $\sqrt{2}$ の Rayleigh 分布を含む.

Theorem 1 実数 $v > 0$ に対し,

$$Z_v(\mu) = \begin{cases} 1 - (\sqrt{1 - \Phi(\beta_{\mu,v})} \sqrt{1 - \Phi_{\mu,v}(\beta_{\mu,v})} + I_{\mu,v}(\beta_{\mu,v}))^2 & \text{if } v < 1 \\ R_{\sqrt{2}}(\mu) & \text{if } v = 1 \\ 1 - (\sqrt{\Phi(\alpha_{\mu,v})} \sqrt{\Phi_{\mu,v}(\alpha_{\mu,v})} + I_{\mu,v}(\infty) - I_{\mu,v}(\alpha_{\mu,v}))^2 & \text{if } v > 1, \end{cases} \quad (5)$$

ただし

$$I_{\mu,v}(x) := \sqrt{\frac{2\sqrt{v}}{1+v}} e^{-\frac{\mu^2}{4(1+v)}} \Phi_{\frac{\mu}{1+v}, \frac{2v}{1+v}}(x), \quad (6)$$

$$I_{\mu,v}(\infty) := \lim_{x \rightarrow \infty} I_{\mu,v}(x) = \sqrt{\frac{2\sqrt{v}}{1+v}} e^{-\frac{\mu^2}{4(1+v)}}. \quad (7)$$

ここで $\lim_{v \rightarrow 0} Z_v(\mu) = \Phi$ が容易にわかる. 従って, Rayleigh-normal 分布関数の族は Rayleigh 分布と標準正規分布をつなぐ.

定理 1 より, Rayleigh-normal 分布関数の一種の対称性を示すことができる.

Lemma 3

$$Z_v(\mu) = Z_{v-1}\left(\frac{\mu}{\sqrt{v}}\right). \quad (8)$$

最後に最も基本的な性質を与える.

Proposition 1 *Rayleigh-normal* 分布関数 Z_v は $v \geq 0$ に対し累積分布関数である.

命題 1 により, 関数 Z_v の族は $\mathbb{R}$ 上の一変数 $v \geq 0$ の確率分布の族を定める. 関数 Z_v によって定まる確率分布を *Rayleigh-normal* 分布関数と呼ぶことにする. *Rayleigh-normal* 分布関数の族は, 2 次漸近解析において最適変換のレートを表すことができる. 次節ではその性質に関して触れる.

2 Rayleigh-Normal 分布の操作的意味

2.1 古典情報理論における乱数変換

古典情報理論における乱数の変換は, 決定的変換と呼ばれる写像によって記述される. また, 決定的変換は仮想的な変換である Majorization 変換と密接に関係しているが, ここでは Majorization 変換の詳細には触れないが, Majorization 変換は量子情報理論において自然な操作的意味を持つことに言及しておく. 本論文では, 2 つの確率分布 P と Q の独立同一分布に対する乱数変換を, 漸近的な文脈で扱う.

ここで F を離散確率分布の間の忠実度 (もしくは Bhattacharyya 係数) を表すとする. そのとき, 変換精度 $0 < \nu < 1$ のもとで, 独立同一な確率分布 P^n から対象の確率分布 Q への最大変換数を以下のように定める.

$$L_n^D(P, Q|\nu) := \max_W \{L[F(W(P^n), Q^L) \geq \nu, W : \text{deterministic conversion}]\}.$$

最大変換数は, 初期の独立同一な確率分布 P^n から対象の確率分布が, 許容精度のもとでいくつ生成できるかを表している.

最大変換数に対して, その 1 次のレートは Shannon エントロピー $H(P)$ と $H(Q)$ の比で表されることが知られている [4]. 近年, より精密な漸近的特徴付けとして, 2 次の漸近解析が注目を集めている [6, 12, 5]. 初期の確率分布, もしくは対象の確率分布が一様分布の場合は, す

で最大変換数の2次の漸近展開は得られている [5, 11]. しかしながら, 非一様分布の場合は, 対応する結果は得られていなかった. Kumagai and Hayashi[9] は Rayleigh-normal 分布関数を用いることで, 一様分布と非一様分布に対して統一的な二次の漸近展開が得られることを示した:

$$L_n^{\mathcal{D}}(P, Q|\nu) = \frac{H(P)}{H(Q)}n + \frac{Z_{C_{P,Q}}^{-1}(1-\nu^2)}{D_{P,Q}}\sqrt{n} + o(\sqrt{n}), \quad (9)$$

ここで $D_{P,Q}$ と $C_{P,Q}$ は P と Q から決まる定数であり, $\cong$ は両辺の差が高々 $o(\sqrt{n})$ であることを表している.

2.2 量子情報理論における LOCC 変換

量子情報理論に置いて様々な量子操作が提案されており, その実行のために特定のエンタングル状態がしばしば必要とされる. 遠く離れたパーティ達がそのような量子操作を実行しようとしたとき, 彼らは事前に望むエンタングル状態を準備しておかなくてはならない. そのような状況において, 局所操作と古典通信の組み合わせ (LOCC) はエンタングル状態準備のための基本的な方法である.

そのような問題意識に基づき, 2 体系上に独立同一に準備された純粋エンタングル状態の間の LOCC 変換に関して考察する. 古典情報理論と同様に, 最大変換数を以下のように定義する:

$$L_n(\psi, \phi|\nu) := \max_{\Gamma: \text{LOCC}} \{L \in \mathbb{N} | F(\Gamma(\psi^{\otimes n}), \phi^{\otimes L}) \geq \nu\}, \quad (10)$$

ここで F は忠実度を表している. LOCC 変換に関して基本的な結果として, Bennett *et. al.* [1] は最適な LOCC 変換レートは, 変換前後の状態の部分状態の von Neumann エントロピー S_ψ と S_ϕ の比で表されることを示した. 言い換えると, 彼らは最大変換数の1次の漸近展開が $L_n(\psi, \phi|\nu) = S_\psi/S_\phi n + o(n)$ のようになることを示した. しかしながらそのような近似はしばしば十分に正確ではない. 特に, 許容精度 (許容できる忠実度) ν を全く反映していない. 従って, そのような問題を解決するために, 標準正規分布の累積分布関数 Φ を用いることで Kumagai and Hayashi [8] は明示的にエンタングルメント抽出とエンタングルメント希釈の二次の漸近レートを以下のように導出した:

$$L_n(\psi, \phi|\nu) = \frac{S_\psi}{S_\phi}n + \text{const}_{\psi, \phi} \Phi^{-1}(1-\nu^2)\sqrt{n} + o(\sqrt{n}), \quad (11)$$

ここで $const_{\psi,\phi}$ は [9] の (148) および (149) で与えられる定数である。実際、エンタングルメント抽出やエンタングルメント希釈に加えて、標準正規分布の累積分布関数は様々な量子情報処理の二次の漸近レートとして現れる。例として、量子仮説検定 [10, 13], 古典-量子通信路符号化 [14], 量子固定長情報源符号化 [13, 2], サイド情報付きのデータ圧縮 [13], 量子サイド情報に対しての乱数抽出 [13], ノイズあり稠密符号化 [2] の 2 次漸近レートは標準正規分布の累積分布関数で表され ([2] も参照せよ)。

本論文では、初期状態と対象の状態が最大エンタングル状態とは限らないような場合での LOCC 変換も対象とする。最大エンタングル状態ではない量子状態を必要とする量子情報処理の例として、測定ベースの量子計算 [3] や量子通信路推定 [7] が挙げられる。驚くべきことに、最大エンタングル状態ではない量子状態の間の LOCC 変換に対しては、最大変換数の 2 次の漸近レートは標準正規分布では表すことはできず、以下のように Rayleigh-normal 分布を用いて表すことができる。

$$L_n(\psi, \phi|\nu) = \frac{S_\psi}{S_\phi} n + \frac{Z_{C_{\psi,\phi}}^{-1}(1-\nu^2)}{D_{\psi,\phi}} \sqrt{n} + o(\sqrt{n}), \quad (12)$$

ここで $D_{\psi,\phi}$ と $C_{\psi,\phi}$ はある定数である。この点において、Rayleigh-normal 分布は非常に非自明な情報理論的役割を担っているといえる。最後に一点、言及すべきこととして、初期状態が対象の状態が最大エンタングル状態のときは、Rayleigh-normal 分布関数は標準正規分布の累積分布関数に一致し、従って上記の漸近展開 (12) は典型的な漸近展開 (11) を復元する。

References

- [1] C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, “Concentrating partial entanglement by local operations,” *Phys. Rev. A*, **53**(4), 2046, (1996).
- [2] N. Datta and F. Leditzky, “Second-order asymptotics for source coding, dense coding and pure-state entanglement conversions,” arXiv:1403.2543, (2014).
- [3] D. Gross, S. T. Flammia and J. Eisert, “Most quantum states are too entangled to be useful as computational resource,” *Phys. Rev. Lett.*, **102**(19), 190501, (2009).

- [4] T. S. Han, *Information-Spectrum Methods in Information Theory*, Springer, New York, (2003).
- [5] M. Hayashi, "Second-order asymptotics in fixed-length source coding and intrinsic randomness," *IEEE Trans. Inform. Theory*, **54(10)**, 4619, (2008).
- [6] M. Hayashi, "Information-Spectrum Approach to Second-Order Coding Rate in Channel Coding," *IEEE Trans. Inform. Theory*, **55(11)**, 4947, 2009.
- [7] M. Hayashi, "Comparison between the Cramer-Rao and the mini-max approaches in quantum channel estimation," *Comm. Math. Phys.*, **304(3)**, 689, (2011).
- [8] W. Kumagai, M. Hayashi, "Entanglement Concentration is Irreversible," *Phys. Rev. Lett.*, **111(13)**, 130407, (2013).
- [9] W. Kumagai, M. Hayashi, "Asymptotics of Classical and LOCC Conversions and Its Application to LOCC Cloning," *arXiv:1306.4166*.
- [10] K. Li, "Second order asymptotics for quantum hypothesis testing," *arXiv:1208.1400*, (2012).
- [11] R. Nomura and T. S. Han, "Second-Order Resolvability, Intrinsic Randomness, and Fixed-Length Source Coding for Mixed Sources," *IEEE Trans. Inform. Theory*, **59(1)**, 1, (2013).
- [12] Y. Polyanskiy, H.V. Poor and S. Verdú, "Channel Coding Rate in the Finite Blocklength Regime", *IEEE Trans. Inform. Theory*, **56(5)**, 2307, 2010.
- [13] M. Tomamichel and M. Hayashi, "A hierarchy of information quantities for finite block length analysis of quantum tasks," *arXiv:1208.1478*, (2012).
- [14] M. Tomamichel and V. Y. Tan, "Second-Order Asymptotics of Classical-Quantum Channels," *arXiv:1308.6503*, (2013).