

古典および量子情報理論における状態識別問題の
誤り確率の下界に関する研究

久保 卓也

電気通信大学 大学院情報システム学研究科
博士（工学）の学位申請論文

2015 年 9 月

古典および量子情報理論における状態識別問題の
誤り確率の下界に関する研究

博士論文審査委員会

主査	長岡浩司	教授
委員	森田啓義	教授
委員	川端勉	教授
委員	小川朋宏	准教授
委員	大坐畠智	准教授

目次

第 1 章	はじめに	1
1.1	考察対象となる問題設定	2
1.2	既存の不等式	5
1.3	研究概要	9
1.4	本論文の構成	11
第 2 章	古典状態識別	13
2.1	+ 型不等式とその応用	13
第 3 章	量子状態識別	18
3.1	問題設定	18
3.2	+ 型不等式とその応用	21
3.3	情報スペクトル的な信頼性関数の上界	24
第 4 章	多重アクセス通信路	27
4.1	研究背景	27
4.2	古典系における問題設定	30
4.3	既存不等式	32
4.4	古典系における + 型不等式とその応用	34
4.5	量子系における問題設定	36
4.6	量子系における + 型不等式とその応用	38
4.7	N-user MAC に関する + 型不等式	42
4.8	通信路符号化問題の逆不等式	43

第 5 章	一般化 Poor-Verdú 不等式の拡張	50
5.1	一般化 Poor-Verdú 不等式の証明	50
5.2	関数型一般化 Poor-Verdú 不等式	52
5.3	量子系への拡張	54
第 6 章	結論	56
6.1	本論文のまとめ	56
6.2	今後の課題	57
付録 A	古典シングルアクセス通信路における既存不等式	58
A.1	既存不等式の証明	58
付録 B	Polyanskiy の meta converse および converse	62
B.1	既存不等式の証明	62
B.2	量子系への拡張	64
付録 C	Han の一般公式と関連不等式	67
C.1	通信路符号化問題における一般公式 (Han の一般公式)	67
C.2	既存不等式の証明	70
参考文献		74
謝辞		77

第 1 章

はじめに

状態識別問題は情報理論、特に通信路符号化問題の根幹をなす問題である。状態識別問題とは、通信路を通して得られた情報から元の状態を推定、識別する問題である。一方、通信路符号化問題はメッセージを符号化し通信路を通して伝送して、元のメッセージを復号する問題である。

通信路符号化問題において、一対一通信路を用いた情報の伝送で、漸近的に推定の誤る確率（誤り確率）を 0 にする符号化および復号が存在する通信速度の限界を示す通信路符号化定理を Shannon[20] が示してから、実に様々なアプローチで研究がなされている。例えば、考察対象となる通信路のクラスとしても、一対一（シングルアクセス）や、多対一（多重アクセス）、古典系や量子系など様々なものがあげられる。また、先に述べた漸近的に誤り確率を 0 にする符号が存在する通信速度の限界以外にも、誤り確率が定数 ε である場合の通信路符号化定理や、誤り確率を 1 にする通信速度の下限（強逆定理）、誤り確率が 0 になる指数的速度（信頼性関数）、誤り確率が 1 になる指数的速度（強逆レート）などが解析対象として挙げられる。

このように、考察すべき様々な対象が挙げられる通信路符号化問題ではあるが、その根幹は復号誤りの評価、より一般には状態識別問題の誤り確率の評価に帰結する。本論文では、特に誤り確率の下界について議論を行う。これは、与えられた通信路に対して符号に関する誤り確率の下限であり、どのような符号を用いてもそれ以上誤り確率が改善できない限界を示す。通信路符号化問題における諸定理は、符号化レートがある量未満ならば、漸近的に目的を達成する符号が存在することを示す順部分 (direct part) と逆に符号

化レートがある量を超えると、漸近的にも目的を達成する符号が存在しないことを示す逆部分 (convex part) に分けて証明される。誤り確率の下界は、逆部分に深く関連している。

本章では、まず、状態識別問題やメッセージ推定問題などの数学的な設定について述べ、続いて先行研究で知られている誤り確率の下界を紹介し、さらに本研究で明らかにすべき点に触れ、最後に本論文の構成について述べる。

1.1 考察対象となる問題設定

前節で述べたように考察の対象となる通信路には、量子通信路や多重アクセス通信路などがある。本論文では、それぞれの通信路に対して3つの設定を考えていく。本節では、最も基本的な古典シングルアクセス通信路に対しての設定を述べる。

1つ目は状態識別問題の問題設定である。これは、以下のとおり定式化される。

- Setting 1 (状態識別問題)

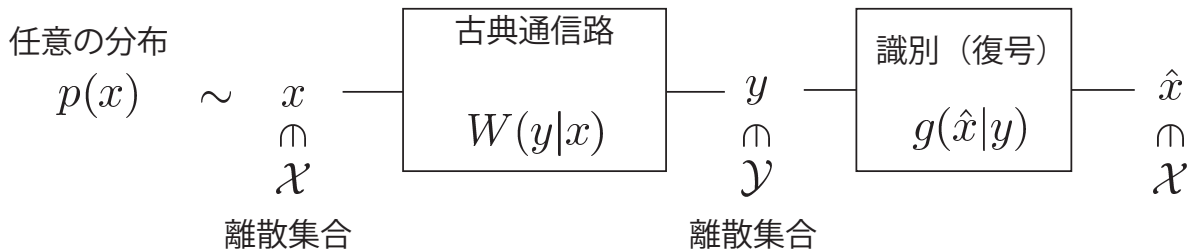


図 1.1 Setting 1

\mathcal{X}, \mathcal{Y} をそれぞれ有限ないし可算無限集合とする。 \mathcal{X}, \mathcal{Y} 上の確率分布 $p(x, y)$ がひとつ与えられているとする。これは通信路 $W(y|x)$ と一般の入力分布 $p(x)$ がひとつ与えられていることに相当する。つまり、 $p(x, y) = p(x)W(y|x)$ である。

このとき、 x の推定を条件付き確率 $g(x|y)$ で表すとすると、誤り確率 Pe は、

$$\text{Pe}(g) = 1 - \sum_{x,y} p(x, y)g(x|y) \quad (1.1)$$

と定義される。

Remark 1.1. 通信路符号化問題において、上記の推定・復号は主に関数を用いて $x = g'(y)$ と表される。この場合は条件付き確率 g を

$$g(x|y) = \begin{cases} 1 & \text{if } x = g'(y) \\ 0 & \text{otherwise} \end{cases}$$

ととることに対応している。なお、復号は関数的な符号化の逆像を用いて行われる事も多い。

Remark 1.2. 上記の問題のことを状態識別問題と呼んでいるが、これは、通信路を x で添字付けされた状態 W_x だとみなすと、この状態の識別を行っていることに相当するためである。またこの問題は、情報理論だけでなく統計学でも重要なものである。

2つ目はメッセージ復号問題の問題設定である。

• **Setting 2(メッセージ復号問題)**

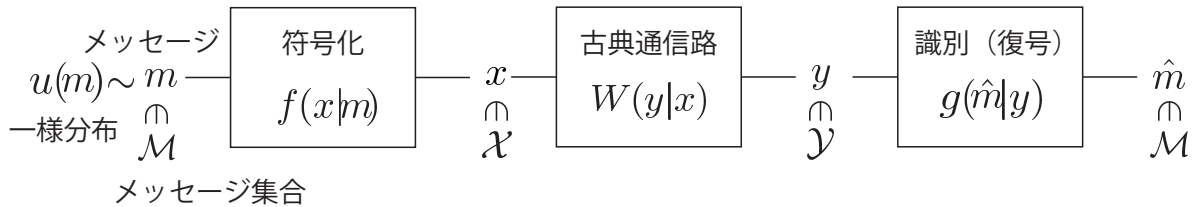


図 1.2 Setting 2

\mathcal{X}, \mathcal{Y} をそれぞれ有限ないし可算無限集合とする。 \mathcal{X} から \mathcal{Y} への通信路 $W(y|x)$ がひとつ与えられているとする。 M を自然数とし、メッセージ集合 \mathcal{M} を $\mathcal{M} := \{1, 2, \dots, M\}$ とし、メッセージは一様分布に従って生成されるとする。

\mathcal{M} から \mathcal{X} への符号化を $f(x|m)$ で表して、これがひとつ与えられているとする。ここで f は \mathcal{M} から \mathcal{X} への条件付き確率である。つまり、符号化として確率的なものも許されているものとする。

このとき、復号を \mathcal{Y} から \mathcal{M} への条件付き確率 $g(m|y)$ で表すと誤り確率 Pe は、

$$\text{Pe}(g) = 1 - \frac{1}{M} \sum_{m,x,y} f(x|m)W(y|x)g(m|y) \tag{1.2}$$

$$= 1 - \sum_{m,x,y} p(m,x,y)g(m|y) \tag{1.3}$$

と定義される。ここで、 $p(m,x,y) = \frac{1}{M}f(x|m)W(y|x)$ である。

Remark 1.3. この問題は、符号化 f と通信路 W を合成したものを新たな通信路と捉えれば、Setting 1 の特別な場合とみなせる。しかし、特に通信路符号化への応用を考えると X から Y への通信路 W が重要であり合成通信路と区別したいことなどの理由から、本論文ではその立場をとらない。この辺りの事情については、第2章で論じる (Remark 2.9 参照)。

最後は先行研究で最もよく用いられる設定である。

• Setting 3

コードブック上の

一様分布

$$u_{\mathcal{C}}(x) \sim x$$

$$\cap$$

$$\mathcal{C}$$

コードブック

$$\cap$$

$$\mathcal{X}$$

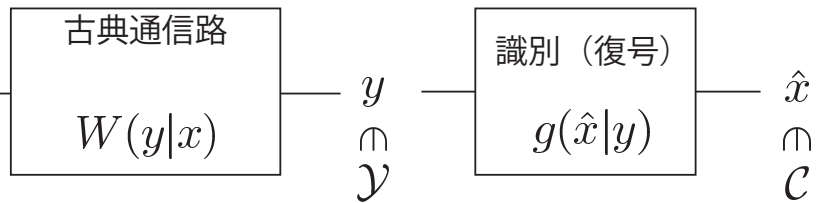


図 1.3 Setting 3

\mathcal{X}, \mathcal{Y} をそれぞれ有限ないし可算無限集合とする。 \mathcal{X} から \mathcal{Y} への通信路 $W(y|x)$ がひとつ与えられているとする。また、 \mathcal{X} 上のコードブック $\mathcal{C}, |\mathcal{C}| = M$ なるものがひとつ与えられているとする。この時、任意の復号 $g(x|y)$ で表すと誤り確率 Pe

は、

$$\text{Pe}(g) = 1 - \frac{1}{M} \sum_{x \in \mathcal{C}, y} W(y|x)g(x|y) \quad (1.4)$$

$$= 1 - \sum_{x, y} p(x, y)g(x|y) \quad (1.5)$$

と定義される。ここで、

$$p(x, y) = \begin{cases} \frac{1}{M}W(y|x) & \text{if } x \in \mathcal{C} \\ 0 & \text{otherwise} \end{cases} \quad (1.6)$$

である。

Remark 1.4. Setting 3 は Setting 1 や Setting 2 の特別な場合に相当する。つまり、Setting 1 で $p(x)$ をコードブック \mathcal{C} 上の一様分布にとったり、Setting 2 で符号化を単射な関数に限れば Setting 3 が得られる。

1.2 既存の不等式

前節で定義した誤り確率に対して以下の下界が知られている。

- Verdú-Han 不等式 [22]

Setting 3 において、任意の復号 g と任意の正数 α に対して、

$$\begin{aligned} \text{Pe}(g) &\geq \Pr\{p(X, Y) \leq \alpha p(Y)\} - \alpha \\ &= \sum_{x, y} p(x, y) \mathbf{1}\{p(x, y) \leq \alpha p(y)\} - \alpha \\ &= \frac{1}{M} \sum_{x \in \mathcal{C}, y} W(y|x) \mathbf{1}\{\frac{1}{M}W(y|x) \leq \alpha p(y)\} - \alpha \\ &= \frac{1}{M} \sum_{x \in \mathcal{C}, y} W(y|x) \mathbf{1}\{W(y|x) \leq \gamma p(y)\} - \frac{\gamma}{M} \end{aligned} \quad (1.7)$$

が成り立つ。ここで、 $\mathbf{1}\{\cdot\}$ は指示関数を表わす。また、確率変数 X, Y は $p(x, y)$ により定義され、 $p(x, y)$ は (3.5) で定義される。さらに $p(y)$ は、 $p(x, y)$ を周辺化して得られる分布である。最後の等式は、正数 γ を $\gamma = M\alpha$ ととれば得られる。

このように、一つの不等式には複数の表現がある。ここで、[22] に表されているのは一番最後の形である。Verdú と Han は古典シングルアクセス一般通信路符号化問題における一般公式の逆部分を導くのにこの不等式を用いた。

- Hayashi-Nagaoka 不等式 [12]

Setting 3 において、任意の復号 g と任意の正数 α 、任意の出力分布 $q(y)$ に対して、

$$\begin{aligned} \text{Pe}(g) &\geq \Pr\{p(X, Y) \leq \alpha q(Y)\} - \alpha \\ &= \sum_{x, y} p(x, y) \mathbf{1}\{p(x, y) \leq \alpha q(y)\} - \alpha \\ &= \frac{1}{M} \sum_{x \in \mathcal{C}, y} W(y|x) \mathbf{1}\left\{\frac{1}{M} W(y|x) \leq \alpha q(y)\right\} - \alpha \end{aligned} \quad (1.8)$$

が成り立つ。

Hayashi-Nagaoka 不等式はもともと [12] で量子系において述べられたものであり、量子シングルアクセス一般通信路符号化問題における一般公式の逆部分を導くのに用いられた。Hayashi-Nagaoka 不等式を Verdú-Han 不等式と比較すると、指示関数の内部の右辺が前者では $p(y)$ であるのに対して、後者では一般の $q(y)$ となっている。

- Poor-Verdú 不等式 [18]

Setting 1 において、任意の識別 g と任意の正数 α に対して、

$$\begin{aligned} \text{Pe}(g) &\geq (1 - \alpha) \Pr\{p(X, Y) \leq \alpha p(Y)\} \\ &= (1 - \alpha) \sum_{x, y} p(x, y) \mathbf{1}\{p(x, y) \leq \alpha p(y)\} \\ &= (1 - \alpha) \sum_{x, y} p(x) W(y|x) \mathbf{1}\left\{\frac{1}{M} W(y|x) \leq \alpha p(y)\right\} \end{aligned} \quad (1.9)$$

が成り立つ。

Poor-Verdú 不等式は Verdú-Han 不等式とほぼ同時期に Poor と Verdú[18] によって導かれた。この不等式は、 $\alpha \Pr\{p(X, Y) > \alpha p(Y)\}$ だけ Verdú-Han 不等式より強い。また、この不等式は通信路符号化問題において符号化レートに対する誤り確率の指数的減衰(信頼性関数)を直接議論するのに適した形をしており、実際ここから導かれる信頼性関

数の上界が真に強いと Poor と Verdú は期待していた。しかしながら、Alajaji と Chen、Riched は [3] でその信頼性関数の上界が真に強くはないことを具体例を構成して示した。なお、[18] には Setting 1 における Verdú-Han 不等式が直接的な証明なしに述べられている。

- 一般化 Poor-Verdú 不等式 [5]

Setting 1 において、任意の識別 g と任意の正数 α および実数 $\theta \geq 1$ に対して、

$$\begin{aligned} \text{Pe}(g) &\geq (1 - \alpha) \Pr\{V^{(\theta)}(X|Y) \leq \alpha\} \\ &= (1 - \alpha) \sum_{x,y} p(x)W(y|x) \mathbf{1}\{V^{(\theta)}(x|y) \leq \alpha\} \end{aligned} \quad (1.10)$$

が成り立つ。ここで、 $V^{(\theta)}$ は

$$V^{(\theta)}(x|y) = \frac{(p(x)W(y|x))^\theta}{\sum_{x'} (p(x')W(y|x'))^\theta} \quad (1.11)$$

であり、 $\theta = 1$ のとき逆向き通信路と一致する。またその時、この不等式は Poor-Verdú 不等式と一致する。

一般化 Poor-Verdú 不等式は Chen と Alajaji[5] がパラメータ θ を導入することで一般化した不等式である。本不等式も信頼性関数の上界の議論に適した形をしているが、その最適性については不明である。

これらの不等式は、情報スペクトル的な方法と関連の深い不等式であり、本論の主要な考察対象である。ここで情報スペクトル的な方法とは、Han and Verdú によって提唱された情報理論における手法であり、従来の期待値量を評価するのではなく、極限を含んだ情報量の分布を評価することで、より広いクラスの通信路を対象とできるようにしたものである。

また、本論文で扱うことはないが、以下の不等式も知られている。

- Fano の不等式 [9]

Setting 3 において、任意の復号 g に対して、

$$\log M \leq \frac{1}{1 - \text{Pe}(g)} \left(\sup_X I(X; Y) + h(\text{Pe}(g)) \right) \quad (1.12)$$

が成り立つ。ここで、 $I(X; Y)$ は相互情報量であり、 h は2値エントロピーである。

- Sphere packing 下界 [21]

Setting 3において、任意の復号 g と十分小さな正数 δ_1, δ_2 に対して、

$$\text{Pe}(g) \geq \exp\{-(E_{sp}(\log M - \delta_1) + \delta_2)\} \quad (1.13)$$

ここで、

$$E_{sp}(R) = \sup_{s \geq 0} [E_0(s) - \rho R], \quad (1.14)$$

$$E_0(s) = \max_{p_X} E_0(s, p_X), \quad (1.15)$$

$$E_0(s, p_X) = -\log \sum_y \left[\sum_x p_X(x) W(y|x)^{1/(1+s)} \right]^{1+s} \quad (1.16)$$

である。

これらの不等式は、定常無記憶通信路における通信路符号化定理や信頼性関数の上界を議論するとき重要な役割を果たす。

最後に、Polyanskiy が彼の博士論文 [16] で示した不等式も、その汎用性の高さや本論文の研究の主旨との関連性から重要である。

- Polyanskiy's meta converse

Setting 2において、任意の復号 g と任意の通信路 $\hat{W}(y|x)$ に対して、

$$1 - \text{Pe}'(g) \geq \beta_{1-\text{Pe}(g)}(p(X)W(Y|X), p(X)\hat{W}(Y|X)) \quad (1.17)$$

が成り立つ。ここで、 β は関数 h を $h: \mathcal{X} \times \mathcal{Y} \rightarrow [0, 1]$ とし、 $p(x, y), q(x, y)$ を $\mathcal{X} \times \mathcal{Y}$ 上の確率分布としたとき、

$$\beta_\alpha(p(X, Y), q(X, Y)) = \min_{h: \sum_{x,y} p(x,y)h(x,y) \geq \alpha} \sum_{x,y} q(x,y)h(x,y) \quad (1.18)$$

で定義され、 $\text{Pe}'(g)$ は

$$\text{Pe}'(g) = 1 - \frac{1}{M} \sum_{m,x,y} f(x|m) \hat{W}(y|x) g(m|y) \quad (1.19)$$

で定義される。また、 $p(x)$ は $p(x) = \frac{1}{M} \sum_m f(x|m)$ である。

- Polyanskiy's converse

Setting 3 において、任意の復号 g に対して、

$$M \leq \sup_p \inf_q \beta_{1-\text{Pe}(g)}(p(X)W(Y|X), p(X)q(Y))^{-1} \quad (1.20)$$

が成り立つ。

これらの不等式は付録 B で詳細を述べる。

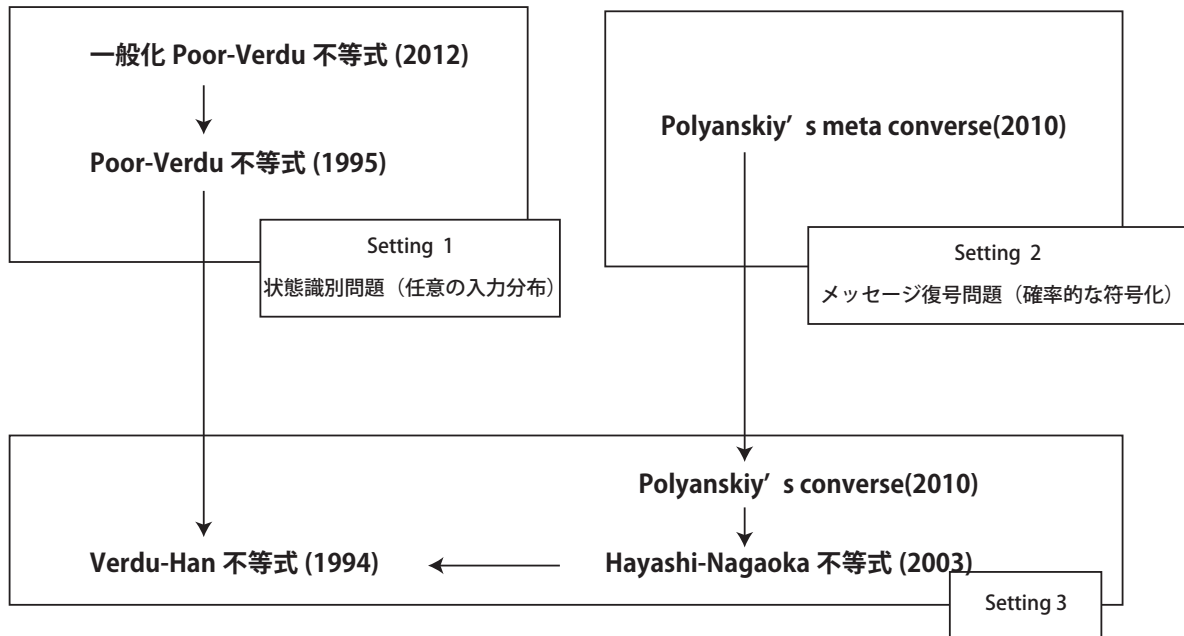


図 1.4 既存不等式の論理的関係図

図 1.4 では、既存不等式のうち本研究と関連の深い不等式の論理的な関係を図示している。図中の矢印は $A \rightarrow B$ のとき A から B が証明できることを示している。

1.3 研究概要

本研究では、誤り確率の下界の中で情報スペクトル的方法と関連の深いものについて、議論する。本研究では、以下の問題に注目した。

- Setting 1 や Setting 2 においてどの不等式が成り立つのか。

既存の下界では、Poor-Verdu 不等式を除けば、ほとんどの不等式が Setting 3 に

において示されており、Setting 1 や Setting 2 への拡張に関する明示的な考察は非常に少なかった。それらの状況で Verdú-Han 不等式や Hayashi-Nagaoka 不等式は成り立つのか。

- 統一的な証明法があるのか、または、証明法の違いと不等式の強さに関連がどうあるのか。

既存の証明方法は、MAP(Maximum A Posteriori) 推定による誤り確率が最適であるという事実を用いたものや、情報理論でよく用いられる union bound を用いたもの、Neyman-Pearson の補題を用いたものなど様々で、統一的に見通すことが難しかった。これらの不等式に統一的な証明があるのか、また無いとすれば、証明法の違いが証明できる不等式の強さと関係するのか。

- 出力分布を任意の q とおくことができる不等式はどれか。

Hayashi-Nagaoka 不等式や Polyanskiy's converse では出力分布を任意の分布にしても成り立ち、Hayashi and Nagaoka[12] ではその事実が応用において重要な役割を果たした。Poor-Verdú 不等式においてもこれは成り立つのか。

- 量子系にした時に何が成り立つのか。

Hayashi-Nagaoka 不等式はもともと量子系で証明された。他の不等式も量子系で成り立つのか、また、成り立たないのはどういう時か。

- 多重アクセス通信路にした時に何が成り立つのか。Han-Verdú 不等式は Han 不等式 [10, 11] として多重アクセス通信路に拡張されている。他の不等式も成り立つのか。

これらの問に対して、本研究の主要な成果は以下のとおりである。

- 統一的な証明のための基礎的な不等式の導出

Setting 1 や 2 において、各種不等式がある基礎的な不等式から導かれることを示した。この不等式は、 $(t)_+ = \max\{t, 0\}$ という記号を用いて表されることから、本論文ではそれを + 型不等式と呼ぶこととする。また、この不等式はシングルアクセス/多重アクセス、古典系/量子系に関わらず成り立つことも明らかにした。

- 量子シングルアクセス通信路符号化問題への拡張およびその応用

Poor-Verdú 不等式を量子系へ拡張することに成功した。その応用例として、量子

シングルアクセス通信路符号化問題における信頼性関数の新しい上界を導いた。

- 量子多重アクセス通信路符号化問題に関する不等式

量子多重アクセス通信路においても新しい誤り確率の下界を得た。その応用として、 ε -通信路容量域および強逆領域に関する不等式を得た。

- 一般化 Poor-Verdú 不等式の量子拡張が不可能であることの検証

+型不等式から量子系での Poor-Verdú 不等式を導くことが可能であったが、一般化 Poor-Verdú 不等式はできていなかった。そこで、この不等式が量子系で成り立つか否かの検証を数値的に行い、否定的な結論を得た。

- 一般化 Poor-Verdú 不等式における「一般化」の拡張

一般化 Poor-Verdú 不等式を +型不等式から導出しようとする試みの中で、一般化 Poor-Verdú 不等式における「一般化」に関する解析を行った。その結果、この一般化は従来の形だけでなく、あるクラスの関数を用いて記述することが可能であるということを見出した。

なお、これらの成果のうち、Poor-Verdú 不等式の量子系への拡張と量子シングルアクセス通信路符号化問題における信頼性関数の新しい上界の導出および量子一般化 Poor-Verdú 不等式の数値計算による成立検証は著者が修士研究 [26] として行ったものである。

1.4 本論文の構成

本論文ではシングルアクセス・多重アクセス、古典系・量子系のそれぞれに対して、+型不等式を証明し、その系を述べる。さらに、量子系においては不等式の応用が新たな結果を導くので、それについても記述している。詳しくは、以下のとおりである。

まず第2章では、基本的な古典シングルアクセス通信路について、Verdú-Han 不等式と Poor-Verdú 不等式の +型不等式による証明を与える。続いて第3章では、第2章の内容を量子系へ拡張する。ここでも +型不等式を扱い、その系としていくつかの下界を証明する。また、Poor-Verdú 不等式の量子版の応用として、情報スペクトル的な信頼性関数の上界について議論する。第4章では、多重アクセス通信路に関する不等式に関する話題を扱う。まず古典系について +型不等式の導出を行い、そこから古典系において有用な不等式である Yagi-Oohama 不等式 [30] が導出されることを見る。その次に量子系の多重

アクセス通信路に関する議論を行う。ここで Yagi-Oohama 不等式型の + 型不等式の量子版を証明し、+ 型不等式の応用として、 ε -通信路容量域と強逆領域に関する評価を行う。第 5 章では、Poor-Verdú 不等式を一般化することで強めた一般化 Poor-Verdú 不等式に関して論じる。一般化 Poor-Verdú 不等式は今のところ、+ 型不等式からの導出ができていない。ここでは、「一般化」が何に起因しているかを明らかにし、さらに量子系への拡張の可否を議論することで、+ 型不等式からの導出の可否や量子系への拡張可能性について考察する。最後に第 6 章でまとめを行い、本論文を終わる。

第 2 章

古典状態識別

本章では、古典シングルアクセス通信路に関する問題を扱う。まず、本研究の主要な不等式である + 型不等式の導出を行う。さらにこの + 型不等式の系として複数の不等式が 1.1 節で述べた Setting 1 や Setting 2 のもとで導出されることも示す。

2.1 + 型不等式とその応用

以下では、本論文で最も重要な不等式である + 型不等式を与える。さらにその不等式の系として、Han-Verdú 不等式や Poor-Verdú 不等式が得られることを述べる。

Theorem 2.1 (古典シングルアクセス通信路に対しての + 型不等式 [29]). *Setting 1* において、任意の推定 g 、任意の正数 α および任意の \mathcal{Y} 上の出力分布 q に対して、以下が成り立つ。

$$1 - \text{Pe}(g) - \alpha \leq \sum_{x,y} (p(x,y) - \alpha q(y))_+ \quad (2.1)$$

ここで

$$(t)_+ := \max\{t, 0\} \quad (2.2)$$

である。

Proof. 任意の関数 $h : \mathcal{Y} \rightarrow \mathbb{R}$ と任意の関数 $g : \mathcal{Y} \rightarrow [0, 1]$ に対して、

$$\sum_y h(y)g(y) \leq \sum_y (h(y))_+ \quad (2.3)$$

が成り立つことから、

$$\begin{aligned} \sum_{x,y} (p(x,y) - \alpha q(y))_+ &\geq \sum_{x,y} (p(x,y) - \alpha q(y)) g(x|y) \\ &= 1 - \text{Pe}(g) - \alpha \end{aligned} \quad (2.4)$$

が成り立つ。最後の等式では、 $\sum_{x,y} q(y)g(x|y) = 1$ を用いた。 \square

この+型不等式は、シングルアクセス・多重アクセス、古典系・量子系を問わずに成り立つ。この事実は次章以降、1つずつ述べていく。

ここで、

$$(p(x,y) - \alpha q(y))_+ = (p(x,y) - \alpha q(y)) \mathbf{1}\{p(x,y) > \alpha q(y)\} \quad (2.5)$$

であることより、系として次が成り立つ。

Corollary 2.2 ([27]). *Setting 1* において、任意の推定 g 、任意の正数 α および任意の \mathcal{Y} 上の出力分布 q に対して、以下が成り立つ。

$$\text{Pe}(g) \geq \Pr\{p(X,Y) \leq \alpha q(Y)\} - \alpha \quad (2.6)$$

Proof. Theorem 2.1 より

$$\begin{aligned} 1 - \text{Pe}(g) - \alpha &\leq \sum_{x,y} (p(x,y) - \alpha q(y))_+ \\ &= \sum_{x,y} (p(x,y) - \alpha q(y)) \mathbf{1}\{p(x,y) > \alpha q(y)\} \\ &\leq \sum_{x,y} p(x,y) \mathbf{1}\{p(x,y) > \alpha q(y)\} \end{aligned} \quad (2.7)$$

が成り立つ。ここで2つ目の不等式は、 $\alpha q(y) \mathbf{1}\{p(x,y) > \alpha q(y)\}$ の項を落とすことにより得られる。 \square

Corollary 2.3. *Setting 1* において、任意の推定 g および任意の正数 α に対して、以下

が成り立つ。

$$\text{Pe}(g) \geq (1 - \alpha) \Pr\{p(X, Y) \leq \alpha p(Y)\} \quad (2.8)$$

ここで $p(y)$ は $p(x, y)$ の周辺分布である。

Proof. Theorem 2.1 より

$$\begin{aligned} 1 - \text{Pe}(g) - \alpha &\leq \sum_{x,y} (p(x, y) - \alpha p(y))_+ \\ &= \sum_{x,y} (p(x, y) - \alpha p(y)) \mathbf{1}\{p(x, y) > \alpha p(y)\} \\ &\leq (1 - \alpha) \sum_{x,y} p(x, y) \mathbf{1}\{p(x, y) > \alpha p(y)\} \end{aligned} \quad (2.9)$$

が成り立つ。ここで 2 つ目の不等式は、 $p(y) \geq p(x, y)$ の事実から得られる。 \square

Remark 2.4. Corollary 2.2 は、Setting 1 における Hayashi-Nagaoka 不等式の古典版に相当する。ここで、 \mathcal{Y} 上の分布 q を周辺分布 p ととれば、Verdú-Han 不等式である。また、Corollary 2.3 は Poor-Verdú 不等式であるが、ここでの証明は出典論文 [18] とは別の証明となっている。

Remark 2.5. Corollary 2.2 は、Setting 3 に適用すれば Hayashi-Nagaoka 不等式の古典版が得られる。さらに \mathcal{Y} 上の分布 q を周辺分布 p ととれば、Verdú-Han 不等式が得られる。

Remark 2.6. Poor-Verdú 不等式は $p(y) \geq p(x, y)$ の事実を用いるため、出力分布が一般の q ではこの証明はできないことに注意が必要である。

Setting 2 において、符号化 f を前置通信路とみなし、 f と W とを結合した通信路を V とおくと、Setting 1 とみなせる。ここで、 $(t)_+$ が凸であるという事実を用いれば、Setting 2 における有用な不等式を Theorem 2.1 から導くことができる。

Corollary 2.7 ([29]). *Setting 2* において、任意の推定 g 、任意の正数 α および任意の \mathcal{Y} 上の出力分布 q に対して、以下が成り立つ。

$$1 - \text{Pe}(g) - \alpha \leq \sum_{m,x,y} \frac{1}{M} f(x|m) (W(y|x) - M\alpha q(y))_+ \quad (2.10)$$

Proof. $p(x|m) = f(x|m), p(y|x) = W(y|x)$ とすると、Theorem 2.1 より次が成り立つ。

$$\begin{aligned} 1 - \text{Pe}(g) - \alpha &\leq \sum_{m,y} (p(m,y) - \alpha q(y))_+ \\ &= \sum_{m,y} \left(\sum_x p(m,x,y) - \alpha q(y) \right)_+ \\ &= \sum_{m,y} \left(\sum_x p(m)p(x|m)p(y|x) - \alpha q(y) \right)_+ \\ &= \sum_{m,y} \left(\sum_x p(x|m) (p(m)p(y|x) - \alpha q(y)) \right)_+ \\ &\leq \sum_{m,x,y} p(x|m) (p(m)p(y|x) - \alpha q(y))_+ \\ &= \sum_{m,x,y} p(m)p(x|m) (p(y|x) - M\alpha q(y))_+ \\ &= \sum_{x,y} p(x) (p(y|x) - M\alpha q(y))_+ \end{aligned} \quad (2.11)$$

ここで、2つ目の等式は Setting 2 のマルコフ性から、2つ目の不等式は $(t)_+$ が凸であることから、Jensen の不等式により得られ、4つ目の等式は $\forall m, p(m) = \frac{1}{M}$ という事実による。 \square

Theorem 2.1 から Corollary 2.2 を得たように、Corollary 2.7 から直ちに次が成り立つ。

Corollary 2.8 ([29]). *Setting 2* において、任意の推定 g 、任意の正数 α および任意の \mathcal{Y} 上の出力分布 q に対して、以下が成り立つ。

$$\text{Pe}(g) \geq \Pr\{W(Y|X) \leq M\alpha q(Y)\} - \alpha \quad (2.12)$$

Corollary 2.8 は Setting 2 における Hayashi-Nagaoka 不等式の古典版である。なお、(2.10) は Poor-Verdú 不等式に拡張することはできない。

Remark 2.9. Setting 2 を Setting 1 の特別な場合とみなし、そのまま Corollary 2.2 や、Corollary 2.3 を適用すると、合成通信路を $V(y|m)$, メッセージ集合上の確率変数を \mathfrak{M} として次が得られる。

$$\text{Pe}(g) \geq \Pr\left\{\frac{1}{M}V(Y|\mathfrak{M}) \leq \alpha q(Y)\right\} - \alpha, \quad (2.13)$$

$$\text{Pe}(g) \geq (1 - \alpha)\Pr\left\{\frac{1}{M}V(Y|\mathfrak{M}) \leq \alpha p(Y)\right\}. \quad (2.14)$$

これらの不等式は、符号化 f を変化させるに応じて V が変化する。通信路符号化問題への応用を考えてみれば、符号が変更される度に情報スペクトル量を計算し直す必要があるということになる。一方、Corollary 2.8 では、そのような事がなく、符号化の変化が入力分布 $p(x)$ の変化のみで表わされ、 W に変化はない。情報理論への応用では、この形が有用である。

また、Corollary 2.8 の証明では、メッセージ集合上の分布が一様であることが重要であった。この設定を外し Setting 1 のようにメッセージ集合上の分布を一般的なものまで許すと、Corollary 2.8 は証明できない。

これらの事情が、Setting 1 の特別な場合として Setting 2 を用意するのではなく、それぞれを別々に用意すべきである理由である。

Remark 2.10. 本論文では + 型不等式という一見証明の途中式に思えるものを定理としている。これは、Setting 3 から Setting 1 や 2 に、Verdú-Han 不等式や Poor-Verdú 不等式が直接拡張できず、この + 型不等式まで戻る必要があることによる。また、4.8 節では量子多重アクセス通信路符号化問題における一般公式への応用にあたって、この + 型不等式そのものが適用されるべきであることを見る。

第 3 章

量子状態識別

本章では、前章に引き続きシングルアクセス通信路に関する問題を扱う。前章では古典通信路を扱っていたが、本章ではそれに対し量子通信路を扱い、量子通信路に対しても古典通信路に対して示した + 型不等式が成立することを示す。なお、本論文で量子通信路と呼んでいる通信路は、正確には古典量子通信路 (classical-quantum channel) と呼ばれ、入力も量子状態である量子量子通信路 (quantum-quantum channel) と区別される。

以下では、まず量子系における問題設定と + 型不等式およびその系の証明を示す。その後、Poor-Verdú 不等式の量子拡張の通信路符号化問題への適用例である情報スペクトル的な信頼性関数の上界を示す。

3.1 問題設定

本節では、第 1 章の Setting 1 ~ 3 に対応する問題設定を述べる。

- Setting Q1

\mathcal{X} を有限ないし可算無限集合とし、 \mathcal{H} を任意のヒルベルト空間とする。 \mathcal{H} 上の半正定値かつトレースが 1 である作用素を状態と呼び、それらの集合である状態集合を $\mathcal{S}(\mathcal{H})$ で表す。一般の入力分布 $p(x)$ と量子通信路 $W : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ がひとつ与えられているとする。

このとき、 x の推定を POVM (Positive Operator-Valued Measure) $Y = \{Y_x\}_{x \in \mathcal{X}}$

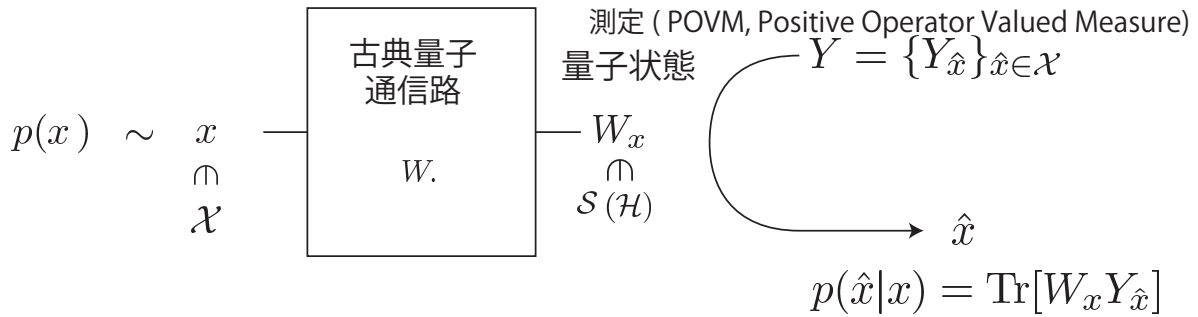


図 3.1 Setting Q1

で表すと、誤り確率 P_e は、

$$P_e(Y) = 1 - \sum_x p(x) \text{Tr}[W_x Y_x] \tag{3.1}$$

と定義される。なお、POVM とは量子系の測定を一般的に表す数学的概念であり、ヒルベルト空間 \mathcal{H} 上の半正定値作用素の集合で、添字で足しあわせたものが恒等作用素 I となるものである。つまりここでは、 $Y_x \geq 0, \sum_x Y_x = I$ である。

• Setting Q2

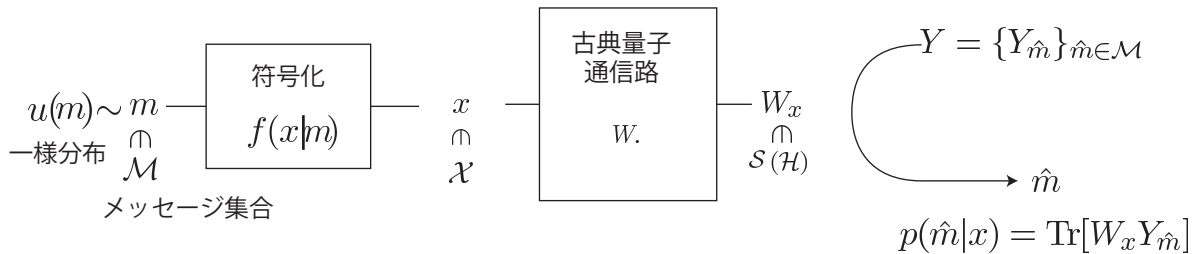


図 3.2 Setting Q2

M を自然数とし、メッセージ集合 \mathcal{M} を $M := \{1, 2, \dots, M\}$ とする。メッセージは一様分布に従って生成されるとする。また、 \mathcal{X} を有限ないし可算無限集合とする。 \mathcal{H} を任意のヒルベルト空間とし、 \mathcal{H} 上の状態集合を $S(\mathcal{H})$ で表す。量子通信路 $W : \mathcal{X} \rightarrow S(\mathcal{H})$ がひとつ与えられているとする。 M から \mathcal{X} への符号化を確率的なものまで許すとし条件付き確率 $f(x|m)$ で表して、これがひとつ与えられているとする。

このとき、復号を POVM $Y = \{Y_m\}_{m \in \mathcal{M}}$ で表すと、誤り確率 Pe は、

$$\text{Pe}(Y) = 1 - \frac{1}{M} \sum_{m,x} f(x|m) \text{Tr}[W_x Y_m] \quad (3.2)$$

と定義される。

• Setting Q3

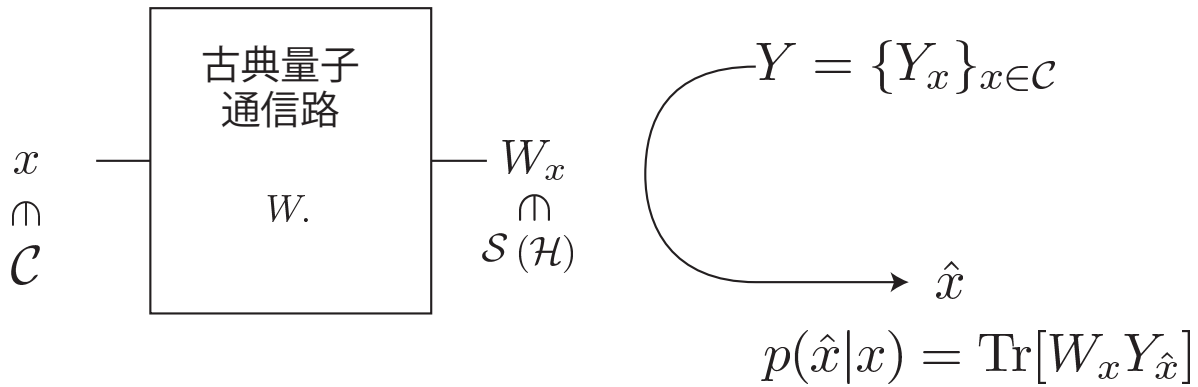


図 3.3 Setting Q3

\mathcal{X} を有限ないし可算無限集合とする。 \mathcal{H} を任意のヒルベルト空間とし、 \mathcal{H} 上の状態集合を $\mathcal{S}(\mathcal{H})$ で表す。量子通信路 $W : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ がひとつ与えられているとする。また、 \mathcal{X} 上のコードブック $\mathcal{C}, |\mathcal{C}| = M$ なるものがひとつ与えられているとする。この時、復号を POVM $Y = \{Y_m\}_{m \in \mathcal{M}}$ で表すと誤り確率 Pe は、

$$\text{Pe}(Y) = 1 - \frac{1}{M} \sum_{x \in \mathcal{C}} \text{Tr}[W_x Y_x] \quad (3.3)$$

$$= 1 - \sum_{x,y} p(x) \text{Tr}[W_x Y_y] \quad (3.4)$$

と定義される。ここで、

$$p(x) = \begin{cases} \frac{1}{M} & \text{if } x \in \mathcal{C} \\ 0 & \text{otherwise} \end{cases} \quad (3.5)$$

である。

3.2 + 型不等式とその応用

ここでは量子系においても、+ 型不等式およびその系が古典系の様に成り立つことを示す。本節で用いる論法は、古典通信路の時とほぼ同じであるが、一部量子系特有のものを用いなければならない。

Theorem 3.1 ([29]). *Setting Q1* において、任意の POVM Y 、任意の正数 α および任意の状態 $\sigma \in \mathcal{S}(\mathcal{H})$ に対して、以下が成り立つ。

$$1 - \text{Pe}(g) - \alpha \leq \sum_x \text{Tr} [(p(x)W_x - \alpha\sigma)_+] \quad (3.6)$$

ここで \mathcal{H} 上のエルミート作用素 A に対して、

$$A = \sum_i \lambda_i E_i \quad (3.7)$$

とスペクトル分解されるときに、 A_+ は、

$$A_+ := \sum_{i:\lambda_i>0} \lambda_i E_i \quad (3.8)$$

と定義される。

Proof. ヒルベルト空間 \mathcal{H} 上の任意のエルミート作用素 A と $0 \leq T \leq I$ を満たす任意の半正定値作用素 T に対して

$$\text{Tr}[AT] \leq \text{Tr}[A_+] \quad (3.9)$$

が成り立つことから、Theorem 1 の場合と同様に

$$\begin{aligned} \sum_x \text{Tr} [(p(x)W_x - \alpha\sigma)_+] &\geq \sum_x \text{Tr} [(p(x)W_x - \alpha\sigma) Y_x] \\ &= 1 - \text{Pe}(Y) - \alpha \end{aligned} \quad (3.10)$$

が成り立つ。 □

ここで \mathcal{H} 上のエルミート作用素 A が (3.7) でスペクトル分解されるとき、射影子

$\{A > 0\}$ を

$$\{A > 0\} := \sum_{i:\lambda>0} E_i \quad (3.11)$$

で定義すると、

$$A_+ = A\{A > 0\} \quad (3.12)$$

であることから、次の不等式が直ちに導かれる。

Corollary 3.2 ([27]). *Setting Q1*において、任意の *POVM* Y 、任意の正数 α および任意の状態 $\sigma \in \mathcal{S}(\mathcal{H})$ に対して、以下が成り立つ。

$$\text{Pe}(Y) \geq \sum_x p(x) \text{Tr}[W_x \{p(x)W_x \leq \alpha\sigma\}] - \alpha \quad (3.13)$$

ただし、

$$\{p(x)W_x \leq \alpha\sigma\} := \{p(x)W_x - \alpha\sigma \leq 0\}. \quad (3.14)$$

Proof. Theorem 3.1 より以下が得られる。

$$\begin{aligned} 1 - \text{Pe}(g) - \alpha &\leq \sum_x \text{Tr} [(p(x)W_x - \alpha\sigma)_+] \\ &= \sum_x \text{Tr} [(p(x)W_x - \alpha\sigma) \{p(x)W_x > \alpha\sigma\}] \\ &\leq \sum_x p(x) \text{Tr} [W_x \{p(x)W_x > \alpha\sigma\}] \end{aligned} \quad (3.15)$$

2つ目の不等式は $\text{Tr}[\sigma \{p(x)W_x > \alpha\sigma\}] \geq 0$ による。

□

Corollary 3.3 ([27]). *Setting Q1*において、任意の *POVM* Y および任意の正数 α に対して、以下が成り立つ。

$$\text{Pe}(Y) \geq (1 - \alpha) \sum_x \text{Tr}[p(x)W_x \{p(x)W_x \leq \alpha W_p\}] \quad (3.16)$$

ここで

$$W_p := \sum_x p(x)W_x. \quad (3.17)$$

Proof. Corollary 3.2 の証明と同様に、Theorem 3.1 より以下が得られる。

$$\begin{aligned} 1 - \text{Pe}(g) - \alpha &\leq \sum_x \text{Tr} \left[(p(x)W_x - \alpha W_p)_+ \right] \\ &= \sum_x \text{Tr} \left[(p(x)W_x - \alpha W_p) \{p(x)W_x > \alpha W_p\} \right] \\ &\leq (1 - \alpha) \sum_x p(x) \text{Tr} \left[W_x \{p(x)W_x > \alpha W_p\} \right] \end{aligned} \quad (3.18)$$

2 つ目の不等式は $\text{Tr}[(W_p - p(x)W_x)\{p(x)W_x > \alpha W_p\}] \geq 0$ による。 \square

Remark 3.4. Corollary 3.2 および Corollary 3.3 はそれぞれ Setting Q1 における Hayashi-Nagaoka 不等式および Poor-Verdú 不等式の量子版である。ここでの証明は本質的に量子 Neyman-Pearson の補題を用いたと解釈できる [27]。

さらに Setting Q2 において、次の不等式が成り立つ。

Corollary 3.5 ([29]). *Setting Q2* において、任意の POVM Y 、任意の正数 α および任意の状態 $\sigma \in \mathcal{S}(\mathcal{H})$ に対して、以下が成り立つ。

$$1 - \text{Pe}(Y) - \alpha \leq \sum_x p(x) \text{Tr} \left[(W_x - M\alpha\sigma)_+ \right] \quad (3.19)$$

ここで、 $p(x) = \frac{1}{M} \sum_m f(x|m)$ である。

Proof. Theorem 3.1 より次が成り立つ。

$$\begin{aligned}
1 - \text{Pe}(Y) - \alpha &\leq \sum_m \text{Tr} \left[\left(\frac{1}{M} \sum_x f(x|m) W_x - \alpha \sigma \right)_+ \right] \\
&\leq \sum_{m,x} f(x|m) \text{Tr} \left[\left(\frac{1}{M} W_x - \alpha \sigma \right)_+ \right] \\
&= \sum_{m,x} \frac{1}{M} f(x|m) \text{Tr} [(W_x - M\alpha\sigma)_+] \\
&= \sum_x p(x) \text{Tr} [(W_x - M\alpha\sigma)_+] \tag{3.20}
\end{aligned}$$

ここで、2つ目の不等式は $\text{Tr}[(\cdot)_+]$ が凸であることから得られる。 \square

またここから直ちに次が得られる。

Corollary 3.6 ([29]). *Setting* $Q2$ において、任意の $POVM$ Y 、任意の正数 α および任意の状態 $\sigma \in \mathcal{S}(\mathcal{H})$ に対して、以下が成り立つ。

$$\text{Pe}(Y) \geq \sum_x p(x) \text{Tr} [W_x \{W_x \leq M\alpha\sigma\}] - \alpha \tag{3.21}$$

Corollary 3.5 と Corollary 3.6 はそれぞれ Corollary 2.7 と Corollary 2.8 の量子系への拡張となっている。

3.3 情報スペクトル的な信頼性関数の上界

もともと Poor-Verdú 不等式 [18] は情報スペクトル的な信頼性関数の上界を直接議論するために導かれたものであった (1.2 節参照)。本節では、量子 Poor-Verdú 不等式 (Corollary 3.3) の適用例として、古典量子通信路符号化問題における信頼性関数の上界について議論する。ここではまず、古典量子通信路符号化問題の設定を述べ、続いて情報スペクトル的な信頼性関数の定義とその上界について述べる。

$\vec{\mathcal{X}} = \{\mathcal{X}^{(n)}\}_{n=1}^{\infty}$ を有限あるいは可算無限である集合の列、 $\vec{\mathcal{H}} = \{\mathcal{H}^{(n)}\}_{n=1}^{\infty}$ をヒルベルト空間の列、 $\vec{W} = \{W^{(n)} : \mathcal{X}^{(n)} \rightarrow \mathcal{S}(\mathcal{H}^{(n)})\}_{n=1}^{\infty}$ を量子通信路の列とする。ここで、通信路 W に対して、メッセージの数を表す自然数 M 、単射な符号化関数 f 、復号を表す

POVM $Y = \{Y_i\}_{i=1}^M$ の三組を符号 Φ と呼ぶと、この符号に関して、

$$|\Phi| := M \quad (3.22)$$

と

$$\text{Pe}(\Phi) := \frac{1}{M} \sum_{i=1}^M (1 - \text{Tr}[W_{\phi(i)} Y_i]), \quad (3.23)$$

がそれぞれ定義できる。さらに、この符号は自然に通信路の列 $\vec{W} = \{W^{(n)}\}_{n=1}^{\infty}$ に対しても定義され、それを $\vec{\Phi} = \{\Phi^{(n)}\}_{n=1}^{\infty}$ で表すこととする。なお \vec{W} に対する符号列全体は $\vec{\mathcal{C}}(\vec{W})$ で表すこととする。

この時、漸近的なメッセージ増加指数（レート R ）に対する誤り確率の減衰指数である信頼性関数 $E(R)$ は、次のように定義される。

$$\begin{aligned} \forall R > 0, \\ E(R) &:= \sup\{\beta > 0 \mid \exists \vec{\Phi} \in \vec{\mathcal{C}}(\vec{W}), \\ &\quad \liminf_{n \rightarrow \infty} \frac{1}{n} \log |\Phi^{(n)}| \geq R, \\ &\quad \liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{\text{Pe}[\Phi^{(n)}]} \geq \beta\}. \end{aligned} \quad (3.24)$$

この $E(R)$ に対して、次を得る。

Theorem 3.7 ([27]).

$$E(R) \leq \sup_{\vec{P}} \inf_{\epsilon > 0} \liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{\pi(P^{(n)}, R - \epsilon)}, \quad (3.25)$$

ここで、 $\vec{P} = \{P^{(n)}\}_{n=1}^{\infty}$ 、 $P^{(n)} \in \mathcal{P}(\mathcal{X}^{(n)})$ であり、 $\pi(P^{(n)}, R)$ は

$$\pi(P^{(n)}, R) := \sum_{x^{(n)} \in \mathcal{X}^{(n)}} P^{(n)}(x^{(n)}) \text{Tr}[W_{x^{(n)}}^{(n)} \{W_{x^{(n)}}^{(n)} \leq e^{nR} W_{P^{(n)}}^{(n)}\}] \quad (3.26)$$

で定義される。この時、 $W_{P^{(n)}}^{(n)}$ は、

$$W_{P^{(n)}}^{(n)} := \sum_{x^{(n)} \in \mathcal{X}^{(n)}} P^{(n)}(x^{(n)}) W_{x^{(n)}}^{(n)}. \quad (3.27)$$

である。

Proof. $P^{(n)}$ を

$$P^{(n)}(x^{(n)}) = \begin{cases} \frac{1}{|\Phi^{(n)}|} & \text{if } \exists i, \varphi(i) = x^{(n)} \\ 0 & \text{otherwise} \end{cases} \quad (3.28)$$

とし、任意の n に対して、 $\alpha = e^{n(R-\epsilon)}/|\Phi^{(n)}|$ とする。ここで、 R は

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log |\Phi^{(n)}| \geq R \quad (3.29)$$

を満たす。これらを量子 Poor-Verdú 不等式 (Corollary 3.3) に適用することにより、

$$\text{Pe}[\Phi^{(n)}] \geq \left(1 - \frac{e^{n(R-\epsilon)}}{|\Phi^{(n)}|}\right) \pi(P^{(n)}, R - \epsilon). \quad (3.30)$$

を得る。これより、以下が成り立つ。

$$\frac{1}{n} \log \frac{1}{\text{Pe}[\Phi^{(n)}]} \leq -\frac{1}{n} \log \left(1 - \frac{e^{n(R-\epsilon)}}{|\Phi^{(n)}|}\right) + \frac{1}{n} \log \frac{1}{\pi(P^{(n)}, R - \epsilon)}. \quad (3.31)$$

この不等式の極限を考えると、(3.29) から右辺第 1 項は 0 に収束することから、

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{\text{Pe}[\Phi^{(n)}]} \leq \liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{\pi(P^{(n)}, R - \epsilon)}. \quad (3.32)$$

を得る。それゆえ、

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{\text{Pe}[\Phi^{(n)}]} \leq \sup_{\mathbf{P}} \inf_{\epsilon > 0} \liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{\pi(P^{(n)}, R - \epsilon)} \quad (3.33)$$

が成り立つ。 □

Remark 3.8. Theorem 3.7 は、[18] における信頼性関数の上界の量子系への拡張に対応する。Poor と Verdú はこの上界が真に強いと [18] 述べているが、それは Alajaji ら [3] によって、具体例を使って否定されている。

第 4 章

多重アクセス通信路

前章までは、シングルアクセス通信路を用いた状態識別問題およびそれに関連する問題を扱った。これに対し本章では、多重アクセス通信路を用いた状態識別問題および関連問題を扱う。

多重アクセス通信路は入力が複数ある通信路のことである。本章では、記述を簡単にするため節 4.7 を除いて多重アクセス通信路の問題の中で最も簡単なものである 2-user MAC(Multiple Access Channel) を扱う。これは入力が 2 つである通信路のモデルである。

本章の主要な目的は量子一般多重アクセス通信路符号化問題の一般公式に関する逆不等式を述べることである。本章ではまず、既存研究を紹介する。次に、既存研究の中でも本研究と関連の深い古典系での不等式について述べる。続いて多重アクセス通信路問題でも + 型不等式が成り立ち、その系として既存の不等式が証明されることを述べる。さらに、その不等式を量子系に拡張し、最後に目的の逆不等式を示す。

4.1 研究背景

多重アクセス通信路を用いた通信路符号化問題は、Shannon[19] 以来研究が続けられている。この問題の基本的な問題設定を簡単に述べると次のようになる。

独立した複数の送信者がそれぞれメッセージを符号化し、それを多重アクセス通信路を通して送信する。受信者は受信した信号ないし量子状態から両者のメッセージを復号す

る。ここでは古典多重アクセス通信路を用いたモデルを図示する（詳しくは、4.2 節や 4.5 節で扱う）。

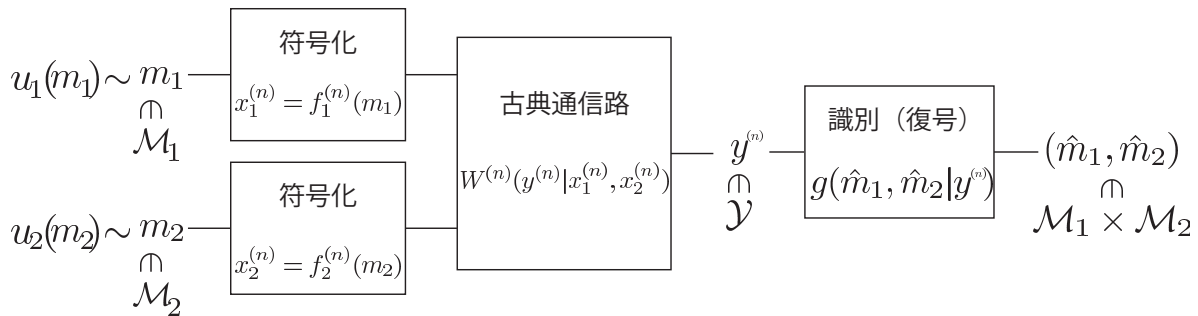


図 4.1 古典多重アクセス通信路符号化問題のモデル

多重アクセス通信路符号化問題では、各符号化レートの組に関する議論となる。つまり、通信路容量などに関わる議論がレートの領域に関する議論となる。例えば、通信路符号化定理では、シングルアクセス通信路の問題の場合、「通信路容量 C に対してそれ未満のレート R であれば、誤り確率を漸近的に 0 にする符号が存在する。」というものであったのに対して、多重アクセス通信路の問題の場合、「通信路容量域 C に対してその内部のレート (R_1, R_2) であれば、誤り確率を漸近的に 0 にする符号が存在する。」というものになる (図 4.2)。

シングルアクセス通信路の場合

多重アクセス通信路の場合

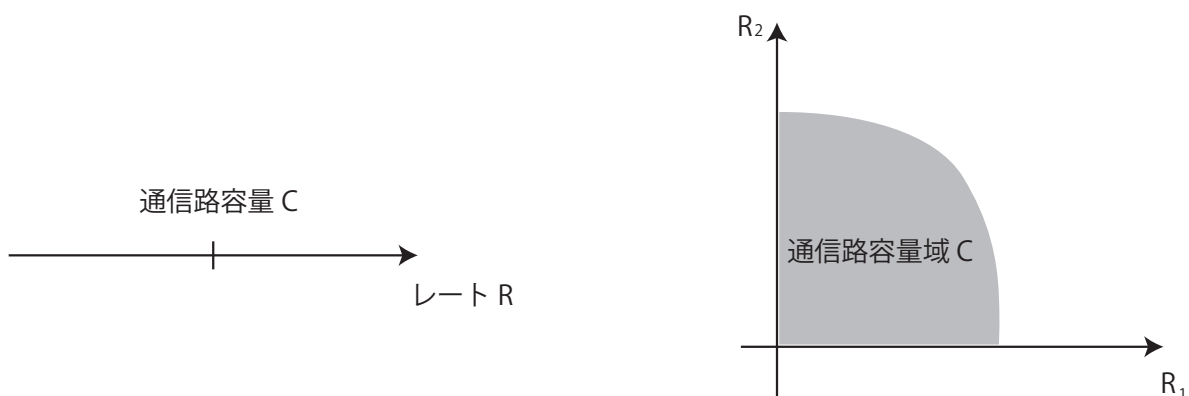


図 4.2 通信路容量域の概念図

ところで、多重アクセス通信路符号化問題は、通信路の種類によって様々な問題設定が考えられる。ここでは通信路符号化問題における既存結果を次の 4 種類に分けて述べる。

すなわち、古典定常無記憶通信路、量子定常無記憶通信路、古典一般通信路、量子一般通信路である。

古典定常無記憶多重アクセス通信路符号化問題では、Ahlsvede[1] と Liao[15] が独立に通信路容量域を求めており、強逆定理が Dueck[8] によって得られている。一方、量子定常無記憶多重アクセス通信路符号化問題では、通信路容量域が Winter[23] によって、強逆定理が Ahlsvede and Cai[2] によって得られている。また、古典一般多重アクセス通信路符号化問題では、Han[10] によって一般公式が得られている。最後に、量子一般多重アクセス通信路符号化問題については、これまで目立った成果は報告されていない。これらをまとめるのが図 4.3 である。なお、定常無記憶通信路と一般通信路とでは通信路符号化問題の諸定理として得られる形が若干異なることに注意が必要である。つまり、一般通信路における諸定理は情報スペクトル量という漸近的な量を用いて記述されるが、定常無記憶通信路における諸定理は漸近的な量ではなく極限を含まない形で記述されるということである。

	通信路符号化定理	強逆定理
古典	定常無記憶通信路 Ahlsvede (1971)	Dueck (1981)
	一般通信路 Han (1998)	Han (1998)
量子	定常無記憶通信路 Winter (2001)	Ahlsvede and Cai(2006)
	一般通信路 なし	なし

図 4.3 多重アクセス通信路符号化問題に関する関連研究図

本章では以降、量子一般多重アクセス通信路符号化問題の一般公式を目的とし考察する。

Remark 4.1. 第3章の冒頭で述べた様に、本論文では簡単のため、量子通信路という言葉省略形として用いている。本論文での量子多重アクセス通信路は正確には、入力が全て古典、出力が量子状態である（（古典古典）量子通信路:(classical-classical) - quantum channel) と呼ばれる。なお、多重アクセス通信路の場合、入力に量子状態と古典状態との両方が想定される通信路（（古典量子）量子通信路:(classical-quantum) - quantum channel) や入力も出力も量子状態である通信路（（量子量子）量子通信路:(quantum-quantum) - quantum channel) が考えられる。これら入力に量子状態を持つ多重アクセス通信路に関する定常無記憶通信路符号化定理は Yard, Hayden, and Devetak[24] が扱っている。

4.2 古典系における問題設定

本節ではシングルアクセス通信路における Setting 1 ~ 3 に対応する問題設定を述べる。

- Setting M1

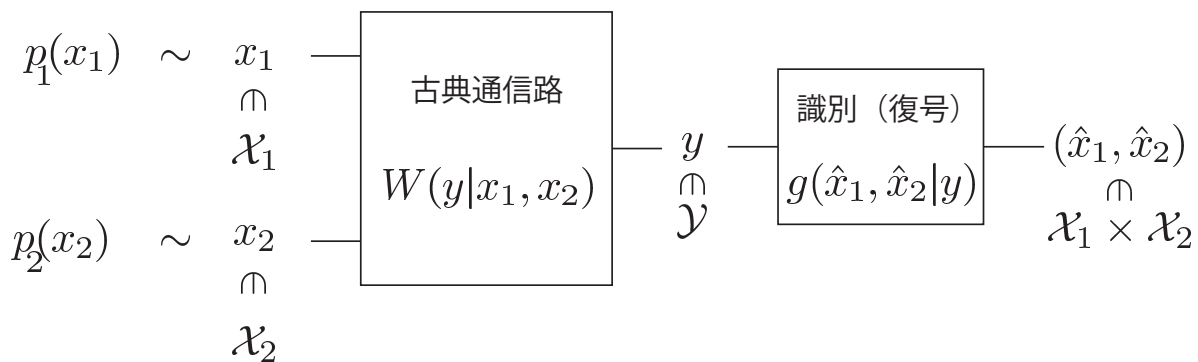


図 4.4 Setting M1

$\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}$ をそれぞれ有限ないし可算無限集合とする。 $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}$ 上の確率分布 $p(x_1, x_2, y)$ がひとつ与えられているとする。これは多重アクセス通信路 $W(y|x_1, x_2)$ と一般の入力分布 $p(x_1, x_2)$ がひとつ与えられていることに相当する。ここで、 $p(x_1, x_2) = p_1(x_1)p_2(x_2)$ となっているのが通常の多重アクセス通信路に関する問題設定である。

このとき、 x の推定を条件付き確率 $g(x_1, x_2|y)$ で表すとすると、誤り確率 Pe は、

$$\text{Pe}(g) = 1 - \sum_{x_1, x_2, y} p(x_1, x_2, y)g(x_1, x_2|y) \quad (4.1)$$

と定義される。

• Setting M2

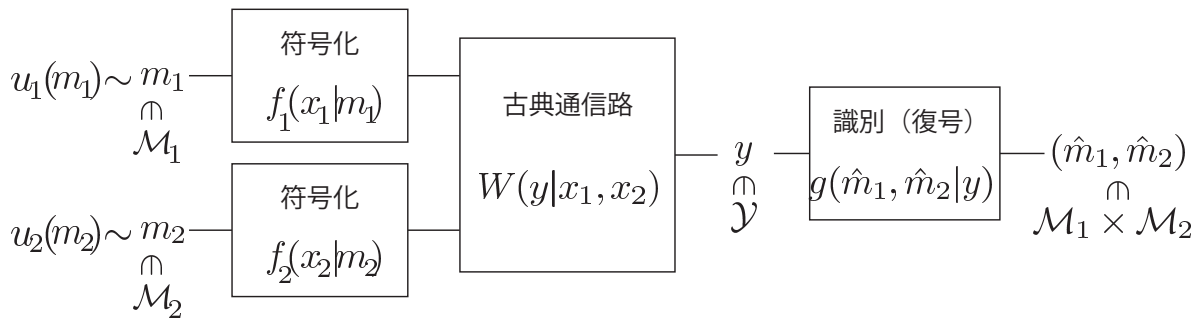


図 4.5 Setting M2

M_1, M_2 を自然数とし、メッセージ集合 $\mathcal{M}_i (i = 1, 2)$ をそれぞれ $\mathcal{M}_i := \{1, 2, \dots, M_i\}$ とする。メッセージは一様分布に従って生成されたとする。また、 $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}$ をそれぞれ有限ないし可算無限集合とする。 $\mathcal{X}_1, \mathcal{X}_2$ から \mathcal{Y} への通信路 $W(y|x_1, x_2)$ がひとつ与えられているとする。

\mathcal{M}_i から \mathcal{X}_i への符号化を確率的なものまで許すとし条件付き確率 $f_i(x_i|m_i)$ で表して、これらがひとつずつ与えられているとする。

このとき、復号を $g(m_1, m_2|y)$ で表すと誤り確率 Pe は、

$$\text{Pe}(g) = 1 - \frac{1}{M_1 M_2} \sum_{m_1, m_2, x_1, x_2, y} f_1(x_1|m_1) f_2(x_2|m_2) W(y|x_1, x_2) g(m_1, m_2|y) \quad (4.2)$$

と定義される。

• Setting M3

$\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}$ をそれぞれ有限ないし可算無限集合とする。 $\mathcal{X}_1, \mathcal{X}_2$ から \mathcal{Y} への通信路 $W(y|x_1, x_2)$ がひとつ与えられているとする。また、 $\mathcal{X}_1, \mathcal{X}_2$ 上のコードブック $\mathcal{C}_i, |\mathcal{C}_i| = M_i (i = 1, 2)$ なるものがそれぞれひとつずつ与えられているとする。この

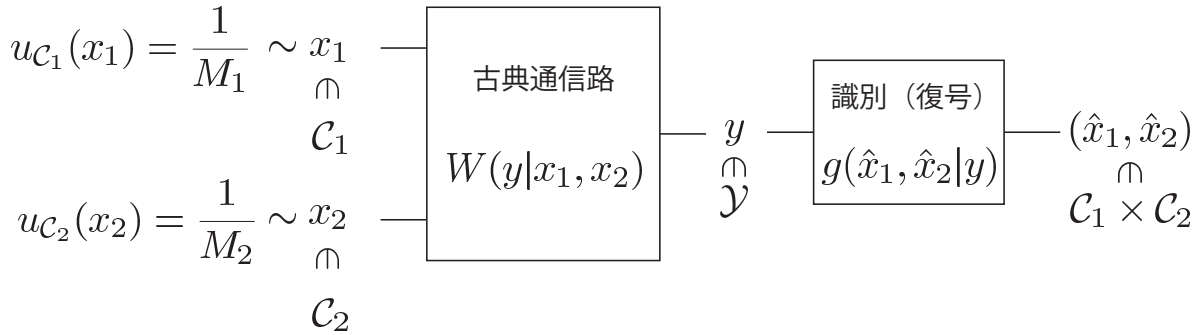


図 4.6 Setting M3

時、任意の復号を条件付き確率 $g(x_1, x_2|y)$ で表すと誤り確率 P_e は、

$$P_e(g) = 1 - \frac{1}{M_1 M_2} \sum_{x_1 \in C_1, x_2 \in C_2, y} W(y|x_1, x_2) g(x_1, x_2|y) \quad (4.3)$$

$$= 1 - \sum_{x, y} p(x_1, x_2, y) g(x_1, x_2|y) \quad (4.4)$$

と定義される。ここで、

$$p(x_1, x_2, y) = \begin{cases} \frac{1}{M_1 M_2} W(y|x_1, x_2) & \text{if } x_1 \in C_1 \text{ and } x_2 \in C_2 \\ 0 & \text{otherwise} \end{cases} \quad (4.5)$$

である。

4.3 既存不等式

本節では、本研究と関連の深い既存研究の不等式について述べる。前節でも述べたように、本論文の焦点は量子一般多重アクセス通信路符号化問題の一般公式である。ここで、Han の公式 [10](付録 C.1 参照) が古典系での対応物であるため重要である。Han の公式において、その逆不等式を得るための誤り確率の下界として Han 不等式が本質的な役割を果たしている。本節ではこの Han 不等式とそれを強めた Yagi-Oohama 不等式を示す。

前節で述べた Setting M3 に対して次が成り立つ。

- Han 不等式 [10, 11]

Setting M3 において、任意の復号 g および任意の正数 γ に対して、次が成り立つ。

$$\text{Pe}(g) \geq \sum_{x_1, x_2, y} p(x_1, x_2, y) \mathbf{1}\{L_1 \cup L_2 \cup L_3\} - 3\gamma, \quad (4.6)$$

ここで

$$L_1 := \{(x_1, x_2, y) | W(y|x_1, x_2) \leq \gamma M_1 p(y|x_2)\},$$

$$L_2 := \{(x_1, x_2, y) | W(y|x_1, x_2) \leq \gamma M_2 p(y|x_1)\},$$

$$L_3 := \{(x_1, x_2, y) | W(y|x_1, x_2) \leq \gamma M_3 p(y)\},$$

$$M_3 := M_1 M_2.$$

であり、 $p(y|x_1)$ などは (4.5) の $p(x_1, x_2, y)$ から定義される。

- Yagi-Oohama 不等式 [30]

Setting M3 において、任意の復号 g 、任意の正数 γ' 、 $\{1, 2, 3\}$ 上の任意の確率分布 π および \mathcal{Y} 上の任意の条件付き確率分布および確率分布 $q_1(y|x_2)$, $q_2(y|x_1)$, $q_3(y)$ に対して、次が成り立つ。

$$\text{Pe}(g) \geq \sum_{x_1, x_2, y} p(x_1, x_2, y) \mathbf{1}\{W(y|x_1, x_2) \leq \gamma' \bar{q}(y|x_1, x_2)\} - \gamma' \sum_i \frac{\pi_i}{M_i}, \quad (4.7)$$

ここで、

$$\bar{q}(y|x_1, x_2) := \pi_1 q_1(y|x_2) + \pi_2 q_2(y|x_1) + \pi_3 q_3(y)$$

である。

Remark 4.2. Yagi-Oohama 不等式において

$$\pi_i = \frac{M_i}{\sum_j M_j} \quad (4.8)$$

とおき、

$$\gamma' = \gamma \sum_j M_j \quad (4.9)$$

とおくと、

$$\text{Pe}(g) \geq \sum_{x_1, x_2, y} p(x_1, x_2, y) \mathbf{1}\{\tilde{L}\} - 3\gamma \quad (4.10)$$

を得る。ただし、

$$\tilde{L} := \{(x_1, x_2, y) | W(y|x_1, x_2) \leq \gamma(M_1 q_1(y|x_2) + M_2 q_2(y|x_1) + M_3 q_3(y))\},$$

ここで、 $\tilde{L} \supset L_i$, $i = 1, 2, 3$ より、Yagi-Oohama 不等式は Han 不等式よりも強いことがわかる。

Han 不等式および Yagi-Oohama 不等式の元論文に忠実な証明は付録 C.2 に記載する。

4.4 古典系における + 型不等式とその応用

シングルアクセス通信路の場合の時と同様に + 型不等式を用いた証明を介して Yagi-Oohama 不等式を量子系に拡張することを考える。以下に述べるように、多重アクセス通信路でも Yagi-Oohama 不等式型であれば、+ 型不等式が成り立つ。

Theorem 4.3 ([14]). *Setting M1* において、任意の正数 $\alpha_1, \alpha_2, \alpha_3$ および任意の分布 $q(y), q_1(x_2, y), q_2(x_1, y)$ に対して、 $q(y) \geq q_1(x_2, y), q(y) \geq q_2(x_1, y)$ を満たすとき、

$$1 - \text{Pe}(g) - \sum_i \alpha_i \leq \sum_{x_1, x_2, y} (p(x_1, x_2, y) - \alpha_1 q_1(x_2, y) - \alpha_2 q_2(x_1, y) - \alpha_3 q(y))_+ \quad (4.11)$$

が成り立つ。

Proof. Theorem 2.1 の証明と同様に、(2.1) より

$$\begin{aligned}
& \sum_{x_1, x_2, y} (p(x_1, x_2, y) - \alpha_1 q_1(x_2, y) - \alpha_2 q_2(x_1, y) - \alpha_3 q(y))_+ \\
& \geq \sum_{x_1, x_2, y} (p(x_1, x_2, y) - \alpha_1 q_1(x_2, y) - \alpha_2 q_2(x_1, y) - \alpha_3 q(y)) g(x_1, x_2 | y) \\
& \geq \sum_{x_1, x_2, y} (p(x_1, x_2, y) - \sum_i \alpha_i q(y)) g(x_1, x_2 | y) \\
& = 1 - \text{Pe}(g) - \sum_i \alpha_i \tag{4.12}
\end{aligned}$$

が成り立つ。 \square

ここからシングルアクセス通信路の場合と同様にして直ちに次が成り立つ。

Corollary 4.4 ([14]). *Setting M1* において、任意の正数 $\alpha_1, \alpha_2, \alpha_3$ および任意の分布 $q(y), q_1(x_2, y), q_2(x_1, y)$ に対して、 $q(y) \geq q_1(x_2, y), q(y) \geq q_2(x_1, y)$ を満たすとき、

$$\text{Pe}(g) \geq \sum_{x_1, x_2, y} p(x_1, x_2, y) \mathbf{1}\{p(x_1, x_2, y) \leq \alpha_1 q_1(x_2, y) + \alpha_2 q_2(x_1, y) + \alpha_3 q(y)\} - \sum_i \alpha_i \tag{4.13}$$

が成り立つ。

Corollary 4.5 ([14]). *Setting M1* において、任意の正数 $\alpha_1, \alpha_2, \alpha_3$ に対して、

$$\text{Pe}(g) \geq (1 - \sum_i \alpha_i) \sum_{x_1, x_2, y} p(x_1, x_2, y) \mathbf{1}\{p(x_1, x_2, y) \leq \alpha_1 p(x_2, y) + \alpha_2 p(x_1, y) + \alpha_3 p(y)\} \tag{4.14}$$

が成り立つ。ここで、 $p(x_1, y)$ や $p(x_2, y)$ 、 $p(y)$ は $p(x_1, x_2, y)$ を周辺化して得られる。

Remark 4.6. Corollary 4.4 は *Setting M1* における Yagi-Oohama 不等式である。実際、Corollary 4.4 を *Setting M3* において $\alpha_i = \gamma' \frac{\pi_i}{M_i}$, $i = 1, 2, 3$ とおけば、(4.7) が得られる。一方、Corollary 4.5 は多重アクセス通信路における Yagi-Oohama 型の Poor-Verdú 不等式である。

さらに *Setting M2* において、これもシングルアクセス通信路の時と同様の証明により次が成り立つ。

Corollary 4.7 ([14]). *Setting M2*において、任意の正数 $\gamma_1, \gamma_2, \gamma_3$ および任意の分布 $q(y), q_1(y|x_2), q_2(y|x_1)$ に対して、 $q(y) \geq \frac{1}{M_2} q_1(y|x_2), q(y) \geq \frac{1}{M_1} q_2(y|x_1)$ を満たすとき、

$$\begin{aligned} 1 - \text{Pe}(g) &= \sum_i \frac{\gamma_i}{M_i} \\ &\leq \frac{1}{M_1 M_2} \sum_{m_1, m_2, x_1, x_2, y} f_1(x_1|m_1) f_2(x_2|m_2) \\ &\quad \cdot (W(y|x_1, x_2) - \gamma_1 q_1(y|x_2) - \gamma_2 q_2(y|x_1) - \gamma_3 q(y))_+ \end{aligned} \quad (4.15)$$

が成り立つ。

ここから、次が成り立つ。

Corollary 4.8 ([14]). *Setting M2*において、任意の正数 $\gamma_1, \gamma_2, \gamma_3$ および任意の分布 $q(y), q_1(y|x_2), q_2(y|x_1)$ に対して、 $q(y) \geq \frac{1}{M_2} q_1(y|x_2), q(y) \geq \frac{1}{M_1} q_2(y|x_1)$ を満たすとき、

$$\begin{aligned} \text{Pe}(g) &\geq \frac{1}{M_1 M_2} \sum_{m_1, m_2, x_1, x_2, y} f_1(x_1|m_1) f_2(x_2|m_2) \\ &\quad \cdot W(y|x_1, x_2) \mathbf{1}\{W(y|x_1, x_2) \leq \gamma_1 q_1(y|x_2) + \gamma_2 q_2(y|x_1) + \gamma_3 q(y)\} \\ &\quad - \sum_i \frac{\gamma_i}{M_i} \end{aligned} \quad (4.16)$$

が成り立つ。

これは *Setting M2* における Yagi-Oohama 不等式である。

4.5 量子系における問題設定

以降では、量子多重アクセス通信路における誤り確率の下界について論じる。まず 2-user MAC の問題設定を拡張したものを述べ、次に、量子系における + 型不等式について論じる。これは、Yagi-Oohama 不等式の量子版を導くことなどを見る。続いて、2-user でなく一般の通信路に限らず一般の多重アクセス通信路における + 型不等式を述べる。最後に通信路符号化問題への応用として ε -通信路容量域や強逆領域に関する逆不等式について論じる。

本節では問題設定を述べる。

• Setting QM1

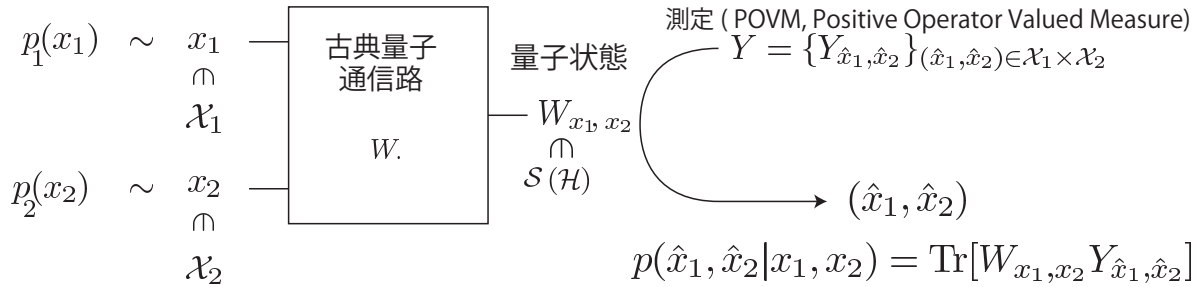


図 4.7 Setting QM1

$\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}$ をそれぞれ有限ないし可算無限集合とする。 $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}$ 上の確率分布 $p(x_1, x_2)$ がひとつ与えられているとする。また、 \mathcal{H} を任意のヒルベルト空間とし、 $S(\mathcal{H})$ で \mathcal{H} 上の状態集合を表す。ここで量子多重アクセス通信路 $W : \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow S(\mathcal{H})$ がひとつ与えられているとする。

このとき、 x_1, x_2 の推定を POVM $Y = \{Y_{x_1 x_2}\}$ で表すとすると、誤り確率 Pe は、

$$\text{Pe}(Y) = 1 - \sum_{x_1, x_2} p(x_1, x_2) \text{Tr}[W_{x_1 x_2} Y_{x_1 x_2}] \quad (4.17)$$

と定義される。

• Setting QM2

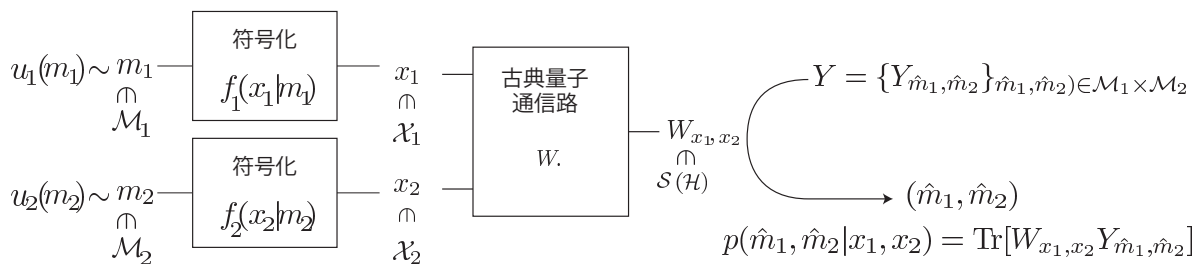


図 4.8 Setting QM2

M_1, M_2 を自然数とし、メッセージ集合 $\mathcal{M}_i (i = 1, 2)$ をそれぞれ $\mathcal{M}_i := \{1, 2, \dots, M_i\}$ とする。メッセージは一様分布に従って生成されるとする。また、 $\mathcal{X}_1, \mathcal{X}_2$ をそれぞれ有限ないし可算無限集合とする。また、 \mathcal{H} を任意のヒルベルト空間とし、 $S(\mathcal{H})$ で \mathcal{H} 上の状態集合を表す。ここで量子多重アクセス通信路

$W : \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{S}(\mathcal{H})$ がひとつ与えられているとする。 \mathcal{M}_i から \mathcal{X}_i への符号化を確率的なものまで許すとし条件付き確率 $f_i(x_i|m_i)$ で表して、これらがひとつずつ与えられているとする。

このとき、復号を POVM $Y = \{Y_{m_1 m_2}\}$ で表すとすると、誤り確率 Pe は、

$$\text{Pe}(Y) = 1 - \frac{1}{M_1 M_2} \sum_{m_1, m_2, x_1, x_2} f_1(x_1|m_1) f_2(x_2|m_2) \text{Tr}[W_{x_1, x_2} Y_{m_1, m_2}] \quad (4.18)$$

と定義される。

4.6 量子系における + 型不等式とその応用

本節では、量子多重アクセス通信路における + 型不等式を与える。これはシングルアクセス通信路と同様の方法で証明される。

Theorem 4.9 ([14]). *Setting QM1* に対して、任意の POVM Y 、任意の正数 $\alpha_1, \alpha_2, \alpha_3$ 、 \mathcal{H} 上の任意の状態 σ と任意の半正定値作用素 $\sigma_{x_1}, \sigma_{x_2}$ に対して、 $\sigma \geq \sigma_{x_1}$ と $\sigma \geq \sigma_{x_2}$ を満たすとき、次が成り立つ。

$$1 - \text{Pe}(Y) - \sum_i \alpha_i \leq \sum_{x_1, x_2} \text{Tr}[(p(x_1, x_2) W_{x_1, x_2} - \sigma_{\alpha, x_1, x_2})_+], \quad (4.19)$$

ここで、

$$\sigma_{\alpha, x_1, x_2} = \alpha_1 \sigma_{x_2} + \alpha_2 \sigma_{x_1} + \alpha_3 \sigma \quad (4.20)$$

である。

Proof. 任意のエルミート作用素 A と $0 \leq T \leq I$ を満たす任意の半正定値作用素 T に対して、 $\text{Tr}[A_+] \geq \text{Tr}[AT]$ であるという事実から、任意の POVM $Y = \{Y_x\}_x$ に対して次

が成り立つ。

$$\begin{aligned}
\sum_{x_1, x_2} \text{Tr}[(p(x_1, x_2)W_{x_1, x_2} - \sigma_{\alpha, x_1, x_2})_+] &\geq \sum_{x_1, x_2} \text{Tr}[(p(x_1, x_2)W_{x_1, x_2} - \sigma_{\alpha, x_1, x_2})Y_{x_1, x_2}] \\
&= 1 - \text{Pe}(Y) - \sum_{x_1, x_2} \text{Tr}[\sigma_{\alpha, x_1, x_2} Y_{x_1, x_2}] \\
&\geq 1 - \text{Pe}(Y) - \sum_{x_1, x_2} \text{Tr}[\sum_i \alpha_i \sigma Y_{x_1, x_2}] \\
&= 1 - \text{Pe}(Y) - \sum_i \alpha_i \tag{4.21}
\end{aligned}$$

ここで2つ目の不等式は、 $\sigma \geq \sigma_{x_1}$ と $\sigma \geq \sigma_{x_2}$ による。 \square

ここで、直ちに Setting QM1 における Yagi-Oohama 不等式の量子版などが得られる。

Corollary 4.10 ([14]). *Setting QM1* に対して、任意の POVM Y 、任意の正数 $\alpha_1, \alpha_2, \alpha_3$ 、 \mathcal{H} 上の任意の状態 σ と 任意の半正定値作用素 $\sigma_{x_1}, \sigma_{x_2}$ に対して、 $\sigma \geq \sigma_{x_1}$ と $\sigma \geq \sigma_{x_2}$ を満たすとき、次が成り立つ。

$$\text{Pe}(Y) \geq \sum_{x_1, x_2} p(x_1, x_2) \text{Tr}[W_{x_1, x_2} \{p(x_1, x_2)W_{x_1, x_2} \leq \sigma_{\alpha, x_1, x_2}\}] - \sum_i \alpha_i \tag{4.22}$$

Corollary 4.11 ([14]). *Setting QM1* に対して、任意の POVM Y 、任意の正数 $\alpha_1, \alpha_2, \alpha_3$ に対して次が成り立つ。

$$\text{Pe}(Y) \geq (1 - \sum_i \alpha_i) \sum_{x_1, x_2} p(x_1, x_2) \text{Tr}[W_{x_1, x_2} \{p(x_1, x_2)W_{x_1, x_2} \leq W_{\alpha, x_1, x_2}\}] \tag{4.23}$$

ここで、

$$W_{\alpha, x_1, x_2} = \alpha_1 W_{p_1, x_2} + \alpha_2 W_{x_1, p_2} + \alpha_3 W_{p_1, p_2} \tag{4.24}$$

$$W_{p_1, x_2} = \sum_{x_1} p(x_1, x_2) W_{x_1, x_2} \tag{4.25}$$

$$W_{x_1, p_2} = \sum_{x_2} p(x_1, x_2) W_{x_1, x_2} \tag{4.26}$$

$$W_{p_1, p_2} = \sum_{x_1, x_2} p(x_1, x_2) W_{x_1, x_2} \tag{4.27}$$

である。

さらに、シングルアクセス通信路の場合と同様に $\text{Tr}[A_+]$ が凸であるという事実から

Setting QM2 において以下が成り立つ。

Corollary 4.12 ([14]). Setting QM2 に対して、任意の POVM Y 、任意の正数 $\gamma_1, \gamma_2, \gamma_3$ 、 \mathcal{H} 上の任意の状態 σ と 任意の半正定値作用素 $\sigma_{x_1}, \sigma_{x_2}$ に対して、

$$\sigma \geq \sigma_{m_1} = \frac{1}{M_1} \sum_{x_1} f(x_1|m_1) \sigma_{x_1}, \quad (4.28)$$

$$\sigma \geq \sigma_{m_2} = \frac{1}{M_2} \sum_{x_2} f(x_2|m_2) \sigma_{x_2}, \quad (4.29)$$

を満たすとき、次が成り立つ。

$$1 - \text{Pe}(Y) - \sum_i \frac{\gamma_i}{M_i} \leq \frac{1}{M_1 M_2} \sum_{m_1, m_2, x_1, x_2} f_1(x_1|m_1) f_2(x_2|m_2) \text{Tr}[(W_{x_1, x_2} - \sigma'_{\gamma, x_1, x_2})_+], \quad (4.30)$$

ここで、

$$\sigma'_{\gamma, x_1, x_2} = \gamma_1 \sigma_{x_2} + \gamma_2 \sigma_{x_1} + \gamma_3 \sigma \quad (4.31)$$

$$M_3 = M_1 M_2 \quad (4.32)$$

である。

Proof. Theorem 4.9 より、任意の正数 $\alpha_1, \alpha_2, \alpha_3$ に対して次が成り立つ。

$$1 - \text{Pe}(Y) - \sum_i \alpha_i \leq \sum_{m_1, m_2} \text{Tr}[(p(m_1, m_2) W_{m_1, m_2} - \sigma_{\alpha, m_1, m_2})_+] \quad (4.33)$$

ここで、

$$p(m_1, m_2) = \frac{1}{M_1 M_2} \quad (4.34)$$

$$W_{m_1, m_2} = \sum_{x_1, x_2} f_1(x_1|m_1) f_2(x_2|m_2) W_{x_1, x_2} \quad (4.35)$$

$$\begin{aligned} \sigma_{\alpha, m_1, m_2} &= \sum_{x_1, x_2} f_1(x_1|m_1) f_2(x_2|m_2) \sigma'_{\alpha, x_1, x_2} \\ &= \alpha_1 \sigma_{m_2} + \alpha_2 \sigma_{m_1} + \alpha_3 \sigma \end{aligned} \quad (4.36)$$

$$\sigma'_{\alpha, x_1, x_2} = \frac{\alpha_1}{M_2} \sigma_{x_2} + \frac{\alpha_2}{M_1} \sigma_{x_1} + \alpha_3 \sigma \quad (4.37)$$

である。それゆえ、 $Tr[A_+]$ の凸性から、

$$1 - \text{Pe}(Y) - \sum_i \alpha_i \leq \sum_{m_1, m_2} \sum_{x_1, x_2} f_1(x_1|m_1) f_2(x_2|m_2) \text{Tr}[(p(m_1, m_2)W_{x_1, x_2} - \sigma'_{\alpha, x_1, x_2})_+] \quad (4.38)$$

が成り立つ。ここで、 $M_i \alpha_i = \gamma_i$ とおけば、

$$\begin{aligned} \sigma'_{\alpha, x_1, x_2} &= \frac{1}{M_1 M_2} \sigma'_{\gamma, x_1, x_2} \\ &= p(m_1, m_2) \sigma'_{\gamma, x_1, x_2} \end{aligned} \quad (4.39)$$

であることから、

$$1 - \text{Pe}(Y) - \sum_i \frac{\gamma_i}{M_i} \leq \sum_{m_1, m_2} \sum_{x_1, x_2} p(m_1, m_2) f_1(x_1|m_1) f_2(x_2|m_2) \text{Tr}[(W_{x_1, x_2} - \sigma'_{\gamma, x_1, x_2})_+] \quad (4.40)$$

が成り立つ。 □

ここから Setting QM2 における Yagi-Oohama 不等式の量子版が得られる。

Corollary 4.13 ([14]). *Setting QM2* に対して、任意の POVM Y 、任意の正数 $\gamma_1, \gamma_2, \gamma_3$ 、 \mathcal{H} 上の任意の状態 σ と 任意の半正定値作用素 $\sigma_{x_1}, \sigma_{x_2}$ に対して、

$$\sigma \geq \frac{1}{M_1} \sum_{x_1} f(x_1|m_1) \sigma_{x_1}, \quad (4.41)$$

$$\sigma \geq \frac{1}{M_2} \sum_{x_2} f(x_2|m_2) \sigma_{x_2}, \quad (4.42)$$

を満たすとき、次が成り立つ。

$$\text{Pe}(Y) \geq \frac{1}{M_1 M_2} \sum_{m_1, m_2, x_1, x_2} f_1(x_1|m_1) f_2(x_2|m_2) \text{Tr}[W_{x_1, x_2} \{W_{x_1, x_2} - \sigma'_{\gamma, x_1, x_2}\}] - \sum_i \frac{\gamma_i}{M_i} \quad (4.43)$$

4.7 N-user MAC に関する + 型不等式

本節では、2-user に限らない一般の N-user MAC に関する + 型不等式について論じる。本節の内容は、論文などに未発表である。

- Setting QM1(N users)

$\mathcal{X}_1, \mathcal{X}_2, \dots, \mathcal{X}_N, \mathcal{Y}$ をそれぞれ有限ないし可算無限集合とする。 $\mathcal{X}_1, \mathcal{X}_2, \dots, \mathcal{X}_N$ 上の確率分布 $p(x_1, x_2, \dots, x_N)$ がひとつ与えられているとする。また、 \mathcal{H} を任意のヒルベルト空間とし、 $\mathcal{S}(\mathcal{H})$ で \mathcal{H} 上の状態集合を表す。ここで量子多端子通信路 $W : \mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_N \rightarrow \mathcal{S}(\mathcal{H})$ がひとつ与えられているとする。

このとき、 x_1, x_2, \dots, x_N の推定を POVM $Y = \{Y_{x_1, x_2, \dots, x_N}\}$ で表すとすると、誤り確率 Pe は、

$$\text{Pe}(Y) = 1 - \sum_{x_1, x_2, \dots, x_N} p(x_1, x_2, \dots, x_N) \text{Tr}[W_{x_1, x_2, \dots, x_N} Y_{x_1, x_2, \dots, x_N}] \quad (4.44)$$

と定義される。

上記の設定のもと、次の不等式が成り立つ。

Theorem 4.14. 任意の POVM Y 、任意の正の実数 $\{\alpha_s\}_{s \in [N]^+}$ および、半正定値作用素 $\{\sigma_s\}_{s \in [N]^-}$ に対して、 $\text{Tr}[\sigma_\emptyset] = 1$ と $\sigma_\emptyset \geq \sigma_s, s \in [N]^-$ が成り立つならば、次が成り立つ。

$$1 - \text{Pe}(Y) - \sum_{s \in [N]^+} \alpha_s \leq \sum_{x_1, \dots, x_N} \text{Tr}[(p(x_1, \dots, x_N) W_{x_1, \dots, x_N} - \sum_{s \in [N]^-} \alpha_s \sigma_s)_+]$$

ここで、

$$[N]^- := \{s \subset \{1, \dots, N\} \mid s \neq \{1, \dots, N\}\}$$

$$[N]^+ := \{s \subset \{1, \dots, N\} \mid s \neq \emptyset\}$$

$$\sigma_s := \sigma_{x_{s_1}, x_{s_2}, \dots, x_{s_l}} \quad \text{if } s = \{s_1, \dots, s_l\} \in [N]^-$$

および、 s^c は s の補集合を表す。

Proof. 任意の $0 \leq T \leq T$ を満たすエルミート作用素 T および、任意のエルミート作用素 A に対して、 $\text{Tr}[AT] \leq \text{Tr}[A_+]$ が成り立つことより、次が成り立つ。

$$\begin{aligned}
& \sum_{x_1, \dots, x_N} \text{Tr}[(p(x_1, \dots, x_N)W_{x_1, \dots, x_N} - \sum_{s \in [N]^-} \alpha_{s^c} \sigma_s)_+] \\
& \geq \sum_{x_1, \dots, x_N} \text{Tr}[(p(x_1, \dots, x_N)W_{x_1, \dots, x_N} - \sum_{s \in [N]^-} \alpha_{s^c} \sigma_s)Y_{x_1, \dots, x_N}] \\
& = 1 - \text{Pe}(Y) - \sum_{x_1, \dots, x_N} \text{Tr}[\sum_{s \in [N]^-} \alpha_{s^c} \sigma_s Y_{x_1, \dots, x_N}] \\
& \geq 1 - \text{Pe}(Y) - \sum_{x_1, \dots, x_N} \text{Tr}[\sum_{s \in [N]^-} \alpha_{s^c} \sigma_\emptyset Y_{x_1, \dots, x_N}] \\
& = 1 - \text{Pe}(Y) - \sum_{s \in [N]^+} \alpha_s \tag{4.45}
\end{aligned}$$

ここで、2つの目の不等式は $\sigma_\emptyset \geq \sigma_s$ による。 \square

この不等式は、本論文でこれまでに示した全ての+型不等式の中で一番数学的に一般的な形であり、他の+型不等式はその特別な場合とみなせる。

4.8 通信路符号化問題の逆不等式

本節では、量子系における多重アクセス通信路+型不等式の適用例である古典量子多重アクセス通信路符号化問題について議論する。特にここでは、 ε -通信路容量域や強逆領域の逆不等式について論じる。これは、[10], [11] で導出された ε -通信路容量域や強逆領域の逆不等式の量子版に相当する。

本節はまず、量子多重アクセス通信路符号化問題の設定を述べる。ここでは、符号化は確率的なものまで許すとする。

$\vec{M}_1 = \{M_1^{(n)}\}_{n=1}^\infty$ と $\vec{M}_2 = \{M_2^{(n)}\}_{n=1}^\infty$ をそれぞれ自然数の列とし、 $\vec{\mathcal{M}}_1 = \{\mathcal{M}_1^{(n)}\}_{n=1}^\infty$ と $\vec{\mathcal{M}}_2 = \{\mathcal{M}_2^{(n)}\}_{n=1}^\infty$ をそれぞれ $\mathcal{M}_1^{(n)}$ と $\mathcal{M}_2^{(n)}$ の要素数が $M_1^{(n)}$ と $M_2^{(n)}$ である集合の列であるとする。 $\vec{\mathcal{X}}_1 = \{\mathcal{X}_1^{(n)}\}_{n=1}^\infty$ と $\vec{\mathcal{X}}_2 = \{\mathcal{X}_2^{(n)}\}_{n=1}^\infty$ をそれぞれ有限ないし可算集合の列とし、 $\vec{\mathcal{H}} = \{\mathcal{H}^{(n)}\}_{n=1}^\infty$ をヒルベルト空間の列とする。

量子多重アクセス通信路の列 $\vec{W} = \{W^{(n)} : \mathcal{X}_1^{(n)} \times \mathcal{X}_2^{(n)} \rightarrow \mathcal{S}(\mathcal{H}^{(n)})\}_{n=1}^\infty$ がひとつ与えられているとする。

それぞれの $W^{(n)}$ に対して、符号化と復号はそれぞれ条件付き確率 $f_1(x_1^{(n)} | m_1^{(n)})$,

$f_2(x_2^{(n)}|m_2^{(n)})$ と POVM $Y^{(n)} = \{Y_{m_1^{(n)}, m_2^{(n)}}^{(n)}\}$ で表されるとすると、誤り確率は各 n に対して、次のように定義される。

$$\text{Pe}^{(n)}(Y^{(n)}) := 1 - \sum_{m_1^{(n)}, m_2^{(n)}, x_1^{(n)}, x_2^{(n)}} \frac{1}{M_1^{(n)} M_2^{(n)}} f_1(x_1^{(n)}|m_1^{(n)}) f_2(x_2^{(n)}|m_2^{(n)}) \cdot \text{Tr}[W_{x_1^{(n)}, x_2^{(n)}}^{(n)} Y_{m_1^{(n)}, m_2^{(n)}}^{(n)}]. \quad (4.46)$$

ここで、符号化と復号の組 $(f_1^{(n)}, f_2^{(n)}, Y^{(n)})$ で誤り確率が ε_n であるものを $(n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n)$ -符号と呼ぶ。

これらの設定が与えられた下で、 \vec{W} に対する ε -通信路容量域 $C(\varepsilon|\vec{W})$ は次のように定義される。

Definition 4.15.

$$\begin{aligned} C(\varepsilon|\vec{W}) := \{ & (R_1, R_2) | \exists (n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n) - \text{符号 } s.t. \\ & \limsup_{n \rightarrow \infty} \varepsilon_n \leq \varepsilon, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_1^{(n)} \geq R_1, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_2^{(n)} \geq R_2. \} \end{aligned} \quad (4.47)$$

また、強逆領域 $C^*(\vec{W})$ は次のように定義される。

Definition 4.16.

$$\begin{aligned} C^*(\vec{W}) := \{ & (R_1, R_2) | \exists (n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n) - \text{符号 } s.t. \\ & \liminf_{n \rightarrow \infty} \varepsilon_n < 1, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_1^{(n)} \geq R_1, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_2^{(n)} \geq R_2. \} \end{aligned} \quad (4.48)$$

ここで、[10] や [11] における J と J^* に相当する関数 K と K^* を定義する。

Definition 4.17.

$$\begin{aligned}
& K(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) \\
& := \limsup_{n \rightarrow \infty} \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) \text{Tr}[W_{x_1^{(n)}, x_2^{(n)}}^{(n)} \\
& \cdot \{W_{x_1^{(n)}, x_2^{(n)}}^{(n)} \leq e^{nR_1} \sigma_{x_2^{(n)}}^{(n)} + e^{nR_2} \sigma_{x_1^{(n)}}^{(n)} + e^{n(R_1+R_2)} \sigma^{(n)}\}], \tag{4.49}
\end{aligned}$$

$$\begin{aligned}
& K^*(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) \\
& := \liminf_{n \rightarrow \infty} \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) \text{Tr}[W_{x_1^{(n)}, x_2^{(n)}}^{(n)} \\
& \cdot \{W_{x_1^{(n)}, x_2^{(n)}}^{(n)} \leq e^{nR_1} \sigma_{x_2^{(n)}}^{(n)} + e^{nR_2} \sigma_{x_1^{(n)}}^{(n)} + e^{n(R_1+R_2)} \sigma^{(n)}\}]. \tag{4.50}
\end{aligned}$$

ここで、 \vec{p}_1 と \vec{p}_2 は \mathcal{X}_1 と \mathcal{X}_2 上の確率分布の列であり、 $\vec{\sigma}$ はそれぞれの n で

$$\sigma^{(n)} = \sum_{x_1^{(n)}} p_1^{(n)}(x_1^{(n)}) \sigma_{x_1^{(n)}}^{(n)} \tag{4.51}$$

および

$$\sigma^{(n)} = \sum_{x_2^{(n)}} p_2^{(n)}(x_2^{(n)}) \sigma_{x_2^{(n)}}^{(n)} \tag{4.52}$$

を満たす状態の組 $(\sigma^{(n)}, \sigma_{x_1^{(n)}}^{(n)}, \sigma_{x_2^{(n)}}^{(n)})$ の列である。

これらに対して、次が成り立つ。

Theorem 4.18 ([14]).

$$C(\varepsilon | \vec{W}) \subset \bigcup_{\vec{p}_1, \vec{p}_2} \bigcap_{\vec{\sigma}} \text{Cl}(\{(R_1, R_2) | K(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) \leq \varepsilon\}), \tag{4.53}$$

ここで、 $\text{Cl}(\cdot)$ は集合の閉包を表す。

Proof. $(R_1, R_2) \in C(\varepsilon | \vec{W})$ とすると、 $C(\varepsilon | \vec{W})$ の定義より任意の正数 γ と十分大きな n に対して、

$$M_1^{(n)} \geq e^{n(R_1 - \gamma)}, \tag{4.54}$$

$$M_2^{(n)} \geq e^{n(R_2 - \gamma)}, \tag{4.55}$$

および

$$\limsup_{n \rightarrow \infty} \varepsilon_n \leq \varepsilon. \quad (4.56)$$

を満たす $(n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n)$ -符号の列が存在する。この符号を用いて、入力分布の列を

$$p_1^{(n)}(x_1^{(n)}) = \frac{1}{M_1^{(n)}} \sum_{m_1^{(n)}} f_1^{(n)}(x_1^{(n)} | m_1^{(n)}), \quad (4.57)$$

$$p_2^{(n)}(x_2^{(n)}) = \frac{1}{M_2^{(n)}} \sum_{m_2^{(n)}} f_2^{(n)}(x_2^{(n)} | m_2^{(n)}). \quad (4.58)$$

とする。ここで、Corollary 4.12 より、(4.51) と (4.51) を満たす任意の σ に対して、

$$1 - \varepsilon_n - 3e^{-n\gamma} \leq \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) \cdot \text{Tr} \left[\left(W_{x_1^{(n)}, x_2^{(n)}}^{(n)} - e^{-n\gamma} \left(M_1^{(n)} \sigma_{x_2^{(n)}}^{(n)} + M_2^{(n)} \sigma_{x_1^{(n)}}^{(n)} + M_1^{(n)} M_2^{(n)} \sigma^{(n)} \right) \right)_+ \right]. \quad (4.59)$$

が成り立つ。(4.54), (4.55) および任意のエルミート作用素 A, B に対して、 $A \leq B$ ならば $\text{Tr}[A_+] \leq \text{Tr}[B_+]$ が成り立つという事実から

$$1 - \varepsilon_n - 3e^{-n\gamma} \leq \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) \cdot \text{Tr} \left[\left(W_{x_1^{(n)}, x_2^{(n)}}^{(n)} - \left(e^{n(R_1-2\gamma)} \sigma_{x_2^{(n)}}^{(n)} + e^{n(R_2-2\gamma)} \sigma_{x_1^{(n)}}^{(n)} + e^{n(R_1+R_2-3\gamma)} \sigma^{(n)} \right) \right)_+ \right] \\ \leq \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) \cdot \text{Tr} \left[\left(W_{x_1^{(n)}, x_2^{(n)}}^{(n)} - \left(e^{n(R_1-2\gamma)} \sigma_{x_2^{(n)}}^{(n)} + e^{n(R_2-2\gamma)} \sigma_{x_1^{(n)}}^{(n)} + e^{n(R_1+R_2-4\gamma)} \sigma^{(n)} \right) \right)_+ \right]. \quad (4.60)$$

をえる。それゆえ、

$$\varepsilon_n \geq \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) \text{Tr} \left[W_{x_1^{(n)}, x_2^{(n)}}^{(n)} \right. \\ \left. \cdot \left\{ W_{x_1^{(n)}, x_2^{(n)}}^{(n)} \leq e^{n(R_1-2\gamma)} \sigma_{x_2^{(n)}}^{(n)} + e^{n(R_2-2\gamma)} \sigma_{x_1^{(n)}}^{(n)} + e^{n(R_1+R_2-4\gamma)} \sigma^{(n)} \right\} \right] \\ - 3e^{-n\gamma}. \quad (4.61)$$

が成り立つ。さらに、(4.56) と (4.61) から、

$$K(R_1 - 2\gamma, R_2 - 2\gamma | \vec{p}_1, \vec{p}_2, \vec{\sigma}) \leq \limsup_{n \rightarrow \infty} \varepsilon_n \leq \varepsilon. \quad (4.62)$$

である。ここで、 γ が任意であったことから、(4.62) から

$$(R_1, R_2) \in \text{Cl}(\{(R_1, R_2) | K(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) \leq \varepsilon\}). \quad (4.63)$$

をえる。 □

さらに、強逆領域 $C^*(\vec{W})$ に対して、次が成り立つ。

Theorem 4.19 ([14]).

$$C^*(\vec{W}) \subset \bigcup_{\vec{p}_1, \vec{p}_2} \bigcap_{\vec{\sigma}} \text{Cl}(\{(R_1, R_2) | K^*(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) < 1\}). \quad (4.64)$$

Proof. $(\cdot)^c$ を補集合を表すものとし、 $\mathcal{R}(\vec{p}_1, \vec{p}_2, \vec{\sigma}) = \text{Cl}(\{(R_1, R_2) | K^*(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) < 1\})$ とする。

もし (R_1, R_2) が (4.64) の右辺の補集合に属しているとする、任意の \vec{p}_1, \vec{p}_2 に対して、ある $\vec{\sigma}$ が存在して、 $(R_1, R_2) \in \mathcal{R}(\vec{p}_1, \vec{p}_2, \vec{\sigma})^c$ である。このとき、十分小さな正数 γ に対して、 $(R_1 - 2\gamma, R_2 - 2\gamma) \in \mathcal{R}(\vec{p}_1, \vec{p}_2, \vec{\sigma})^c$ が成り立つ。 $\mathcal{R}(\vec{p}_1, \vec{p}_2, \vec{\sigma})^c$ は開集合なので、

$$K^*(R_1 - 2\gamma, R_2 - 2\gamma | \vec{p}_1, \vec{p}_2, \vec{\sigma}) = 1. \quad (4.65)$$

が成り立つ。一方、十分大きな n と (4.65) で使われている γ に対して (4.54) および (4.55) を満たす全ての $(n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n)$ -符号に対して、(4.57) および (4.58) で定められた入力分布の列は明らかに独立である。さらに、そのような符号は (4.61) を満たす。

それゆえ、(4.61) と (4.65) とを併せて、

$$\lim_{n \rightarrow \infty} \varepsilon_n = 1. \quad (4.66)$$

を得る。これは、 $(R_1 - \gamma, R_2 - \gamma) \in C^*(\vec{W})^c$ を意味する。任意の正数 $S_1 < S'_1$ および $S_2 < S'_2$ に対して、もし $(S_1, S_2) \in C^*(\vec{W})^c$ ならば $(S'_1, S'_2) \in C^*(\vec{W})^c$ が成り立つことより、 $(R_1, R_2) \in C^*(\vec{W})^c$ が成り立つ。 □

Remark 4.20. 上記 Theorem 4.18, 4.19 の証明には量子系における Yagi-Oohama 不等式でなく、Yagi-Oohama 型の + 型不等式が必要であった。特に、(4.59),(4.60) において不等式評価する際に量子 Yagi-Oohama 不等式を直接適用することでは評価できない。

この問題は古典系においては生じない。これは、古典系においては、 $p_1 < \alpha q_1 \Rightarrow p_2 < \alpha q_2$ ならば指示関数の大小関係 $\mathbf{1}\{p_1 < \alpha q_1\} > \mathbf{1}\{p_2 < \alpha q_2\}$ が言え、これを評価に用いているからである。一方、量子系では $\rho_1 < \alpha \sigma_1 \Rightarrow \rho_2 < \alpha \sigma_2$ から射影子の大小関係 $\{\rho_1 < \alpha \sigma_1\} > \{\rho_2 < \alpha \sigma_2\}$ が一般には言えない。これが、+ 型不等式が必要であった理由である。

Remark 4.21. 古典系における Han の一般公式と Theorem 4.18, 4.19 との関係は以下のとおりである。

まず $\vec{W}_p = \{(W_{p_1^{(n)} p_2^{(n)}}^{(n)}, W_{x_1^{(n)} p_2^{(n)}}^{(n)}, W_{p_1^{(n)} x_2^{(n)}}^{(n)})\}$ を以下の関係を満たす様に定義する。

$$W_{p_1^{(n)} p_2^{(n)}}^{(n)} := \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) W_{x_1^{(n)} x_2^{(n)}}^{(n)}, \quad (4.67)$$

$$W_{x_1^{(n)} p_2^{(n)}}^{(n)} := \sum_{x_2^{(n)}} p_2^{(n)}(x_2^{(n)}) W_{x_1^{(n)} x_2^{(n)}}^{(n)}, \quad (4.68)$$

$$W_{p_1^{(n)} x_2^{(n)}}^{(n)} := \sum_{x_1^{(n)}} p_1^{(n)}(x_1^{(n)}) W_{x_1^{(n)} x_2^{(n)}}^{(n)}. \quad (4.69)$$

すると Theorems 4.18 , 4.19 より

$$C(\varepsilon|\vec{W}) \subset \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | K(R_1, R_2|\vec{p}_1, \vec{p}_2, \vec{W}_p) \leq \varepsilon\}) \quad (4.70)$$

および

$$C^*(\vec{W}) \subset \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | K^*(R_1, R_2|\vec{p}_1, \vec{p}_2, \vec{W}_p) < 1\}). \quad (4.71)$$

を得る。古典系において、Yagi-Oohama 不等式が Han 不等式よりも強いこと (4.3 節参照) を考えると、

$$K(R_1, R_2|\vec{p}_1, \vec{p}_2, \vec{W}_p) \geq J(R_1, R_2|\mathbf{X}_1, \mathbf{X}_2) \quad (4.72)$$

および

$$K^*(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{W}_p) \geq J^*(R_1, R_2 | \mathbf{X}_1, \mathbf{X}_2) \quad (4.73)$$

を直ちに得る。ここで、 J および J^* は [10] [11] で定義される量である（付録 C.1 参照）。それゆえ、

$$\{(R_1, R_2) | K \leq \varepsilon\} \subset \{(R_1, R_2) | J \leq \varepsilon\}, \quad (4.74)$$

$$\{(R_1, R_2) | K^* < 1\} \subset \{(R_1, R_2) | J^* < 1\}. \quad (4.75)$$

が成り立つ。ここで注意すべきは、[10] [11] においては、その順部分も証明されているということである。それゆえ、古典系においては次が成り立つ。

$$C(\varepsilon | \vec{W}) = \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | J \leq \varepsilon\}), \quad (4.76)$$

$$C^*(\vec{W}) = \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | J^* < 1\}), \quad (4.77)$$

その結果、古典系においては

$$\bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | K \leq \varepsilon\}) = \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | J \leq \varepsilon\}) \quad (4.78)$$

$$\bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | K^* < 1\}) = \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | J^* < 1\}) \quad (4.79)$$

が成り立つ。

Remark 4.22. Theorem 4.18, 4.19 から量子一般多重アクセス通信路の一般公式が次の形で成り立つことが予想される。

$$C(\varepsilon | \vec{W}) = \bigcup_{\vec{p}_1, \vec{p}_2} \bigcap_{\vec{\sigma}} \text{Cl}(\{(R_1, R_2) | K(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) \leq \varepsilon\}), \quad (4.80)$$

$$C^*(\vec{W}) = \bigcup_{\vec{p}_1, \vec{p}_2} \bigcap_{\vec{\sigma}} \text{Cl}(\{(R_1, R_2) | K^*(R_1, R_2 | \vec{p}_1, \vec{p}_2, \vec{\sigma}) < 1\}). \quad (4.81)$$

これを証明するには順部分が必要である。その証明には誤り確率の良い上界が必要であるが、今のところそのような上界は得られていない。

第 5 章

一般化 Poor-Verdú 不等式の拡張

本章では、一般化 Poor-Verdú 不等式について議論する。この不等式は古典系における誤り確率の下界であり、本研究と関連の深い不等式であるが、今のところ + 型不等式からの証明ができておらず、量子系への拡張も不明である。以降では、この一般化 Poor-Verdú 不等式の一般化を拡張し、数値計算を通して量子一般化 Poor-Verdú 不等式が成立しないことを示す。

5.1 一般化 Poor-Verdú 不等式の証明

古典状態識別問題 (Setting 1) において、一般化 Poor-Verdú 不等式と呼ばれる次の不等式が成り立つ。

- 一般化 Poor-Verdú 不等式 [5]

Setting 1 において、任意の識別 g と任意の正数 α および実数 $\theta \geq 1$ に対して、

$$\text{Pe}(g) \geq (1 - \alpha) \Pr\{V^{(\theta)}(X|Y) \leq \alpha\} \quad (5.1)$$

が成り立つ。ここで、

$$V^{(\theta)}(x|y) = \frac{(p(x)W(y|x))^\theta}{\sum_{x'} (p(x')W(y|x'))^\theta} \quad (5.2)$$

である。

一般化 Poor-Verdú 不等式は $\theta = 1$ の時、Poor-Verdú 不等式と等しくなる。また、 $\theta \rightarrow \infty$ のとき MAP 識別による誤り確率の評価に漸近することが知られている。

以下にこの不等式の証明を述べる。証明には以下の補題が必要である。

Lemma 5.1. 任意の y と任意の $\theta \geq 1$ に対して、

$$\max_x p(x|y) \leq \max_x p^{(\theta)}(x|y). \quad (5.3)$$

が成り立つ。ここで、

$$p^{(\theta)}(x|y) := \frac{p^\theta(x|y)}{\sum_x' p^\theta(x'|y)} \quad (5.4)$$

$$= \frac{p^\theta(x, y)}{\sum_x' p^\theta(x', y)} \quad (5.5)$$

Proof[5]. $\theta \geq 1$ かつ $\xi \leq 1$ のとき、 $\xi \geq \xi^\theta$ なので、任意の y と任意の $\theta \geq 1$ に対して、

$$\arg \max_x p(x|y) = \arg \max_x p^{(\theta)}(x|y). \quad (5.6)$$

であることに注意すると任意の x, y で、

$$\frac{p(x|y)}{\max_{x'} p(x'|y)} \geq \left(\frac{p(x|y)}{\max_{x'} p(x'|y)} \right)^\theta \quad (5.7)$$

$$= \frac{p^\theta(x|y)}{\max_{x'} p^\theta(x'|y)}. \quad (5.8)$$

が成り立つ。ここで x に関して和をとることで、

$$\sum_x \frac{p(x|y)}{\max_{x'} p(x'|y)} \geq \sum_x \frac{p^\theta(x|y)}{\max_{x'} p^\theta(x'|y)} \quad (5.9)$$

$$\Leftrightarrow \frac{1}{\max_{x'} p(x'|y)} \geq \frac{1}{\max_{x'} p^{(\theta)}(x'|y)} \quad (5.10)$$

$$\Leftrightarrow \max_{x'} p(x'|y) \leq \max_{x'} p^{(\theta)}(x'|y). \quad (5.11)$$

□

この補題を用いることで一般化 Poor-Verdú 不等式は次のように証明される。

一般化 Poor-Verdú 不等式の証明. 第 2 章で示した Poor-Verdú 不等式の証明の (A.8) と

Lemma 5.1 より

$$\begin{aligned}
\max_x V(x|y) &\leq \alpha + (1 - \alpha) \max_x V(x|y) \mathbf{1}\{\max_x V(x|y) > \alpha\} \\
&\leq \alpha + (1 - \alpha) \max_x V(x|y) \mathbf{1}\{\max_x V^{(\theta)}(x|y) > \alpha\} \\
&\leq \alpha + (1 - \alpha) \sum_x V(x|y) \mathbf{1}\{V^{(\theta)}(x|y) > \alpha\}
\end{aligned} \tag{5.12}$$

これより目的の不等式を得る。 \square

5.2 関数型一般化 Poor-Verdú 不等式

次の関数のクラスを考える。

$$\mathcal{F} = \{f : [0, 1] \rightarrow [0, \infty) \mid \forall a, b \in [0, 1], f(ab) \leq af(b)\}, \tag{5.13}$$

この関数のクラスを用いて、一般化 Poor-Verdú 不等式は次のように拡張される。

Theorem 5.2 ([28]).

$$\begin{aligned}
&\forall \hat{p}, \forall \alpha \in [0, 1], \forall f \in \mathcal{F}, \\
\text{Pe}(\hat{p}) &\geq (1 - \alpha) \sum_{x,y} p(x, y) \mathbf{1}\{p^{(f)}(x|y) \leq \alpha\},
\end{aligned} \tag{5.14}$$

ここで、

$$p^{(f)}(x|y) := \frac{f(p(x|y))}{\sum_{x'} f(p(x'|y))}. \tag{5.15}$$

で定義される関数である。

ここで、 f を $f : \xi \mapsto \xi^\theta$ とすれば、一般化 Poor-Verdú 不等式となる。

Remark 5.3. 上で述べたように、 f は次の条件を満たす。

$$f : [0, 1] \rightarrow [0, \infty) \tag{5.16}$$

$$\forall a, b \in [0, 1], \quad f(ab) \leq af(b). \tag{5.17}$$

2番目の条件は、 $f(t)/t$ が単調増加することと同値であり、これらの条件から f は $f(0) = 0$ を満たす単調増加関数であることがわかる。付け加えると、 $f(0) = 0$ を満たす非負な凸関数は、これらの条件を満たす。

証明にあたって以下の Lemma が必要である。

Lemma 5.4.

$$\begin{aligned} \forall y, \forall f \in \mathcal{F}, \\ \arg \max_x p(x|y) = \arg \max_x p^{(f)}(x|y). \end{aligned} \quad (5.18)$$

Proof. f の満たすべき (5.16)(5.17) の条件より

$$\begin{aligned} \arg \max_x p(x|y) &= \arg \max_x f(p(x|y)) \\ &= \arg \max_x p^{(f)}(x|y). \end{aligned} \quad (5.19)$$

である。 □

Lemma 5.5.

$$\begin{aligned} \forall y, \forall f \in \mathcal{F}, \\ \max_x p(x|y) \leq \max_x p^{(f)}(x|y). \end{aligned} \quad (5.20)$$

Proof.

$$a = \frac{p(x|y)}{\max_{x'} p(x'|y)}, \quad (5.21)$$

$$b = \max_{x'} p(x'|y) \quad (5.22)$$

を $f(ab) \leq af(b)$ に代入すると任意の x, y において、

$$\begin{aligned} \frac{p(x|y)}{\max_{x'} p(x'|y)} &\geq \frac{f(p(x|y))}{f(\max_{x'} p(x'|y))} \\ &= \frac{f(p(x|y))}{\max_{x'} f(p(x'|y))} \end{aligned} \quad (5.23)$$

を得る。ここで、等号は Lemma による。(5.23) の両辺で和をとれば、目的の不等式を得る。 □

関数型一般化 Poor-Verdú 不等式の証明は、これらの Lemma を用いて、前節の一般化 Poor-Verdú 不等式と同様に行われる。

5.3 量子系への拡張

一般化 Poor-Verdú 不等式や関数型 Poor-Verdú 不等式は + 型不等式からの導出ができておらず、量子系で成立するかどうかわからない。本節では、一般化 Poor-Verdú 不等式が量子系で成り立つか否かを数値計算を用いて検証する。

一般化 Poor-Verdú 不等式の量子系への拡張として、次の不等式が考えられる。

$$\forall Y, \forall \alpha \in [0, 1], \forall \theta \geq 1, \\ \text{Pe}[Y] \geq (1 - \alpha) \sum_x p(x) \text{Tr}[W_x \{p^\theta(x) W_x^\theta \leq \alpha W_p^{(\theta)}\}], \quad (5.24)$$

ここで、

$$W_p^{(\theta)} := \sum_x p^\theta(x) W_x^\theta \quad (5.25)$$

である。

ここで、この不等式に対する反例が構成できる [13] ことを以下に示す。反例を構成するために、 $\mathcal{X} = \{0, 1\}$ 、 $\mathcal{H} = \mathbb{C}^2$ としたとき、つまり二次元二状態識別問題で数値計算を行った。二状態識別問題であれば誤り確率の最小値は

$$\min_Y \text{Pe}[Y] = p(0) - \text{Tr}[\tilde{W} \{\tilde{W} > 0\}] \quad (5.26)$$

と求められる。ここで、

$$\tilde{W} := p(0)W_0 - p(1)W_1 \quad (5.27)$$

である。図 5.1 は、 $p(0) = 0.3$ 、 $p(1) = 0.7$ 、

$$W_0 = \begin{bmatrix} 0.95 & 0 \\ 0 & 0.05 \end{bmatrix}, \quad W_1 = \frac{1}{2} \begin{bmatrix} 1 & -0.8 \\ -0.8 & 1 \end{bmatrix}$$

として計算を行ったものある。横軸は α の値、縦軸は (5.24) の右辺の計算値と (5.26) の計算値であり、確率量である。

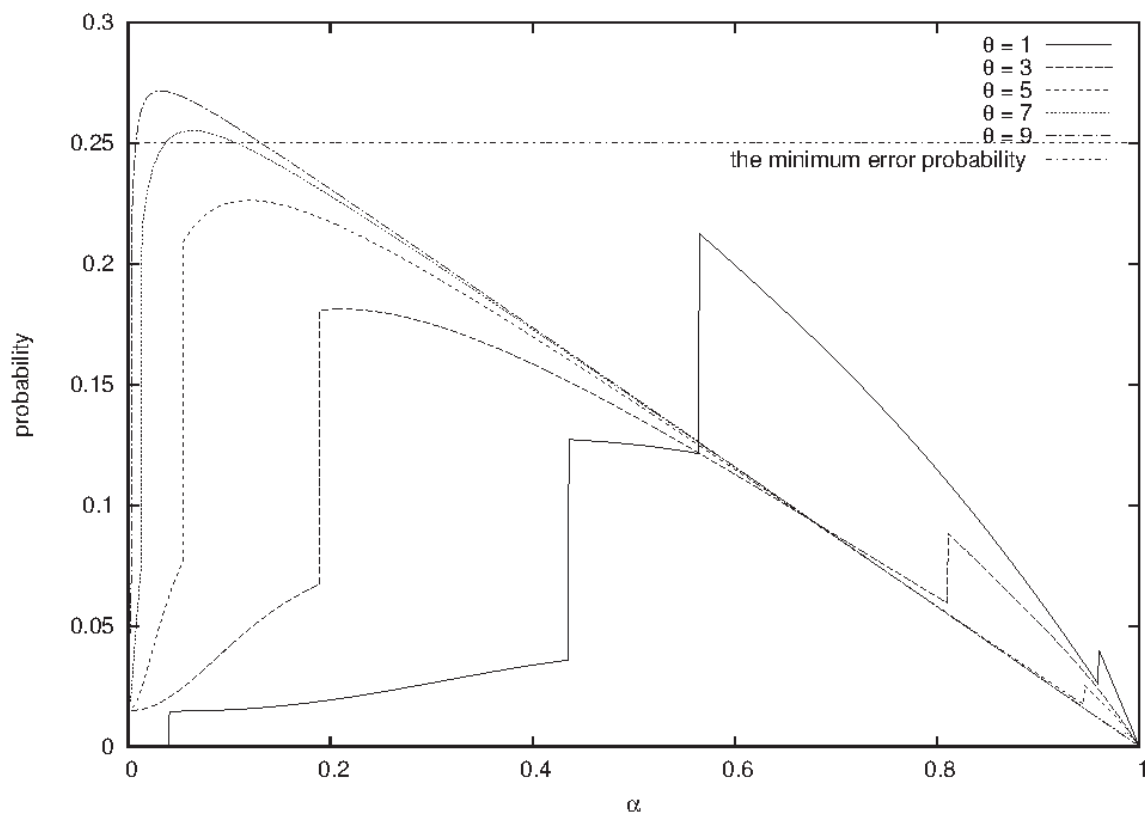


図 5.1 量子一般化 Poor-Verdú 不等式の反例

ここで、 $\theta = 7, 9$ のとき $\alpha = 0.1$ 付近で (5.24) の右辺の計算値が (5.26) の計算値を超えていることがわかる。これは明らかに反例である。

量子系で一般に成立しないことから、一般化 Poor-Verdú 不等式は + 型不等式からの証明がないことが示唆される。

第 6 章

結論

6.1 本論文のまとめ

本論文では、古典/量子、シングルアクセス/多重アクセスの各通信路に対して、Setting 1 ~ 3 といった状態識別問題やそれに類似する問題設定を考え、それら問題設定での誤り確率の下界について議論し、その通信路符号化問題への応用についても考察した。本論文を通して得られた成果および知見は以下のとおりである。

まず、シングルアクセス/多重アクセス、古典系/量子系に関わらず + 型不等式が成立することを見た。また、それらの + 型不等式をもちいて、各種不等式が導かれることを示した (2.1 節、3.2 節、4.4 節、4.6 節)。ここで、Remark 2.9 では古典シングルアクセス通信路に関する問題において、Setting 1 における誤り確率の下界をそのまま Setting 2 に適用することは通信路符号化問題への適用を考慮すると望ましくないということを述べた。一方で、この問題は + 型不等式の段階で適用すれば、回避されることも 2.1 節で見た。この事情は、シングルアクセス/多重アクセス、古典系/量子系に関わらない。

次に Poor-Verdú 不等式の量子シングルアクセス通信路符号化問題へ応用として、信頼性関数の新しい上界を導いた (3.3 節)。

さらに、量子多重アクセス通信路に関する + 型不等式を評価することによって、量子多重アクセス通信路において新たな誤り確率の下界を得た (4.6 節、4.7 節)。またその応用として、 ε -通信路容量域および強逆領域の逆不等式を得た (4.8 節)。なお、ここで得られた逆不等式は確率的な符号化に対してのものであり、従来の単射的な符号化のみのものよ

りも適用範囲が広いものであった。

最後に、一般化 Poor-Verdú 不等式の2つの方向への拡張を検討した。1つは一般化のさらなる拡張である。これに関しては、一般化 Poor-Verdú 不等式の関数型を発見した(5.2節)。いま1つは量子系への拡張である。一般化 Poor-Verdú 不等式が量子系で成り立つか否かの検証を数値的に行い、否定的な結論を得た(5.3節)。

6.2 今後の課題

本研究の今後の課題として主に次の2つのことが挙げられる。

1つは、一般化 Poor-Verdú 不等式の量子系への拡張についてである。5.3節で一般化 Poor-Verdú 不等式は量子系へ拡張することができないことを数値計算によって検証したが、とくに $1 \leq \theta \leq 2$ において(5.24)が破れるという例は今のところ発見できていない。 θ がこの範囲にあるときにおいて、一般化 Poor-Verdú 不等式を量子系へ拡張することができるか否かを明らかにすべきである。

いま1つは、量子多重アクセス通信路符号化問題についてである。4.8節で通信路容量域に関する逆不等式を導いたが、この不等式が十分に強く通信路符号化定理を導くか否かはまだわからない。これを明らかにするためには通信路容量域に関する順不等式、ないし誤り確率に関するよい上界が必要である。

付録 A

古典シングルアクセス通信路における既存不等式

A.1 既存不等式の証明

本節では、本論文の焦点である情報スペクトル的な手法に関連の深い不等式の出典論文に忠実な証明を紹介する。なお、証明中の数式の表記法は本論文の表記法に合わせている。

- Verdú-Han 不等式

Setting 3 において、任意の復号 g と任意の正数 α に対して、

$$P_e(g) \geq \Pr\{p(X, Y) \leq \alpha p(Y)\} - \alpha \quad (\text{A.1})$$

が成り立つ。

Proof[22]. 任意の正数 α に対して次が成り立つ。

$$\begin{aligned}
& \sum_{x,y} p(x,y) \mathbf{1}\{p(x,y) \leq \alpha p(y)\} \\
&= \sum_{x,y} p(x,y) \mathbf{1}\{p(x,y) \leq \alpha p(y)\} g(x|y) \\
&\quad + \sum_{x,y} p(x,y) \mathbf{1}\{p(x,y) \leq \alpha p(y)\} (1 - g(x|y)) \\
&\leq \sum_{x,y} p(x,y) \mathbf{1}\{p(x,y) \leq \alpha p(y)\} g(x|y) + \sum_{x,y} p(x,y) (1 - g(x|y)) \\
&\leq \sum_{x,y} \alpha p(y) \mathbf{1}\{p(x,y) \leq \alpha p(y)\} g(x|y) + \sum_{x,y} p(x,y) (1 - g(x|y)) \\
&\leq \sum_{x,y} \alpha p(y) g(x|y) + \sum_{x,y} p(x,y) (1 - g(x|y)) \\
&= \alpha + \text{Pe}(g)
\end{aligned} \tag{A.2}$$

ここで、1つ目と3つ目の不等式は

$$\mathbf{1}\{p(x,y) \leq \alpha p(y)\} \leq 1 \tag{A.3}$$

により、2つ目の不等式は

$$p(x,y) \mathbf{1}\{p(x,y) \leq \alpha p(y)\} \leq \alpha p(y) \mathbf{1}\{p(x,y) \leq \alpha p(y)\} \tag{A.4}$$

による。 □

- Poor-Verdu 不等式

Setting 1 において、任意の識別 g と任意の正数 α に対して、

$$\text{Pe}(g) \geq (1 - \alpha) \Pr\{V(X|Y) \leq \alpha\} \tag{A.5}$$

が成り立つ。ただし、 $V(x|y)$ は逆向き通信路であり、

$$p(x)W(y|x) = V(x|y) \sum_{x'} p(x')W(y|x') \tag{A.6}$$

で定義される。

Proof[18]. \mathcal{Y} 上の分布 $W_p(y)$ を

$$W_p(y) = \sum_x p(x)W(y|x) \quad (\text{A.7})$$

で定義する。任意の復号 g および任意の正数 α に対して、以下が成り立つ。

$$\begin{aligned} \text{Pe}(g) &= 1 - \sum_{x,y} p(x)W(y|x)g(x|y) \\ &\geq 1 - \sum_y W_p(y) \max_x V(x|y) \\ &\geq 1 - \sum_y W_p(y) \left(\alpha + (1 - \alpha) \sum_x V(x|y) \mathbf{1}\{V(x|y) > \alpha\} \right) \\ &= (1 - \alpha) \sum_{x,y} p(x)W(y|x) \mathbf{1}\{V(x|y) \leq \alpha\} \end{aligned} \quad (\text{A.8})$$

ここで、1つ目の不等式は、MAP(Maximum A Posteriori) 復号により、2つ目の不等式は、

$$\begin{aligned} \max_x V(x|y) &\leq \alpha + (1 - \alpha) \max_x V(x|y) \mathbf{1}\{\max_x V(x|y) > \alpha\} \\ &\leq \alpha + (1 - \alpha) \sum_x V(x|y) \mathbf{1}\{V(x|y) > \alpha\} \end{aligned} \quad (\text{A.9})$$

という事実による。 □

Remark A.1. これ以外にも、Hayashi-Nagaoka 不等式も情報スペクトル的な手法と関連が深い。この不等式は Neyman-Pearson の補題に基づいた証明が [12] でされており、この証明法は本論文の考え方により近い。

Remark A.2. ここでは2つの不等式の論文に忠実な証明を述べたが、これらが同様の手法による証明であるとは言いがたい。もちろん、Han-Verdú 不等式よりも Poor-Verdú 不等式のほうが強い不等式であるので、後者の証明が統一的な証明であると言うことは可能である。しかしながら、本論文の主題の一つである量子系への拡張を考えると、この証明法をそのまま拡張することは難しい。例えば、(A.2) を Setting Q1 に拡張しようとすると、1つ目の不等式が一般には成り立たない。即ち、

$$\sum_x p(x) \text{Tr} [W_x \{p(x)W_x \leq \alpha\sigma\} (I - Y_x)] \leq \sum_x p(x) \text{Tr} [W_x (I - Y_x)]$$

は左辺が一般には実数でないため、成立しない。

一方、MAP 識別による誤り確率の評価は、Yuen[25] による表現が存在するものの、それを適用する手段は未だ見つかっていない。また、(A.9) を直接量子系に拡張するためには逆向き通信路 $V(y|x)$ を量子系で表現する必要があるが、これはほとんど不可能である。

付録 B

Polyanskiy の meta converse および converse

ここでは、誤り確率の下界であり、本研究と同様に仮説検定を証明の基礎とする Polyanskiy の meta converse および converse についてその証明を紹介する。また、これらの不等式が量子系へ拡張される事も述べる。

B.1 既存不等式の証明

- Polyanskiy's meta converse

Setting 2 において、任意の復号 g と任意の通信路 $\hat{W}(y|x)$ に対して、

$$1 - \text{Pe}'(g) \geq \beta_{1-\text{Pe}(g)}(p(X)W(Y|X), p(X)\hat{W}(Y|X)) \quad (\text{B.1})$$

が成り立つ。ここで、 β は関数 h を $h : \mathcal{X} \times \mathcal{Y} \rightarrow [0, 1]$ とし、 $p(x, y), q(x, y)$ を $\mathcal{X} \times \mathcal{Y}$ 上の確率分布としたとき、

$$\beta_\alpha(p(X, Y), q(X, Y)) = \min_{h: \sum_{x,y} p(x,y)h(x,y) \geq \alpha} \sum_{x,y} q(x,y)h(x,y) \quad (\text{B.2})$$

で定義され、 $\text{Pe}'(g)$ は

$$\text{Pe}'(g) = 1 - \frac{1}{M} \sum_{m,x,y} f(x|m)\hat{W}(y|x)g(m|y) \quad (\text{B.3})$$

で定義される。また、 $p(x)$ は $p(x) = \frac{1}{M} \sum_m f(x|m)$ である。

この不等式は正確には Setting 2 を拡張した設定で証明される。即ち、Setting 2 において、メッセージ集合上の分布は一様に限らず、一般の確率分布 $p(m)$ でよいとする。この時、 Pe および Pe' は

$$\text{Pe}(g) = 1 - \sum_{m,x,y} p(m)f(x|m)W(y|x)g(m|y) \quad (\text{B.4})$$

$$\text{Pe}'(g) = 1 - \sum_{m,x,y} p(m)f(x|m)\hat{W}(y|x)g(m|y) \quad (\text{B.5})$$

と定義される。これらを用いて Polyanskiy の meta converse は以下の様に証明される。

Proof.[16]. 条件付き確率 $f'(m|x)$ を

$$p(m)f(x|m) = f'(m|x)p(x) \quad (\text{B.6})$$

を満たすように定義する。ここで、

$$p(x) = \sum_m p(m)f(x|m) \quad (\text{B.7})$$

である。この $f'(m|x)$ を用いて $h(x, y)$ を

$$h(x, y) = \sum_m f'(m|x)g(m|y) \quad (\text{B.8})$$

で定義すると、

$$1 - \text{Pe}(g) = \sum_{x,y} p(x)W(y|x)h(x, y) \quad (\text{B.9})$$

$$1 - \text{Pe}'(g) = \sum_{x,y} p(x)\hat{W}(y|x)h(x, y) \quad (\text{B.10})$$

である。ここで β の定義を思い出すと、(B.1) が得られる。□

この meta converse を Setting 3 に適用すると、次が得られる。

- Polyanskiy's converse

Setting 3 において、任意の復号 g に対して、

$$M \leq \sup_p \inf_q \beta_{1-\text{Pe}(g)}(p(X)W(Y|X), p(X)q(Y))^{-1} \quad (\text{B.11})$$

が成り立つ。

Proof.[16]. Setting 3 において $\hat{W}(y|x) = q(y)$ とすると、

$$\begin{aligned} 1 - \text{Pe}'(g) &= \frac{1}{M} \sum_{x \in \mathcal{C}, y} q(y)g(x|y) \\ &\leq \frac{1}{M} \end{aligned} \quad (\text{B.12})$$

である。これと meta convexe とを併せると (B.11) が成り立つ。 \square

B.2 量子系への拡張

前節で紹介した不等式は量子系へ拡張できる。この際、用いる論法は古典系におけるそれと完全に対応している。

Theorem B.1 (quantum version of Polyanskiy's meta convexe). *Setting Q2* において、メッセージ集合上の分布は一様に限らず、一般の確率分布 $p(m)$ でよいとする。この設定において、任意の $POVM Y = \{Y_m\}$ と任意の量子通信路 σ_x に対して、

$$1 - \text{Pe}'(Y) \geq \beta_{1-\text{Pe}(Y)}(p(X)W_X, p(X)\sigma_X) \quad (\text{B.13})$$

が成り立つ。ここで、 β は T_x を $0 \leq T_x \leq I$ を満たすエルミート作用素としたとき、

$$\beta_\alpha(p(X)\rho_X, q(X)\sigma_X) = \min_{T=\{T_x\}_{x: \sum_x p(x)\text{Tr}[\rho_x T_x] \geq \alpha}} \sum_x q(x)\text{Tr}[\sigma_x T_x] \quad (\text{B.14})$$

で定義され、 $\text{Pe}(Y)$ 、 $\text{Pe}'(Y)$ は

$$\text{Pe}(Y) = 1 - \sum_{m,x} p(m)f(x|m)\text{Tr}[W_x Y_m] \quad (\text{B.15})$$

$$\text{Pe}'(Y) = 1 - \sum_{m,x} p(m)f(x|m)\text{Tr}[\sigma_x Y_m] \quad (\text{B.16})$$

で定義される。また、 $p(x)$ は $p(x) = \sum_m p(m)f(x|m)$ である。

Proof. 条件付き確率 $f'(m|x)$ を (B.6) で定義し、エルミート作用素 T_x を

$$T_x = \sum_m f'(m|x)Y_m \quad (\text{B.17})$$

で定義する。この時、明らかに $0 \leq T_x \leq I$ である。この T_x を用いると

$$1 - \text{Pe}(Y) = \sum_x p(x)\text{Tr}[W_x T_x] \quad (\text{B.18})$$

$$1 - \text{Pe}'(Y) = \sum_x p(x)\text{Tr}[\sigma_x T_x] \quad (\text{B.19})$$

である。ここで β の定義を思い出すと、(B.13) が得られる。□

古典系の場合と同様に、Setting Q3 において $\sigma_x = \sigma$ と添字によらないものとする、

$$\begin{aligned} 1 - \text{Pe}'(Y) &= \frac{1}{M} \sum_{x \in \mathcal{C}} \text{Tr}[\sigma Y_x] \\ &\leq \frac{1}{M} \end{aligned} \quad (\text{B.20})$$

が成り立つことから、次の Corollary も成り立つ。

Corollary B.2 (quantum version of Polyanskiy's converse). *Setting Q3* において、任意の POVM $Y = \{Y_x\}$ に対して、

$$M \leq \sup_p \inf_{\sigma} \beta_{1-\text{Pe}(Y)}(p(X)W_X, p(X)\sigma)^{-1} \quad (\text{B.21})$$

が成り立つ。

Remark B.3. Setting Q3 において Polyanskiy's converse を用いた + 型不等式の証明

は次のようになる。まず、次の不等式を考える。

$$\begin{aligned}
\sum_x p(x) \text{Tr}[(W_x - \alpha \sigma_x) T_x] &\leq \max_{T' = \{T'_x\}_x: \sum_x p(x) \text{Tr}[\rho_x T'_x] \geq 1 - \text{Pe}(g)} \sum_x p(x) \text{Tr}[(W_x - \alpha \sigma_x) T'_x] \\
&= 1 - \text{Pe}(g) - \beta_{1 - \text{Pe}(g)}(p(X) \rho_X, p(X) \sigma_X) \\
&\leq \max_{T' = \{T'_x\}_x} \sum_x p(x) \text{Tr}[(W_x - \alpha \sigma_x) T'_x] \\
&= \sum_x p(x) \text{Tr}[(W_x - \alpha \sigma_x)_+] \tag{B.22}
\end{aligned}$$

これを整理して Polyanskiy's converse を考えると、

$$\begin{aligned}
(1 - \text{Pe}(Y)) - \frac{\alpha}{M} &\leq (1 - \text{Pe}(Y)) - \alpha(1 - \text{Pe}'(Y)) \\
&\leq (1 - \text{Pe}(Y)) - \alpha \beta_{1 - \text{Pe}(Y)}(p(X) W_X, p(X) \sigma) \\
&\leq \sum_x p(x) \text{Tr}[(W_x - \alpha \sigma_x)_+] \tag{B.23}
\end{aligned}$$

を得る。ここで、1つめの不等式は Polyanskiy's converse の証明に現れた (B.20) であり、2つめの不等式は Polyanskiy's meta converse である。また、1行目から3行目へかけての不等式は Neyman-Pearson の補題の基礎となった不等式によっている。

これらのことを総合的に考えれば、+型不等式の証明においては Polyanskiy's (meta) converse を経由して証明する必要はないと考えられる。

付録 C

Han の一般公式と関連不等式

ここでは古典一般多重アクセス通信路符号化問題での重要な定理である Han の一般公式を紹介し、その一般公式と関連が深い不等式の証明を述べる。

C.1 通信路符号化問題における一般公式 (Han の一般公式)

本節では Han の一般公式について述べる。Han の公式は古典シングルアクセス一般通信路符号化問題における公式であり、以下の設定で成り立つ。

$\vec{M}_1 = \{M_1^{(n)}\}_{n=1}^{\infty}$ と $\vec{M}_2 = \{M_2^{(n)}\}_{n=1}^{\infty}$ をそれぞれ自然数の列とし、 $\vec{\mathcal{M}}_1 = \{\mathcal{M}_1^{(n)}\}_{n=1}^{\infty}$ と $\vec{\mathcal{M}}_2 = \{\mathcal{M}_2^{(n)}\}_{n=1}^{\infty}$ をそれぞれ $\mathcal{M}_1^{(n)}$ と $\mathcal{M}_2^{(n)}$ の要素数が $M_1^{(n)}$ と $M_2^{(n)}$ である集合の列であるとする。 $\vec{\mathcal{X}}_1 = \{\mathcal{X}_1^{(n)}\}_{n=1}^{\infty}$ と $\vec{\mathcal{X}}_2 = \{\mathcal{X}_2^{(n)}\}_{n=1}^{\infty}$ をそれぞれ有限ないし可算集合の列とし、 $\vec{\mathcal{Y}} = \{\mathcal{Y}^{(n)}\}_{n=1}^{\infty}$ を任意の集合の列とする。

古典多重アクセス通信路の列 $\vec{W} = \{W^{(n)}(y^{(n)}|x_1^{(n)}, x_2^{(n)})\}_{n=1}^{\infty}$ がひとつ与えられているとする。

それぞれの通信路 $W^{(n)}$ に対して、符号化がそれぞれ単射的な関数 $x_1^{(n)} = f_1(m_1^{(n)})$, $x_2^{(n)} = f_2(m_2^{(n)})$ 、復号が条件付き確率 $g^{(n)}(m_1^{(n)}, m_2^{(n)}|y_2^{(n)})$ で表されるとすると、誤り

確率 Pe は各 n に対して、次のように定義される。

$$\begin{aligned} \text{Pe}^{(n)}(g^{(n)}) := 1 - \sum_{m_1^{(n)}, m_2^{(n)}, x_1^{(n)}, x_2^{(n)}, y^{(n)}} \frac{1}{M_1^{(n)} M_2^{(n)}} & f_1(x_1^{(n)} | m_1^{(n)}) f_2(x_2^{(n)} | m_2^{(n)}) \\ & \cdot W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}) g^{(n)}(m_1^{(n)}, m_2^{(n)} | y_2^{(n)}). \end{aligned} \quad (\text{C.1})$$

ここで、符号化と復号の組 $(f_1^{(n)}, f_2^{(n)}, g^{(n)})$ で誤り確率が ε_n であるものを $(n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n)$ -符号と呼ぶ。

これらの設定が与えられた下で、 \vec{W} に対する ε -通信路容量域 $C(\varepsilon | \vec{W})$ と強逆領域 $C^*(\vec{W})$ は次のように定義される。

Definition C.1.

$$\begin{aligned} C(\varepsilon | \vec{W}) := \{ & (R_1, R_2) | \exists (n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n) - \text{符号 } s.t. \\ & \limsup_{n \rightarrow \infty} \varepsilon_n \leq \varepsilon, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_1^{(n)} \geq R_1, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_2^{(n)} \geq R_2. \} \end{aligned} \quad (\text{C.2})$$

Definition C.2.

$$\begin{aligned} C^*(\vec{W}) := \{ & (R_1, R_2) | \exists (n, M_1^{(n)}, M_2^{(n)}, \varepsilon_n) - \text{符号 } s.t. \\ & \liminf_{n \rightarrow \infty} \varepsilon_n < 1, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_1^{(n)} \geq R_1, \\ & \liminf_{n \rightarrow \infty} \frac{1}{n} \log M_2^{(n)} \geq R_2. \} \end{aligned} \quad (\text{C.3})$$

これらは 4.8 節の Definition 4.15 や Definition 4.16 と表記も同じである。

ここで、(条件付) 相互情報量スペクトルの同時分布を規定する 2 変数関数 $J(R_1, R_2 | \vec{p}_1, \vec{p}_2)$ と $J^*(R_1, R_2 | \vec{p}_1, \vec{p}_2)$ を次のように定義する。

Definition C.3.

$$\begin{aligned}
& J(R_1, R_2 | \vec{p}_1, \vec{p}_2) \\
& := \limsup_{n \rightarrow \infty} \sum_{x_1^{(n)}, x_2^{(n)}, y^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}) \mathbf{1}\{L_1^{(n)} \cup L_2^{(n)} \cup L_3^{(n)}\}
\end{aligned} \tag{C.4}$$

$$\begin{aligned}
& J^*(R_1, R_2 | \vec{p}_1, \vec{p}_2) \\
& := \liminf_{n \rightarrow \infty} \sum_{x_1^{(n)}, x_2^{(n)}, y^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}) \mathbf{1}\{L_1^{(n)} \cup L_2^{(n)} \cup L_3^{(n)}\}
\end{aligned} \tag{C.5}$$

ここで、 \vec{p}_1 と \vec{p}_2 は \mathcal{X}_1 と \mathcal{X}_2 上の確率分布の列であり、 $L_1^{(n)}, L_2^{(n)}, L_3^{(n)}$ は

$$L_1^{(n)} := \{(x_1^{(n)}, x_2^{(n)}, y^{(n)}) | W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}) \leq e^{nR_1} p^{(n)}(y^{(n)} | x_2^{(n)})\}, \tag{C.6}$$

$$L_2^{(n)} := \{(x_1^{(n)}, x_2^{(n)}, y^{(n)}) | W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}) \leq e^{nR_2} p^{(n)}(y^{(n)} | x_1^{(n)})\}, \tag{C.7}$$

$$L_3^{(n)} := \{(x_1^{(n)}, x_2^{(n)}, y^{(n)}) | W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}) \leq e^{n(R_1+R_2)} p^{(n)}(y^{(n)})\} \tag{C.8}$$

であり、 $p^{(n)}(y^{(n)} | x_2^{(n)}), p^{(n)}(y^{(n)} | x_1^{(n)}), p^{(n)}(y^{(n)})$ は

$$p^{(n)}(y^{(n)} | x_2^{(n)}) = \sum_{x_1^{(n)}} p_1^{(n)}(x_1^{(n)}) W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}), \tag{C.9}$$

$$p^{(n)}(y^{(n)} | x_1^{(n)}) = \sum_{x_2^{(n)}} p_2^{(n)}(x_2^{(n)}) W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}), \tag{C.10}$$

$$p^{(n)}(y^{(n)}) = \sum_{x_1^{(n)}, x_2^{(n)}} p_1^{(n)}(x_1^{(n)}) p_2^{(n)}(x_2^{(n)}) W^{(n)}(y^{(n)} | x_1^{(n)}, x_2^{(n)}) \tag{C.11}$$

である。

これらを用いて次が得られる。

- Han の公式 ([10, 11])

$$C(\varepsilon | \vec{W}) = \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | J(R_1, R_2 | \vec{p}_1, \vec{p}_2) \leq \varepsilon\}), \tag{C.12}$$

$$C^*(\vec{W}) = \bigcup_{\vec{p}_1, \vec{p}_2} \text{Cl}(\{(R_1, R_2) | J^*(R_1, R_2 | \vec{p}_1, \vec{p}_2) < 1\}) \tag{C.13}$$

ここで、 $\text{Cl}(\cdot)$ は集合の閉包を表す。

4.8 節の Theorem 4.18 と Theorem 4.19 を古典系に制限し、 $\sigma = W$ ととれば、(C.12) と (C.13) の逆部分に相当する不等式が得られる (Remark 4.21 参照)。

Remark C.4. (C.13) は正確には [10, 11] には明示されていない。しかしながら、(C.13) に相当する定理がそれらの文献中で証明されている。

C.2 既存不等式の証明

本節では、Han の一般公式で重要な役割を果たす Han 不等式とその不等式と関連が深い Yagi-Oohama 不等式の証明を紹介する。

- Han 不等式

Setting M3 において、任意の復号 g および任意の正数 γ に対して、次が成り立つ。

$$\text{Pe}(g) \geq \sum_{x_1, x_2, y} p(x_1, x_2, y) \mathbf{1}\{L_1 \cup L_2 \cup L_3\} - 3\gamma, \quad (\text{C.14})$$

ここで

$$L_1 := \{(x_1, x_2, y) | W(y|x_1, x_2) \leq \gamma M_1 p(y|x_2)\},$$

$$L_2 := \{(x_1, x_2, y) | W(y|x_1, x_2) \leq \gamma M_2 p(y|x_1)\},$$

$$L_3 := \{(x_1, x_2, y) | W(y|x_1, x_2) \leq \gamma M_3 p(y)\},$$

$$M_3 := M_1 M_2.$$

であり、 $p(y|x_1)$ などは $p(x_1, x_2, y)$ から定義される。

Proof[10, 11]. 基本的には Verdú-Han 不等式の証明と同様である。

$$W_{p_1, p_2}(y) := \sum_{x_1, x_2} p_1(x_1) p_2(x_2) W(y|x_1, x_2) \quad (\text{C.15})$$

$$W_{p_1}(y|x_2) := \sum_{x_1} p_1(x_1) W(y|x_1, x_2) \quad (\text{C.16})$$

$$W_{p_2}(y|x_1) := \sum_{x_2} p_2(x_2) W(y|x_1, x_2) \quad (\text{C.17})$$

で定義する。このとき、任意の正数 γ に対して、

$$\begin{aligned}
& \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)\mathbf{1}\{L_1 \cup L_2 \cup L_3\} \\
&= \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)\mathbf{1}\{L_1 \cup L_2 \cup L_3\}g(x_1, x_2|y) \\
&\quad + \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)\mathbf{1}\{L_1 \cup L_2 \cup L_3\}(1 - g(x_1, x_2|y)) \\
&\leq \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)\mathbf{1}\{L_1 \cup L_2 \cup L_3\}g(x_1, x_2|y) \\
&\quad + \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)(1 - g(x_1, x_2|y)) \\
&\leq \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)(\mathbf{1}\{L_1\} + \mathbf{1}\{L_2\} + \mathbf{1}\{L_3\})g(x_1, x_2|y) \\
&\quad + \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)(1 - g(x_1, x_2|y)) \\
&\leq \sum_{x_1, x_2, y} \gamma(W_{p_1, p_2}(y) + p_1(x_1)W_{p_2}(y|x_1) + p_2(x_2)W_{p_1}(y|x_2))g(x_1, x_2|y) \\
&\quad + \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)(1 - g(x_1, x_2|y)) \\
&\leq 3\gamma \sum_{x_1, x_2, y} W_{p_1, p_2}(y)g(x_1, x_2|y) \\
&\quad + \sum_{x_1, x_2, y} p_1(x_1)p_2(x_2)W(y|x_1, x_2)(1 - g(x_1, x_2|y)) \\
&= 3\gamma + \text{Pe}(g) \tag{C.18}
\end{aligned}$$

が成り立つ。 □

- Yagi-Oohama 不等式

Setting M3 において、任意の復号 g 、任意の正数 γ' および \mathcal{Y} 上の任意の条件付き確率および確率 $q_1(y|x_2), q_2(y|x_1), q_3(y)$ に対して、次が成り立つ。

$$\text{Pe}(g) \geq \sum_{x_1, x_2, y} p(x_1, x_2, y)\mathbf{1}\{W(y|x_1, x_2) \leq \gamma\bar{q}(y|x_1, x_2)\} - \gamma \sum_i \frac{\pi_i}{M_i}, \tag{C.19}$$

ここで、

$$\bar{q}(y|x_1, x_2) := \pi_1 q_1(y|x_2) + \pi_2 q_2(y|x_1) + \pi_3 q_3(y) \tag{C.20}$$

この不等式を証明するのに次の補題が必要である。

- Yagi-Oohama's converse [30]

Setting M3 において、任意の復号 g および \mathcal{Y} 上の任意の条件付き確率および確率 $q_1(y|x_2), q_2(y|x_1), q_3(y)$ に対して、次が成り立つ。

$$\beta_{1-\text{Pe}(g)}(p(X_1, X_2)W(Y|X_1, X_2), p(X_1, X_2)\bar{q}(Y|X_1, X_2)) \leq \sum_i \frac{\pi_i}{M_i} \quad (\text{C.21})$$

ここで、 $h: \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y} \rightarrow [0, 1]$ としたとき、

$$\begin{aligned} & \beta_{1-\varepsilon}(p(X_1, X_2, Y), q(X_1, X_2, Y)) \\ &= \min_{h: \sum_{x_1, x_2, y} p(x_1, x_2, y)h(x_1, x_2, y) \geq 1-\varepsilon} \sum_{x_1, x_2, y} q(x_1, x_2, y)h(x_1, x_2, y) \end{aligned} \quad (\text{C.22})$$

であり、 $\bar{q}(y|x_1, x_2)$ は (C.20) で与えられる。

Proof[30]. 2つの入力分布 $p(y|x_1, x_2), q(y|x_1, x_2)$ が与えられたとき、それぞれの誤り確率を $\text{Pe}(g), \text{Pe}(g)'$ で表すと、

$$\text{Pe}(g) = 1 - \frac{1}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} p(y|x_1, x_2)g(x_1, x_2|y) \quad (\text{C.23})$$

$$\text{Pe}(g) = 1 - \frac{1}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} q(y|x_1, x_2)g(x_1, x_2|y) \quad (\text{C.24})$$

となる。Polyanskiy の meta converse より

$$\beta_{1-\text{Pe}(g)}(p(X_1, X_2, Y), q(X_1, X_2, Y)) \leq 1 - \text{Pe}(g)' \quad (\text{C.25})$$

が成り立つ。ここで、 q を \bar{q} とすると、

$$\begin{aligned}
1 - \text{Pe}(g)' &= \frac{1}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} \bar{q}(y|x_1, x_2) g(x_1, x_2|y) \\
&= \frac{\pi_1}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} q_1(y|x_2) g(x_1, x_2|y) \\
&\quad + \frac{\pi_2}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} q_2(y|x_1) g(x_1, x_2|y) \\
&\quad + \frac{\pi_3}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} q_3(y) g(x_1, x_2|y) \\
&\leq \frac{\pi_1}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, x'_2 \in \mathcal{C}_2, y} q_1(y|x'_2) g(x_1, x_2|y) \\
&\quad + \frac{\pi_2}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x'_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} q_2(y|x'_1) g(x_1, x_2|y) \\
&\quad + \frac{\pi_3}{M_1 M_2} \sum_{x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, y} q_3(y) g(x_1, x_2|y) \\
&\leq \frac{\pi_1}{M_1 M_2} \sum_{x'_2 \in \mathcal{C}_2} 1 + \frac{\pi_2}{M_1 M_2} \sum_{x'_1 \in \mathcal{C}_1} 1 + \frac{\pi_3}{M_1 M_2} \\
&= \sum_i \frac{\pi_i}{M_i} \tag{C.26}
\end{aligned}$$

が成り立つことから、併せて (C.22) が成り立つ。 \square

これを用いて Yagi-Oohama 不等式が証明される。

Proof of the Yagi-Oohama bound[30]. Neyman-Pearson の補題より、任意の正数 γ に対して

$$\begin{aligned}
1 - \text{Pe}(g) &\leq \sum_{x_1, x_2, y} p(x_1, x_2, y) \mathbf{1}\{p(y|x_1, x_2) > \gamma q(y|x_1, x_2)\} \\
&\quad + \gamma \beta_{1-\text{Pe}(g)}(p(X_1, X_2, Y), q(X_1, X_2, Y)) \tag{C.27}
\end{aligned}$$

が成り立つ。これと Yagi-Oohama's converse より目的の不等式を得る。 \square

参考文献

- [1] Ahlswede., R., “Multi-way communication channels.,” *2nd Int. Symp. Inf. Theory*, pp. 23–52. Hungarian Academy of Sciences, Budapest, 1971.
- [2] Ahlswede., R. and Cai., N., “A Strong Converse Theorem for Quantum Multiple Access Channels,” *General Theory of Information Transfer and Combinatorics*, pp. 460–485, 2006.
- [3] Alajaji, F., Chen P. N., and Rached Z. “A note on the Poor-Verdú upper bound for the channel reliability function”, *IEEE Trans. Inform. Theory*, vol. 48, no. 1, pp. 309-313, January 2002.
- [4] Bowen, G. and Datta, N., “Beyond i.i.d. in Quantum Information Theory,” *ISIT2006*, Seattle, USA, July 2006.
- [5] Chen, P.-N. and Alajaji, F., “A Generalized Poor-Verdu Error Bound for Multihypothesis Testing”, *IEEE Trans. Inform. Theory*, vol. 58, no. 1, pp. 311–316, 2012.
- [6] Cover, M. T. and Thomas, J. A., *Elements of Information Theory second edition*, Wiley, 2006.
- [7] Csiszar, I. and Korner, J., *INFORMATION THEORY Coding Theorems for Discrete Memoryless Systems*, Academic Press, 1981.
- [8] Dueck, G., “The strong converse to the coding theorem for the multiple-access channel,” *J. Comb. Inform. Syst. Sci.*, Vol.6, pp.187–196, 1981.
- [9] Fano, R. M. Class notes for Taransmission of Information, course 6.574(Technical Report). MIT, Cambridge, 1952.
- [10] Han, T. S., “An information-spectrum approach to capacity theorems for the

- general multiple-access channel,” *IEEE Trans. Inform. Theory*, vol. 44, no. 7, pp. 2773–2795, 1998.
- [11] Han, T. S., *Information-Spectrum Methods in Information Theory*, Springer, 2003.
- [12] Hayashi, M. and Nagaoka, H., “General formulas for capacity of classical-quantum channels,” *IEEE Trans. Inform. Theory*, vol. 49, no. 7, pp. 1753–1768, 2003.
- [13] Kubo, T. and Nagaoka, H., “Lower Bounds on the Error Probability in Classical and Quantum State Discrimination,” *ISITA2012*, Honolulu, USA, October 2012.
- [14] Kubo, T. and Nagaoka, H., “A Fundamental Inequality for Lower-bounding the Error Probability for Classical and Quantum Multiple Access Channels and Its Applications,” *IEICE Trans.* to be published in December 2015, arXiv:1503.06914, March 2015.
- [15] Liao, H., “Multiple-access channels,” Ph. D. thesis, University Hawaii, 1972.
- [16] Polyanskiy, Y., “Channel coding: non-asymptotic fundamental limits,” Ph. D. thesis, Department of Electrical Engineering, Princeton University, 2010.
- [17] Polyanskiy, Y., Poor, H. V., and Verdú, S., “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2307–2358, 2010.
- [18] Poor, H. V. and Verdú, S., “A lower bound on the probability of error in multi-hypothesis testing,” *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1992–1994, 1995.
- [19] Shannon, C. E., “Two-way communication channels,” *4th Berkeley Symp. Math. Stat. Prob.*, vol. 1, pp.611–644. University of California Press, Berkeley, CA, 1961.
- [20] Shannon, C. E., “A mathematical theory of communication,” *Bell Syst. Tech. J.*, vol. 27, pp.379–423, 1948.
- [21] Shannon, C. E., Gallager, R. G., and Berlekamp, E. R., “Lower bounds to error probability for coding on discrete memoryless channels i,” *Inf. Contr.*, vol. 10,

- pp.65–103, 1967.
- [22] Verdú, S. and Han, T. S., “A General formula for channel capacity,” *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1147–1157, 1994.
- [23] Winter, A., “The Capacity of the Quantum Multiple-Access Channel,” *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3059–3065, 2001.
- [24] Yard, J., Hayden, P., and Devetak, I., “Capacity Theorems for Quantum Multiple-Access Channels: Classical-Quantum and Quantum-Quantum Capacity Regions,” *IEEE Trans. Inform. Theory*, vol. 54, no.7, pp. 3091–3112, 2008.
- [25] Yuen, H. P., “Communication theory of Quantum Systems,” MIT Res. Lab. Electron., 1971.
- [26] 久保 卓也, 古典・量子識別問題における誤り確率の下界に関する研究, 電気通信大学修士論文, 2012.
- [27] 久保 卓也, 長岡 浩司, “古典・量子状態推定における誤り確率の下界について,” *QIT25*, Osaka, Japan, November 2011.
- [28] 久保 卓也, 長岡 浩司, “一般化 Poor-Verdú 不等式に関するいくつかの考察,” *SITA2012*, Oita, Japan, December 2012.
- [29] 久保 卓也, 長岡 浩司, “古典および量子多重アクセス通信路における誤り確率の下界に関する考察,” *SITA2014*, Toyama, Japan, December 2014.
- [30] 八木 秀樹, 大濱 靖匡, “多重アクセス通信路における有限ブロック長解析と複合仮説検定の関係,” *SITA2012*, Oita, Japan, December 2012.

謝辞

本研究は電気通信大学大学院情報システム学研究科情報ネットワークシステム学専攻 長岡浩司教授のもとで行いました。本研究は長岡教授との共同研究です。特に Setting 2 に対する検討を行う部分は教授のアイデアによるものでした。さらに、博士後期課程における私の研究活動は博士前期課程以上の迷走と停滞の連続でした。そのような私に教授は研究に対する姿勢はもとより、生活、精神面まで幅広く助言を下さいました。そのような教授の根気強さに、このような私に研究を最後まで進めさせてくださった教授に深く感謝申し上げます。

本研究を進めるにあたり、数多くの理論や解釈など様々な助言をしていただき、たくさん時間を割いていただいた同専攻 小川朋宏准教授に感謝申し上げます。同期というものが事実上存在せず、また、同方向の研究をしている近い世代の学生や研究者を殆ど知らない私は心が折れそうになったり、また実際折れた事も有りました。そのような中で准教授が同じ分野で素晴らしい研究成果を上げているというのは、大変励みになりました。

また、特に物理学的な側面からアドバイスをいただき、学生生活の生活面で支えていただいた同専攻 鈴木淳助教にも深く感謝いたします。

本研究の起点となる助言をいただいた韓太瞬名誉教授に感謝申し上げます。2012 年の別府 SITA での一言がなければ、私はこの研究を始めていなかったかもしれません。

さらに、本研究の直接の先行研究の著者である電気通信大学大学院情報理工学研究科の八木秀樹准教授にも感謝申し上げます。准教授には、本研究を進めるにあたり、数回の議論を行っていただきました。

学生生活全般よりお世話になりました、電気通信大学長岡・小川研究室の各氏、情報システム学研究科事務の横山氏と吉村氏をはじめとする各氏に深く感謝いたします。

最後に、私に本学で学ぶ機会を与えてくださり、経済的精神的な面で様々な援助をして

くださった家族に心より感謝申し上げます。