量子情報理論とその難しさ —より多くの人に知ってもらうために—

Quantum Information Theory and Its Difficulty
—For Broad Understanding—

林 正人 Masahito HAYASHI

アブストラクト

近年の電子情報通信に関するデバイス技術の進化にしたがって、物理層の奥深くまで踏み込んだ情報処理が可能になりつつある。このような事情から、究極の情報処理理論として量子情報理論が定式化され、様々なバックグラウンドを持った研究者の努力により急激に進展した。しかしながら、量子情報理論では、これまでブラックボックスとして扱っていた部分に踏み込んで情報処理理論を展開するので、基本的概念の理解のレベルでさえ様々な参入障壁がある。本稿では、これらの障壁を取り除くため、初学者が誤解しやすい点や概念に重点を絞って解説する。例えば、波動関数と密度行列の違い、物理量と POVM、状態複製と状態準備の違いなどについて丁寧に触れる。同時に、量子情報理論の最近の研究動向を解説する。具体的には状態識別、量子通信路符号化、量子鍵配送などの最新に成果にも触れる。

キーワード 密度行列, POVM, 偏光, qubit, コピー不可能性, 状態識別, 量子鍵配送

1. はじめに

最近、量子情報理論に興味があるのであるが、難しくてよく分からないので、なかなか勉強できないという話をよく耳にするようになった。確かに、量子情報理論は専門外の方にはいると難しい部分がある。一つには、量子情報理論を習得するには量子力学の知識とシャノン理論を含む情報理論の知識が必要となる点である。これらを完全に理解するのは大変かもしれない。また、量子情報理論の研究会に行くと、様々なバックグラウンドの研究者がいて、人によって言っていること、使っている言葉が異なり、「分かりにくい」かもしれない。

学部時代に、量子力学のさわりを講義で教わったが、不確定性という言葉が出てきて、量子力学には「よく分からない」という印象だけが残っているのではないだろうか？一方で、量子情報理論で出てくる量子に関する内容と学部の量子力学講義で出てくる内容に微妙な相違があることに気が付いて、混乱してしまう方もいるのではないだろうか？

事実、量子情報理論は、単純な量子力学と情報理論の組合せだけではないため、単純に両者の知識を組合せれば理解できるという内容ではない。従来の情報理論では物理層の奥深くの量子力学的現象には一切触れずに、その上位の階層のみに注目することで、古典力学的世界観が成立する世界でのみ情報処理を考え、古典力学的記述が成立する素子の組合せで情報処理の理論を組み立てていた。

しかし、量子情報理論では、図 1 で示すように、逆に積極的に物理層の奥深くに入り込み、古典力学的世界観が成立しない世界で、情報処理を考えることになる。そもそも、情報処理とは確定している情報を基礎に行うものである。波束の干渉効果があり、不確定性原理が成り立つ世界で、情報処理を考えること自体が矛盾しているようにも見える。この矛盾を避けるためには、注意深く個々の概念を扱う必要があり、これまでの古典力学的世界観に基づいた情報理論では生じなかった問題が多数生じる。とにかく、このような概念的難しさが量子情報理論への新規参入者の参入を難しくしているようである。量子情報理論ではこれまでふたをしていた物理層の奥深くにある量子力学的世界と向き合って情報を扱うことになるので、従来問題にならなかった概念を扱うことになり、それなりの覚悟が必要となる。

このような現状を踏まえ、今回の原稿では、あえて量子情報理論の難しさを前提にして、初学者が混乱しやすいところに重点を置きながら、量子情報の基本概念を解説する。同時に、量子情報理論の幾つかの基本テーマについて解説する。量子情報については幾つかのテキストが出版されているものの⁽¹⁾⁻⁽⁷⁾、研究の進展が日進月歩であることもあり、最新の研究動向はこれらのテキストでは十分扱えていないので、本稿ではこのような最新の研究動向についても触れる。

始めに、2. では量子情報処理が現在の情報処理の枠組みといかに異なっているか説明する。そして、3. では偏光と量子系との関係について述べる。次に 4. では量子系での状態と測定の定式化を与え、状態が密度行列で与えられることを説明する。5. では、合成系について扱い、6. では、物理量と測定概念である POVM との関係について述べる。7. では、シュレーディン

林 正人 正員 東北大学大学院情報科学研究科
E-mail hayashi@math.is.tohoku.ac.jp
Masahito HAYASHI, Member (Graduate School of Information Sciences, Tohoku University, Sendai-shi, 980-8579 Japan).
Fundamentals Review Vol.3 No.1 pp.44-56 2009 年 7 月

図1 量子情報では従来の古典的通信路の内部構造まで最適化の対象とする。

ガー描像とハイゼンベルグ描像の関係を扱い、8. では、ハミルトニアン役割について述べる。9. では、量子系での状態変化の定式化を与える。10. では、量子情報で有効な手法である群の対称性を用いて、二つの純粋状態を識別する問題を扱う。11. では、複数の状態が準備された設定での量子状態の統計的推測を扱う。12. では、量子系では無限次元系を扱う必要性が生じることを述べる。13. では、ノイズのある量子通信路を用いて、情報を送る問題について触れる。14. では、量子暗号の中の一つのテーマである量子鍵配送について触れる。

2. 量子コンピュータができないと量子情報処理ができない？

現在の情報処理は、コンピュータ上で処理されている。同様に量子情報処理も、量子コンピュータ上で処理されるはずであるので、量子コンピュータが実現されない限り、量子情報処理は実現できないのではないかな？

この問題に答えるために、量子情報処理の枠組みについて触れたい。量子情報処理とは量子力学的な素子を直接操作するタイプの情報処理である。その一つに、量子素子を用いて演算を行う量子コンピュータが挙げられる。現在のコンピュータに置き換わる量子コンピュータを実現するには、極めて大きなサイズの量子素子のコヒーレンスを保持することが求められる。これは技術的に極めて困難なことである。しかし、量子情報処理は上記で述べたように、直接ハードウェア内部の測定装置の設計までを情報処理の枠組みでとらえる。そのため、量子情報処理には現在の情報処理との単純なアナロジーではとらえきれない部分が多い。少なくとも、

（量子情報処理） （量子コンピュータ上の情報処理）

であることには注意してもらいたい。

例えば、後に述べる量子暗号（量子鍵配送）では、通信路を量子的なものに置き換えることで、これまでの通信の形態ではできなかったことを実現する。また、量子暗号では量子的な装置の不完全性を、現在のコンピュータによる情報処理によって補う形になっている。14. で述べるように、既にフィールドテストも行われ、実用に向けた段階に入りつつある。また、量子通信の長距離化に向けて不可欠な量子中継器では、小規模な量子演算を行うことになっている。したがって、量子中継器は小形量子コンピュータと言えなくもない。

これらの技術の先に現在のコンピュータに置き換わるようなタイプの量子コンピュータがあるのが妥当であろう。ただ、量子情報処理は、現在の情報処理と守備範囲が異なり、現在の情報処理と異なるパラダイムでとらえる必要がある。ゆえに、

現在の情報処理と同じ目線で量子情報処理をとらえると、その能力を誤って評価する危険がある。一方で、異なるパラダイムの上に立脚する量子情報の研究では、情報処理そのものを基礎から問い直すことが可能である。そのため、現在の情報科学の基礎を振り返る上でも、量子情報の成果は大変意義深いものがある。

3. 量子系と光の偏光

量子系を扱うには最初に系を表す複素ベクトル空間 $\mathcal{H}$ を考える。 $\mathcal{H}$ は有限次元の場合もあるが、無限次元の場合もある。無限次元の場合はエルミート内積に基づいて空間を定義するので $\mathcal{H}$ は ヒルベルト 空間になる。それゆえ、以下では有限次元の場合も含み、エルミート内積が定義された、複素ベクトル空間 $\mathcal{H}$ を ヒルベルト 空間と呼ぶ。特に、 $\mathcal{H}$ が二次元空間 $\mathbb{C}^2$ の場合は qubit と呼ばれ、量子情報で非常によく用いられる。特に光の波の向きを表す偏光からなる量子系は二次元の ヒルベルト 空間で記述される。

量子力学では 状態は 波動関数と呼ばれる $\mathcal{H}$ のノルム (長さ)1 のベクトル $|\phi\rangle$ で与えられる。また、 $|\phi\rangle$ に対して、スカラー $e^{i\theta}$ を掛けたベクトル $e^{i\theta}|\phi\rangle$ は $|\phi\rangle$ と同じ状態を表していると考ええる。

光の偏光状態には図2にあるように、垂直偏光、水平偏光、45°偏光、135°偏光などがある。垂直偏光をベクトル $|V\rangle$ 、水平偏光をベクトル $|H\rangle$ で表すと、45°偏光、135°偏光はそれぞれ、ベクトル $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ とベクトル $\frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ で表される。ここで、 $\{|V\rangle, |H\rangle\}$ は二次元のヒルベルト空間 $\mathbb{C}^2$ の正規直交基底とする。一般には、角度 θ の偏光は $\cos\theta|H\rangle + \sin\theta|V\rangle$ で与えられる。

ここで一つ疑問が沸く。 $\mathbb{C}^2$ の要素は複素係数も許すはずである。したがって、ノルム1のベクトルは、一般に $e^{i\theta}\cos\theta|H\rangle + e^{i\theta'}\sin\theta|V\rangle$ と書ける。スカラー $e^{i\theta}$ を掛けたベクトルは同じ状態を表すので、 $|H\rangle$ の係数を正の実数とする

図2 光の偏光状態1

図3 光の偏光状態2

表示を用いると、一般には $\cos\theta|H\rangle + e^{i(\theta'-\theta)}\sin\theta|V\rangle$ と書ける。これまで与えた偏光の向きだけでは、 $e^{i(\theta'-\theta)}$ が ± 1 以外にはなり得ない。 $\sin\theta|V\rangle$ の係数が ± 1 以外の一般の複素数となる光の偏光はないのであろうか？実は、偏光がクルクルと回っている状態もあるのである。右回り偏光と左回りの偏光があり、それぞれが、 $\frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle)$ に対応する(図3)。右回りと左回りのどちらが $\frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ に対応するかについては、文献によって異なるので注意を要する。このように偏光の回転を考慮に入れると、光の偏光は二次元の量子系 $\mathbb{C}^2$ すなわち qubit 系で記述できる。

4. なぜ密度行列なのか？

量子力学では $\mathcal{H} = \mathbb{C}^d$ であるとき、 $d \times d$ のエルミート行列を物理量と呼ぶ^{注1)}。一方、前の章では、量子系の状態は量子系を表すヒルベルト空間 $\mathcal{H}$ のノルム1の要素と与えられると述べた。しかし、量子情報では $d \times d$ の半正定値エルミート行列でそのトレースが1となるものを密度行列と呼び、これが状態を表していると考えられる。

この状態の意味をはっきりさせるために、測定を記述する概念を導入しよう。量子情報では $d \times d$ の半正定値エルミート行列の組 $\{M_i\}_{i \in I}$ で $\sum_{i \in I} M_i$ が単位行列となるものを POVM(Positive Operator Valued Measure) と呼び、量子情報理論ではこれが測定を記述していると考えられる。ここで、注意すべきことは、行列の集まり $\{M_i\}_{i \in I}$ が一つの測定を表しているわけで、個々の M_i が測定を表しているわけではない。集合 I がその測定の測定値の集合を表し、それぞれの i が測定値に対応する。

それでは、これらがどういう意味で、状態と測定を表しているのだろうか？系の状態が密度行列 ρ で与えられ、POVM $\{M_i\}_{i \in I}$ に対応する測定を行った場合を考えよう。このとき、測定値 i が得られる確率 $P(i)$ は $\text{Tr} M_i \rho$ で与えられる。このようにして定義される確率空間 I 上の確率分布 P が確率の公理を満たすことは、密度行列と POVM の定義から容易に確認できる。この議論は POVM $\{M_i\}_{i \in I}$ に対応する測定を行ったときの測定値の出現確率を与えている。後に正確に述べるように、この意味ですべての測定に対応する POVM が存在する。ここで一つの疑問が湧く。先にも述べたように量子力学のテキストでは、量子状態は波動関数で与えられるのが普通であるの

に、なぜ密度行列なのか？

この疑問に答えるため、若干の記法を導入しよう。まず、異なる二つの波動関数 ϕ, ψ の内積を $\langle \psi | \phi \rangle$ と記す。ここで、 $\langle \psi |$ は $\mathcal{H}$ の内積の下での $\mathcal{H}$ の双対空間の要素とみなすことができるので、写像 $|\phi'\rangle \in \mathcal{H} \mapsto (\langle \psi | \phi' \rangle) |\phi\rangle$ を $|\phi\rangle\langle \psi|$ と記す。なお、エルミート行列 A に対して、 $\langle A \psi | \phi \rangle = \langle \psi | A \phi \rangle$ となるので、これらの値を $\langle \psi | A | \phi \rangle$ と記すが、この記号を用いると、 $\text{Tr} A |\phi\rangle\langle \psi|$ と同等になる。

このような表記を量子論では Braket と呼ぶが、波動関数 ϕ に対して、 $|\phi\rangle\langle \phi|$ は一次元の射影になり、密度行列になる。したがって、対応 $\phi \mapsto |\phi\rangle\langle \phi|$ の下で、波動関数 ϕ も状態とみなすことができる。しかし、波動関数を用いて記述できる密度行列は密度行列の一部にすぎない。これは波動関数を用いても記述できない状態があるということを意味する。波動関数で記述できない状態とはどのような状態だろうか？例えば、 $\mathcal{H}$ が二次元空間 $\mathbb{C}^2$ である場合に、二つの互いに直交する波動関数 $|0\rangle, |1\rangle$ を考えよう。 p を $0 < p < 1$ を満たす実数とすると、 $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ も密度行列となる。この状態は正規直交基底 $\{|0\rangle, |1\rangle\}$ の下で行列表示すると、

$$\begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix} \quad (1)$$

となる。しかし、これは一次元の射影ではないので波動関数では記述できない。この状態は、状態 $|0\rangle\langle 0|$ と状態 $|1\rangle\langle 1|$ を比率 $p:1-p$ で混ぜ合わせたものである。それでは、重ね合わせ状態 $\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle$ とはどのように異なるのであろうか？(ここで、ノルムが1になるために、係数 $\sqrt{p}, \sqrt{1-p}$ が平方根となっていることに注意。) 重ね合わせ状態 $\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle$ を密度行列で表すと、 $(\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle)(\sqrt{p}\langle 0| + \sqrt{1-p}\langle 1|) = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| + \sqrt{p(1-p)}(|0\rangle\langle 1| + |1\rangle\langle 0|)$ となる。行列表示の下では

$$\begin{pmatrix} p & \sqrt{p(1-p)} \\ \sqrt{p(1-p)} & 1-p \end{pmatrix} \quad (2)$$

となる。したがって、 $\sqrt{p(1-p)}(|0\rangle\langle 1| + |1\rangle\langle 0|)$ が差となる。この部分は基底 $|0\rangle, |1\rangle$ の下で行列表示した場合、非対角成分に対応する。POVM $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ で測定した場合、二つの状態 $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ と $(\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle)(\sqrt{p}\langle 0| + \sqrt{1-p}\langle 1|)$ の間で差は生じない。ここで、 $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ を用いて、POVM $\{E_+, E_-\}$ を以下で定義しよう。

$$E_+ := |+\rangle\langle +| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$E_- := |-\rangle\langle -| = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

すると、POVM $\{E_+, E_-\}$ の下では、状態が (1) である場合と状態が (2) である場合を比較すると、測定値 $+$ が得られる確率は異なる。例えば、状態が (1) である場合、 $+$ を検出する確率は

(注1): 一般には物理量 A は $\mathcal{H}$ から $\mathcal{H}$ への線形写像 A で自己共役なものとして定義される。

$$\begin{aligned}
& \text{Tr } E_+(p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|) \\
&= \text{Tr} \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix} \\
&= \frac{p}{2} + \frac{1-p}{2} = \frac{1}{2}
\end{aligned}$$

となる．一方，状態が (2) である場合，+ を検出する確率は

$$\begin{aligned}
& \text{Tr } E_+(\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle)(\sqrt{p}\langle 0| + \sqrt{1-p}\langle 1|) \\
&= |\langle + | (\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle)|^2 \\
&= \left| \sqrt{\frac{p}{2}} + \sqrt{\frac{1-p}{2}} \right|^2 = \frac{1}{2} + \frac{\sqrt{p(1-p)}}{2}
\end{aligned}$$

となる．したがって，これらの状態の間で，+ の検出確率が異なる．このように，状態 (1) と状態 (2) は異なるので注意を要する．

なお，波動関数では，状態 $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ のように，一定の比率で異なる二つの状態を混ぜ合わせた状態は記述できない．このように波動関数で得られる状態のことを純粋状態と呼ぶ．また，対象となる系がノイズを含んでいる場合，必然的に複数の状態を混ぜ合わせた状態にならざるを得ない．このように，一つの波動関数だけで記述できない状態のことを混合状態と呼ぶ．情報処理を考える上では，不可避な量子論的なノイズを記述する必要がある，そのためには，密度行列によって状態を記述する必要がある．

ここで新たな疑問が沸く．上述のような物理系のノイズを含めて系の状態を記述するには，波動関数についての確率分布を考えれば十分記述できるのではないか？確かに波動関数についての確率分布を用いれば，このようなノイズを記述できるが，以下に述べるように，不必要な意味のない混乱の原因となる情報を含んでしまい適切ではない．

それでは，比率 $\frac{1}{2} : \frac{1}{2}$ で状態 $|0\rangle\langle 0|$ と状態 $|1\rangle\langle 1|$ を混ぜ合わせた状態 $\rho_{\text{mix}} := \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ を考えよう．ここで，比率 $\frac{1}{2} : \frac{1}{2}$ で状態 $|+\rangle\langle +|$ と状態 $|-\rangle\langle -|$ を混ぜ合わせた状態 $\frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$ を考えよう．実は

$$\frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$

となり，両者は一致する．すなわち，両者を共に密度行列で記述すると一致してしまい，両者を測定によって識別する方法は存在しない．したがって，上記の状態はどの波動関数を等確率で混ぜ合わせたものであるか判定することはできない．あくまでも，我々の能力で判定できるのは，状態がどの密度行列で記述できるかという情報だけである．したがって，密度行列以上の情報は操作的には意味がないので，量子情報では状態を波動関数の確率的な混ぜ合わせとして記述することはしない．

5. なぜ合成系はテンソル積なのか

二つの量子系 $\mathcal{H}$ と $\mathcal{K}$ を考えよう．この二つの系からなる合成系はテンソル積空間 $\mathcal{H} \otimes \mathcal{K}$ となる．テンソル積空間 $\mathcal{H} \otimes \mathcal{K}$ は $\mathcal{H}$ と $\mathcal{K}$ のそれぞれの正規直交基底を $\{|v_i\rangle\}_{i=1}^k$ と $\{|u_j\rangle\}_{j=1}^l$

とすると， $\{|v_i, u_j\rangle\}_{1 \leq i \leq k, 1 \leq j \leq l}$ が正規直交基底となる空間である．時々，直和空間 $\mathcal{H} \oplus \mathcal{K}$ が合成系を表すと考えがちであるが，合成系を表すのはテンソル積空間 $\mathcal{H} \otimes \mathcal{K}$ である．直和空間 $\mathcal{H} \oplus \mathcal{K}$ では正規直交基底が $\{|v_i\rangle\}_{i=1}^k \cup \{|u_j\rangle\}_{j=1}^l$ となる．古典的な場合，合成系の状態はそれぞれの系の状態が個別に定まる．したがって，古典系な場合が基底に対応すると考えると，合成系の基底は $\{|v_i\rangle\}_{i=1}^k \cup \{|u_j\rangle\}_{j=1}^l$ ではなく， $\{|v_i, u_j\rangle\}_{1 \leq i \leq k, 1 \leq j \leq l}$ となる．それゆえ，合成系はテンソル積空間 $\mathcal{H} \otimes \mathcal{K}$ になる．

次に系 $\mathcal{H}$ と系 $\mathcal{K}$ に独立に状態 ρ と σ が準備された場合を考えよう．この場合， $\rho = \sum_{i,i'=1}^k a_{i,i'} |v_i\rangle\langle v_{i'}|$ ， $\sigma = \sum_{j,j'=1}^l b_{j,j'} |u_j\rangle\langle u_{j'}|$ であるとする，合成系上の状態は $\rho \otimes \sigma := \sum_{i,i'=1}^k \sum_{j,j'=1}^l a_{i,i'} b_{j,j'} |v_i, u_j\rangle\langle v_{i'}, u_{j'}|$ で与えられる．以下，議論を簡単にするために，これらが共に対角の場合 $\rho = \sum_{i=1}^k a_i |v_i\rangle\langle v_i|$ ， $\sigma = \sum_{j=1}^l b_j |u_j\rangle\langle u_j|$ について考えよう．この場合， $\rho \otimes \sigma = \sum_{i=1}^k \sum_{j=1}^l a_i b_j |v_i, u_j\rangle\langle v_i, u_j|$ となり，古典的に見ると，事象 (v_i, u_j) が確率 $a_i b_j$ で起きるということを意味している．したがって，古典的な場合の独立性と矛盾しない．このような事情から，量子系では独立に状態が準備された場合，状態はテンソル積状態になる．

ここで，波動関数 $|v\rangle = \sum_{i=1}^k c_i |v_i\rangle$ ， $|u\rangle = \sum_{j=1}^l f_j |u_j\rangle$ のテンソル積 $|v\rangle \otimes |u\rangle = \sum_{i=1}^k \sum_{j=1}^l c_i f_j |v_i, u_j\rangle$ が基底の取り方に依存しないことを注意しておく必要がある．この事実を確認するには，異なる $\mathcal{H}$ と $\mathcal{K}$ の正規直交基底 $\{|\tilde{v}_i\rangle\}_{i=1}^k$ と $\{|\tilde{u}_j\rangle\}_{j=1}^l$ に基づいた定義したテンソル積が $|v\rangle \otimes |u\rangle = \sum_{i=1}^k \sum_{j=1}^l c_i f_j |v_i, u_j\rangle$ に一致することを示せば十分である．波動関数 $|v\rangle$ ， $|u\rangle$ が $|v\rangle = \sum_{s=1}^k \tilde{c}_s |\tilde{v}_s\rangle$ ， $|u\rangle = \sum_{t=1}^l \tilde{f}_t |\tilde{u}_t\rangle$ と記述できるとき， $\{|\tilde{v}_s\rangle\}_{s=1}^k$ と $\{|\tilde{u}_t\rangle\}_{t=1}^l$ に基づいた定義した場合のテンソル積は $\sum_{s,t} \tilde{c}_s \tilde{f}_t |\tilde{v}_s, \tilde{u}_t\rangle$ である．ユニタリ行列 U, V が $|\tilde{v}_s\rangle = \sum_i V_{s,i} |v_i\rangle$ ， $|\tilde{u}_t\rangle = \sum_j U_{t,j} |u_j\rangle$ を満たすすると， $c_s = \sum_i \tilde{c}_s V_{s,i}$ ， $f_t = \sum_j \tilde{f}_t U_{t,j}$ となる．よって，

$$\begin{aligned}
& \sum_{s,t} \tilde{c}_s \tilde{f}_t |\tilde{v}_s, \tilde{u}_t\rangle \\
&= \sum_{s,t,i,j} \tilde{c}_s \tilde{f}_t V_{s,i} U_{t,j} |v_i, u_j\rangle \\
&= \sum_{i,j} c_i f_j |v_i, u_j\rangle
\end{aligned}$$

を得る．したがって， $\mathcal{H}$ 上の行列 A と $\mathcal{K}$ 上の行列 B のテンソル積についても，

$$A \otimes B(|v\rangle \otimes |u\rangle) := (A|v\rangle) \otimes (B|u\rangle) \quad (3)$$

と定義することで，合成系 $\mathcal{H} \otimes \mathcal{K}$ 上の線形写像として定義される．なお， $|v\rangle$ と $|u\rangle$ のテンソル積が基底の取り方に依存しないので，写像 $A \otimes B$ の定義も基底の取り方に依存しない．したがって，密度行列 $\rho = \sum_{i,i'=1}^k a_{i,i'} |v_i\rangle\langle v_{i'}|$ ， $\sigma = \sum_{j,j'=1}^l b_{j,j'} |u_j\rangle\langle u_{j'}|$ のテンソル積状態 $\rho \otimes \sigma$ は基底の取り方に依存せずに定義でき， $\sum_{i,i'=1}^k \sum_{j,j'=1}^l a_{i,i'} b_{j,j'} |v_i, u_j\rangle\langle v_{i'}, u_{j'}|$ で与えられる．なお，合成系 $\mathcal{H} \otimes \mathcal{K}$ 上の状態は上記のようにテンソル積で与えられる状態 $\rho \otimes \sigma$ (テンソル積状態) やその凸結合 $\sum_i p_i \rho_i \otimes \sigma_i$ で記述できる状態 (セパラブル状態) だけではない (p_i は確率

を表し、 ρ_i, σ_i はそれぞれ、 $\mathcal{H}, \mathcal{K}$ 上の密度行列を表す。) 例えば、ベクトル $\sum_i \sqrt{p_i} |v_i, u_j\rangle$ で与えられる純粋状態はテンソル積状態の凸結合として表せないで、セパラブル状態ではない。そのような状態はもつれ合った(エンタングルした)状態といわれ、量子情報処理の資源として、大変盛んに研究されている。合成系 $\mathcal{H} \otimes \mathcal{K}$ 上の状態が密度行列

$$\rho = \sum_{i,i'=1}^k \sum_{j,j'=1}^l c_{i,j,i',j'} |v_i, u_j\rangle \langle v_{i'}, u_{j'}|$$

で与えられているとき、系 $\mathcal{H}$ だけに注目した場合、系 $\mathcal{H}$ 上の状態はどのように与えられるであろうか？この場合の系 $\mathcal{H}$ 上の状態は以下を満たす状態 $\text{Tr}_{\mathcal{K}} \rho$ で与えられると考えるのが妥当である。

$$\text{Tr}(\text{Tr}_{\mathcal{K}} \rho) A = \text{Tr} \rho (A \otimes I_{\mathcal{K}}).$$

状態 $\text{Tr}_{\mathcal{K}} \rho$ は以下で与えられ、 $\text{Tr}_{\mathcal{K}}$ は部分トレースと呼ばれる。

$$\text{Tr}_{\mathcal{K}} \rho = \sum_{i,i'=1}^k \sum_{j,j'=1}^l c_{i,j,i',j'} |v_i\rangle \langle v_{i'}|.$$

なお、 ρ が基底 $\{|v_i, u_j\rangle\}_{i,j}$ の下で対角である場合は、部分トレースは対角成分からなる確率分布の周辺分布と一致する。

現在の情報処理システムでは、計算機の内部のすべてのプロセスが、AND ゲートなどの幾つかの基本操作の組合せで得られることが知られている。量子情報でも、同様に基本操作がある。量子情報の場合、bit の代わりに qubit を考え、複数の qubit からなる合成系を考えることが多い。この場合、個々の qubit 上のユニタリ行列 U を以下のように施す操作は最も基本的である。

$$\rho \mapsto U \rho U^\dagger.$$

しかしながら、複数の qubit 間の相関を用いた処理には、少なくとも二つの qubit に跨る操作が必要である。最も基本的な操作は C-NOT (Controlled NOT, 制御 NOT, 図 4) ゲートと呼ばれる操作 $U_{\text{C-NOT}}$ であり、以下で与えられる。

$$U_{\text{C-NOT}} |x, y\rangle = |x, x+y\rangle$$

ここで、 $x+y$ は x と y の排他的論理和を表す。この操作と各 qubit 上のユニタリ行列の組合せで、多くの量子操作を構成できることが知られている。

図 4 C-NOT ゲート

6. なぜ測定が物理量ではなく POVM で与えられるか

なぜ、量子情報では測定は物理量ではなく POVM で与えられるのか？

この疑問も、多くの物理学者の量子情報理論への参入を阻んできた。文字どおり、物理量 (observable) は観測可能量であり、対象となる物理系 $\mathcal{H}$ 上のエルミート行列で記述できる。それではエルミート行列 A を観測すると、その測定値はどのような確率で得られるのであろうか？そのためには結局、POVM を考えることになる。行列 A はエルミートであるので、対角化が可能となる。この場合、 A の固有値を $a_1, \dots, a_k$ とすると、それぞれの固有値に対応するノルムが 1 の固有ベクトル $\phi_1, \dots, \phi_k$ がある。ここで、固有値に重複はないとすると、 A は $A = \sum_{i=1}^k a_i |\phi_i\rangle \langle \phi_i|$ と記述することができる。そして、状態の密度行列が ρ で与えられている場合、測定値 a_i が得られる確率は $\text{Tr} |\phi_i\rangle \langle \phi_i| \rho = \langle \phi_i | \rho | \phi_i \rangle$ で与えられる。すなわち、POVM $\{|\phi_i\rangle \langle \phi_i|\}_{i=1}^k$ でこれらの確率は記述できる。また、固有値 a_i に重複がある場合、固有値 a_i の固有ベクトルではなく、固有ベクトルからなる固有空間への射影 E_i を考える。そして、その射影を用いて、 A は $A = \sum_{i=1}^k a_i E_i$ と記述できる。すなわち、測定は POVM $\{E_i\}_{i=1}^k$ で記述できる。このように、POVM $\{M_i\}_{i=1}^k$ のうち、 M_i が射影となるものは数列 $\{a_i\}_{i=1}^k$ を適当に選ぶことで、物理量 $\sum_{i=1}^k a_i M_i$ の測定を表しているとみなすことができる。このような射影性を満たす POVM を PVM (Projection Valued Measure) と呼ぶ。しかし、PVM でない POVM は、物理量に対応させることができない。事実、射影性を満たさない測定は以下のように存在する。今ここで、測定 $\{E_+, E_-\}$ を行おうとしよう。

しかし、測定器の不備により、確率 p でその測定値が反転するとしよう。この場合、状態 ρ であるときに、測定値 $+$ が得られる確率は

$$(1-p) \text{Tr} \rho E_+ + p \text{Tr} \rho E_- = \text{Tr} \rho ((1-p) E_+ + p E_-)$$

であり、測定値 $-$ が得られる確率は

$$(1-p) \text{Tr} \rho E_- + p \text{Tr} \rho E_+ = \text{Tr} \rho ((1-p) E_- + p E_+)$$

である。したがって、

$$E'_+ := (1-p) E_+ + p E_-, \quad E'_- := (1-p) E_- + p E_+$$

と定義すると、このときに行う測定は POVM $\{E'_+, E'_-\}$ で与えられる。すなわち、このような不完全な測定も PVM でない POVM $\{E'_+, E'_-\}$ を用いることで、容易に記述できる。

一般に、測定による測定値の出現確率を記述するには、密度行列 ρ から確率空間が測定値集合となる確率分布 P_ρ を与える写像 P を与えれば十分である。この写像は、密度行列に関する凸結合を保存する。すなわち、 ρ_1, ρ_2 を二つの密度行列とすると、測定値 i の検出確率について、 $P_{\lambda \rho_1 + (1-\lambda) \rho_2}(i) = \lambda P_{\rho_1}(i) + (1-\lambda) P_{\rho_2}(i)$ となる。この性質を満たす写像 P に対して、 $P_\rho(i) = \text{Tr} \rho M_i$

図 5 Naïmark 拡張

となる POVM $\{M_i\}_{i=1}^k$ が存在することが示せる^{(2) (8)}。すなわち、どのような測定に対しても、状態が密度行列 ρ であるときの測定値 i の検出確率 P_i を $\text{Tr } \rho M_i$ で与える POVM $\{M_i\}_{i=1}^k$ が存在する。ゆえに、測定値 i の検出確率 P_i を与える必要最小限の情報が POVM であり、操作的に情報処理に必要な情報はすべて POVM で記述できる。

また、PVM でない POVM $\{M_i\}_{i=1}^k$ であっても、以下のように系を拡大することで、拡大した系の PVM を用いて表すことができる。補助系 $\mathcal{K}$ と補助系上の初期状態 ρ_0 及び合成系 $\mathcal{H} \otimes \mathcal{K}$ 上の PVM $\{E_i\}_{i=1}^k$ を POVM $\{M_i\}_{i=1}^k$ に応じて適切に選べば、任意の $\mathcal{H}$ 上の状態 ρ に対して、以下の等式が成り立つ。(図 5)

$$\text{Tr } M_i \rho = \text{Tr } E_i \rho \otimes \rho_0.$$

この式は補助系の初期状態を ρ_0 とし、合成系上で PVM $\{E_i\}_{i=1}^k$ に対応する測定を行えば、実質的に系 $\mathcal{H}$ 上での POVM $\{M_i\}_{i=1}^k$ に対応する測定が行えることを示している。そのため、任意の物理量の測定が可能であるのであれば、任意の POVM に対応する測定も原理的には可能であることになる。この拡大系での PVM を Naïmark 拡張と呼ぶ⁽⁹⁾。

それでは、物理量という表現にはどのような意味があるのだろうか？ 個々の物理量の行列の形には物理的意味がある。物理的意味とは、その物理量がその物理系で持っている意味であり、その意味を考えることで、その物理量の測定の実現方法が分かる場合が多い。例えば、その物理量が Z 軸方向のスピンという物理的意味を持っていたとすると、磁界と相互作用させればよい。このように、物理量の意味からその測定の実現方法がわかる。したがって、POVM と物理量の両者は測定を記述しているのであるが、互いに異なる測定の側面を与えている。POVM は測定を行った場合の各測定値の検出確率の計算に必要な最小限の情報を与え、物理量は測定の実現に必要な情報を与える。両者はその得意とする部分が異なるので、どのような文脈で議論しているかに応じて使い分ける必要がある。なお、ここで述べた役割分担は、量子系に限らずどこでも行われていることである。例えば、古典系では通信路は確率遷移行列で与えられる。確率遷移行列が持つ情報は、その通信路を用い、誤り訂正を組合せ

て、情報伝送する場合には大変重要な情報である。しかし、そのような確率遷移行列で与えられる通信路を設計するためには、通信路内部の力学変化にまで踏み込んだ議論が必要となる。ゆえに POVM による測定の表現は、測定を単なる情報処理プロセスとしてとらえ、測定を最適化する場合に有効となる。一般に、量子情報理論では、ここで述べた視点で扱うことが多いので、多くの場合 POVM を用いて測定が議論される。

7. ハイゼンベルグ描像とシュレーディンガー描像

量子情報ではなぜ確率変数を物理量で置き換えて量子化を考えないか？

普通、物理学の量子力学のテキストには、密度行列など現れない。テキストによっては、スカラー量である古典的な物理量を単純に作用素である量子的な物理量で量子化を与えているものもある。この事実は多くの物理学者の量子情報理論への参入を阻んできた。

物理では、状態変化を記述するシュレーディンガー描像と、物理量の時間発展を記述するハイゼンベルグ描像があり、普通これらは等価であることになっている。ハイゼンベルグ描像では、問題を量子化するときあらかじめスカラー量である古典的な物理量を考え、それを単純に作用素（または行列）に置き換えることで、量子化の操作がなされる。このような理由から物理学では、ハイゼンベルグ描像を用いることが標準になっている。古典的なニュートン力学の場合時間に応じた位置の変化を追うことが普通である。量子系の場合、位置の変化を追うことは位置を表す物理量の時間的変化を追うことにほかならない。この事実も物理学でハイゼンベルグ描像が用いられる要因となっている。これらの議論に共通していることは、物理学で扱う文脈では、あらかじめ注目する物理量が決まっていることである。

非量子的な情報理論では、情報が確率分布を記述する（連続または離散）パラメータとして与えられるので、確率分布の時間に伴う変化に注目する。量子情報の場合も同様で、情報が状態を記述する（連続または離散）パラメータとして与えられるので、状態の時間に伴う変化に注目する。そのため、状態の時間発展を考えるシュレーディンガー描像を採用することが多い。また、量子情報では、測定を表す POVM を最適化することが多い。そのため、あらかじめ特定の物理量に注目して議論することが少ないので、ハイゼンベルグ描像を用いるメリットは少ない。

8. なぜ ハミルトニアン による時間発展が余り現れないのか？

一般に物理学では系の状態がどのように時間発展するか興味がある。系の時間発展は ハミルトニアン を用いて記述できるので、ハミルトニアン に関する議論が主流になる。

一方、量子情報では系の持つ情報を扱うため系の時間発展を問題にしているかのように考えられる。しかし、系の持つ情報を

表 1 ハミルトニアンに関する役割分担

	最適な処理の探索	与えられた処理の設計
ハミルトニアンに関する議論	不要	必要

議論するには、単なる系の時間発展だけでは議論できない。むしろ、量子情報では、系の持つ情報は最適な処理を行った場合、（もしくは最適に近い処理を行った場合）どれだけ情報が手に入るによって、系の持つ情報を定義する。すなわち、操作を考え、その操作に基づいて、系の情報を定義することになる。もちろん、情報処理を行うには、その処理に応じた時間発展が必要である。すなわち、与えられた処理の実現には時間発展の議論が必要となり、ハミルトニアンに関する議論が不可欠である。しかし、第 1 段階では、どのような処理が最適であるか議論する必要があり、その段階ではハミルトニアンに関する議論が不要になる。要約すると、表 1 のような役割分担がなされている。

非量子論的な現代の通信技術では、デバイス技術と情報処理技術の住み分けがなされている。現状は、量子情報に関しては、十分にデバイス技術と情報処理技術の分業が進んでおらず、未分化の状態である。端的にいうなら、デバイス技術に対応する議論ではハミルトニアンに関する議論は不可欠であり、情報処理技術に対応する議論ではハミルトニアンに関する議論は不要となる。しかし、量子情報技術が完全に現代の情報処理技術と全く同じ分業になるとは限らない。どのような分業になるに依りては、今後の進展を待たねばならない。

9. 量子情報では なぜ時間発展の微分方程式が 現れないか？

この疑問も、上記の疑問と類似であるが、ノイズがある場合を含むので、改めて議論することにする。

ノイズや散逸のある場合の時間発展は、物理学では、物理量に関する微分形式で記述されることが多い。確かに、実際の系の状況からどのような時間発展をするか考察するには、このような議論は大変有効である。

一方、時間発展をシステムの入出力関係にとらえ、その入出力関係だけを記述するには、必ずしも微分形式で記述することが有効とは限らない。

簡単のため、古典的な系を考えよう。古典的なシステムの入出力関係は、入出力の要素の数が有限であれば、単純に確率遷移行列で記述できる。もちろん、ダイナミクスから確率遷移行列を導出するには内部の力学を記述する微分方程式は重要となる。しかし、システムの入出力を記述しそのシステムを用いてどのようなことが可能であるか議論するには、入出力関係の原因を与える微分方程式は必要ではなく、その結果のみを記述する確率遷移行列だけが重要となる。

量子系の場合、確率遷移行列の代わりに状態から状態を与える写像が与えられる。すなわち、入力系が $\mathcal{H}$ であり、出力系が $\mathcal{K}$ である場合は $\mathcal{H}$ 上の密度行列の集合 $\mathcal{S}(\mathcal{H})$ から $\mathcal{K}$ 上の密度

行列の集合 $\mathcal{S}(\mathcal{K})$ への写像 Λ で与えられる。この場合、凸結合 $\lambda\rho_1 + (1-\lambda)\rho_2$ ($0 < \lambda < 1$) の意味を考えると、自然に以下の等式が成り立つ。

$$\Lambda(\lambda\rho_1 + (1-\lambda)\rho_2) = \lambda\Lambda(\rho_1) + (1-\lambda)\Lambda(\rho_2).$$

更に、写像 Λ を $\mathcal{H}$ 上のエルミート行列の空間 $B(\mathcal{H})$ から、 $\mathcal{K}$ 上のエルミート行列の空間 $B(\mathcal{K})$ へ拡大すると、以下の線形性: $\Lambda(aA + bB) = a\Lambda(A) + b\Lambda(B)$ が成り立つことが知られている。(ここで、 a, b は任意の実数であり、 A, B は $B(\mathcal{H})$ の要素である。) しかし、単純に線形性を満たす、写像 Λ が状態変化を与えるわけでない。

少なくとも、 $\mathcal{S}(\mathcal{H})$ の要素は $\mathcal{S}(\mathcal{K})$ の要素に移らなければならない。この条件は、以下の二つの条件の組合せと同値である。正値性: $A \geq 0 \Rightarrow \Lambda(A) \geq 0$

トレース保存性: $\text{Tr } A = \text{Tr } \Lambda(A)$

しかし、この三つの条件を満たすだけでは、必ずしも状態変化とは言い切れない。この部分が量子系の難しいところである。

ここで、補助系 $\mathbb{C}^n$ を考えよう。補助系との合成系 $\mathcal{H} \otimes \mathbb{C}^n$ での状態変化を考えよう。補助系と系 $\mathcal{H}$ の間には相互作用がないとし、補助系では状態変化が起こらないとする。すると、合成系 $\mathcal{H} \otimes \mathbb{C}^n$ での状態変化は $\Lambda \otimes id_n$ で与えられる。この写像 $\Lambda \otimes id_n$ の定義は以下である。

$$\Lambda \otimes id_n (A \otimes B) := \Lambda(A) \otimes B.$$

そして、この写像 $\Lambda \otimes id_n$ も正値性を満たす必要がある。

n 正値性: $X \geq 0 \Rightarrow \Lambda \otimes id_n (X) \geq 0$. ただし、 X は $\mathcal{H} \otimes \mathbb{C}^n$ 上の行列である。

特に、任意の n について n 正値性を満たす条件を完全正値性と呼ぶ。

完全正値性: 任意の n について n 正値性が成り立つ。

これらの議論から、状態変化は線形性、完全正値性、トレース保存性を満たすことが確認できる。実は、その逆に、線形性、完全正値性、トレース保存性を満たす Λ に対応する状態変化が原理的に存在することが知られている。

この議論については、以下の Stinespring 表現から確認できる⁽¹⁰⁾。任意のトレースを保存する完全正写像 Λ に対して、以下の条件を満たす、環境系 $\mathcal{E}$ 上の初期状態 $\rho_{0,E}$ 、出力系 $\mathcal{K}$ 上の初期状態 $\rho_{0,K}$ 、合成系 $\mathcal{H} \otimes \mathcal{K} \otimes \mathcal{E}$ 上のユニタリ行列 U の組で以下を満たすものが存在する。任意の状態 $\rho \in \mathcal{S}(\mathcal{H})$ に対して、

$$\Lambda(\rho) = \text{Tr}_{\mathcal{H} \otimes \mathcal{E}} U \rho \otimes \rho_{0,E} \otimes \rho_{0,K} U^\dagger$$

が成り立つ。すなわち、以下のようなプロセスで、状態変化 Λ が実現できる。

$$\begin{aligned} \rho &\mapsto \rho \otimes \rho_{0,E} \otimes \rho_{0,K} \\ &\mapsto U \rho \otimes \rho_{0,E} \otimes \rho_{0,K} U^\dagger \\ &\mapsto \text{Tr}_{\mathcal{H} \otimes \mathcal{E}} U \rho \otimes \rho_{0,E} \otimes \rho_{0,K} U^\dagger. \end{aligned}$$

例えば、光通信の場合、光ファイバが外の物理系と相互作用がない場合、入力系 $\mathcal{H}$ 、出力系 $\mathcal{K}$ 、環境系 $\mathcal{E}$ はそれぞれ、図 6 で

図 6 光通信での Stinespring 表現

与えられる．

なお，量子情報では，しばしば，出力系以外の系を出力系とする以下の通信路 Λ_E を扱う．この通信路は盗聴があった場合での情報漏えいの評価にも用いられる．

$$\Lambda_E(\rho) := \text{Tr}_K U \rho \otimes \rho_{0,E} \otimes \rho_{0,K} U^\dagger.$$

また， Λ の入出力系が同一の場合は，Stinespring 表現は以下のように簡単化できる．すなわち，入出力系を $\mathcal{H}$ とする量子通信路 Λ に対して，以下の条件を満たす環境系 $\mathcal{E}$ ，環境系 $\mathcal{E}$ 初期状態 $\rho_{0,E}$ ，合成系 $\mathcal{H} \otimes \mathcal{E}$ 上のユニタリ行列 U の組合せで以下を満たすものが存在する．任意の状態 $\rho \in \mathcal{S}(\mathcal{H})$ に対して，

$$\Lambda(\rho) = \text{Tr}_E U \rho \otimes \rho_{0,E} U^\dagger$$

が成り立つ．

10. コピーと状態識別

量子力学系では，完全な状態のコピーはできない．もし，同一状態を完全にコピーできると，同一状態を幾らでも複製できる．そうすると，限りなく 100 % に近い確率で，状態を同定することができる．しかし，量子系では非直交なベクトル $|\phi_+\rangle, |\phi_-\rangle$ からなる状態 $|\phi_+\rangle\langle\phi_+|, |\phi_-\rangle\langle\phi_-|$ を確率 1 で識別することは以下に述べるように，不可能である．よって，完全な状態の複製は不可能である．

では状態 $|\phi_+\rangle\langle\phi_+|, |\phi_-\rangle\langle\phi_-|$ の識別がどのように困難であるか考えよう^(注2)．この問題は量子系での対称性が有効に働く最も簡単な例であるので，量子系の特徴を理解するために格好の例題である．始めに，簡単のため， $\langle\phi_+|\phi_-\rangle > 0$ とする．そして，

$$|\phi_\pm\rangle = \cos\theta|0\rangle \pm \sin\theta|1\rangle \quad (4)$$

となるように， $\theta, |0\rangle, |1\rangle$ を選ぶ．ただし， $\sin\theta, \cos\theta \geq 0$ すなわち， $\pi/2 \geq \theta \geq 0$ とする．そして，(4) より， $\cos 2\theta = \langle\phi_+|\phi_-\rangle$ となる．この場合， $|0\rangle, |1\rangle$ から生成される二次元空間で問題を考えれば十分である．以下，行列を表示を用いる場合は，基底 $|0\rangle, |1\rangle$ の下での行列表示を用いることにする．

この識別問題では，状態の候補が二つしか与えられていないので，我々の判断を与える二次元空間上での POVM は $M := \{M_+, M_-\}$ と書ける．二つの状態が，同等の確率で現れるとすると，誤って識別する確率は $\epsilon(M) := \frac{1}{2}(\langle\phi_+|M_-|\phi_+\rangle + \langle\phi_-|M_+|\phi_-\rangle)$ となる． M_- を

$$M_- = \begin{pmatrix} a+b & c+d\sqrt{-1} \\ c-d\sqrt{-1} & a-b \end{pmatrix} \quad (5)$$

と表示すると，

$$\langle\phi_+|M_-|\phi_+\rangle = (a+b)\cos^2\theta + 2c\cos\theta\sin\theta + (a-b)\sin^2\theta.$$

となり，係数 d は現れない． $\langle\phi_-|M_+|\phi_-\rangle$ についても同様である．そして，条件 $M_- \geq 0$ より，

$$a \geq 0, \quad a^2 \geq b^2 + c^2 + d^2$$

となる．一方，条件 $I \geq M_-$ より，

$$1-a \geq 0, \quad (1-a)^2 \geq b^2 + c^2 + d^2$$

となる．この条件を要約すると

$$1 \geq a \geq 0, \quad \min\{(1-a)^2, a^2\} \geq b^2 + c^2 + d^2 \quad (6)$$

となる．よって $d=0$ の場合が，他の係数 a, b, c に対する条件が最も緩い．係数 d は誤り確率には現れないので， $d=0$ の場合を解析すれば十分である．すなわち， M_+, M_- は共に実対称行列であるとして問題ない．次に，行列

$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

を用いると，

$$Z|\phi_\pm\rangle\langle\phi_\pm|Z = |\phi_\mp\rangle\langle\phi_\mp| \quad (7)$$

となる．よって，

$$\begin{aligned} \epsilon(M) &= \frac{1}{2}(\langle\phi_+|M_-|\phi_+\rangle + \langle\phi_-|M_+|\phi_-\rangle) \\ &= \frac{1}{2}(\langle\phi_+|ZZM_-ZZ|\phi_+\rangle + \langle\phi_-|ZZM_+ZZ|\phi_-\rangle) \\ &= \frac{1}{2}(\langle\phi_-|ZM_-Z|\phi_-\rangle + \langle\phi_+|ZM_+Z|\phi_+\rangle) \end{aligned}$$

を得る．したがって，

$$\begin{aligned} \epsilon(M) &= \frac{1}{4}(\langle\phi_+|M_-|\phi_+\rangle + \langle\phi_-|M_+|\phi_-\rangle) \\ &\quad + \frac{1}{4}(\langle\phi_+|ZM_+Z|\phi_+\rangle + \langle\phi_-|ZM_-Z|\phi_-\rangle) \\ &= \frac{1}{2}\langle\phi_+|\frac{1}{2}(M_- + ZM_+Z)|\phi_+\rangle \\ &\quad + \frac{1}{2}\langle\phi_-|\frac{1}{2}(M_+ + ZM_-Z)|\phi_-\rangle \end{aligned}$$

を得る．この式は，POVM $\{M_+, M_-\}$ の性能が POVM $\{\frac{1}{2}(M_- + ZM_+Z), \frac{1}{2}(M_+ + ZM_-Z)\}$ の性能と同じであることを示している．ここで， $d=0$ とした (5) での M_- のパラメータ表示を用いると，

$$\frac{1}{2}(M_- + ZM_+Z) = \begin{pmatrix} \frac{1}{2} & c \\ c & \frac{1}{2} \end{pmatrix}$$

となる．すなわち， $\frac{1}{2}(M_- + ZM_+Z)$ は X と可換な行列になる．したがって， $\frac{1}{2}(M_+ + ZM_-Z)I - \frac{1}{2}(M_- + ZM_+Z)$ に注

(注2)：二つの純粋状態の識別問題は Helstrom⁽¹⁾によってなされたが，ここで述べる導出は，Helstrom によるものと異なる．

意すると,

$$\epsilon(M) = \frac{1}{2} + 2c \cos \theta \sin \theta = \frac{1}{2} + c \sin 2\theta$$

となる. $\pi/2 \geq \theta \geq 0$ であるので, $\cos \theta \sin \theta \geq 0$ である. また, 条件 (6) より, $\min\{(1-a)^2, a^2\} \leq \frac{1}{4}$ であるから, $c^2 \leq \frac{1}{4}$ である. よって, $c = -\frac{1}{2}$ の場合, $\epsilon(M)$ は最小値 $\frac{1}{2}(1 - \sin 2\theta) = \frac{1}{2}(1 - \sqrt{1 - \langle \phi_+ | \phi_- \rangle^2})$ を取る. そして,

$$M_- = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

のときに, 最小値を実現する.

このように, $|\phi_+\rangle$ と $|\phi_-\rangle$ が直交しない場合は $\frac{1}{2}(1 - \sqrt{1 - \langle \phi_+ | \phi_- \rangle^2})$ は 0 にならず, 誤り確率 0 で識別することは不可能である. なお, ここでは Z で生成される位数 2 の群の表現による対称性を用いた. 量子情報処理での群の表現を用いた議論は Holevo⁽¹¹⁾により始められ, 量子情報の大変有力な手法になっている. ここでの議論は, 量子情報で群の表現を用いたものの中で最も簡単なものである.

11. 状態の統計的推測

一方, 統計的に状態を識別する場合, 複数の系からなる合成系を考えることになる. 同じ系 $\mathcal{H}$ が n 個ある場合は, $\mathcal{H}$ のテンソル積を n 回考えることになり, 合成系は $\mathcal{H}^{\otimes n} := \underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_n$ で与えられる. そして, それぞれの系での状態が同じ状態 ρ に準備されたとして, ρ を同定することが多い. この場合, 合成系上の状態は $\rho^{\otimes n} := \underbrace{\rho \otimes \cdots \otimes \rho}_n$ となる.

ここで, $\rho^{\otimes n}$ は状態 ρ をコピーした状態であるので, 先の量子状態のコピー不可能性に反するのではないかと疑問が沸く. 確かに, 物理操作により, 未知の ρ から $\rho^{\otimes n}$ へ状態変化させることは不可能である. しかし, 状態がどのような密度行列で書けるか未知であっても, その状態を生成する手段 (手続き) は既知であるはずである. 状態を統計的に推測するということは, あらかじめ定められた手続きで, 系の状態を生成するとき, その状態がどの密度行列 ρ で記述されるか推測する問題である. 1 度しか系に状態を準備しなかった場合には, どうしても正確に推測することが困難になる. そのため, 同じ手続きにしたがって, 状態を複数回 (n 回) 生成し, 合成系上の状態 $\rho^{\otimes n}$ を推測することになる. この問題は量子状態の統計的推測と呼ばれ, 量子情報の基礎的なテーマとして盛んに研究されているが⁽¹²⁾, ししばしば, コピーと混同されるので注意を要する.

以下では, 典型的な例として, 二つの状態 $|\phi_+\rangle\langle\phi_+|, |\phi_-\rangle\langle\phi_-|$ のどちらかが n 個独立に与えられた場合を考えよう. この場合は, $|\phi_+\rangle\langle\phi_+|^{\otimes n}, |\phi_-\rangle\langle\phi_-|^{\otimes n}$ を識別する問題に帰着される. 二値の POVM $M = \{M_+, M_-\}$ によるこの識別問題の誤り確率を $\epsilon_n(M)$ とする. すると, $\langle \phi_+^{\otimes n} | \phi_-^{\otimes n} \rangle = \langle \phi_+ | \phi_- \rangle^n$ であるので, 前節の議論より最小誤り確率は $\min_M \epsilon_n(M) = \frac{1}{2}(1 - \sqrt{1 - \langle \phi_+ | \phi_- \rangle^{2n}}) \cong \frac{1}{4} \langle \phi_+ | \phi_- \rangle^{2n}$ となり, 指数的に 0 に収束する. すなわち, 以下のように最適な誤り確率の減少指

数が計算できる.

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \min_M \epsilon_n(M) = \log \langle \phi_+ | \phi_- \rangle^2.$$

実は, 二つの混合状態 ρ と σ を識別する場合でも, 同じように指数的に誤り確率は 0 に収束する. n 個独立に与えられた場合に, POVM M を用いた場合での誤り確率を $\epsilon_n(M)$ とすると,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \min_M \epsilon_n(M) = \min_{0 \leq s \leq 1} \psi(s|\rho||\sigma)$$

となる⁽¹³⁾ (14). ただし,

$$\psi(s|\rho||\sigma) := \log \text{Tr} \rho^{1-s} \sigma^s$$

と定義した. すなわち, 最適な誤り確率の減少指数は $\min_{0 \leq s \leq 1} \psi(s|\rho||\sigma)$ で与えられる. ここで, ρ^{1-s} の定義が気になるが, 任意の関数 f とエルミート行列 A に対して, 行列 $f(A)$ は A の射影分解を $A = \sum_i a_i E_i$ とすると, $f(A) := \sum_i f(a_i) E_i$ で定義される.

12. なぜ無限次元

コンピュータサイエンスに携わっていると情報処理の基本単位はビットになる. したがって, 量子系でも, 情報処理の基本単位はビットを量子化した二次元の量子系 $\mathbb{C}^2$ (qubit 系) であると考えるのが自然である. この qubit 系は量子情報では基本的な概念である.

しかし, 一方で, 量子情報では, 従来扱わなかった, 物理層の奥深くの量子的な素子の構造にまで立ち入るという側面がある. 現実の物理系は, ほとんどの場合, 有限次元ではなく, 無限次元である. したがって, 多くの場合, 実際に作られた二次元の量子系 $\mathbb{C}^2$ は近似的なものに過ぎず, より大きな無限次元系 $\mathcal{H}$ の部分系として実現される場合が多い.

また, 量子暗号などのように光子を用いた通信を考えると, 光子のなす系は無限次元であるので, 必然的に無限次元系を扱わねばならない. このような理由から, 量子情報処理では, 無限次元系を扱うことがしばしば起きる.

13. 量子誤り訂正と量子通信路符号化

古典系を量子系に拡張した場合, その拡張が一意に意味が定まらないことがしばしばある. 特に, 誤り訂正の量子版には, 2 種の拡張が考えられ, 混乱することがしばしばあるので注意を要する. 一つ目の量子版は, ノイズのある量子的な通信路 (媒体) を用いて, 誤りなく古典的な情報を送る問題である. 二つ目の量子版は, ノイズのある量子的な通信路を用いて誤りなく量子状態を送る問題である. 前者はしばしば量子通信路符号化と呼ばれるのに対し, 後者は量子誤り訂正と呼ばれる.

更に, 前者については量子的な通信路について 2 種類の設定があり, ししばしば混乱を起こすことがあるので注意を要する. 量子通信路を変調方式 + 光ファイバとしてとらえるか, 光ファイバだけとしてとらえるかに依存して設定が異なる. 変調方式 +

図 7 古典-量子通信路と量子-量子通信路

光ファイバの場合，入力は古典系となり，出力は量子系になり，しばしば古典-量子通信路と呼ばれる．この場合，各古典系での入力 $x \in \mathcal{X}$ に応じた出力系での量子状態 ρ_x を与えることで，通信路が定義される．一方，光ファイバだけに注目する場合は，入出力共に量子系になるので，量子-量子通信路と呼ばれる．量子-量子通信路は 9. で与えたトレースを保存する完全正写像 Λ で与えられる．両者の関係は図 7 で図示されている．

始めに，古典情報を伝送する問題を考えよう．通信路の入出力が古典系 $\mathcal{X}, \mathcal{Y}$ である場合，通信路は確率遷移行列 $W^{Y|X}(y|x)$ で与えられる．そして，この通信路を n 回，相関なく用いた場合，誤り 0 で伝送できる 1 回の通信当りのビット数の限界は通信路容量 $C(W)$ と呼ばれる．通信路容量 C を与えるには，確率分布 P のシャノンエントロピー $H(P) := -\sum_{y \in \mathcal{Y}} P(y) \log_2 P(y)$ が重要な役割を果たす．これを用いて，通信路容量 $C(W)$ は以下で与えられる⁽¹⁵⁾．

$$C(W) = \max_{p \in \mathcal{P}(\mathcal{X})} \left[H(W_p) - \sum_{x \in \mathcal{X}} p(x) H(W_x) \right].$$

ただし， $W_x(y) := W^{Y|X}(y|x)$, $W_p(y) := \sum_{x \in \mathcal{X}} p(x) W_x(y)$ である．

古典-量子通信路 $W : x \mapsto W_x$ に対しても，最適な測定に基づく復号を行うと考えると，同じように通信路容量 $C(W)$ を定義することができる．そして，密度行列 ρ のフォンノイマンエントロピー $H(\rho) := -\text{Tr} \rho \log_2 \rho$ が重要な役割を果たす．すると，通信路容量 $C(W)$ は以下で与えられる^{(16) (17)}．

$$C(W) = \max_{p \in \mathcal{P}(\mathcal{X})} \left[H(\rho_p) - \sum_{x \in \mathcal{X}} p(x) H(\rho_x) \right].$$

ただし， $W_p := \sum_{x \in \mathcal{X}} p(x) W_x$ である．古典系では Csiszár-Körner⁽¹⁸⁾により，タイプ理論を用いることで，通信路の形に依存しない符号化・復号が構成されている．量子系でも同様に，群の既約表現論を用いることにより，類似の議論が可能である⁽¹⁹⁾．次に，量子-量子通信路 Λ の場合を考えよう． Λ の入力系が $\mathcal{H}$ であり，出力系が $\mathcal{K}$ である場合，同じ通信路 Λ を n 回用いた通信路は，入力系 $\mathcal{H}^{\otimes n}$ から出力系 $\mathcal{K}^{\otimes n}$ への通信路 $\Lambda^{\otimes n} := \underbrace{\Lambda \otimes \cdots \otimes \Lambda}_n$ で与えられる．この設定での利点は，入力系での入力状態に，複数の系にエンタングルした状態を送ることが可能である点である．このような入力も許した上で，先と同様に通信路容量 $C(\Lambda)$ を定義することができる．すると，通信路容量 $C(\Lambda)$ は以下で与えられる．

$$C(\Lambda) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_{p \in \mathcal{P}_1(\mathcal{H}^{\otimes n})} \left(H(\Lambda^{\otimes n}(\rho_p)) - \sum_{\phi \in \mathcal{H}^{\otimes n}} p(\phi) H(\Lambda^{\otimes n}(|\phi\rangle\langle\phi|)) \right)$$

ただし， $\mathcal{P}_1(\mathcal{H})$ は $\mathcal{H}$ 上の純粋状態に値を持つ確率分布の集合を表し， ρ_p は $\sum_{\phi \in \mathcal{H}} p(\phi) |\phi\rangle\langle\phi|$ を表す．ここで， $C(\Lambda)$ を与える公式に現れる最適化を図 6 のように $n = 1$ の場合に制限できるか否か興味のあるところである．

$$C(\Lambda) = \max_{p \in \mathcal{P}_1(\mathcal{H})} \left[H(\Lambda(\rho_p)) - \sum_{\phi \in \mathcal{H}} p(\phi) H(\Lambda(|\phi\rangle\langle\phi|)) \right]. \quad (8)$$

この問題は加法性問題と呼ばれ，長い間，量子情報理論の最大の未解決問題であった^{(20)–(22)}． Λ がある条件を満たす場合については (8) は成り立つが，Hastings⁽²³⁾により，一般には成立しないことが示された．この事実は，量子的な相関を符号化の際に用いれば，通信速度が原理的には増加するというを示しており，大変興味深い．現在，多くの研究者が，どのような原理で，量子的な相関が通信速度の向上に寄与するか検討しているところである．次に，量子状態を伝送する問題を考えよう． Λ を入力系が $\mathcal{H}$ であり，出力系が $\mathcal{K}$ である量子-量子通信路としよう．量子通信路 Λ を n 回用いた場合に，誤りなく量子状態を伝送できる 1 通信路当りの qubit 数の限界として，量子容量 $C_Q(\Lambda)$ を定義しよう．この量の公式は知られているが，若干複雑である．これを与えるために， $\mathcal{H}$ と同じ次元の参照系 $\mathcal{R}$ を考え，合成系 $\mathcal{H} \otimes \mathcal{R}$ 上の純粋状態 $|\Phi\rangle\langle\Phi|$ を考える． $\text{Tr}_{\mathcal{R}} |\Phi\rangle\langle\Phi| = \rho$ となるとき， $|\Phi\rangle\langle\Phi|$ は ρ の純粋状態化と呼ばれる． ρ の純粋状態化 $|\Phi\rangle\langle\Phi|$ を用いて，重要な役割を果たす Coherent information $I_c(\rho, \Lambda)$ を以下で定義する⁽²⁴⁾．

$$I_c(\rho, \Lambda) := H(\Lambda(\rho)) - H(\Lambda \otimes \text{id}_{\mathcal{R}}(|\Phi\rangle\langle\Phi|)).$$

すると，量子容量 $C_Q(\Lambda)$ は以下で与えられる^{(6) (7) (25)}．

$$C_Q(\Lambda) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_{\rho \in \mathcal{S}(\mathcal{H}^{\otimes n})} I_c(\rho, \Lambda^{\otimes n}).$$

先と同じように，最大化の範囲を $n = 1$ の場合だけに限定できないか興味のあるところである．この問題は，早くから解決されており，ほとんどの場合，最大化の範囲を $n = 1$ の場合には制限できない．量子通信路 Λ に対して，ある量子通信路 Λ' が存在して，

$$\Lambda_E(\rho) = \Lambda'(\Lambda(\rho))$$

を任意の ρ に対して満たすとき，量子通信路 Λ は degraded と呼ぶ．量子通信路 Λ が degraded であるとき，

$$C_Q(\Lambda) = \max_{\rho \in \mathcal{S}(\mathcal{H})} I_c(\rho, \Lambda)$$

と単純化できる．幾つかの特別な degraded となる通信路については，その量子容量が陽に求まっている^{(6) (7)}．

古典系で実際に用いる誤り訂正は代数的な誤り訂正符号に限られている．同じように，実装コストを考慮すると，量子系でも，ある種の対称性を満たすものに限定することは自然である．以下では，最も簡単な場合，すなわち，入出力系が共に qubit 系で与えられている場合のみ考える．この場合，上記のような代数的な対称性を持つ誤り訂正符号は符号長の多項式オーダー

の個数の C-NOT ゲート を組合せることで構成できる^{(26) (27)}.
 ここでは, そのような対称性を持つ符号で漸近的に達成できる
 1 通信路当りの qubit 数 $\tilde{C}_Q(\Lambda)$ を考える. そのために, 量子
 通信路 Λ の離散 twirling $T(\Lambda)$ を与える.

$$T(\Lambda)(\rho) := \frac{1}{4}\Lambda(\rho) + \frac{1}{4}X\Lambda(X\rho X)X \\ + \frac{1}{4}Z\Lambda(Z\rho Z)Z + \frac{1}{4}XZ\Lambda(XZ\rho ZX)ZX.$$

すると,

$$\tilde{C}_Q(\Lambda) \geq I_c(\rho_{\text{mix}}, T(\Lambda)).$$

すなわち, 計算量さえ無視すれば, C-NOT ゲート の組合せで,
 $I_c(\rho_{\text{mix}}, T(\Lambda))$ まで伝送できることになる⁽²⁸⁾.

14. 量子鍵配送って本当に安全なの？

現在, 最も実用に向けて盛んに研究されている量子情報のテーマとして, 量子鍵配送が挙げられる. 量子鍵配送では, 遠隔地にいる 2 者が量子通信と古典的な公開通信を適切に組合せることで, 安全に秘密鍵を共有するプロトコルである. このプロトコルを通じて共有した秘密鍵を用いて, 後に秘匿通信を行うことになる.

量子鍵配送には, 光を用いることが多い. 量子鍵配送では多くの場合, 二次元の量子系 (qubit) を用いる場合が多いが, 無限次元系を用いる場合もある. また, 単一光子が生成できれば, 完全な qubit になるが, 光源の不完全性のために, その安全性のためには無限次元系を扱わざるを得ない場合もある.

単一光子を用いた光子から qubit を作る場合, 代表的な方法として, 光の偏光を用いる方法がある. 他に, 光の二つの経路を準備し, 経路によって qubit を構成する場合もある.

以下では, 代表的な BB84 プロトコル²⁹ を述べることにする. このプロトコルの本質は, 2 種類の基底 (+ 基底 $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ と $\times$ 基底 $\{|+\rangle\langle +|, |-\rangle\langle -|\}$) をランダムに使うところである. $\times$ 基底では $|+\rangle\langle +|$ がビット値 0, $|-\rangle\langle -|$ がビット値 1 に対応していると考えて, 量子鍵配送のプロトコルを与える.

(1) 送信者である Alice が $|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|$ のうちの一つの状態をランダムに等確率で送る. このとき, 送った状態のビット値 (0, 1) と基底 +, $\times$ を記録する.

(2) 受信者である Bob は二つの測定 $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ からランダムに一つの測定を選び, 測定し, 測定値 0, 1 と基底 +, $\times$ を記録する.

* 上記の操作を複数回繰り返す.

(3) Alice と Bob は互いが用いた基底の情報を公開通信路を用いて照合し, 基底が一致した部分のビット値のみ残す.

(4) Alice と Bob は基底が一致した部分の情報のうち, それぞれの基底について, 一部をランダムに選択し, 公開通信路を用いて照合する. (図 8)

(5) 照合した際, 完全に両者の情報が一致していたら, 盗聴がなかったと判断し, 残った情報を, 秘密鍵として利用する. 両者の情報に不一致が見つかったら盗聴が存在していたと判断し, 残った情報を捨てる.

Alice		Bob	
ビット	基底	基底	ビット
0	+	+	0
0	+	$\times$	1
1	$\times$	$\times$	1
0	$\times$	+	0
0	+	+	0
1	$\times$	$\times$	1
0	$\times$	+	1
1	$\times$	$\times$	1
1	$\times$	+	1
0	+	+	0

図 8 量子鍵配送における基底照合

上記のプロトコルでは, 通信路にノイズがない場合であれば, 盗聴があると, 通信路が乱される. 照合に用いるビット数を十分大きく取れば, 極めて高い確率で, 照合時に不一致が検出され, 盗聴を検出することができる.

しかし, ノイズがある場合に本当に安全なのかという疑問をよく耳にする. 確かに, ノイズに紛れた盗聴は一定範囲で可能である.

ノイズがある場合には, 上記のプロトコルだけでは, 安全な鍵を生成することはできない. そもそも, ノイズがあれば, 照合の際に不一致があるので, 極めて高い確率で残った情報を捨てることになる. そのため, 照合の際の情報の不一致が想定されたノイズの範囲であれば, 鍵を残すように処理を変える必要がある. また, 最終鍵の間に不一致が残るので, 誤りを訂正する必要がある. そして, これが最も深刻なことであるが, ノイズに紛れて盗聴がなされていると考えられるので, 情報漏えいのない情報に変換する必要がある. これらに対処するため, 処理 (5) を以下の (5)' に変更し, 更に, 処理 (6) から (9) を追加する.

(5)' 照合した際, 情報の不一致が双方の基底についてあらかじめ想定した割合 p よりも小さかったら盗聴がなかったと判断する. Alice はそれぞれの基底の残った情報を, 生鍵 X_+ , $X_\times$ として, 保管する. Bob もそれぞれの基底の残った情報を, 生鍵 X'_+ , $X'_\times$ として, 保管する. 割合 p よりも大きかったら盗聴が存在していたと判断し, 残った情報を捨てる.

* 以下では + 基底についての生鍵 X_+ , X'_+ から最終鍵を生成する手順のみ述べる.

(6) 古典的な誤り訂正符号 C を用いる. Alice は C の要素 Y をランダムに選び, 公開通信路を用いて, $Y + X_+$ を Bob に送る.

(7) Bob は受け取った情報 $Y + X_+$ を $Z := Y + X_+ - X'_+$ に変換し, 古典的な通信路 $Y \mapsto Y + X_+ - X'_+$ に対する誤り訂正符号の復号化プロセスを適用し, Y' を Y の推測値として得る.

(8) Alice, Bob は手元の C の要素 Y, Y' を F_2^k の要素に変換する.

(9) Alice と Bob は 2 値の $l \times k$ のランダム行列 A を生成し、最終鍵をそれぞれ AY, AY' とする。ここで、 l は $l = (1 - h(p + \delta))n$ とする。なお、 n は生鍵 X_+ のビット数であり、 $h(x) := -x \log_2 x - (1 - x) \log_2 (1 - x)$ である。また、 $\delta > 0$ は想定されるチェックビットの統計誤差の幅などを考慮して選ぶ。

なお、ここではランダム行列 A の成分を完全にランダムに選ぶ必要はない。 $A = (A_{i,j})$ の各成分が $k + l - 1$ 個の独立な 2 値乱数 $B_1, \dots, B_{k+l-1}$ を用いて以下のように与えれば十分である。このようなランダム行列はテブリティツ行列と呼ばれる^{(30) (31)}。

$$A_{i,j} = B_{i+j-1}.$$

このプロトコルは変形 BB84 プロトコルと呼ばれる。

このような処理を追加することで、生鍵の部分での + 基底、 $\times$ 基底の部分のエラー率がほぼ p 以下であることが確認できる。ここでは、それぞれの基底でランダムにチェックビットを選んでいく。したがって、チェックビットの数を m 、生鍵のビット数を n とすると、全体で $n + m$ 個となる標本から、ランダムに m 個の標本を取り出し、抽出した標本のデータから残りの n の標本を推定することと理論的に同じである。この議論は、統計学では非復元抽出もしくはランダムサンプリングと呼ばれ、工場での不良品の推定などに用いられる。基本的に、抽出標本数が十分多ければ、抽出標本でのエラー率は残りの生鍵の部分のエラー率とほぼ一致する。

そして、+ 基底の生鍵についての盗聴情報量は $\times$ 基底のエラー率で評価することができる。一般に、 $\times$ 基底のエラー率が p であれば、(9)において $l = (1 - h(p'))n$ を代入すれば ($\frac{1}{2} \geq p' > p$)、漸近的には、最終鍵の盗聴情報量は 0 に収束することが知られている^{(32) (33)}。

これら二つの事実を組合せると、十分サイズを大きくすると安全な最終鍵が生成できることが確認できる^{(32) (34)}。

しかし、現実には、単一光子源を完全に実装することは現状では困難なので、不完全性を考慮した解析が必要となる⁽³⁵⁾⁻⁽³⁷⁾。また、この不完全性による攻撃の選択枝を減らす方法として、decoy 法と呼ばれる手法があり⁽³⁸⁾⁻⁽⁴¹⁾、これを上述の変形 BB84 プロトコルに組合せた手法が現在の主流として考えられている。なお、BB84 プロトコルについては、最近では、光源の不完全性やランダムサンプリングの統計誤差を考慮した量子鍵配送システムも実装されている⁽⁴²⁾。これらの研究活動を受けて、国内の機関である情報処理機構 (IPA)、情報通信研究機構 (NICT)、産業技術総合研究所 (AIST) が協力して、その標準化に向けて動き出している⁽⁴³⁾。同時に、ヨーロッパでは EU の European Telecommunications Standards Institute (ETSI) が Secure Communication based on Quantum Cryptography (SECOQC) というプログラムの下で大々的に、その標準化に向けた活動を行っている。その他、偏光板を用いた模擬実験により、量子鍵配送の原理を体験する試みもなされており⁽⁴⁴⁾、量子鍵配送は大変身近なものになりつつある (図 9)。

図 9 偏光板を用いた量子鍵配送の模擬実験

15. む す び

量子情報理論の基本概念について、初学者がつまづきやすいポイントに重点を置いて解説した。学部で学習する量子力学で重点が置かれる部分と、量子情報理論の基本概念の間には、一定のギャップがある。前半部では、このギャップを埋めるための説明に重点を置いた。

後半部では、量子状態識別、量子通信路符号化、量子鍵配送などの量子情報理論の主要テーマについて、最新の研究動向も含めて解説した。群論的対称性が有効に機能する典型例として、量子状態識別を取り扱った。量子情報理論の主要テーマとして、量子情報源符号化やエンタングルメント操作があるが、紙数の都合で今回は割愛した。これらのテーマについては文献^{(3) (6) (7)}などが参考になる。本稿をきっかけに、これまでとつきにくかった量子情報理論に興味を持つ読者が現れたら筆者にとって幸いである。

文 献

- (1) C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, 1976.
- (2) A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam, 1982; Originally published in Russian, 1980.
- (3) M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
- (4) 小芦雅斗, 小柴健史, 「量子暗号理論の展開」 SGC ライブラリ 67, サイエンス社, 東京, 2008.
- (5) 根本香絵, 「量子力学の考え方」 ~ 物理で読み解く量子情報の基礎 ~, SGC ライブラリ 68, サイエンス社, 東京, 2009.
- (6) 林正人, 「量子情報理論入門」 SGC ライブラリ 32, サイエンス社, 東京, 2004.
- (7) M. Hayashi, *Quantum Information: An Introduction*, Springer-Verlag, 2006.
- (8) M. Ozawa, "Optimal measurements for general quantum systems," *Rep. Math. Phys.*, **18**, 11-28, 1980.
- (9) M. A. Naimark, *Comptes Rendus (Doklady) de l'Academie des Science de l'URSS*, vol. **41**, no. 9, 359, 1943.
- (10) W. F. Stinespring, "Positive Functions on C^* -Algebras," *Proc. Am. Math. Soc.*, vol. **6**, 211 1955.
- (11) A. S. Holevo, "Covariant measurements and uncertainty relations," *Rep. Math. Phys.*, vol. **16**, 385-400, 1979.
- (12) *Asymptotic Theory of Quantum Statistical Inference: Selected Papers*, M. Hayashi eds., World Scientific,

2005.

- (13) K.M.R. Audenaert, J. Calsamiglia, Ll. Masanes, R. Muñoz-Tapia, A. Acín, E. Bagan, and F. Verstraete, "The Quantum Chernoff Bound," *Phys. Rev. Lett.*, vol. **98**, 160501, 2007.
- (14) M. Nussbaum and A. Szkoła, "A lower bound of Chernoff type for symmetric quantum hypothesis testing," *Annals of Statistics*, vol. **37**, no. 2, 1040-1057, 2009.
- (15) C.E. Shannon, "A mathematical Theory of communication," *Bell Syst. Tech. J.*, vol. **27**, 379-423, 623-656, 1948.
- (16) A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. **44**, 269, 1998.
- (17) B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. **56**, 131, 1997.
- (18) I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, 1981.
- (19) M. Hayashi, "Universal coding for classical-quantum channel" to appear in *Commun. Math. Phys.*, arXiv:0805.4092.
- (20) K. Matsumoto, T. Shiono, and A. Winter, "Remarks on additivity of the Holevo channel capacity and of the entanglement of formation," *Commun. Math. Phys.*, vol. **246**, no. 3, 427-442 2004.
- (21) P. W. Shor, "Equivalence of Additivity Questions in Quantum Information Theory," *Comm. Math. Phys.*, vol. **246**, no. 3, 453-473 2004.
- (22) 林 正人, "量子情報理論における加法性問題" 2005 信学ソ大, AP-1-1, Sept. 2005.
- (23) M. B. Hastings, "A counterexample to additivity of minimum output entropy," *Nature Physics* vol. **5**, 255 (2009).
- (24) B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Phys. Rev. A*, vol. **54**, 2629, 1996.
- (25) I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. **51**, 44 - 55, 2005.
- (26) A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. **78**, 405-408, 1997.
- (27) D. Gottesman, "Theory of fault-tolerant quantum computation," *Phys. Rev. A*, vol. **57**, 127 - 137, 1998.
- (28) M. Hamada, "Information rates achievable with algebraic codes on quantum discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. **51**, 4263 - 4277, 2005.
- (29) C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (Bangalore, India, IEEE, New York, 1984. 175.
- (30) L. Carter and M. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. **18**, no. 2, 143-154, 1979.
- (31) H. Krawczyk, "LFSR-based hashing and authentication. Advances in Cryptology," *CRYPTO '94. Lect. Notes Comput. Science*, vol. 839, pp 129-139, 1994.
- (32) P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. **85**, 441, 2000.
- (33) M. Hayashi, "Practical evaluation of security for quantum key distribution," *Phys. Rev. A*, vol. **74**, 022307, 2006.
- (34) D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," In *Advances in Cryptology - Proc. Crypto'96*, vol. 1109 of *Lect. Notes Comput. Sci.* (N. Kobitz Ed., Springer-Verlag, New York, 1996. 343; *J. Assoc. Comput.*, vol. **48**, 351, 2001.
- (35) D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum. Inf. Comput.*, vol. **5**, 325 - 360, 2004.
- (36) H. Inamori, N. Lütkenhaus, and D. Mayers "Unconditional security of practical quantum key distribution," *European Physical Journal D*, vol. **41**, 599, 2007.
- (37) M. Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," *Phys. Rev. A*, vol. **76**, 012329 2007.
- (38) W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.*, vol. **91**, 057901, 2003.
- (39) H.-K. Lo, X.-F. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. **94**, 230504, 2005.
- (40) X.-B. Wang, "Beating the PNS attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. **94**, 230503, 2005.
- (41) M. Hayashi, "General theory for decoy-state quantum key distribution with an arbitrary number of intensities," *New J. Phys.*, vol. **9** 284, 2007.
- (42) J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, "Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics," arXiv:0705.3081.
- (43) D. Dodson, M. Fujiwara, P. Grangier, M. Hayashi, K. Imafuku, K. Kitayama, P. Kumar, C. Kurtsiefer, G. Lenhart, N. Luetkenhaus, T. Matsumoto, W. J. Munro, T. Nishioka, M. Peev, M. Sasaki, Y. Sata, A. Takada, M. Takeoka, K. Tamaki, H. Tanaka, Y. Tokura, A. Tomita, M. Toyoshima, R. van Meter, A. Yamagishi, Y. Yamamoto and A. Yamamura, "Updating quantum cryptography report," quant-ph/arXiv:0905.4325.
- (44) 林 正人, 木村 元, 東北大学サイエンスカフェ実施報告—偏光板による量子鍵配送の模擬実験—, 数学通信 vol. 14, no.2, Aug. 掲載予定.

(平成 21 年 3 月 31 日受付 平成 21 年 5 月 26 日最終受付)

林 正人 (正員)

1994 京大・理卒・1999 同大学院 理学研究科 博士後期課程了 1998 日本学術振興会 特別研究員・2000 理化学研究所 脳科学総合研究センター 脳数理研究チーム 研究員・2003 ERATO 今井量子計算機構プロジェクト 技術参事・2006 ERATO-SORST 量子情報システムアーキテクチャ グループリーダー・2007 東北大 大学院情報科学研究科 准教授として現在に至る。量子情報理論の研究に従事。著書 Quantum Information: An Introduction など。