

Majorization と量子情報

文責:Physics Lab.2023 量子班 渡邊開人

2023年5月11日

目次

第 1 章	初めに	2
第 2 章	リソース理論の一般論	3
2.1	リソース理論とは	3
2.2	リソース理論の数学的な枠組み	4
第 3 章	古典確率分布とエントロピー	6
3.1	確率分布と遷移行列	6
3.2	Shannon エントロピーと Kullback-Leibler divergence	7
3.3	Rényi エントロピーと Rényi divergence	8
3.4	f -divergence と凸性, 単調性	10
第 4 章	Majorization の数理	13
4.1	モチベーション	13
4.2	Majorization	13
第 5 章	量子情報における情報理論と Majorization	16
5.1	CPTP 写像, ユニタリ写像	16
5.2	von Neumann エントロピーと量子 KLD	17
5.3	Quantum majorization	17
第 6 章	エンタングルメントのリソース理論	20
6.1	Majorization 束と近似問題	23
付録 A	Hardy-Littlewood-Polya の定理の証明	25
付録 B	(δ_d, \prec) が束となることの証明	28
B.1	半順序と束	28
B.2	Majorization 束	29
参考文献		32

第1章

初めに

表題にある majorization は例えば2つの確率分布の間にある関係のことをいう。特に有名であるのは、経済の分野で登場するジニ係数である。これは、社会における所得格差の指標となっている。

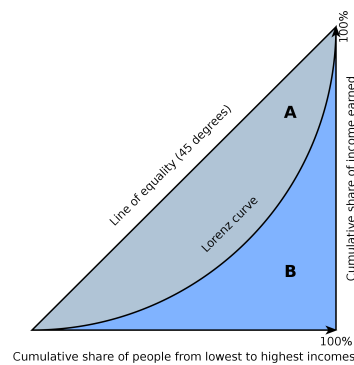


図 1.1 ローレンツ曲線 (wikipedia より引用)

この定義を理解するには、さほど高度な数学を必要としない。しかしながら、majorization は非常に興味深い性質を持っていて、これらは幾分か的应用先を持っている。この記事では、量子情報への应用を紹介する。また、熱力学への应用は、同じ Physics Lab. 2023 の統計物理班の記事「熱力学とリソース」に譲る。

量子情報理論の基本については、ある程度の知識を仮定している。(CPTP くらい) 基本 k 的な事項については [1] や [2] などを参照していただきたい。また、4 章などの内容は、[3] を大いに参考にした。また、6.1 節の内容は、[4] を参考にした。

第2章

リソース理論の一般論

2.1 リソース理論とは

リソース理論は、例えば量子情報理論の分野で用いられる枠組みで、コストなしで用意出来る状態の集合と自由に行える操作の集合を定めたときに、2つの状態の間の遷移が可能かを議論し、ここからリソース状態を見出すことを一つの目的としている。^{*1}わかりやすく、歴史も長いリソース理論の例として、エンタングルメントのリソース理論が挙げられる。空間的に離れた2者(以下、AliceとBobと呼ぶ事にする。)がそれぞれ1つずつ量子を持っているとする。例えば、この2者の間で共有された状態が

$$|\psi\rangle = \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}} \quad (2.1)$$

という風に表されたとき、これは古典ではありえないような相関を持つことがわかっている。^{*2}このような状態をエンタングル状態という。AliceとBobに許される操作として、

- 自分のもつ量子に対する操作(ゲート操作や測定など) (局所操作 **Local Operation**)
- 行った測定結果を古典通信でもう一方に送ること (古典通信 **Classical Communication**)

を採用し、コストなしで用意出来る状態の集合としてエンタングルしていない状態の集合を採用すると、この状態の集合から任意にとった集合に、局所操作と古典通信 (**LOCC**) をかけていったとしても、エンタングル状態は生成されないことが知られている。よって、エンタングル状態はこの状態の集合と操作の集合では実現出来ないので、エンタングル状態はリソースといえる。

用語をいくつか導入しておく。以上の説明で登場した、コストなしに用意出来る状態の集合を \mathcal{F} とかき、**free states** と呼ぶ。また、許容された操作の集合を \mathcal{O} とかき、**free operation** と呼ぶ。このとき、これらは勝手に決まる組ではなく、

$$\forall \rho \in \mathcal{F}, \forall \Lambda \in \mathcal{O} \quad \Lambda(\rho) \in \mathcal{F} \quad (2.2)$$

を満たさねばならない。これは、上のエンタングルメントの話と整合する。また、リソース状態は $\mathcal{S} \setminus \mathcal{F}$ とする。ただし、 \mathcal{S} は状態全体の集合とする。今のエンタングルメントのリソース理論のセッティングでは、 \mathcal{F} がセパラブル状態の集合、 $\mathcal{S} \setminus \mathcal{F}$ がエンタングル状態の集合である。つまり、リソース理論を用いると、リソー

^{*1} すごくざっくりした説明なので、詳しくは [5] を参照してください。

^{*2} これは、例えば Bell の不等式の破れなどに現れる。

ス状態について操作論的な定義が出来ることがある。今回の場合は、エンタングル状態は free state から free operation で実現出来ない状態と定義出来る。

また、制限された操作下での遷移可能性の議論は、熱力学でも重要な役割を果たす。ある作業物質 (例えば、窒素 1 mol. 窒素 1 mol と窒素 2 mol は異なる作業物質とみなす。) の取りうる平衡状態全体の集合を Γ とする。 $X, Y \in \Gamma$ に対して、 X から Y に断熱過程で到達出来るとき、 $X \prec Y$ とかく。このとき、いくつかのほとんど自明な要請と、比較仮説

$$\forall X, Y \in \Gamma \quad X \prec Y \text{ or } Y \prec X \quad (2.3)$$

と、不可逆過程の存在

$$\exists X_0, X_1 \text{ s.t. } X_0 \prec X_1, X_1 \not\prec X_0 \quad (2.4)$$

を仮定したとき、

$$X \prec Y \Leftrightarrow S(X) \leq S(Y) \quad (\Leftrightarrow -S(X) \geq -S(Y)) \quad (2.5)$$

を満たす $S : \Gamma \rightarrow \mathbb{R}$ が、アフィン変換の自由度を除いて一意に定まることが知られている [6]. 以下、この関数 S をエントロピーとよぶ。このとき、断熱過程で変化させると、 $-S$ が非増加となる。このケースにおいて具体的に free state を指摘することは難しいが、任意の 2 状態に対してどちらがよりリソースに富んでいるかがこの二項関係 \prec で、また前述のエントロピーの存在から、単に $-S$ の値の大小でも特徴づけられる。このように、制限された操作の元での遷移可能性を基に、各状態がどのくらいリソースに富んでいるかを表現する関数を持つてくることもできる。これもリソース理論の一つの恩恵である。

2.2 リソース理論の数学的な枠組み

以下では、リソース理論の枠組み (の一部) を導入する。あくまでこの記事に必要な分のみを紹介するにとどめるが、より詳細な内容については [5] を参照されたい。

定義 2.2.1 (リソース理論). \mathcal{O} は、入力と出力に対応する物理系の組 (A, B) (それぞれの系に対応するヒルベルト空間は $\mathcal{H}_A, \mathcal{H}_B$ であるとする) を $\mathcal{O}(A \rightarrow B) \subset \{\Lambda \in \mathcal{L}(\mathcal{H}_A \rightarrow \mathcal{H}_B) | \Lambda \text{ は CPTP}\}$ に対応づける写像であるとする。また、特に $\mathcal{F}(\mathcal{H}) = \mathcal{O}(C \rightarrow \mathcal{H})$ とする。以下の 2 つの条件が満足されているとき、 $\mathcal{R} = (\mathcal{F}, \mathcal{O})$ をリソース理論という。

- $\forall A$ (物理系) $\text{id}^A \in \mathcal{O}(A) \quad (\equiv \mathcal{O}(A \rightarrow A))$
- $\forall A, B, C$ (物理系) $\Psi \in \mathcal{O}(A \rightarrow B), \Lambda \in \mathcal{O}(B \rightarrow C) \Rightarrow \Lambda \circ \Psi \in \mathcal{O}(A \rightarrow C)$

CPTP については、5 章を参照。特に、この \mathcal{F} を free state といい、 \mathcal{O} を free operation という。また、 $S(A) \setminus \mathcal{F}(A)$ を resource state という。この定義から、 $\mathcal{F} \subset \mathcal{O}$ であるが、以降この記事では free operation は $\mathcal{O} \setminus \mathcal{F}$ を指す。また、簡単にわかることとして、以下が成立する。

定理 2.2.2 (リソース理論の黄金律).

$$\forall A, B \text{ (物理系)}, \Lambda \in \mathcal{O}(A \rightarrow B), \rho \in \mathcal{F}(A) \Rightarrow \Lambda(\rho) \in \mathcal{F}(B) \quad (2.6)$$

これは、free state を free operation で写してもリソースは生まれなことを示している。

リソース理論の定義は、free state や free operation の決め方について何も言及していない。つまり、free state や free operation は定義にあるような条件さえ満たしていればこちら側が自由に決めてよいということになる。特に、実際の実験に沿った free operation や free state を定めてやれば、意味のある結果を得られることが期待できる。

例えば実験的な制約によって free state または free operation のいずれかが与えられたとき、もう他方は一意に定まるのかはかなり気になる所ではあると思う。そのための準備として、リソース理論のテンソル積構造を導入する。

定義 2.2.3 (テンソル積構造 (TPS)). リソース理論 $\mathcal{R} = (\mathcal{F}, \mathcal{O})$ がテンソル積の構造 (TPS) をもつとは、以下の3つの条件をみたすことである。

1. Free operation は”**completely free**”である。つまり、

$$\forall A, B, C \text{ (物理系)}, \forall \Phi \in \mathcal{O} \quad \text{id}^C \otimes \Phi \in \mathcal{O}(CA \rightarrow CB) \quad (2.7)$$

をみたす。

2. 補助系として free state を加えることは free operation である。
3. 系を破棄することは free operation である。 (\Leftrightarrow トレースは free operation)

リソース理論に TPS が入っていると、いくつかのご利益がある。例えば以下が言える。

命題 2.2.4 (free operation のテンソル積は free operation).

$$\Phi \in \mathcal{O}(A \rightarrow B), \Phi' \in \mathcal{O}(A' \rightarrow B') \Rightarrow \Phi \otimes \Phi' \in \mathcal{O}(AA' \rightarrow BB') \quad (2.8)$$

Proof.

$$\Phi \otimes \Phi' = (\text{id}^B \otimes \Phi') \circ (\Phi \otimes \text{id}^{A'}) \in \mathcal{O}(AA' \rightarrow BB') \quad (2.9)$$

□

ここから、部分トレースも free operation であるし、replacement

$$\Phi_\sigma[X] = \text{Tr}[X]\sigma \quad (2.10)$$

も free operation である。

さて、free operation の集合 \mathcal{O} が与えられたとき、

$$\mathcal{F}_{min}(A) = \{\rho \in \mathcal{S}(A) | \forall \sigma \in \mathcal{S}(A), \exists \Phi \in \mathcal{O}(A) \text{ s.t. } \rho = \Phi(\sigma)\} \quad (2.11)$$

としたとき、これは $\mathcal{F}_{min} \subset \mathcal{F}$ はすぐにわかる。もし replacement が free operation なら、 $\mathcal{F}_{min} \supset \mathcal{F}$ もすぐにわかり、 $\mathcal{F}_{min} = \mathcal{F}$ となる。つまり、与えられた free operation に replacement が含まれるなら、これと整合する free state は一意に定まる。しかし、free state の集合 \mathcal{F} が与えられたとき、これと整合する free operation の集合は一般には一意に定まらないことが知られている。

第3章

古典確率分布とエントロピー

3.1 確率分布と遷移行列

以下、 \mathcal{P}_d を d 次元の確率分布全体の集合とする。

定義 3.1.1. (supp と rank) 確率分布 $p = \{p_i\}_i \in \mathcal{P}_d$ に対して、 p の台 $\text{supp}[p]$ を

$$\text{supp}[p] = \{i : p_i > 0\} \subseteq \{1, \dots, d\} \quad (3.1)$$

と定義する。また、 $\text{rank}[p] = |\text{supp}[p]|$ を p のランクという。とくに、 $\text{rank}[p] = d$ のとき、フルランクという。

次に確率遷移行列を定義する。

定義 3.1.2. (確率遷移行列)

古典的な確率分布の時間発展は、確率遷移行列 T で表現され、

$$p'_i = \sum_j T_{ij} p_j \quad (3.2)$$

とかける。^{*1}

ここで、以下のことが簡単にわかる。

命題 3.1.3.

$$\sum_i T_{ij} = 1 \quad (3.3)$$

Proof. $p' = \{p'_j\}$ の規格性より、

$$1 = \sum_i p'_i = \sum_{i,k} T_{ik} p_k \quad (3.4)$$

^{*1} もちろん、一般には $p \in \mathcal{P}_d$, $p' \in \mathcal{P}_{d'}$ ($d \neq d'$) でも構わないが、ここでは $d = d'$ 、つまり確率遷移行列が正方行列であるような系を考える。

が任意の $p \in \mathcal{P}_d$ に対して成立する. よって, $p_k = \delta_{jk}$ を持ってくれば,

$$1 = \sum_{i,k} T_{ik} \delta_{jk} \quad (3.5)$$

$$= \sum_i T_{ij} \quad (3.6)$$

□

定義 3.1.4. 確率遷移行列 T が

$$\sum_j T_{ij} = 1 \quad (3.7)$$

もみたすとき, **2重確率遷移行列**という.

$u \in \mathcal{P}_d$ を一様分布 ${}^t u = (\frac{1}{d}, \dots, \frac{1}{d})$ とする. 2重確率遷移行列に対して, 以下のような特徴づけが出来る.

命題 3.1.5. (2重確率遷移行列の特徴づけ) 以下は同値.

- T は 2重確率遷移行列
- 一様分布 u は T の固定点. つまり, $u = Tu$

Proof. 新しい確率分布の第 i 成分を計算すると,

$$p'_i = \sum_j T_{ij} u_j \quad (3.8)$$

$$= \frac{1}{d} \sum_j T_{ij} \quad (3.9)$$

より, これを眺めるとわかる. □

3.2 Shannon エントロピーと Kullback-Leibler divergence

定義 3.2.1. (Shannon エントロピー)

確率分布 $p = \{p_i\}_i \in \mathcal{P}_d$ に対して, **Shannon エントロピー**を

$$S(p) = - \sum_i p_i \ln p_i \quad (3.10)$$

と定義する.*2

確率 0 の事象に対して, $0 \ln 0 = 0$ としている. すぐわかる事実として, $S(p) \geq 0$ がわかる.

定義 3.2.2. (相対エントロピー, Kullback-Leibler divergence)

$p = \{p_i\}_i, q = \{q_i\}_i \in \mathcal{P}_d$ を確率分布とする.

$$S(p||q) = \sum_i p_i \ln \frac{p_i}{q_i} \quad (3.11)$$

*2 以下, エントロピーなどに登場する対数に関しては, 適宜適切な底を取ることにする.

を相対エントロピー, **Kullback-Leibler divergence** という. (以下, KLD とかく.)

このとき, $\text{supp } [p] \not\subseteq \text{supp } [q]$ のときは $S(p||q) = +\infty$ と定義しておく. のちに KLD の単調性を導入してからこの非負性を示すが, 結論から言えば Jensen の不等式から示すことになる. 興味があればチャレンジされたい.

定義 3.2.3. (相互情報量)

有限集合 A, B 上の確率分布 p_{AB} に対して, それを周辺化した確率分布を p_A, p_B とする. このとき, 確率分布 p_{AB} に対する相互情報量を

$$I^{A:B}(p_{AB}) = S(p_A) + S(p_B) - S(p_{AB}) \quad (3.12)$$

と定義する.

相互情報量は, 物理的 (?) には, $A(B)$ についての情報を得たとき, $B(A)$ についての情報がどのくらい得られるかに対応している. また, 相互情報量の定義をさらに計算すると, (i を A の方のインデックス, j を B の方のインデックスとする.)

$$I^{A:B}(p_{AB}) = S(p_A) + S(p_B) - S(p_{AB}) \quad (3.13)$$

$$= -\sum_{i \in A} p_i \ln p_i - \sum_{j \in B} p_j \ln p_j + \sum_{(i,j) \in A \times B} p_{ij} \ln p_{ij} \quad (3.14)$$

$$= \sum_{(i,j) \in A \times B} p_{ij} \ln \frac{p_{ij}}{p_i p_j} \quad (3.15)$$

$$= S(p_{ij} || p_i \otimes p_j) \quad (3.16)$$

と書ける. このあと, KLD の非負性を示す. ここから相互情報量の非負性も示される. また, 今のところ導入するつもりがあまりないが, 条件付きエントロピーを用いると

$$I(X : Y) = S(X) - S(X|Y) \quad (3.17)$$

と変形できる.

3.3 Rényi エントロピーと Rényi divergence

Shannon エントロピーを包含する概念として Rényi エントロピーがある.

定義 3.3.1. (Rényi エントロピーと divergence)

確率分布 $p \in \mathcal{P}_d$ と $0 \leq \alpha \leq \infty$ に対して, **Rényi α -エントロピー**を

$$S_\alpha(p) := \frac{1}{1-\alpha} \ln \left(\sum_{i=1}^d p_i^\alpha \right) \quad (3.18)$$

と定義する. また, $p, q \in \mathcal{P}_d$ に対して, **Rényi α -divergence** を

$$S_\alpha(p||q) := \frac{1}{\alpha-1} \ln \left(\sum_i \frac{p_i^\alpha}{q_i^{\alpha-1}} \right) \quad (3.19)$$

と定義する.

これらはいずれも非負である。エントロピーの方は直ぐ確認できる。divergenceの方はあとで一氣に示す。以下は簡単に確認できる。

命題 3.3.2. (Rényi \leftrightarrow Shannon,KLD) Rényi 1-エントロピーは Shannon エントロピーと一致し, Rényi 1-divergence は KLD と一致する。つまり,

$$S_1(p) = S(p) \quad (3.20)$$

$$S_1(p||q) = S(p||q) \quad (3.21)$$

Proof. エントロピーの方に関しては,

$$S_1(p) = -\lim_{\alpha \rightarrow 1} \frac{1}{\alpha - 1} \ln \left(\sum_i p_i^\alpha \right) \quad (3.22)$$

$$= -\frac{d}{d\alpha} \ln \left(\sum_i p_i^\alpha \right) \Big|_{\alpha=1} \quad (3.23)$$

$$= -\frac{\sum_i p_i^\alpha \ln p_i}{\sum_i p_i^\alpha} \Big|_{\alpha=1} \quad (3.24)$$

$$= -\sum_i p_i \ln p_i = S(p) \quad (3.25)$$

となる。divergence に対しては,

$$S_1(p||q) = \lim_{\alpha \rightarrow 1} \frac{1}{\alpha - 1} \ln \left(\sum_i \frac{p_i^\alpha}{q_i^{\alpha-1}} \right) \quad (3.26)$$

$$= \frac{d}{d\alpha} \ln \left(\sum_i \frac{p_i^\alpha}{q_i^{\alpha-1}} \right) \Big|_{\alpha=1} \quad (3.27)$$

$$= \frac{\sum_i q_i (p_i/q_i)^\alpha \ln(p_i/q_i)}{\sum_i \frac{p_i^\alpha}{q_i^{\alpha-1}}} \Big|_{\alpha=1} \quad (3.28)$$

$$= \sum p_i \ln \frac{p_i}{q_i} = S(p||q) \quad (3.29)$$

とかける。よって OK. □

また, $\alpha = 0, \infty$ の場合は重要だし, この後割と使う。

命題 3.3.3. ($\alpha = 0, \infty$ のときの Rényi エントロピーとダイバージェンス)

$$S_0(p) = \ln(\text{rank}[p]) \quad (3.30)$$

$$S_\infty(p) = -\ln \left(\max_i p_i \right) \quad (3.31)$$

$$S_0(p||q) = -\ln \left(\sum_{i:p_i>0} q_i \right) \quad (3.32)$$

$$S_\infty(p||q) = \ln \left(\max_i \frac{p_i}{q_i} \right) \quad (3.33)$$

証明は略。

3.4 f -divergence と凸性, 単調性

定義 3.4.1. (Convexity と Concavity) $I \subset \mathbb{R}$ を区間とする. $f: I \rightarrow \mathbb{R}$ が

$$\forall x, y \in I, \forall \lambda \in [0, 1] \quad f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y) \quad (3.34)$$

をみたすとき, 下に凸 (**convex**) という. 逆の不等式が成立するなら, 上に凸 (**concave**) という.

f -divergence を以下で定義する.

定義 3.4.2. (f -divergence) $p, q \in \mathcal{P}_d$ とする. また, $f: (0, \infty) \rightarrow \mathbb{R}$ を下に凸の関数とする.

$$D_f(p||q) = \sum_i q_i f\left(\frac{p_i}{q_i}\right) \quad (3.35)$$

を f -divergence という.

この $f(x)$ を $f(x) = x \ln x$ と選べば, これは下に凸で, このときの f -divergence は KLD と一致する. また, $f(x) = x^\alpha$ として \log を取って $\frac{1}{\alpha-1}$ 倍すれば Rényi divergence となる.

定理 3.4.3. f を下に凸な関数とし, $p, q, p', q' \in \mathbb{R}^d$ とする. また, q, q' の全ての成分は正であるとする. T を確率遷移行列として, $p' = Tp, q' = Tq$ ならば

$$\sum_i q'_i f\left(\frac{p'_i}{q'_i}\right) \leq \sum_i q_i f\left(\frac{p_i}{q_i}\right) \quad (3.36)$$

上に凸の関数ならば, 逆向きの不等式が成立する.

Proof.

$$\frac{p'_j}{q'_j} = \sum_i \frac{T_{ji} p_i}{q'_j} = \sum_i \frac{T_{ji} q_i}{q'_j} \frac{p_i}{q_i} \quad (3.37)$$

$$\sum_i \frac{T_{ji} q_i}{q'_j} = 1 \quad (3.38)$$

に注意すれば, Jensen の不等式から,*3

$$\sum_j q'_j f\left(\frac{p'_j}{q'_j}\right) = \sum_j q'_j f\left(\sum_i \frac{T_{ji} q_i}{q'_j} \frac{p_i}{q_i}\right) \quad (3.39)$$

$$\leq \sum_j \sum_i q'_j \frac{T_{ji} q_i}{q'_j} f\left(\frac{p_i}{q_i}\right) \quad (3.40)$$

$$= \sum_i q_i f\left(\frac{p_i}{q_i}\right) \quad (3.41)$$

上に凸ならば Jensen の不等式が逆向きになる. □

ここから, 以下の系が従う.

*3 凸不等式. wikipediaなどを参照してください.

系 3.4.4. T を 2 重確率遷移行列として, $p, p' \in \mathbb{R}^d$ とする. このとき, 下に凸な関数 $f(x)$ に対して

$$\sum_i f(p'_i) \leq \sum_i f(p_i) \quad (3.42)$$

Proof. $q = (1, \dots, 1) = du$ とすれば, $q' = du$. これを代入すれば OK. \square

これを用いれば, いろいろ保留してきたことが示せる. その前に, 以下のような行列を定義しておく.

$$U = \begin{pmatrix} \frac{1}{d} & \cdots & \frac{1}{d} \\ \vdots & \ddots & \vdots \\ \frac{1}{d} & \cdots & \frac{1}{d} \end{pmatrix} \quad (3.43)$$

これは確かに確率遷移行列であることが確かめられる. この行列は任意の確率分布を一様分布 u にうつす.

系 3.4.5. (KLD ≥ 0)

$p, q \in \mathcal{P}_d$ とする. このとき,

$$S(p||q) \geq 0 \quad (3.44)$$

Proof. $u = Up = Uq$ に留意すれば, $f(x) = x \ln x$

$$S(p||q) = D_f(p||q) \quad (3.45)$$

$$\geq D_f(Up||Uq) \quad (3.46)$$

$$= D_f(u||u) = 0 \quad (3.47)$$

よって OK. \square

系 3.4.6. (Rényi α -divergence ≥ 0)

$p, q \in \mathcal{P}_d$ とする. このとき,

$$\forall \alpha \in [0, \infty] \quad S_\alpha(p||q) \geq 0 \quad (3.48)$$

Proof. $f(x) = x^\alpha$ とする. $\alpha = 1$ なら KLD であるのはすでに示したので, $\alpha > 1$ と, $1 > \alpha > 0$ に分けて考える必要があるが, $\alpha > 1$ のみ考える. もう一方は同じように証明出来る. $f(x) = x^\alpha$ とすれば, これは下に凸. このとき,

$$D_f(p||q) \geq D_f(Up||Uq) \quad (3.49)$$

$$= \sum_i (Uq)_i f(1) \quad (3.50)$$

$$= \sum_i \frac{1}{d} \times 1 = 1 \quad (3.51)$$

これに \log をとって, $\alpha - 1 (> 0)$ でわると Rényi α -divergence になるから,

$$S_\alpha(p||q) \geq \frac{1}{\alpha - 1} \log 1 = 0 \quad (3.52)$$

となり, OK. \square

さらに, Rényi α -divergence について, 以下の関係が成立する.

系 3.4.7. $p, q \in \mathcal{P}_d$ とする. このとき,

$$\alpha \leq \alpha' \Rightarrow S_\alpha(p||q) \leq S_{\alpha'}(p||q) \quad (3.53)$$

Proof. $\alpha' > \alpha$ のとき, $f(x) = x^{(\alpha-1)/\alpha'-1}$ ととる. このとき,

$$f''(x) = \frac{(\alpha-1)(\alpha-\alpha')}{(\alpha'-1)^2} x^{(\alpha-1)/(\alpha'-1)-2} \quad (3.54)$$

となるので, $\alpha < 1$ なら下に凸, $\alpha > 1$ なら上に凸. 一旦, $\alpha < 1$ について考える. Jensen の不等式から,

$$S_\alpha(p||q) = \frac{1}{\alpha-1} \ln \left(\sum_i p_i \left(\frac{p_i}{q_i} \right)^{\alpha-1} \right) \quad (3.55)$$

$$= \frac{1}{\alpha-1} \ln \left(\sum_i p_i \left(\frac{p_i}{q_i} \right)^{(\alpha'-1) \frac{\alpha-1}{\alpha'-1}} \right) \quad (3.56)$$

$$\leq \frac{1}{\alpha-1} \ln \left(\sum_i p_i \left(\frac{p_i}{q_i} \right)^{\alpha'-1} \right)^{\frac{\alpha-1}{\alpha'-1}} \quad (3.57)$$

$$= \frac{1}{\alpha'-1} \ln \left(\sum_i p_i \left(\frac{p_i}{q_i} \right)^{\alpha'-1} \right) = S_{\alpha'}(p||q) \quad (3.58)$$

□

最後に, divergence とエントロピーを結びつける. まず, u を一様分布として, $S(u) = -\sum_i \frac{1}{d} \ln \frac{1}{d} = \ln d$. 任意の確率分布 $p \in \mathcal{P}_d$ に対して

$$S(p||u) = \sum_i p_i \ln \frac{p_i}{1/d} \quad (3.59)$$

$$= \ln d - S(p) \geq 0 \quad (3.60)$$

となる. 等号成立は $p = u$ の時のみである. よって, 任意の確率分布 p に対して, そのエントロピーの取りうる値の範囲は,

$$0 \leq S(p) \leq \ln d \quad (3.61)$$

となる. また, KLD の単調性から, T を 2 重確率遷移行列とすれば,

$$S(p||u) \geq S(Tp||Tu) = S(Tp||u) \quad (3.62)$$

$$\ln d - S(p) \geq \ln d - S(Tp) \quad (3.63)$$

$$S(Tp) \geq S(p) \quad (3.64)$$

$p^G = e^{-\beta E_i} / Z$ (カノニカル分布) に対して, $\beta \rightarrow 0$, つまり高温極限をとると一様分布 u となる. ここで, 2 重確率遷移行列 T が u の固定点であるというのは, T が高温極限を取った系における時間発展を記述する行列であり, 平衡分布が平衡分布にうつるということに対応する. これとまったく同様に, $S_\alpha(p||u) = \ln d - S_\alpha(p)$ であるから, 同じようにして

$$S_\alpha(Tp) \geq S_\alpha(p) \quad (3.65)$$

とわかる. 有限温度で同様の議論をするためには, 次章で説明する Majorization が強力な武器となる.

第4章

Majorization の数理

4.1 モチベーション

すでに説明してあるように, $p, p' \in \mathcal{P}_d$ と T (2重確率遷移行列) に対して, $p' = Tp$ ならば, $S(p') \geq S(p)$ が成立する. しかし, 逆は一般には成立しない. つまり, $S(p') \geq S(p)$ が成立するとき, $p' = Tp$ をみたす2重確率遷移行列 T の存在は一般には保証されない. この必要十分条件を与えるのが Majorization である.

4.2 Majorization

$p \in \mathcal{P}_d$ に対して, p^\downarrow を, p の成分を降順 (つまり, 大きい順) に並びかえたものと定義する. つまり, p^\downarrow は

$$p^\downarrow = (p_1^\downarrow, p_2^\downarrow, \dots, p_d^\downarrow) \quad (4.1)$$

$$p_1^\downarrow \geq p_2^\downarrow \geq \dots \geq p_d^\downarrow \quad (4.2)$$

をみताす. このとき, Majorization は以下のように定義できる.

定義 4.2.1. ((古典)Majorization)

$p, p' \in \mathcal{P}_d$ とする. 以下の条件をみたすとき, p が p' を **Majorize** するといひ, $p \succ p'$ とかく.

$$\forall k \in \{1, \dots, d\} \quad \sum_{i=1}^k p_i^\downarrow \leq \sum_{i=1}^k p_i^{\prime\downarrow} \quad (4.3)$$

これは, 以下のように図を書くとわかりやすい.

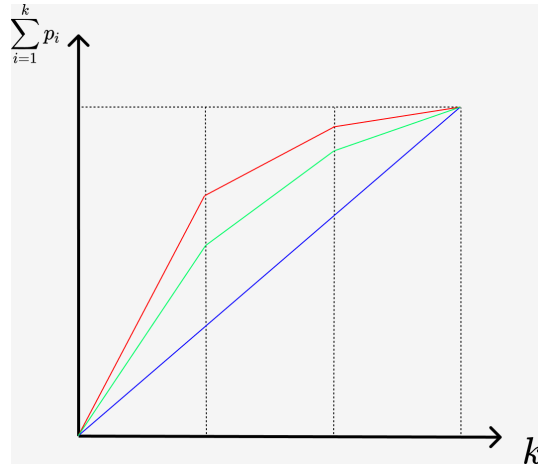


図 4.1 Majorization をあらわすローレンツカーブの例. 赤の曲線で表される確率分布は緑の曲線で表される確率分布を Majorize する. 青は一様分布.

横軸に k , 縦軸に $\sum_i p_i^\downarrow$ をとれば, これは上に凸な折れ線を描くことがわかる. これをローレンツカーブという. また, 簡単にわかるように, 一様分布のローレンツカーブは単に直線となる. 簡単にわかるように, $p \succ p'$ であるための必要十分条件は, p のローレンツカーブは p' のローレンツカーブより常に上側にあることである. また, $\forall p \in \mathcal{P}_d \ p \succ u$ が成立する.

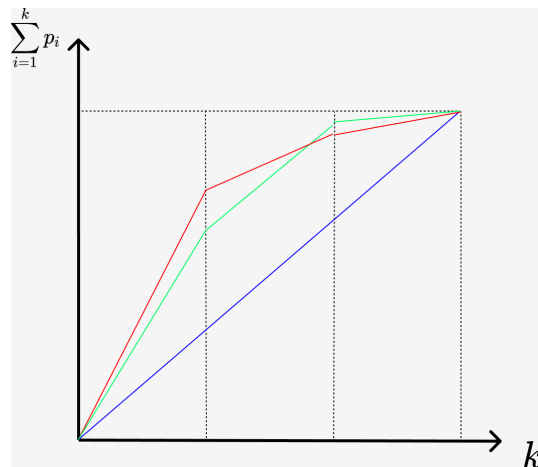


図 4.2 $p \succ p'$ も $p' \succ p$ も成立しない例

以下は, 重要である.

定理 4.2.2 (Hardy-Littlewood-Polya). $p, p' \in \mathcal{P}_d$ とする. 以下は全て同値.

1. $p' \prec p$
2. $\forall t \in \mathbb{R} \quad \sum_i^d |p'_i - t| \leq \sum_i^d |p_i - t|$
3. 任意の下に凸な関数 f に対して $\sum_i^d f(p'_i) \leq \sum_i^d f(p_i)$
4. ある 2 重確率遷移行列 T が存在して, $p' = Tp$

証明は、あとで元気があれば Appendix で書くことにする。(まあまあ大変) この 3 番目の条件に関して,
 $f(x) = x \ln x$ とすれば, $S(p') \geq S(p)$ がしたがう.

第5章

量子情報における情報理論と Majorization

以下の内容は古典のエントロピーの内容と対応する。以下、考える系や補助系のヒルベルト空間は有限次元であるとする。また、 $\mathcal{L}(\mathcal{H})$ は \mathcal{H} 上の線形演算子全体の集合とする。また、

$$\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{L}(\mathcal{H}) \mid \text{Tr}[\rho] = 1, \rho \geq 0\} \quad (5.1)$$

を密度演算子全体の集合とし、この元を密度演算子と呼ぶ。

5.1 CPTP 写像, ユニタリ写像

定義 5.1.1 (CPTP 写像). $\mathcal{H}_A, \mathcal{H}_B$ をそれぞれヒルベルト空間とする。 $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ を線形写像とする。このとき、 \mathcal{E} が **Trace preserving (TP)** であるとは、

$$\forall \rho \in \mathcal{L}(\mathcal{H}_A) \quad \text{Tr}(\rho) = \text{Tr}(\mathcal{E}(\rho)) \quad (5.2)$$

をみたすことをいう。また、 \mathcal{E} が **positive** であるとは、

$$\forall \rho (\geq 0) \in \mathcal{L}(\mathcal{H}_A) \quad \mathcal{E}(\rho) \geq 0 \quad (5.3)$$

であることをいう。

$$\forall n \in \mathbb{N} \quad (\mathcal{E} \otimes \mathcal{I}_n) : \mathcal{L}(\mathcal{H}_A) \otimes \mathbb{C}^n \rightarrow \mathcal{L}(\mathcal{H}_B) \otimes \mathbb{C}^n \quad (5.4)$$

が、 $(\mathcal{E} \otimes \mathcal{I}_n) \geq 0$ をみたすとき、 \mathcal{E} は **Completely positive (CP)** であるという。CP かつ TP な写像を **CPTP 写像** という。

定義 5.1.2 (ユニタリ写像). \mathcal{H} をヒルベルト空間とする。 $\mathcal{E} : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H})$ を線形写像とする。 \mathcal{E} がユニタリ写像であるとは、 \mathcal{E} が

$$\mathcal{E}(I) = I \quad (5.5)$$

をみたすことをいう。

ユニタリ写像は、古典の情報理論でいうところの2重確率遷移行列に相当する。正直な話、もっとマシな名前は無かったのかと思う。

5.2 von Neumann エントロピーと量子 KLD

定義 5.2.1 (von Neumann エントロピー). $\rho \in \mathcal{S}(\mathcal{H})$ とする. このとき,

$$S_1(\rho) = -\text{Tr}[\rho \ln \rho] \quad (5.6)$$

を von Neumann エントロピーという.

密度行列はエルミートなので, ユニタリ行列で対角化できる. つまり, \mathcal{H} のある正規直交基底 $\{\phi_i\}_i$ をうまく持ってくれば, $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ とかける. このとき, von Neumann エントロピーは, Shannon エントロピーと一致する.

また, Shannon エントロピーの性質から,

$$0 \leq S_1(\rho) \leq \ln d \quad (\forall \rho \in \mathcal{S}(\mathcal{H})) \quad (5.7)$$

が成立する. また, Tr の循環性から, 任意のユニタリ演算子 U に対して, $S_1(U\rho U^\dagger) = S_1(\rho)$ が成立する.

定義 5.2.2. 量子 Kullback-Leibler divergence $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ とする. このとき,

$$S_1(\rho||\sigma) = \text{Tr}[\rho \ln \rho - \rho \ln \sigma] \quad (5.8)$$

を量子 Kullback-Leibler divergence という.

証明は複雑(らしい. 追ったことはない)なので省略するが, 量子 KLD に対しても単調性が成立する.

定理 5.2.3. $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, $\Lambda : \mathcal{S}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{H})$ とする. このとき,

$$S_1(\rho||\sigma) \geq S_1(\Lambda(\rho)||\Lambda(\sigma)) \quad (5.9)$$

が成立する.

5.3 Quantum majorization

量子状態に対しても Majorization を導入できる. $\rho, \sigma \in \mathcal{L}(\mathcal{H})$

定義 5.3.1 (Quantum majorization). $\rho, \sigma \in \mathcal{L}(\mathcal{H})$ とし, これらのスペクトル分解を

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|, \quad \sigma = \sum_i q_i |\psi_i\rangle\langle\psi_i| \quad (5.10)$$

とする. このとき, $\rho \prec \sigma$ であるとは, $p \prec q$ であることをいう.

このとき, HLP の定理と同様な定理が成立する.

定理 5.3.2. $\rho, \sigma \in \mathcal{L}(\mathcal{H})$ とする. 以下は全て同値.

1. $\rho \prec \sigma$
2. $\rho = \mathcal{E}(\sigma)$ を満たす CPTP ユニタリ写像 \mathcal{E} が存在する.

3. あるユニタリ写像の列 $\{U_k\}$ と, $\sum_k r_k = 1$, $r_k \geq 0$ をみたす数列 $\{r_k\}$ が存在して,

$$\rho = \sum_k r_k U_k \sigma U_k^\dagger \quad (5.11)$$

をみたす.

Proof. (1 \Rightarrow 2) $\rho \prec \sigma$ をみたすとき, $p \prec q$ が成立する. このとき, HLP の定理から, 2重確率遷移行列 T が存在して, $p = Tq$ をみたす. このとき,

$$\mathcal{E}(\sigma) = \sum_{i,j} T_{ij} |\phi_i\rangle\langle\psi_j| \sigma |\psi_j\rangle\langle\phi_i| \quad (5.12)$$

というふうに \mathcal{E} を構成する. このとき, $M_{ij} = \sqrt{T_{ij}} |\phi_i\rangle\langle\psi_j|$ とおくと, これは $\sum_{i,j} M_{ij}^\dagger M_{ij} = I$ をみたす. よって, この \mathcal{E} は CPTP 写像である. (\because クラウス表現). よって OK.

(2 \Rightarrow 1) \mathcal{E} は CPTP ユニタリであるとし, T_{ji} を

$$T_{ji} = \langle\phi_j| \mathcal{E}(|\psi_i\rangle\langle\psi_i|) |\phi_j\rangle \quad (5.13)$$

とすると, $\sum_i T_{ji} = \sum_j T_{ji} = 1$, $T_{ji} \geq 0$ であり, T_{ji} は 2重確率遷移行列である. また, このとき $q = Tp$ より, $\rho \prec \sigma$

(3 \Rightarrow 2) は明らか. (ユニタリの混合は CPTP ユニタリ.)

(1 \Rightarrow 3) を示す. $\rho \prec \sigma$ を仮定する. このとき, 2重確率遷移行列 T が存在して, $p = Tq$ を満たす. Birkhoff の定理 (証明はラックス線形代数を参照.) から, 置換行列 P_k を用いて $P_k = \sum_k r_k P_k$ をみたす. このとき, P_k を $\{|\phi_k\rangle\}$ を入れ替える写像とし, $\{|\phi_k\rangle\}$ を $\{|\psi_k\rangle\}$ に変換する写像を V とすれば,

$$\rho = \sum_k r_k V P_k \sigma P_k V \quad (5.14)$$

この $P_k V$ はユニタリなので, OK. □

最後に, 状態遷移の必要条件, 十分条件について述べる.

定理 5.3.3 (状態遷移の必要条件). $(\rho, \sigma) \prec (\rho', \sigma')$ ならば,

$$S_0(\rho' || \sigma') \leq S_0(\rho || \sigma), \quad S_\infty(\rho' || \sigma') \leq S_\infty(\rho || \sigma) \quad (5.15)$$

が成立する.

Proof. divergence の単調性による. (示していないけどね.) □

定理 5.3.4 (状態遷移の十分条件).

$$S_\infty(\rho' || \sigma') \leq S_0(\rho || \sigma) \quad (5.16)$$

ならば, $(\rho', \sigma') \prec (\rho, \sigma)$ が成立する.

Proof. 具体的に $\rho' = \mathcal{E}(\rho)$, $\sigma' = \mathcal{E}(\sigma)$ なる \mathcal{E} を実際に構成する. 具体的には, 測定をして得られた結果を基に状態を準備する. P_ρ を ρ の台への射影として, $\{P_\rho, I - P_\rho\}$ で表される射影測定を行う. (それぞれを結

果 0,1 と対応づけることにする。) Rényi 0-divergence が $S_0(\rho||\sigma) = -\ln[\text{Tr}[P_\rho\sigma]]$ で与えられることを思い出せば, ρ, σ それぞれの状態について, 結果が 0,1 となる確率は

$$P(0|\rho) = 1, \quad P(1|\rho) = 0, \quad P(0|\sigma) = c, \quad P(1|\sigma) = 1 - c \quad (5.17)$$

と書ける. ただし, $c = e^{-S_0(\rho||\sigma)}$ とした. $c = 1$ ならば $S_0(\rho||\sigma) = 0$ であり, 仮定から $S_\infty(\rho||\sigma) = 0$ となる. 補題??から, このとき $\rho' = \sigma'$ がいえるので, 入力によらず任意の状態を ρ' に写す写像を持ってくれば, これは CPTP. あとは $c \neq 1$ の場合を考えればよい. 入力した状態に対して上で示した射影測定を行い, 測定の結果が 0 であれば ρ' , 1 であれば

$$\sigma'' := \frac{\sigma' - c\rho'}{1 - c} \quad (5.18)$$

を用意することにする. σ'' が半正定値であることは, $S_\infty(\rho'|\sigma') \leq S_0(\rho||\sigma)$ から,

$$\sigma'' \geq \frac{\sigma' - e^{-S_\infty(\rho'|\sigma')}\rho'}{1 - c} \geq 0 \quad (5.19)$$

から従う. ただし, 最後の不等号は $S_\infty(\rho'|\sigma')$ の定義を用いた. これが $\mathcal{E}(\sigma) = \sigma'$ を満たすことは簡単に示せる. □

第6章

エンタングルメントのリソース理論

リソース理論は、考えたい各問題に対して、始終態から終状態への遷移が、問題で許容される操作のもとで可能か、その中でリソースがどの程度消費(生産)されるかを考える分野。らしい。この章では、アリスとボブの2者間で共有された qubit に対して、LOCC を施して、ある状態から別の状態に変換することのできる必要十分条件を考えたい。

LOCC について、以下の命題が成立する。証明は概略にとどめる。

命題 6.0.1. LOCC によって $|\psi\rangle$ から $|\phi\rangle$ に状態が変化するとする。このとき、この操作は以下のプロトコルで達成出来る。

- Alice が測定する。
- 測定結果を Bob に送る。
- Bob が受け取った結果に基づいてユニタリ変換を施す

Proof. LOCC による変換は、一方が測定を行い、その結果を古典通信で送り、結果に基づいた測定を行うことを繰り返すことで実現出来る。(らしい。) 証明のポイントは、Bob が測定することは、Alice が測定して、結果に応じたユニタリ変換を Bob 側で施すことでシミュレートできる。最後に、この複数の操作をひとまとめにすることで求める結果を得る。 □

以下、定理。

定理 6.0.2. 2者間で共有された純粋状態 $|\psi\rangle$ を別の純粋状態 $|\phi\rangle$ に LOCC で変換できる必要十分条件は、 $\lambda_\psi \prec \lambda_\phi$ である。ただし、 $\rho_\phi = \text{Tr}_B(|\phi\rangle\langle\phi|)$ 、 $\rho_\psi = \text{Tr}_B(|\psi\rangle\langle\psi|)$ であり、 $\lambda_\phi, \lambda_\psi$ はこれらの固有値である。

以上の定理からわかることとして、例えばベル状態 $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ はエンタングル状態の中でも最強であることがわかり、ある LOCC が存在して、任意の純粋状態に移れる。また、Alice と Bob の共有している状態 $|\psi\rangle$ から $|\phi\rangle$ に変換出来ないときも、触媒 $|c\rangle$ を単に付け加えることで遷移が可能になることがある。

触媒によって遷移可能となる例

Alice と Bob がそれぞれ 4 準位の量子を持っているとし、これらの初期状態 $|\psi\rangle$ と、得たい状態 $|\phi\rangle$ は

$$|\psi\rangle = \sqrt{0.4}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.1}|22\rangle + \sqrt{0.1}|33\rangle \quad (6.1)$$

$$|\phi\rangle = \sqrt{0.5}|00\rangle + \sqrt{0.25}|11\rangle + \sqrt{0.25}|22\rangle \quad (6.2)$$

であるとする。このとき、 $\rho_\psi = \text{Tr}_B[|\psi\rangle\langle\psi|]$ 、 $\rho_\phi = \text{Tr}_B[|\phi\rangle\langle\phi|]$ とすれば、直ぐに確かめられるように、これらは一方がもう一方に majorize されるような関係性がない。

しかしながら、これとは別の量子ビット $|c\rangle = \sqrt{0.6}|00\rangle + \sqrt{0.4}|11\rangle$ を持つてくることで、 $|c\rangle$ の状態はそのままに $|\psi\rangle \rightarrow |\phi\rangle$ の変換が可能になる。実際、

$$\rho_{\psi \otimes c} = \text{diag}(0.24, 0.16, 0.24, 0.16, 0.06, 0.04, 0.06, 0.04) \quad (6.3)$$

$$\rho_{\phi \otimes c} = \text{diag}(0.30, 0.20, 0.15, 0.10, 0.15, 0.10, 0, 0) \quad (6.4)$$

となるので、 $\rho_{\psi \otimes c} \prec \rho_{\phi \otimes c}$ が成り立つ。定理 6.0.2 から、 $|\psi\rangle \otimes |c\rangle \rightarrow |\phi\rangle \otimes |c\rangle$ の遷移が可能になる。このような、適切な補助系を付ければ、それ自体は変化しないもののある遷移が可能になるとき、この補助系のビットを触媒という。また、 ρ_ϕ は ρ_ψ を **catalytic majorize** するという。

以下、証明。

Proof. (\Rightarrow) 命題 6.0.1 より、Alice は測定演算子 $\{M_i\}$ で表される測定をし、結果 j を得て、それを Bob に送り、Bob はユニタリ演算子 U_j を自身のビットに作用させるとしてよい。このとき、測定をした後 Bob がどんな操作をしようと、Bob のビットをトレースアウトすることを考えれば

$$M_j \rho_\psi M_j^\dagger = p_j \rho_\phi \quad (6.5)$$

ここで、 $M_j \sqrt{\rho_\psi} = P_j V_j$ と極分解することを考える。ただし、 P_j は半正定値、 V_j はユニタリ。このとき、 $P_j = \sqrt{M_j \rho_\psi M_j^\dagger} = \sqrt{p_j \rho_\phi}$ と取れば、

$$M_j \sqrt{\rho_\psi} (M_j \sqrt{\rho_\psi})^\dagger = M_j \rho_\psi M_j^\dagger \quad (6.6)$$

$$P_j V_j (P_j V_j)^\dagger = \sqrt{M_j \rho_\psi M_j^\dagger} V_j V_j^\dagger \sqrt{M_j \rho_\psi M_j^\dagger} = M_j \rho_\psi M_j^\dagger \quad (6.7)$$

となり、辻褄がきちんと合う。 $M_j \sqrt{\rho_\psi}$ に、その共役を左からかけて j についての和を取れば、

$$\sum_j \sqrt{\rho_\psi} M_j^\dagger M_j \sqrt{\rho_\psi} = \sum_j V_j^\dagger \sqrt{p_j \rho_\phi} \sqrt{p_j \rho_\phi} V_j \quad (6.8)$$

$$\sqrt{\rho_\psi} \left(\sum_j M_j^\dagger M_j \right) \sqrt{\rho_\psi} = \sum_j p_j V_j^\dagger \rho_\phi V_j \quad (6.9)$$

$$\rho_\psi = \sum_j p_j V_j^\dagger \rho_\phi V_j \quad (6.10)$$

とかける。よって、定理 5.3.2 から、 $\rho_\psi \prec \rho_\phi$ が示せる。

(\Leftarrow) について、一旦 ρ_ψ が正則であるとして議論を進める。正則でない密度行列についても、このあと議論

する。今、 $\rho_\psi \prec \rho_\phi$ を仮定しているので、離散の確率分布 $\{p_i\}$ と、ユニタリ演算子の列 $\{U_i\}$ が存在して、

$$\rho_\psi = \sum_j p_j U_j \rho_\phi U_j^\dagger \quad (6.11)$$

とかける。この時、Alice の系に対する演算子 M_j を、 $M_j \equiv \sqrt{p_j \rho_\phi} U_j^\dagger \rho_\psi^{-\frac{1}{2}}$ となるように定める。このとき、簡単に確認出来るように、 $\sum_j M_j^\dagger M_j = I$ である。Alice がこの M_j に対応する測定を行い、結果 j に対応する状態 $|\psi_j\rangle \propto M_j |\psi\rangle$ を得たとする。このとき、測定後の Alice 側の縮約密度行列は、

$$\rho_j \propto M_j \rho_\psi M_j^\dagger = \sqrt{p_j \rho_\phi} U_j^\dagger \rho_\psi^{-\frac{1}{2}} \rho_\psi \left(\sqrt{p_j \rho_\phi} U_j^\dagger \rho_\psi^{-\frac{1}{2}} \right)^\dagger \quad (6.12)$$

$$= p_j \rho_\phi \quad (6.13)$$

とかける。右辺と左辺のトレースはいずれも 1 なので、 $\rho_j = \rho_\phi$ とわかる。B 系も考慮に入れてやれば、全体の状態ケットは $|\phi\rangle, |\psi_j\rangle$ となる。これらは、結局同じ縮約密度行列の二つの純粋化であり、ユニタリで移り変わることが出来る。よって、Bob は結果を聞いた後、結果に対応するユニタリ操作をすれば $|\phi\rangle$ を得る。

また、 ρ_ψ が可逆でないとき、 ρ_ψ は、

$$\rho_\psi = \sum_{i=1}^k p_i |\psi_i\rangle\langle\psi_i| \quad (k < d) \quad (6.14)$$

という風にスペクトル分解出来る。いま、 $\rho_\psi \prec \rho_\phi$ を仮定しているから、 ρ_ϕ をスペクトル分解したとき、非 0 な固有値は k 以下である。

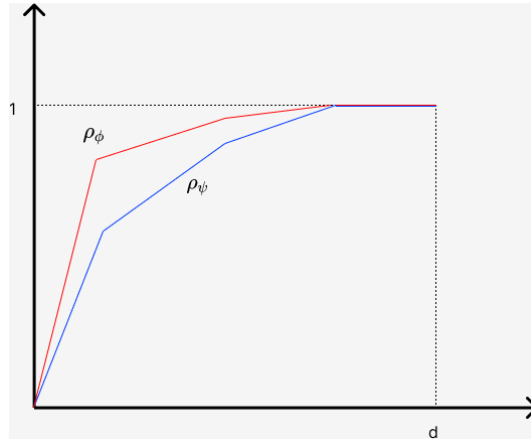


図 6.1 $\rho_\psi \prec \rho_\phi$ なので、図より ρ_ϕ をスペクトル分解したとき、非 0 な固有値は k 以下。

あとは、適切に U_j の定義域や値域を絞ってやれば、そこでは ρ_ψ が可逆になる。そこからは以上の議論とまったく同じである。□

6.1 Majorization 束と近似問題

6.1.1 近似問題

詳細は AppendixB に譲るが, majorization による確率分布間の二項関係 \prec は擬順序をなす. さらに, \mathcal{P}_d を

$$\delta_d = \{p \in \mathcal{P}_d \mid p_i \geq p_{i+1}\} \subseteq \mathcal{P}_d \quad (6.15)$$

という風に制限してやると, \prec は半順序になり, AppendixB での証明により, (δ_d, \prec) は束をなすことがわかる. この束を以下では **majorization 束** と呼ぶことにする. 特に, 任意の $p, q \in \delta_d$ に対して $p \wedge q$ と $p \vee q$ は具体的に構成することでその存在を確かめられる. 詳細は AppendixB を参照頂きたい.

6 節では, Alice と Bob が共有している 2 量子の純粋状態の間での遷移可能条件が縮約密度行列の Majorization で与えられることを見た. また, 純粋状態 $|\phi\rangle, |\psi\rangle$ を任意に取ってきたとき, 一般には $|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle$ の変換は可能とは限らない. $|\psi\rangle \rightsquigarrow |\phi\rangle$ な二つの純粋状態に対して, $|\psi\rangle$ を初期状態として, LOCC によってせめて $|\phi\rangle$ と近い状態を得たい. これをここでは近似問題と呼ぶことにする. 以上のことを改めて定式化する.

近似問題

初期状態 $|\psi\rangle$ と標的状態 $|\phi\rangle$ を, Alice と Bob が共有している, $|\psi\rangle \rightsquigarrow |\phi\rangle$ (LOCC) な任意の 2 つの 2 量子純粋状態とする. このとき,

$$|\chi^{opt}\rangle = \underset{|\chi\rangle: |\psi\rangle \xrightarrow{\text{LOCC}} |\chi\rangle}{\text{argmax}} F(|\phi\rangle, |\chi\rangle) \quad (6.16)$$

を探す問題を近似問題と呼ぶ. ただし, $F(\cdot, \cdot)$ は忠実度であり, 純粋状態なら $F(|\phi\rangle, |\chi\rangle) = |\langle \phi | \chi \rangle|^2$ である. この解 $|\chi^{opt}\rangle$ はすでに知られている.

ここで, 簡単に得られる解として,

$$|\chi^{sup}\rangle = \sum_i \sqrt{\chi_i^{sup}} |i_A\rangle |i_B\rangle \quad (6.17)$$

$$\chi^{sup} = \psi \vee \phi \quad (6.18)$$

とする. ただし, $|i_A\rangle, |i_B\rangle$ はシュミット基底, χ^{sup} は, $|\psi\rangle, |\phi\rangle$ それぞれのシュミット係数からその上限を計算したものである. 今回の問題のセッティングでは, 以下が成立する.

- $|\psi\rangle$ と $|\phi\rangle$ は比較可能でない
- $|\psi\rangle \prec |\chi^{opt}\rangle$
- $|\psi\rangle \prec |\chi^{sup}\rangle$
- $|\phi\rangle \prec |\chi^{sup}\rangle$

よって, $|\phi\rangle, |\psi\rangle, |\chi^{sup}\rangle$ のハッセ図を固定して, $|\chi^{opt}\rangle$ の位置で場合分けすると, 以下のようになる.

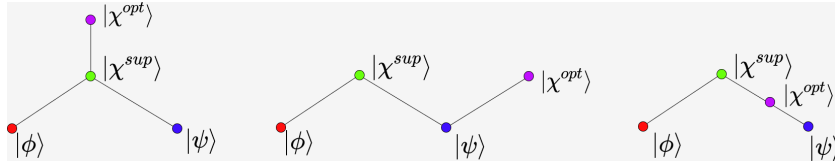


図 6.2 問題設定から許容されるハッセ図

実は、以下の定理から、許されるハッセ図は一つに限られる。

定理 6.1.1.

$$\phi \prec \chi^{sup} \prec \chi^{opt} \quad (6.19)$$

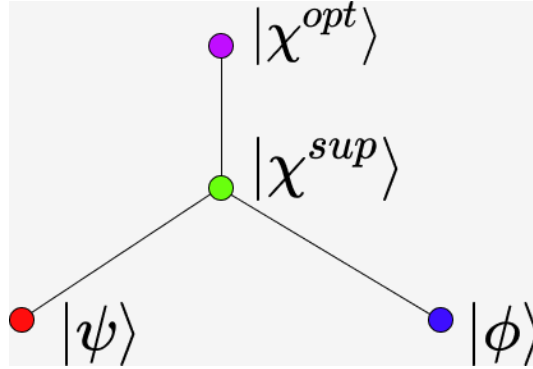


図 6.3 定理 6.1.1 に対応するハッセ図.

この図を見ればわかるように、忠実度の観点で得られた最適解よりも、ハッセ図上では $|\chi^{sup}\rangle$ の方がより標的状態 $|\phi\rangle$ に近いといえる。さらに、束の構造を生かせば、 $p, q \in \delta_d$ に対して、

$$d(p, q) = H(p) + H(q) - 2H(p \vee q) \quad (6.20)$$

という風な関数を考えてやれば、これは距離としての要件をみたくことが知られている。ただし、 $H(\cdot)$ は Shannon エントロピーである。量子状態に関して言えば、Shannon エントロピーをエンタングルメントエントロピーに全て置き換えればよい。このとき、 $|\chi^{sup}\rangle$ は、この距離における近似問題の最適解である。

定理 6.1.2. 初期状態 $|\psi\rangle$ と標的状態 $|\phi\rangle$ を、Alice と Bob が共有している、 $|\psi\rangle \leftrightarrow |\phi\rangle$ (LOCC) な任意の 2 つの 2 量子純粋状態とする。このとき、

$$|\chi^{sup}\rangle = \operatorname{argmin}_{|\chi\rangle: |\psi\rangle \xrightarrow{\text{LOCC}} |\chi\rangle} d(|\phi\rangle, |\chi\rangle) \quad (6.21)$$

付録 A

Hardy-Littlewood-Polya の定理の証明

この補遺では, Hardy-Littlewood-Polya の定理を証明する. 主張をまとめておく.

定理 A.0.1. (Hardy-Littlewood-Polya) $p, p' \in \mathcal{P}_d$ とする. 以下は全て同値.

1. $p' \prec p$
2. $\forall t \in \mathbb{R} \quad \sum_{i=1}^d |p'_i - t| \leq \sum_{i=1}^d |p_i - t|$
3. 任意の下に凸な関数 f に対して, $\sum_{i=1}^d f(p'_i) \leq \sum_{i=1}^d f(p_i)$
4. 2重確率遷移行列 T が存在して, $p' = Tp$ が成立する.

Proof. 4 \Rightarrow 3 は f -divergence の凸性から従う. 3 \Rightarrow 2 は $f(x) = |x - t|$ が下に凸であることから従う.

2 \Rightarrow 1 を示す. $t = p_k^\downarrow$ とおく. このとき,

$$\sum_{i=1}^d |p_i - t| = \sum_{i=1}^k (p_i^\downarrow - t) - \sum_{i=k+1}^d (p_i^\downarrow - t) \quad (\text{A.1})$$

$$= 2 \sum_{i=1}^k p_i^\downarrow - 1 + (d - 2k)t \quad (\text{A.2})$$

$$\sum_{i=1}^d |p'_i - t| \geq \sum_{i=1}^k (p'_i - t) - \sum_{i=k+1}^d (p'_i - t) \quad (\text{A.3})$$

$$= 2 \sum_{i=1}^k p_i^{\prime\downarrow} - 1 + (d - 2k)t \quad (\text{A.4})$$

$$(\text{A.5})$$

より, 仮定の不等式から

$$\forall k \in \{1, 2, \dots, d\} \quad \sum_{i=1}^k p_i^\downarrow \geq \sum_{i=1}^k p_i^{\prime\downarrow} \quad (\text{A.6})$$

が示せた. 最後に, 1 \Rightarrow 4 を示す. このために, 以下の定理を示す.

定理 A.0.2. (超平面分離定理) $A, B \subset \mathbb{R}^n$ を, 互いに素な空でない凸部分集合とする. このとき, ある $v \in \mathbb{R}^n (v \neq \mathbf{0}), c \in \mathbb{R}$ が存在して,

$$\langle x, v \rangle \geq c, \quad \langle y, v \rangle \leq c \quad (\text{A.7})$$

を満たす.

これを以下で証明するが, そのために以下の補題を先に示す.

補題 A.0.3. K を \mathbb{R}^n の空でない閉凸部分集合とする. 集合 K について, 最小ノルムを持つベクトルは一意に存在する.

Proof. (補題) K 上のベクトル X のノルムの下限を $\delta = \inf |x| \mid x \in K$ とする. (ノルムは 0 以上なので, 下界が存在し, 実数の連続性から下限の存在も言える.) $|x_j|$ となるような K 上の数列 $\{x_j\}$ について, K の凸性から $\frac{x_i + x_j}{2} \in K$ が成立する. また,

$$\left| \frac{x_i + x_j}{2} \right| \geq \inf |x| = \delta \quad (\text{A.8})$$

より,

$$|x_i - x_j|^2 = 2|x_i|^2 + 2|x_j|^2 - |x_i + x_j|^2 \leq 2|x_i|^2 + 2|x_j|^2 - 4\delta^2 \quad (\text{A.9})$$

となる. この右辺の極限は 0 なので, $|x_i - x_j| \rightarrow 0$ となる. つまり, これはコーシー列であり, K は完備(らしい)なので, その収束先は K の中に入る. よって, δ はベクトル $x \in K$ の最小ノルム. $r \in K$ もノルムが δ ならば, 同様の計算により,

$$|x - y|^2 \leq 2|x|^2 + 2|y|^2 - 4\delta^2 = 0 \quad (\text{A.10})$$

となるので, $x = y$ である. □

Proof. (超平面分離定理) 互いに素な空でない凸集合 A, B を考えたとき, K を

$$K = A + (-B) = \{x - y \mid x \in A, y \in B\} \quad (\text{A.11})$$

とする. この K も凸集合であり, 交わりがないことから $0 \in K$ である. K の閉包 \bar{K} は凸だから, \bar{K} 上で最小のノルムを持つベクトル $v \in \bar{K}$ が一意に定まる. \bar{K} の凸性から, 任意の $u \in K$ に対して

$$0 \leq \forall t \leq 1 \quad v + t(u - v) \in \bar{K} \quad (\text{A.12})$$

が成立する. よって,

$$|v|^2 \leq |v + t(u - v)|^2 = |v|^2 + 2t \langle v, u - v \rangle + t^2 |u - v|^2 \quad (\text{A.13})$$

$$t|u - v|^2 + 2 \langle v, u \rangle - 2|v|^2 + t|u - v|^2 \geq 0 \quad (\text{A.14})$$

がいえる. $t \rightarrow 0$ の極限を取れば,

$$\langle v, u \rangle = \langle v, x - y \rangle \geq |v|^2 \quad (\text{A.15})$$

$$\inf_{x \in A} \langle x, v \rangle \geq |v|^2 + \sup_{y \in B} \langle y, v \rangle \quad (\text{A.16})$$

$|v|^2 \neq 0$ より OK. □

Hardy-Littlewood-Polya の定理の (1 \Rightarrow 4) の部分の証明に戻る. 一旦考える全体の集合を \mathbb{R}^n まで拡張する. 2重確率遷移行列 T の法を動かすことで, Tp の形で書けるようなベクトルの集合を S とすると, S は凸

集合であることが簡単に確かめられる。このとき、 $p' \notin S$ を仮定して矛盾を導きたい。 p' もやはり凸集合であることに留意すれば、超平面分離定理から、あるベクトル r に対してある $z \in S$ が存在して

$$r^T z < r^T p \quad (\text{A.17})$$

と出来る。 r, p を降順に並べなおす置換行列をそれぞれ P, Q として、 $q' = Pp'$ とおき、 $z = PQp$ と選べば、

$$r^{\downarrow T} (p^{\downarrow} - q') < 0 \quad (\text{A.18})$$

と書ける。ここで、 q' は p' を置換しただけなので、 $q' \prec p$ をみます。一方、任意に選んだ、降順に並んだ n 次元ベクトル w に対して、

$$w^T (p^{\downarrow} - q') = \sum_{i=1}^n w_i (p_i^{\downarrow} - q'_i) \quad (\text{A.19})$$

$$= \sum_{i=1}^n (w_i - w_{i+1}) \sum_{k=1}^i (p_k^{\downarrow} - q'_k) \geq 0 \quad (\text{A.20})$$

と描きなおせる。これは、 $w = r^{\downarrow}$ とすれば矛盾する。よって、4が示せた。□

付録 B

(δ_d, \prec) が束となることの証明

B.1 半順序と束

Majorization の \prec は, 反射律

$$\forall p \in \mathcal{P}_d \quad p \prec p \tag{B.1}$$

と, 推移律

$$\forall p, q, r \in \mathcal{P}_d \quad p \prec q, q \prec r \Rightarrow p \prec r \tag{B.2}$$

を満たす. つまり, 擬順序である. しかしながら, 反対称律

$$\forall p, q \in \mathcal{P}_d \quad p \prec q, q \prec p \Rightarrow p = q \tag{B.3}$$

は成立しない. ($p = (1, 0)$, $q = (0, 1)$ が反例である.) つまり, この後件が成立するには, 自由閹達に成分を入れ替えられては困るわけである. よって, これ以降しばらくは

$$\delta_d = \{p \in \mathcal{P}_d \mid p_i \geq p_{i+1}\} \subseteq \mathcal{P}_d \tag{B.4}$$

を考える. (つまり, すでに成分が降順に並び変えてある確率分布のみ考える.) こうすると, majorization は半順序になる.

以下, 束の定義を確認する.

定義 B.1.1. 最大元, 最小元, 極大元, 極小元半順序集合 (A, \leq) に対して,

- $\forall x \in A \quad x \leq a$ なる $a \in A$ を A の最大元という.
- $\forall x \in A \quad b \leq x$ なる $b \in A$ を A の最小元という.
- $a \leq x, x \in A \Rightarrow a = x$ なる $a \in A$ を A の極大元という.
- $x \leq b, x \in A \Rightarrow b = x$ なる $b \in A$ を A の極小元という.
- $M \subseteq A$ に対して, $\forall x \in M \quad x \leq a$ を満たすとき, a を M の上界という. 上界全体の集合に最小元が存在するなら, これを上限といい, $\sup M$ と書く.
- $M \subseteq A$ に対して, $\forall x \in M \quad b \leq x$ を満たすとき, b を M の下界という. 下界全体の集合に最大元が存在するなら, これを下限といい, $\inf M$ と書く.

定義 B.1.2. 束 (順序集合的な定義) 半順序集合 (A, \leq) に対して, $\forall a, b \in A \exists \sup\{a, b\}, \inf\{a, b\}$ をみたすとき, (A, \leq) を束という.

また, 代数的には以下のように定義される.

定義 B.1.3. 束 (代数的な定義) 集合 A と A 上で閉じている 2 項演算 \wedge, \vee が以下の等式を全て満たすとき, (A, \wedge, \vee) を束という.

- 冪等律: $a \wedge a = a, a \vee a = a$
- 交換律: $a \wedge b = b \wedge a, a \vee b = b \vee a$
- 結合律: $(a \wedge b) \wedge c = a \wedge (b \wedge c), (a \vee b) \vee c = a \vee (b \vee c)$
- 吸収律: $a \wedge (a \vee b) = a, a \vee (a \wedge b) = a$

$\sup\{a, b\} = a \vee b, \inf\{a, b\} = a \wedge b$ と解釈すればよい. これらの定義は同値であることが知られている. また, (特に有限な) 半順序集合を簡単に記述する方法として, ハッセ図が知られている. これは, 元の間順序集合のうち, 推移律からはわからないものをエッジでつないだものである.

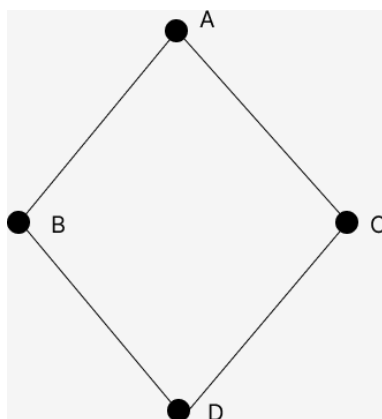


図 B.1 ハッセ図の例. 例えば $B \leq A$.

B.2 Majorization 束

実は, (δ_d, \prec) は束である. これを示すためには,

$$\forall p, q \in \delta_d \exists! s(p, q) \in \delta_d \text{ s.t. } p \prec s, q \prec s, \forall t \in \delta_d, p \prec t, q \prec t \Rightarrow s \prec t \quad (\text{B.5})$$

なる元 (上限, $p \vee q$) と,

$$\forall p, q \in \delta_d \exists! i(p, q) \in \delta_d \text{ s.t. } i \prec p, i \prec q, \forall t \in \delta_d, t \prec p, t \prec q \Rightarrow t \prec i \quad (\text{B.6})$$

なる元 (下限, $p \wedge q$) が存在することを言えればよい. 特に下限の方は, 単にローレンツカーブのうち小さい方を選び続けるとよい.

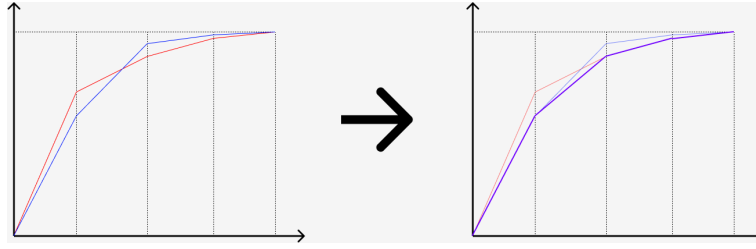


図 B.2 $p, q \in \delta_d$ から $p \wedge q$ を構成する方法.

つまり, $\alpha(p, q) = (a_1, \dots, a_d)$ を以下のように構成する.

$$a_i = \min \left\{ \sum_{j=1}^i p_j, \sum_{j=1}^i q_j \right\} - \sum_{j=1}^{i-1} a_j \quad (\text{B.7})$$

このとき, 順番に計算していけば,

$$\sum_{i=1}^k a_i = \min \left\{ \sum_{i=1}^k p_i, \sum_{i=1}^k q_i \right\} \quad (\text{B.8})$$

がわかる. この α は δ_d の元であることが簡単に確かめられる.

自然な発想をすれば, この方法を $\min \rightarrow \max$ として書き直せば上限が得られると思うであろうが, 実はこれではうまくいかない. というのも, 一般にこの方法で構成した確率分布は δ_d の元ではない. しかし, この確率分布から以下の手順に沿った変換を施せば, $p \vee q$ が得られる.

$p \vee q$ を得るためのプロトコル

- $p_j > p_{j-1}$ をみたす最小の整数を j とする.
- $i \in \{1, 2, \dots, j-1\}$ を, $p_{i-1} > \frac{\sum_{r=1}^j p_r}{j-i+1} = a$ を満たす最大の整数とする.
- 新しい確率分布 q を,

$$q = \begin{cases} a & (r = i, i+1, \dots, j) \\ p_r & (\text{otherwise}) \end{cases} \quad (\text{B.9})$$

とする.

- 以降, この新しく得られた q に対して同じ操作を繰り返す.

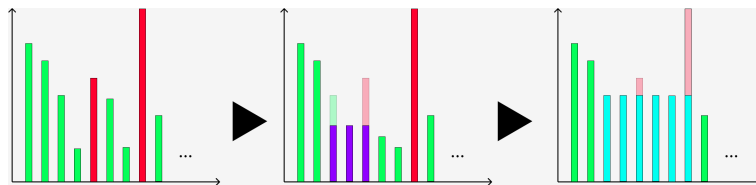


図 B.3 $p \vee q$ を得るためのプロトコル

つまり, 数列が初めて増加する j が見つければ, そこから戻って, 数列が単調減少であって, かつ変化も最小となるように値を均す.

この構成の方法からすぐわかるように, この操作は有限回 (最大 $d-1$ 回) で終了する. これが $p \vee q$ であるこ

とも示せる.

参考文献

- [1] Isaac L. Chuang Michael A. Nielsen. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- [2] 小川 朋宏石坂 智ほか. 量子情報科学入門. 共立出版, 2012.
- [3] Takahiro Sagawa. Entropy, divergence, and majorization in classical and quantum thermodynamics. Springer, 2020.
- [4] G.M. Bosyk, et al. Approximate transformations of bipartite pure-state entanglement from the majorization lattice. <https://doi.org/10.1016/j.physa.2016.12.083>, 2017.
- [5] Gilad Gour Eric Chitambar. Quantum resource theories. arXiv:1806.06107v3, 2019.
- [6] Jakob Yngvason Elliott H. Lieb. The mathematical structure of the second law of thermodynamics. arXiv:math-ph/0204007v2, 2002.