社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

# 量子情報理論における仮説検定の役割

林　　正人†

† 独立行政法人 科学技術振興機構 今井量子計算機構プロジェクト
〒 113-0033 文京区本郷 5-28-3 第二本郷ホワイトビル 201 号
E-mail: †masahito@qci.jst.go.jp

あらまし　量子情報理論では量子通信路を用いた、古典的メッセージ及び量子状態の伝送、さらには、量子暗号のように盗聴者が居る場合での通信、情報源の圧縮など、様々なテーマが取り扱われる。これらのテーマの漸近的特性は量子仮説検定を通じて統一的に理解することができる。本講演では、これらの点に注目して、量子情報理論での漸近理論を統一的に理解する枠組を提案する。
キーワード　量子仮説検定、量子通信路、量子暗号、量子情報源符号化

# Role of Hypothesis Testing in Quantum Information Theory

Masahito HAYASHI†

† Quantum Computation and Information Project, Japan Science and Technology Agency
201 Daini Hongo White Bldg. 5-28-3, Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
E-mail: †masahito@qci.jst.go.jp

**Abstract**　There are several information processing topics, for example, classical information transmission via quantum channel, quantum cryptography, information compression, etc, in quantum information theory. We can unifiedly understand these topics through quantum hypothesis testing. In thins talk, I propose an unified framework to understand several asymptotic analyses in quantum information theory.
**Key words**　quantum hypotheses testing, quantum channel, quantum cryptography, quantum source coding

## 1. はじめに

量子情報理論では量子通信路を用いた、古典的メッセージ及び量子状態の伝送、さらには、量子暗号のように盗聴者が居る場合での通信、情報源の圧縮など、様々なテーマが提案され、その漸近的な性能が議論されている。これらのテーマの多くは従来の ( 非量子的な ) 情報理論でも取り扱われており、これらと仮説検定との関係は数多く指摘されている。その中でも、韓は情報スペクトルを導入することで、一般情報源に対して様々な情報理論の問題を解析するとともに、これらの問題と仮説検定との関係も明らかにした。いわば、情報スペクトルにおいては、個々の問題を一般情報源に対して解析することと、その問題と仮説検定との関係を明らかにすることとの間には表裏一体の関係にある。本講演では、このような類似の視点を量子情報理論に持ち込み、上述のテーマと量子仮説検定との関係を表す不等式を紹介する。

基本的に仮説検定では Neymann-Pearson の補題が基本となり、ここで基本となる概念は尤度である。しかし、この尤度の概念を量子化するにはいくつかの任意性があり、ここが最も量子性の現れる部分である。情報理論の隣接分野として数理統計学という分野が知られているが、両者の理論的な部分では、ある確率分布を仮定し、その下での漸近的極限定理が中心的な役割を果たすという点で類似している。しかし、一方で、前者は主に大偏差型の評価が中心的な役割を果たすのに対し、後者はどちらかというと、平均 2 条誤差の漸近的振舞いのように、極限値の近傍での振舞いを問題にすることが多い。このような注目する漸近的部分の違いが、複数ある尤度の量子化のどれを選ぶかに影響してしまう。とにかく、ここで重要なことは尤度の概念の量子版を考えるにしても、個々の問題設定に応じて適切なものを選ぶ必要があるということである。

さらに、両者を結ぶ世界のテーマとして、量子推定において誤差を大偏差で評価するという問題があるが、この問題については非常に取り扱いが難しく、仮説が 2 つの場合の仮説検定の極限として捉えた場合と、ある種の超有効性を排除した範囲で最適化を考えた場合とでは、異なった限界が得られる。ある意味、前者は情報理論的世界での尤度の量子版から自然に導かれる構造であり、後者は数理統計学的世界での尤度の量子版から自然に導かれる構造である。この問題は本講演では扱えないが、

このような中間にある問題を考えることで、両者の構造を同じ基準で比較することができ、如何に相容れない構造になっているかが理解できる。

このような状況の下、本講演では、これらのテーマのうち量子仮説検定と、それに関連した情報理論的問題について、ある種の尤度の量子版を中心として統一的に理解できることを解説する。なお、近いうちのこのような視点で著者によって書かれたテキスト「量子情報理論入門」が出版予定であるので詳しくはそれを見て頂きたい [1]。ただ、残念ながら、ここで述べる世界は広い意味での量子情報理論の一部の世界に過ぎない。

## 2. 量子仮説検定と尤度の量子版

量子情報理論では対象とする物理系に対してエルミート内積つき複素ベクトル空間が対応し、これを有限次元の場合も含めて Hilbert 空間とよぶことにする。そして、確率分布に対応する概念として、系の様子すなわち状態を表す概念として密度行列がある。密度行列は Hilbert 空間 $\mathcal{H}$ 上のエルミート行列 $\rho$ で半正定値でありそのトレースが 1 のものである。なお、以下 $X$ が半正定置であるとき $X \geqq 0$ と記すことにし、$X - Y \geqq 0$ であるとき $X \geqq Y$ と記す。一方、これが我々にどのような情報を意味するものであるか、明確にするには、実際に我々が得るデータとの関係を明確にする必要がある。そのためには、状態の概念の他に、測定の概念を導入する必要がある。仮に状態が同じでも、我々の行なう測定が異なれば、異なったデータの分布が得られる。その測定を表す概念として POVM (Positive Operator Valued Measure) がある。それは測定値の集合を $\Omega$ としたとき、その各要素 $\omega \in \Omega$ に対して、半正定値なエルミート行列 $M_\omega$ を対応させたもので、その総和 $\sum_{\omega\in\Omega} M_\omega$ が単位行列 $I$ になるものであり、$M = \{M_\omega\}_\omega \in \Omega\}$ を POVM とよぶことにする。この POVM $M$ が測定を表しているという意味は以下である。系の状態が密度行列 $\rho$ で記述されているとし、POVM $M$ に対応する測定を行なったとき、測定値 $\omega \in \Omega$ が得られる確率は $\mathrm{Tr}\, M_\omega \rho$ で与えられる。

以下では、帰無仮説、対立仮説がともに 1 つの量子状態 $\rho, \sigma$ で与えられている場合での仮説検定を考えよう。この場合、測定値は帰無仮説の受容、棄却の 2 つであるので、2 値の POVM $\{M_0, M_1\}$ で表される。さらに総和が $I$ であることから、受容に対応する半正定値なエルミート行列 $T$ を 1 つ決めると $T$ は $I \geqq T \geqq 0$ を満たすことになり、自然に棄却に対応する半正定値なエルミート行列は $I - T$ となり、その場合の第 1 種誤り確率と第 2 種誤り確率はそれぞれ $\epsilon_1(T) \stackrel{\mathrm{def}}{=} \mathrm{Tr}\, \rho(I-T), \epsilon_2(T) \stackrel{\mathrm{def}}{=} \mathrm{Tr}\, \sigma T$ で与えられる。

そして、一般のエルミート行列 $X$ は $x_i$ が固有値であり、$E_i$ 対応する固有空間への射影であるとき、$X = \sum_i x_i E_i$ と分解できるがそのとき、射影 $\sum_{i:x_i\geqq 0} E_i$ を $\{X \geqq 0\}$ で記すことにする。同様に、$\{X > 0\}, \{X \leqq 0\}, \{X < 0\}$ も定義できる。そして、今扱っている仮説検定では、実数 $a$ に対して、$T$ が $\{\rho - e^a\sigma \geqq 0\}$ となる場合が重要で、この場合の 2 つの誤り確率は

$$\epsilon_1(\{\rho - e^a\sigma \geqq 0\}) = \mathrm{Tr}\, \rho\{\rho - e^a\sigma < 0\} \tag{1}$$

$$\epsilon_1(\{\rho - e^a\sigma \geqq 0\}) = \mathrm{Tr}\, \sigma\{\rho - e^a\sigma \geqq 0\}. \tag{2}$$

となる。逆に、任意の実数 $a$ と検定を表す $T$ に対して、

$$\epsilon_1(T) + e^a\epsilon_2(T) \geqq \mathrm{Tr}\, \rho\{\rho - e^a\sigma < 0\}.$$

が成立し、検定の性能の限界が評価できる。

ただ、実際には $\rho$ と $\sigma$ に非可換性がある場合には、上の公式はそのまま使えない場合が多い。それを補うために、$\sigma = \sum_i s_i E_i$ とし、$\overline{\rho} \stackrel{\mathrm{def}}{=} \sum_i E_i \rho E_i$ と $\sigma$ の固有値の数 $v$ に注目した以下の不等式を考える。実数 $a$ と $0 < s < 1$ となる実数 $s$ に対して以下の不等式が成り立つ。

$$\mathrm{Tr}\, \sigma\{\overline{\rho} - e^a\sigma \geqq 0\} \leqq v e^{sa}\, \mathrm{Tr}\, \rho\sigma^{(1-s)/2}\rho^{s-1}\sigma^{(1-s)/2}$$

$$\mathrm{Tr}\, \rho\{\overline{\rho} - e^a\sigma < 0\} \leqq v e^{(1-s)a}\, \mathrm{Tr}\, \rho\sigma^{(1-s)/2}\rho^{s-1}\sigma^{(1-s)/2}$$

さらに $I \geqq T \geqq 0$ と実数 $a$ と $s > 0$ に対して、不等式

$$\frac{1}{v}\, \mathrm{Tr}\, \rho T \leqq e^{sa}\, \mathrm{Tr}\, \sigma^{1+s}\rho^{-s} + e^a\, \mathrm{Tr}\, \sigma T$$

が成立する。

そして、これらの公式を用いることで、以下に定義する $0 \leqq \epsilon < 1$ and $r > 0$ に依存した仮説検定の漸近的な性能を議論することができる。

$$B(\epsilon) \stackrel{\mathrm{def}}{=} \sup_{\{T_n\}} \left\{ \underline{\lim} \frac{-\log \epsilon_2(T_n)}{n} \middle| \exists \{T_n\} : \overline{\lim}\, \epsilon_1(T_n) \leqq \epsilon\, \mathrm{Tr}\, \rho \right\},$$

$$B_e(r) \stackrel{\mathrm{def}}{=} \sup_{\{T_n\}} \left\{ \underline{\lim} \frac{-\log \epsilon_2(T_n)}{n} \middle| \exists \{T_n\} : \underline{\lim} \frac{-\log \epsilon_2(T_n)}{n} \geq r \right\}.$$

ただし、$T_n$ は 帰無仮説 $\rho^{\otimes n}$、対立仮説 $\sigma^{\otimes n}$ の仮説検定でのテストを表す。そしてこれらの値は以下のように評価できる [3] ~ [5]。

$$B(\epsilon) = D(\rho\|\sigma) \stackrel{\mathrm{def}}{=} \mathrm{Tr}\, \rho(\log\rho - \log\sigma)$$

$$B_e(r) \geq \max_{0\leqq s\leqq 1} \frac{-sr - \tilde{\psi}(s)}{1-s}, \quad \forall r > 0$$

$$\tilde{\psi}(s) \stackrel{\mathrm{def}}{=} \log \mathrm{Tr}\, \rho\sigma^{(1-s)/2}\rho^{s-1}\sigma^{(1-s)/2}.$$

## 3. 量子通信路符号化 ( 古典的メッセージ伝送 )

ノイズのある量子通信路を用いて古典的なメッセージを伝送する問題では、通信路を古典的なアルファベットを入力し、量子状態を出力する古典-量子通信路 $x \in \mathcal{X} \mapsto \rho_x$ として扱うことが許される。

この場合、符号化はメッセージ $\{1, \ldots, M\}$ からアルファベットを与える写像 $\phi : i \in \{1, \ldots, M\} \mapsto \phi(i) \in \mathcal{X}$ で表され、復号化のプロセスは、メッセージに集合 $\{1, \ldots, M\}$ に値を持つ POVM $Y = \{Y_j\}_{j=1}^M$ と記述される。この場合、符号は 3 つ組 $\mathcal{C} \stackrel{\mathrm{def}}{=} (M, \phi, Y)$ で記述され、符号のサイズ $M(\mathcal{C}) \stackrel{\mathrm{def}}{=} M$ と平

均誤り確率 $\epsilon(\mathcal{C}) \stackrel{\rm def}{=} \frac{1}{M}\sum_{i=1}^{M}\left(1-\mathrm{Tr}\,\rho_{\phi(i)}Y_i\right)$ の trade-off を扱うことになる。

そして、任意の確率分布 $p$ に対して、以下の符号 $\mathcal{C}$ が存在することが示せる。

$$\begin{aligned}\epsilon(\mathcal{C}) \leqq & 2\sum_x p(x)\,\mathrm{Tr}\,\rho_x\left\{\rho_x - M(\mathcal{C})\overline{\rho}_p\ <0\right\}\\ & +4\sum_x p(x)\,\mathrm{Tr}\,\overline{\rho}_p\left\{\rho_x - M(\mathcal{C})\overline{\rho}_p \geqq 0\right\},\end{aligned}$$

ただし、$\overline{\rho}_p \stackrel{\rm def}{=} \sum_x p(x)\rho_x$ である [10]。逆に、任意の符号 $\mathcal{C}$ は任意の実数 $a$ に対して以下の不等式を満たすことも示せる。

$$\epsilon(\mathcal{C}) + e^a M(\mathcal{C})^{-1} \geqq \sum_{i=1}^{M}\frac{1}{M(\mathcal{C})}\,\mathrm{Tr}\,\rho_{\phi(i)}\left\{\rho_{\phi(i)} - e^a\overline{\rho}_{\mathcal{C}}\ <0\right\}$$

ただし、$\overline{\rho}_{\mathcal{C}} \stackrel{\rm def}{=} \sum_{i=1}^{M}\frac{1}{M(\mathcal{C})}\rho_{\phi(i)}$ である [10]. さらに、$\mathcal{C}_n$ を古典-量子通信路 $x^n=(x_1,\ldots,x_n)\in\mathcal{X}^n \mapsto \rho_{x_1}\otimes\cdots\otimes\rho_{x_n}$ に対する符号として

$$\begin{aligned}R(\epsilon) &\stackrel{\rm def}{=} \sup_{\{\mathcal{C}_n\}}\left\{\underline{\lim}\,\frac{\log M(\mathcal{C}_n)}{n}\,\middle|\,\overline{\lim}\,\epsilon(\mathcal{C}_n)\leqq\epsilon\right\}\\ R_e(r) &\stackrel{\rm def}{=} \sup_{\{\mathcal{C}_n\}}\left\{\underline{\lim}\,\frac{\log M(\mathcal{C}_n)}{n}\,\middle|\,\underline{\lim}\,\frac{-\log\epsilon(\mathcal{C}_n)}{n}\geqq r\right\},\end{aligned}$$

を定義すると、これらは以下のように特徴付けられる [6] ~ [10].

$$R(\epsilon) = \max_p\sum_x p(x)D(\rho_x\|\overline{\rho}_p)$$

$$R_e(r) \geqq \max_p\max_{0\leqq s<1}\frac{-r-\tilde{\psi}_p(s)}{1-s}, \forall r>0,$$

ただし、

$$\tilde{\psi}_p(s) \stackrel{\rm def}{=} \log\sum_x p(x)\,\mathrm{Tr}\,\rho_x\overline{\rho}_p^{(1-s)/2}\rho_x^{s-1}\overline{\rho}_p^{(1-s)/2}$$

である。

## 4. 量子情報源符号化

量子情報源符号化では量子情報源は量子状態 $\rho_x$ を指定するラベルのなす集合 $\mathcal{X}$ 上の確率分布として記述され、visible と blind の 2 種の設定がある。

visible な設定では、符号化はラベルの集合 $\mathcal{X}$ から次元の小さい空間 $\mathcal{K}$ 上の密度行列への写像 $e$ で記述され、blind な設定では符号化は元の空間 $\mathcal{H}$ 上の密度行列から小さい空間 $\mathcal{K}$ 上の密度行列を与える完全正写像で与えられる。そして、復号化は双方の設定で空間 $\mathcal{K}$ 上の密度行列から空間 $\mathcal{H}$ 上の密度行列を与える完全正写像 $D$ で与えられる。そして、visible な設定では符号は $\mathcal{C}_v \stackrel{\rm def}{=} (\mathcal{K},e,D)$ で与えられ、blind な設定では符号は $\mathcal{C}_b \stackrel{\rm def}{=} (\mathcal{K},E,D)$ で与えられる。そして blind な符号化 $E$ に対して $e(x)\stackrel{\rm def}{=}E(\rho_x)$ となる visible な符号化 $e$ を考えることができるので、後者は前者に含まれる。そして、これらの設定では符号のサイズ $M(\mathcal{C}_v)\stackrel{\rm def}{=}\dim\mathcal{K}$ と誤りの度合 $\varepsilon(\mathcal{C}_v)\stackrel{\rm def}{=}\sum_x p(x)(1-(\mathrm{Tr}|\sqrt{\rho_x}\sqrt{D(e(x))}|)^2)$ の trade-off を扱うことになる。

そして、以下の条件を満たす blind な符号 $\mathcal{C}_b$ と visible な符号 $\mathcal{C}_v$ が存在する。

$$\begin{aligned}\varepsilon(\mathcal{C}_b) &\leqq 2\,\mathrm{Tr}\,\overline{\rho}_p\left\{\overline{\rho}_p - e^a\ <0\right\},\\ M(\mathcal{C}_b) &= \mathrm{Tr}\left\{\overline{\rho}_p - e^a\geqq 0\right\},\\ \varepsilon(\mathcal{C}_v) &\leqq \mathrm{Tr}\,\overline{\rho}_p\left\{\overline{\rho}_p - e^a\ <0\right\},\\ M(\mathcal{C}_v) &= \mathrm{Tr}\left\{\overline{\rho}_p - e^a\geqq 0\right\}.\end{aligned}$$

一方、$\rho_x$ が全て純粋状態である場合には任意の符号 $\mathcal{C}_v$ は任意の実数 $a$ に対して、以下の条件を満たす [11].

$$\varepsilon(\mathcal{C}_v) + e^a M(\mathcal{C}_v) \geqq \mathrm{Tr}\,\overline{\rho}_p\left\{\overline{\rho}_p - e^a\ <0\right\}$$

そして、これらの公式は量子情報源符号化が $\sigma=I,\rho=\overline{\rho}_p,\epsilon_1(T)=\varepsilon(\mathcal{C}),\epsilon_2(T)=M(\mathcal{C})$. となる量子仮説検定と密接な関係にあることを示している。これらの公式を用いて、符号の性能の限界について漸近的評価をしてみよう。そのために $x^n=(x_1,\ldots,x_n)\mapsto\rho_{x_1}\otimes\cdots\otimes\rho_{x_n}$ となる情報源の列を考え、その情報源に対する blind な符号 $\mathcal{C}_{b,n}$ を考え、その無限列 $\{\mathcal{C}_{b,n}\}$ に注目して、以下の量を定義する。

$$\begin{aligned}R(\epsilon) &\stackrel{\rm def}{=} \sup_{\{\mathcal{C}_{b,n}\}}\left\{\overline{\lim}\,\frac{\log M(\mathcal{C}_{b,n})}{n}\,\middle|\,\overline{\lim}\,\epsilon(\mathcal{C}_{b,n})\leqq\epsilon\right\}\\ R_e(r) &\stackrel{\rm def}{=} \sup_{\{\mathcal{C}_{b,n}\}}\left\{\overline{\lim}\,\frac{\log M(\mathcal{C}_{b,n})}{n}\,\middle|\,\underline{\lim}\,\frac{-\log\epsilon(\mathcal{C}_{b,n})}{n}\geqq r\right\}.\end{aligned}$$

すると、これらの量は以下のように計算できる [9], [11], [12]。

$$\begin{aligned}R(\epsilon) &= H(\overline{\rho}_p)\stackrel{\rm def}{=}-\mathrm{Tr}\,\overline{\rho}_p\log\overline{\rho}_p\\ R_e(r) &= \min_{0\leqq s\leqq 1}\frac{sr+\psi(s)}{1-s},\quad \psi(s)\stackrel{\rm def}{=}\log\mathrm{Tr}\,\overline{\rho}_p^s.\end{aligned}$$

なお、同様の結果は visible な符号の場合にも成り立つ。

## 5. エンタングルメント集中化

量子情報処理では完全なエンタングルド状態を用いるものが数多い。しかし、与えられたエンタングルド状態は必ずしも完全なエンタングルド状態とは限らない。そのような状況では部分なエンタングルド状態から完全なエンタングルド状態を作り出す必要がある。このような操作は最初に与えられたエンタングルド状態が純粋状態 $\phi\in\mathcal{H}_A\otimes\mathcal{H}_B$ である場合はエンタングルメント集中化とよばれる。このプロトコルでは局所操作 (local operation) と古典通信 (classical communication) を組み合わせた操作で完全なエンタングルメント状態を作ることになり、2 種類の問題設定がある。1 つ目の設定ではその操作の後の状態を出来る限り所望の完全なエンタングルド状態にするプロトコルである。この場合我々の操作を $\mathcal{F}_1$ で表すことすると、その性能は、目標となる完全なエンタングルド状態の大きさ $L(\mathcal{F}_1)$ 及びそのときの終状態 $\mathcal{F}_1(|\phi\rangle\langle\phi|)$ と目標となる状態 $|\psi_L\rangle\langle\psi_L|$ との近さ $\varepsilon(\mathcal{F}_1)\stackrel{\rm def}{=}1-\langle\psi_L|\mathcal{F}_1(|\phi\rangle\langle\phi|)|\psi_L\rangle$ で与えられ、これらの trade-off が問題となり、$\rho\stackrel{\rm def}{=}\mathrm{Tr}_B\,|\phi\rangle\langle\phi|$ とおくと、

$$\max_{L(\mathcal{F}_1)=L}(1-\varepsilon(\mathcal{F}_1)) = \max_{T:\text{射影},\mathrm{Tr}\,T=L}\left(\mathrm{Tr}\sqrt{\frac{\rho}{L}}T\right)^2$$
$$=\left(\sqrt{\mathrm{Tr}\,\frac{1}{L}\{\rho\geqq\frac{1}{L}\}}\sqrt{\mathrm{Tr}\,\rho\{\rho\geqq\frac{1}{L}\}}\right.$$
$$\left.+\sqrt{1-\mathrm{Tr}\,\frac{1}{L}\{\rho\geqq\frac{1}{L}\}}\sqrt{\mathrm{Tr}\,\rho\{\rho<\frac{1}{L}\}}\right)^2$$

が成り立つ [13] ~ [15]。

もう 1 つの問題設定では失敗確率を許し、成功した場合には所望の完全なエンタングルド状態となるようにするプロトコルである。この設定では我々の操作 $\mathcal{F}_2$ の性能はその失敗確率 $\varepsilon(\mathcal{F}_2)$ と成功したときに出来る完全なエンタングルド状態のサイズ $L(\mathcal{F}_2)$ で与えられる。この設定では

$$\max_{\mathcal{F}_2}\{L(\mathcal{F}_2)|\,\varepsilon(\mathcal{F}_2)\leqq h(x)\} = \left[\frac{1-h(x)}{x}\right],$$
$$h(x)\stackrel{\text{def}}{=}\mathrm{Tr}(\rho-x)\{\rho\geqq x\}$$

となる [13] ~ [15]。

次に、これらの設定の下で、その漸近的な性能について考えてみよう。すなわち、部分的なエンタングルド状態 $\phi$ のテンソル積状態 $\phi^{\otimes n}$ からできるだけサイズの大きい完全なエンタングルド状態を構成する操作 $cF_{1,n}$ を考え、その無限列 $\{cF_{1,n}\}$ に注目する。

$$B(\epsilon)\stackrel{\text{def}}{=}\sup_{\{\mathcal{F}_{1,n}\}}\left\{\underline{\lim}\,\frac{\log L(\mathcal{F}_{1,n})}{n}\middle|\,\underline{\lim}\,\varepsilon(\mathcal{F}_{1,n})\leqq\epsilon\right\}$$
$$B_e(r)\stackrel{\text{def}}{=}\sup_{\{\mathcal{F}_{1,n}\}}\left\{\underline{\lim}\,\frac{\log L(\mathcal{F}_{1,n})}{n}\middle|\,\underline{\lim}-\frac{\log\varepsilon(\mathcal{F}_{1,n})}{n}\leqq r\right\}$$

すると、$\psi(s)\stackrel{\text{def}}{=}\log\mathrm{Tr}\,\rho^s$ とおくと、これらは

$$B(\epsilon)=H(\rho), 1>\forall\epsilon\geqq 0$$
$$B_e(r)=\sup_{s\geqq 1}\frac{r+\psi(s)}{1-s}$$

と計算できる [15] ~ [17]。また、$\mathcal{F}_2$ に注目した場合についても同様の式が成り立つ。

## 6. 量子通信路 Resolvability

最後に入力系である確率分布に従う乱数を発生させた場合に出力系での量子状態を入力系で一様乱数を発生させて得られる出力系での量子状態で近似する問題を考える。この問題の古典版は通信路 Resolvability とよばれ、Ahlswede & Dueck [18] により提案された同定符号という問題の限界を与える過程で Han & Verdu [19] により提案された。同じように、古典-量子通信路を用いて出力系の量子状態を近似する問題を量子通信路 Resolvability とよぶことにする。この量子通信路 Resolvability は同じように量子通信路の同定符号 [20] を扱うために有効となるが、次の節で述べる盗聴者が存在する場合での通信を考える上でも基礎になる問題となる。量子通信路 Resolvability は次のように定式化できる。はじめに古典-量子通信路 $\rho_\cdot:\mathcal{X}\to\mathcal{S}(\mathcal{H})$ と量子状態 $\overline{\rho}_p$ を考える。そしてサイズが $M$ の一様分布を考え、これを $\{1,\ldots,M\}$ からアルファベットの集合 $\mathcal{X}$ 上の写像 $\varphi$ を用いて変換し、そのときの古典-量子通信路 $\rho_\cdot$ による出力系での状態 $\rho_\varphi\stackrel{\text{def}}{=}\frac{1}{M}\sum_{j=1}^M\rho_{\varphi(j)}$ を十分に量子状態 $\overline{\rho}_p$ に近似させるにはサイズ $M$ はどれだけ必要であるかという問題を考える。近似の度合はトレースノルム $\|\rho_\varphi-\overline{\rho}_p\|_1$ を用いて評価することにする。なぜならトレースノルムは 2 つの状態の識別できる度合を表す量であるからである。もちろん、$M$ を大きくすれば、$\rho_\varphi$ が十分 $\overline{\rho}_p$ に近い $\phi$ を作ることは可能であるがここでは、出来る限り $M$ を小さくしたいというわけである。さらに、この問題では入力系での分布 $p_\phi(x)=\#\{\phi^{-1}\{x\}\}/M$ が $p$ に似ていなくても、$\rho_\cdot$ が受けるノイズを利用することで $\overline{\rho}_{p_M}$ を $\overline{\rho}_p$ に近似することができることがポイントである。この問題では我々のプロトコルは $\Phi\stackrel{\text{def}}{=}(M,\varphi)$ を用いて表され、その性能は $M=|\Phi|$ と $\varepsilon[\Phi]\stackrel{\text{def}}{=}\left\|\left(\frac{1}{M}\sum_{j=1}^M\rho_{\varphi(j)}\right)-\overline{\rho}_p\right\|_1$ を用いて表すことができる。そして、以下の条件を満たす $\{1,\ldots,M\}$ から $\mathcal{X}$ への写像 $\varphi$ が存在する。

$$\left\|\left(\frac{1}{M}\sum_{i=1}^M\rho_{\varphi(i)}\right)-\overline{\rho}_p\right\|_1$$
$$\leqq 4\sqrt{\sum_x p(x)\,\mathrm{Tr}\,\rho_x\{\mathcal{E}_{\overline{\rho}_p}(\rho_x)-C\overline{\rho}_p\geqq 0\}}+\sqrt{\frac{Cv}{M}}.$$

ただし $v$ は $\overline{\rho}_p$ の固有値の数である。ここで $\mathcal{E}_{\overline{\rho}_p}(\rho_x)$ は $\overline{\rho}_p$ のスペクトル分解を $\overline{\rho}_p=\sum_i s_iE_i$ としたとき、$\sum_i E_i\rho_xE_i$ で与えられる。さらに、$s\leqq 0$ に対して以下が成り立つ。

$$\sum_x p(x)\,\mathrm{Tr}\,\rho_x\{\mathcal{E}_{\overline{\rho}_p}(\rho_x)-C\overline{\rho}_p\geqq 0\}\leqq C^s\exp(\phi(s|\rho_\cdot,p))$$
$$\phi(s|\rho_\cdot,p)\stackrel{\text{def}}{=}\log\left(\sum_x p(x)\,\mathrm{Tr}\,\rho_x^{1-s}\overline{\rho}_p^s\right)$$

そして $\rho_\cdot$ の $n$ 次の定常無記憶通信路 $\rho_\cdot^{(n)}$ を用いて $\overline{\rho}_p^{\otimes n}$ を近似するプロトコルを $\Phi^{(n)}$ としたとき、その漸近的な限界は

$$C(\rho_\cdot,\overline{\rho}_p)\stackrel{\text{def}}{=}\inf_{\{\Phi^{(n)}\}}\left\{\overline{\lim}\,\frac{1}{n}\log|\Phi^{(n)}|\middle|\,\lim\varepsilon[\Phi^{(n)}]=0\right\}$$

で与えられ、$C(\rho_\cdot,\overline{\rho}_p)$ は以下の式を満たす。

$$C(\rho_\cdot,\overline{\rho}_p)\leqq I(p,\rho_\cdot)$$

## 7. 他の問題への応用

量子系を用いて安全に秘密鍵を配布するプロトコルとして、BB84 プロトコル [21] が知られている。既に、このプロトコルを実現した実験は数多くなされ [22], [23]、最近ではファイバーを用いることで、100km を超える伝送に成功し [24], [25]、実用化に近付きつつある。しかし、最初の BB84 の論文では、通信路の途中でノイズが無いことを仮定していたが、現実のこれらの通信では一定のノイズは不可避である。しかも、このようなノイズがあると、盗聴者はノイズに隠れて、一定の情報を秘密裏に得ることができる。このような状況を考えると、盗聴者が一定の情報を得ていることを承知の上で、情報のやりとりをする必要がある。

このような問題設定は wire-tapp 通信路とよばれ、古典系の場合には Wyner [26] によって始めて考えられ、その量子系への拡張 (量子 wire-tapp 通信路) は Devetak [27] によってなされた。すなわち、盗聴者が存在する場合に、盗聴者にはほとんど情報が洩れず、正規受信者に、正確に情報を送るプロトコルでの通信速度の限界について考えることになる。この問題設定は、BB84 プロトコルそのものとは異なるが、これと類似の問題を扱うことがノイズのある場合での BB84 の安全性の証明に繋がる。

実はこの問題は量子通信路符号化と量子 Resovability を組み合わせることでできることが知られており、この問題を考えるにおいても両者の基礎となる仮説検定の重要性が理解できる。さらに、秘密分散 [28], [29] の量子版である量子秘密分散 [30], [31] を考えることも可能であり、それはここで述べた量子 wire-tapp 通信路の延長で捉えることが可能である [1]。その他、量子状態そのものをノイズから守って伝送する問題でも、その漸近的な限界を達成する符号は量子 wire-tapp 通信路における符号から構成できる [27]。

## 8. ま と め

このように量子情報理論の様々なテーマを漸近論の枠組で紹介した。この議論の導出には記号 $\{\rho - e^a\sigma \geqq 0\}$ が重要な役割を果たす。この記号を用いた評価を非漸近的に導くことで、これらの問題は量子仮説検定に帰着できる。同様に、この記号を用いた評価から一般情報源での結果を導出することも可能である。

なお、この講演の内容は電気通信大学の長岡浩司助教授、東京大学の小川朋宏助手との共同研究による成果を含んでいる。

## 文 献


[1] 林 正人, 量子情報理論入門, サイエンス社から出版予定.

[2] 韓太舜, 情報理論における情報スペクトル的方法, 培風館, (1998); English translation: *Information-Spectrum Methods in Information Theory*, (Springer-Verlag, New York, 2002).

[3] F. Hiai and D. Petz, "The proper formula for relative entropy and its asymptotics in quantum probability," *Commun. Math. Phys.*, **143**, 99-114 (1991).

[4] T. Ogawa and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing," *IEEE Trans. Inform. Theory*, **46**, 2428-2433 (2000);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/9906090 (1999).

[5] T. Ogawa and M. Hayashi, "On Error Exponents in Quantum Hypothesis Testing,"
LANL E-print http://xxx.lanl.gov/abs/quant-ph/0206151 (2002).

[6] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inform. Theory*, **IT-44**, 269 (1998);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/9611023 (1996).

[7] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A* **56**, 131 (1997).

[8] T. Ogawa and H. Nagaoka, "Strong converse to the quantum channel coding theorem," *IEEE Trans. Inform. Theory*, **45**, 2486-2489 (1999);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/9808063 (1998).

[9] A. Winter, "Coding Theorems of Quantum Information Theory," Ph.D. dissertation, Uni Bielefeld (2000);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/9907077 (1999).

[10] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inform. Theory*, **49**, 1753-1768 (2003);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/0206186 (2002).

[11] "Exponents of quantum fixed-length pure state source coding," *Phys. Rev. A*, **66**, 032321 (2002);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/0202002 (2002).

[12] B. Schumacher, "Quantum coding," *Phys. Rev. A* **51**, 2738-2747 (1995).

[13] M. A. Nielsen, "Conditions for a Class of Entanglement Transformations," *Phys. Rev. Lett.*, **83**, 436, (1999);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/9811053 (1998).

[14] H.-K. Lo and S. Popescu, "Concentrating entanglement by local actions: Beyond mean values," *Phys. Rev. A* **63**, 022301 (2001);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/9707038 (1997).

[15] M. Hayashi, "General formulas for fixed-length quantum entanglement concentration,"
LANL E-print http://xxx.lanl.gov/abs/quant-ph/0206187 (2002).

[16] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher "Concentrating partial entanglement by local operations," *Phys. Rev.* A **53**, 2046, (1996);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/9511030 (1995).

[17] M. Hayashi, M. Koashi, K. Matsumoto, F. Morikoshi and A. Winter, "Error exponents for entangle concentration," *J. Phys. A: Math. and Gen.* **36** 527-553 (2003);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/0206097 (2002).

[18] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Trans. Info. Theor.*, **35**, 15-29 (1989).

[19] T.S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inform. Theory*, **39**, 752–772 (1993).

[20] R. Ahlswede and A. Winter, " Strong Converse for Identification via Quantum Channels," *IEEE Trans. Info. Theor.*, **48**, 569-579 (2002);
LANL E-print http://xxx.lanl.gov/abs/quant-ph/0012127 (2000).

[21] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, (Bangalore, India), pp. 175179, (1984).

[22] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," *New Journal of Physics*, **4**, 41.1-41.8 (2002).

[23] E. Klarreich, "Quantum cryptography: Can you keep a secret?" *Nature*, **418**, 270 - 272 18 Jul (2002).

[24] H. Kosaka, A. Tomita, Y. Nambu, N. Kimura, and K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector," *Electron. Lett.* **39**, No. 16, 1199-1201 (2003).

[25] A. Shields ,et al., "Conference on Lasers and Electro-Optics (CLEO)," Baltimore, US, 5 June (2003)

[26] A. D. Wyner, "The wire-tap channel," *Bell. Sys. Tech. Jour.*, **54**, 1355-1387, (1975).

[27] I. Devetak, "The private classical information capacity and quantum information capacity of a quantum channel," LANL E-print http://xxx.lanl.gov/abs/quant-ph/0304127 (2003).

[28] G. Blakely, "Safeguarding cryptographic keys," *Proc. AFIPS* **48**, 313 (1979).

[29] A. Shamir, "How to share a secret," *Communications of the ACM*, **22**, 612 (1979).

[30] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.* **82**, 648 (1999); LANL E-print http://xxx.lanl.gov/abs/quant-ph/9901025 (1999).

[31] D. Gottesman, "On the Theory of Quantum Secret Sharing," *Phys. Rev. A* **61**, 042311 (2000); LANL E-print http://xxx.lanl.gov/abs/quant-ph/9910067 (1999).