SGC ライブラリ- 32

量子情報理論入門

An Introduction to Quantum Information

林　正人 著

サイエンス社

はじめに

このテキストは現在発展段階にある量子情報理論について基礎から最先端の話題までを含めて，極めて初等的な知識のみを仮定し，著者の能力で可能な限りシンプルな議論でこれらを解説したものである．量子情報理論は現在進行中の分野であり，物理学や情報科学など様々な分野をバックグラウンドに持った研究者が集結し，これまでそれぞれの分野では欠けていた要素を互いに補いながらここ５年ほどの間で急速に進展した分野である．

昨今，学際化が叫ばれているが個別の分野が必要以上に細分化したため，広い視野で教育・研究を実施し評価することが不可能になりつつあることが背景にあると思われる．そのような中，物理学や情報科学を含む複数の分野に跨るテーマを扱う量子情報理論はこれらの分野の間の橋渡しとなることが期待でき，細分化の弊害を取り除くことに貢献できるものと思われる．そもそも，情報科学と一言に言っても，コンピュータサイエンスから，数理統計学，シャノンの情報理論など様々な分野があり，これらが個別的に研究されているのが現状である．だが，これらの分野の立場から量子情報理論に取り組むとなると，再度基礎に立ち返って考える必要があり，そのような基礎的なレベルでは，ほとんど分野の壁など意味が無く，既存の分野の枠組みを超えた研究交流がなされている．

このテキストはこのような現状をふまえ，複数の分野に予備知識が必要な量子情報理論に対して，これらの知識が効率よく身に付くよう書かれている．仮定された予備知識は大学の一般教養課程レベルの線形代数，微積分及び確率・統計の知識に限られており，量子力学に関する知識は一切仮定しない．ただ，理論的な側面に重点を置いたため，物理的実現のモデルや，それに関連したテーマについてはほとんど触れることができなかった．さらに，紙数の都合上，演習問題の解答や，幾つかの証明，**文献番号が数字の参考文献** については下記のサポートページに載せることになった．

http://www.saiensu.co.jp/support.htm

演習問題の中には単独で解くには難しいものも含まれるが，是非ともトライして頂きたい．これらについて１つ１つ解答を自分で作って行けば，実力が付くことは間違いない．なお，このテキストは部分的にオリジナルな内容も含んでおり，それらについてはコメントを付してある．

東京大学の今井浩教授，理化学研究所 脳科学総合研究センターの甘利俊一教授，京都大学の上野健爾教授をはじめとして，ERATO 今井量子計算機構プロジェクト，理化学研究所 脳科学総合研究センター，京都大学数学教室の皆様には著者に研究環境を提供して下さり感謝している．

さらに，量子情報理論をともに研究してきた電気通信大学の長岡浩司助教授，大阪大学の藤原彰夫助教授，国立情報学研究所の松本啓史助教授，東京大学の小川朋宏助手には私の身勝手なディスカッションに付き合って頂き，また色々と忠告して頂き感謝している．彼らとの共同研究やディスカッション無しにはこのようなテキストはできなかったと思われる．

その他，Steklov 数学研究所の Holevo 教授，東北大学の小澤正直教授，東京工業大学の松本隆太郎博士，NTT の森越文明博士，理化学研究所の渡辺曜大博士，ERATO 今井量子計算機構プロジェクトの浜田充，津田美幸，Heng Fan，Xiangbin Wang の各博士及び下野寿之氏にはこのテキストに必要な内容について有益なコメントを頂いた．この場を借りて感謝の意を表したい．また，サイエンス社の平勢耕介氏には激励しながら筆の遅い筆者を辛抱強く待って頂き感謝している．

2003 年 12 月 4 日　　本郷にて

林　正人

目　次

第 0 章
序章

0.1 量子情報理論への招待

我々が物体を認識し，それから情報を得るという行為とは何なのかという問題は，太古は哲学や宗教のテーマとして扱われ，最近では認知科学，心理学や脳科学のテーマとしても扱われてきた．実はこのテーマは現在物理学の基礎をなす量子力学においても避けて通れない重要な問題でもある．我々が物体を認識するには，いわゆる五感を用いるわけであり，全ての場合その対象から直接情報を得るわけではなく，なんらかの物理的媒体を必要とする．例えば視覚は，光を媒体として情報を得ている．このように，観測とは物理的な媒体を通した情報処理と考えることができるので，物理学として扱うことのできるテーマでもある．さらに，情報処理であるから情報科学的な視点が必要であることはいうまでもない．

この観測というプロセスをミクロな世界に当てはめたとき，物理学者は 20 世紀の初頭に信じがたい事実に出会った．まず，光には粒子としての性質と波としての性質が混在するという，矛盾した性質が見つかった．そのため，光はその波長を固定すると最小のエネルギー単位を持つ粒子（光子）としての性質を持つことになる．つまり，光を用いた観測では，観測対象となる物体と光が衝突などの相互作用した結果の光を目にすることになる．例えば，物体の位置を測定したい場合は，光子との衝突などの相互作用の結果の光子を観測することになる．しかも，光子もエネルギーと運動量を持っているので，その物体の速さは不可避的に乱される．その上，その物体の質量が光のエネルギーの最小単位に対して，相対的に小さいと，この測定による擾乱は無視できない．このような事情から，最初の位置の測定後に速さを測ったとしても，その物体の速さが乱された後なので，元の物体の速さを正確に測ることは不可能である．逆に速さを測っても，不可避的に，位置を乱してしまうので，このような事情から我々がナイーヴに考える「完璧な測定」は不可能となる．それでも，我々が日

第 1 章
量子系の数学的定式化

この章では後の章の準備として線形代数の基礎概念と量子力学の定式化について述べる．これらの内容は地味であるが，量子情報処理全般を議論するために不可欠な部分であるので，一通り理解しておく必要がある．最初の節ではこのテキストで必要となる線形代数の基礎的概念及び，記号などについてまとめ，次の節では量子力学の定式化を与える．その後には，最も基本的な例である量子 2 準位系について述べ，最後にテンソル積と行列不等式について述べる．より進んだ線形代数の議論については付録を参照されたい．

1.1 量子系と線形代数

量子系での情報処理を扱うには，問題となる物理系や測定，状態などの基礎的な概念を数学的に記述する必要がある．まずはじめに物理系であるが，これは**表現空間** とよばれる Hilbert 空間 $\mathcal{H}$ （エルミート内積付き，有限次元もしくは無限次元の複素ベクトル空間）で記述される．この節では，測定，状態などの他の重要な概念に入る前に，線形代数については量子力学を扱う場合の基礎であると同時に，量子力学の場合に特有の記法もあるので，はじめにこれらについて簡単にまとめておく．Hilbert 空間というときは数学では無限次元のエルミート内積付きの複素ベクトル空間を指すことが多いが，量子情報理論では有限次元のエルミート内積つき複素ベクトル空間も含めて意味することが多い．量子力学においては本質的にエルミート内積つき複素ベクトル空間という構造が重要なので，このようなよび方をする．無限次元のエルミート内積つき複素ベクトル空間は有限次元のエルミート内積つき複素ベクトル空間と類似の扱いができる場合が多いので，このテキストでは有限次元の場合のみ扱い，その次元は特に断らない限り，d とする．

問題となる系の表現空間は物理的な考察と実証から決められており，例えば，電子などの Spin-$\frac{1}{2}$ の粒子とよばれる粒子は軌道運動の他に，内部的な「回転」

第 2 章
古典系での情報量とパラメータ推定

量子情報理論を扱うには，これまで量子的でない設定で研究されてきた情報理論や数理統計学，それに情報幾何学などの知識が必要となる．この章ではこれらの基礎的な数学的理論を簡単に要約する．この章で扱う内容は従来ばらばらに扱われてきたので，量子的でないこれらの理論の要約としても十分に有益である．

2.1 古典系での情報量

問題となる密度行列 $\rho_1, \ldots, \rho_n$ が全て可換であるときは，共通の正規直交基底 $\{u^1, \ldots, u^d\}$ を用いて $\rho_1 = \sum_i p_{1,i}|u^i\rangle\langle u^i|, \ldots, \rho_n = \sum_i p_{n,i}|u^i\rangle\langle u^i|$ と同時に対角化でき，本質的に確率分布 $p_1, \ldots, p_n$ の問題に帰着できることが多い．このような場合のことを以下では「**古典的**」とよぶことにする．ここでは，確率分布に対して，定義される情報量を以後の準備として簡単に紹介する．

2.1.1 エントロピー

よく知られている量が**エントロピー**であるが，これは確率分布 $p = \{p_i\}_{i=1}^k$ に対して，

$$H(p) \stackrel{\text{def}}{=} \sum_{i=1}^{k} -p_i \log p_i$$

で定義される[*1)]．確率変数 X を扱うときは，その確率分布を P_X と書き，P_X のエントロピーを $H(X)$ と書くことにする．特に $k = 2$ のときは確率分布 $(x, 1-x)$ のエントロピー $h(x) \stackrel{\text{def}}{=} -x\log x - (1-x)\log(1-x)$ は **2 値エントロピー**とよばれる．後に示すように確率分布 p が値をとる集合（すなわち p の確率空間）の要素の数（今の場合は k）を用いて

*1) ここで $0\log 0$ は 0 とする．

第 3 章
量子仮説検定と状態識別

量子系においても様々な情報処理を考えることができるが，これらの情報処理のなかで最も基本的と思われるのが 2 状態の状態識別と仮説検定である．この問題の解析が他の量子情報処理を解析する上で基礎となることが多く，この問題には量子系特有の非可換性による取り扱いの難しさが最も端的に現れるという特色もある．そのような理由から，このテキストでは状態識別と仮説検定をいくつかある量子系での情報処理の中で先に扱う．

2 状態の状態識別では未知状態の候補が 2 つあり，測定を行い測定値からどちらであるか判断する．ここでは 2 つの仮説を対称に扱っていることに注意されたい．一方，この 2 つの仮説を非対称に扱う場合は仮説検定とよばれ，状態識別とは区別される．驚くべきことに，この仮説検定という問題はそれ自身が興味あるテーマであるだけでなく，その中心テーマの 1 つである量子 Stein の補題は第 4 章で述べる量子系での通信路符号化と密接に結び付く．それどころか，この量子 Stein の補題は 8.5 節で述べる最大エンタングルメント状態の抽出問題や，第 9 章で述べる話題とも繋がっている．しかし，Stein の補題などで扱う状態は同一の状態からなるテンソル積状態であるため，そのようなテンソル積状態は普通の通信においてはほとんど現れない．だが，このテンソル積状態の漸近理論を解析することが，実は多くの量子通信の問題の漸近論を解析する上で鍵となる．このような理由から敢えてこのテーマを始めに扱うことにした．

3.1 量子系での 2 状態の識別

今，量子系 $\mathcal{H}$ にある状態が密度行列 ρ または σ であることが分かっており，そのどちらであるか測定により判断することを考える．このような手続きは $\mathcal{H}$ 上のエルミート行列 T で $I \geq T \geq 0$ を満たすもので与えられ，状態識別とよばれる．以下その理由を簡単に記す．

第 4 章
量子通信路符号化（メッセージ伝送）

現在の私たちは日常的にネットを駆使してコンピュータを使っているが，その通信の途中はノイズにさらされているため，本来は常に情報が誤って伝えられる危険性が含まれている．しかしながら，そのような危険は結果的にはほとんど回避できている．なぜ，そのようなことが可能なのだろうか？ 例えば，1 か 0 の 2 つに 1 つの情報を送る場合，0 の代りに 0 0 0 を 1 の代りに 1 1 1 を送るとの受信者との約束の下で通信を行ったとする．このとき受け手側は 0 1 0 や 1 0 0 を受け取ったとすると，送り手は 0 を送ったと推測する．一方，1 1 0 や 1 0 1 を受け取ると 1 を送ったと推測する．このように，通信を冗長にすることで誤りが起きる危険を減らすことができる．しかし，このような単純な方法では誤りが起きる危険を小さくするためには，際限無く冗長度を上げる必要が生じ，当初多くの人々は，誤り確率を減らすためには冗長度が際限無く大きくなることは不可避だと考えていた．しかし，1948 年に Shannon [259] は符号*1) を複雑にすることで，冗長度を一定値以上，大きくせずに誤り確率を際限無く小さくできることを示した．これは当初の予想と正反対であったため，多くの人たちに驚きを持って受け入れられた．Shannon の方法の独自性は，通信を 0 と 1 のような記号的なものとして捉え，符号とよばれる手法でノイズに対抗したことにあった．しかし，現実の通信を考えた場合，光ファイバーや銅線などを用いた通信では，0 や 1 のような記号が物理的な媒体に変換されて送られている訳である．特に，光ファイバーの場合はより理論的な限界まで通信の速度を上げるのであれば，個々のメッセージに対応する物理媒体を量子力学で取り扱われるべきミクロなものとして扱う必要が生ずる．このような状況においては，送信の際に行われる符号化を単に 0 や 1 の列への変換と捉えず，送りたいメッセージから量子状態への変換と捉え，復号化と受信過程を 1 つに統

*1) 通信の際のメッセージの変換規則．正確には送信の際の変換規則が符号化とよばれ，受信の際の変換規則が復号化とよばれる．

第 5 章
量子系での状態変化と完全正写像

これまでに扱った問題では，我々が量子系に対して行える操作は測定のみであった．しかし，本格的に量子系での情報処理を扱うには，これだけでは不十分であり，量子状態そのものを操作する必要が生じる．この章では量子系で状態操作を行う際，原理的にどのような操作が許されているのか調べ，それらの性質について議論する．

5.1 量子系での状態変化の記述

量子力学系 $\mathcal{H}$ では t 時間後の時間発展はハミルトニアンとよばれる $\mathcal{H}$ 上のエルミート行列 H を用いて，

$$\rho \mapsto e^{itH}\rho e^{-itH}$$

で表されると考えられている．しかし，これは系 $\mathcal{H}$ が他の系と相互作用が無いと考えられている場合のみであり，相互作用がある場合の状態変化をこのようには書けない．しかも，情報処理で扱うプロセス（状態変化）は必ずしも入力系と出力系の量子系が同じであるとは限らない．問題設定によっては，入出力系が異なるからこそ意味がある場合もある．以下では，量子系 $\mathcal{H}_A$ を入力系とし量子系 $\mathcal{H}_B$ を出力系とするシステムを考え，その入出力関係（状態変化）を与える $\mathcal{S}(\mathcal{H}_A)$ から $\mathcal{S}(\mathcal{H}_B)$ への写像 κ の性質について調べる．まず第 1 に写像 κ が満たすべき性質として，$1 > \lambda > 0$ となる λ と任意の $\rho_1, \rho_2 \in \mathcal{S}(\mathcal{H}_A)$ に対して，

$$\kappa(\lambda\rho_1 + (1-\lambda)\rho_2) = \lambda\kappa(\rho_1) + (1-\lambda)\kappa(\rho_2)$$

となることが要請される．この性質は**アファイン性**とよばれ，空間 $\mathcal{S}(\mathcal{H}_A)$ が線形空間でないために，κ に対して線形性を課すことはできないが，ほとんど線形性と同等な条件である．事実，写像 κ は以下のように $\mathcal{H}_A$ 上のエルミート行列

第 6 章
量子情報幾何と量子推定

前述の第 3 章では未知の量子状態の候補が 2 つしかない場合に未知状態を識別する問題を扱った．この章では未知状態は連続値のパラメータ θ で記述されており，そのパラメータを推定する問題を扱う．量子系の特徴の 1 つに測定を行なうと状態破壊が不可避的に起こることが挙げられる．そのため，状態推定のための測定は可能限りたくさんの情報を引き出す測定を行なう必要がある．このような問題は量子推定とよばれ，そこでは測定の最適化が重要なテーマとなる．

一方，2.3 節で述べたように古典的な（確率分布の）推定の理論では内積などの幾何学的な構造が推定と密接に関連している．同じように量子系での推定でも幾何学的な構造が重要な役割を果たすことが期待できる．このような量子状態のなす空間の幾何構造を扱う分野は量子情報幾何とよばれ，量子情報理論の重要なテーマの一つである．この章では量子系での幾何学構造について述べ，ついでその推定論への応用について述べる．

6.1 量子力学的な内積

量子状態のなす空間の幾何学を考えたとき，その空間に入る計量を扱う問題は避けては通れない．この問題を議論するために，以下では 2.3 節で推定の準備として扱った Fisher 情報量やそれと関連した内積 (2.48) の量子版を考えることにする．今，(2.48) に現れる A, B, p を互いに可換なエルミート行列 Y, X, ρ の同時対角化したときの対角成分とすると，内積 (2.48) は $\mathrm{Tr}\, Y(X\rho)$ に一致する．一般に 2 つの行列の積のトレースはその積の順番に依存しないが，3 つ以上の行列の積のトレースはその積の順番に依存するので，これらが互いに非可換な場合では，この内積の値は $X\rho$ の部分の積の順番の取り方に任意性が残る．この $X\rho$ に対応する部分の積の定義の仕方として，少なくとも以下の 3 通りが考えられる．

第 7 章
量子測定と状態変化

量子力学では測定による状態変化は波束の収束とよばれ問題視されることが多い．しばしば何故に波束の収束が起きるのか不明であるため，必要以上に神秘的な扱いをしてしまい，どのような状態変化が起きるのかという状態変化の記述さえ不十分である場合が多い．しかし 7.1 節で説明するように[*1)]，測定による状態変化は 1.2 節で与えた量子力学の定式化から必然的に起るものである．この章では 1.2 節と 1.4 節で与えた定式化から出発して，測定に伴う状態変化を正確に記述する．そして，7.2 節ではこの概念を用いて不確定性関係に関係する話題に触れる[*2)]．

7.1 測定にともなう状態変化

これまでは測定についてはその測定値が得られる確率についてのみ扱った．しかし，同一の系に対する繰り返し測定などを考えるには，測定にともなう状態変化を正確に記述する必要がある．以下，POVM $\boldsymbol{M} = \{M_\omega\}$ に対応する測定を行なった場合での典型的な状態変化を天下り的に与え，その後に，5.1 節と同様の議論を用いて 1.2 節で与えた公理的な枠組から一般的に測定に伴う状態変化が満たすべき条件を導出する．

POVM $\boldsymbol{M} = \{M_\omega\}$ に対応する典型的な測定を行ない，測定値 ω が得られたときの測定後の状態（すなわち終状態）は

$$\frac{1}{\operatorname{Tr}\rho M_\omega}\sqrt{M_\omega}\rho\sqrt{M_\omega} \tag{7.1}$$

---

*1) 7.1 節の議論は定理 7.2 以外のほとんどの部分は小澤 [224]~[227], [229], [230] による議論を著者の視点でこのテキストの流れに合わせて再構成したものである．この辺りの歴史的な経緯やここで扱った内容についてより深く勉強するには小澤 [234] やその参考文献を読んで頂きたい．

*2) この部分についての歴史的な経緯などこのテキストで不十分なところについては巻末の主要参考文献で挙げた [小澤] を参考にして頂きたい．

第 8 章
エンタングルメントと局所量子操作

量子力学が日常的な常識に反する原因は単に測定値が確率的にしか予測できないだけではなく，エンタングルメントとよばれる量子系特有の相関にある．このタイプの相関は我々が日常的に扱う巨視的な物体については通常は働かないと考えられており，これを用いることで非局所的な現象を起こすことができる．このような相関を持つ状態はエンタングルド状態（もしくはエンタングルメントがある状態）とよばれ，その中でも最もエンタングンルメントの度合いが強い状態は最大エンタングルド状態，もしくは EPR 状態とよばれる．後者の名称は Einstein, Podolsky 及び Rosen により，初めてエンタングルド状態による非局所的効果が指摘されたことによる．

一般に量子状態を測定すると状態の破壊が起きるため，あるところにある量子状態を離れたところに送るにはそれを測定せずにその状態そのものを送らないといけない．しかし，両者がエンタングルド状態を共有していれば，送信者は送信したい量子系とエンタングルした片方の系の合成系にまたがる測定を行い，その測定値を送ることで，直接量子状態を送ること無しに，手元の量子状態を送ることができる．ここで送信者と受信者の間にまたがった量子操作を全く行わず，局所量子操作と古典的な情報通信しか行っていないことに注意されたい．このプロトコルは量子テレポーテーションとよばれ量子系でのエンタングルメントの効果を明確に表すものである．その他にも，エンタングルメントを用いることによる効果は色々と研究されており，第 9 章でも取り上げられる．

だが，十分にエンタングルしていない状態を共有しているだけでは，エンタングルメントによりメリットを十分に引き出すことは難しい．それゆえ，エンタングルメントの度合いの低い状態から，最大エンタングルド状態をどの程度取り出せるかが一つのテーマとなる．もちろん，この際 2 つの系にまたがった量子操作を許せばいくらでも最大エンタングルド状態を作り出すことができる．このような問題設定では，局所量子操作と古典的な情報通信しか許さないということが重要な意味を持つ．

第 9 章
様々な形の量子通信

第 4 章で扱った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や，第 3 章，第 6 章で扱った量子状態を検定したり推定したりする問題は，古典系でも考えることができる．これらの問題では量子系特有の問題というよりは，量子系特有の取り扱いの難しさ（非可換性）が問題のポイントであった．

しかし，量子系での情報処理には古典系での情報処理を単に非可換化したものではなく，古典系では考えられなかったものも含まれる．それゆえ，量子情報理論は従来の情報理論の非可換化以上の意味を持つことになる．この中で鍵となるのは第 8 章でも取り扱ったエンタングルメントである．第 8 章ではエンタングルメントの定量的な取り扱いしか行なわなかったが，この章では，エンタングルメントを用いることで初めて実現できる古典系では考えられなかったタイプの通信を紹介する．それに加えて，量子状態の伝送（量子誤り訂正）や，盗聴者を考慮した通信，その他第 4 章で扱えなかった複雑なタイプの通信も合わせて紹介する．しかも，量子状態の伝送と盗聴者を考慮した通信は密接な関係にあり，量子状態の伝送におけるノイズと，盗聴者がいる場合の量子通信における盗聴者との間には明確な対応関係がある．

9.1 量子テレポーテーション

もともとエンタングルド状態に注目するという発想は Einstein らによって量子力学の不完全性を主張するために用いられた．しかし，最近になって，Bennett [19] らが逆にその効果を利用する量子操作である量子テレポーテーションを提案したことで，エンタングルド状態の取り扱われ方も変わってきた．この量子テレポーテーションに必要な数学的知識は初等的なものに限られており，その理解も容易であるので，ここで紹介することにする．

量子テレポーテーションとは，エンタングルド状態をあらかじめ共有することで，量子状態を直接送ることなく，古典的なメッセージを伝送するだけで，量

第 10 章
量子系での情報源符号化

我々がコンピュータを使うときには圧縮ソフトはもはや不可欠なツールとなっている．なぜそのようなことが可能なのだろうか？ 我々が日常的に接している情報は色々な意味で冗長である場合が多い．これは言葉を変えるとある種の規則性があるということになる．たしかに，目の前のキーボードを全くでたらめに打ち込んでもそれが意味のある文章やプログラムになることはまずない．例えば，0 と 1 の系列で，$2n$ 番目の数と $2n+1$ 番目の数が全く同じになる数列が 1000 桁並んでいたとしよう．この場合，電話で相手にこの数字の列を伝えるときに，そのまま全部を口頭で伝える人はまずいないであろう．はじめに，$2n$ 番目の数と $2n+1$ 番目が全く同じであることを告げ，その後に，偶数番目の（もしくは奇数番目の）数字のみ伝えるであろう．もしくは，さらなる規則性がないか考えるのではないであろうか？ コンピュータの圧縮ツールではそれぞれの文字列（もしくは数字の列）をそれを再現する別の文字列に変換することで，記憶に必要なメモリを圧縮することに成功している．このように圧縮プロセスは符号化とも見ることができ，第 4 章で扱った通信路符号化と区別するためしばしば情報源符号化とよばれる．

量子系でも同様に冗長な情報があれば，それをより小さい量子メモリで保存もしくは伝送できるのであれば有効であろう．しかし古典系と異なり，どのような状況を考えるかによって，少なくとも 2 つの問題設定が考えられる．

1 つは量子コンピュータのメモリの圧縮であり，量子コンピュータが実用可能なレベルで実現されれば十分に需要が現れると思われる．メモリの圧縮においては，ある系の状態を別のより次元の小さい系の状態に変換し，再び，変換された系から元の系の元の状態に復元することが要求される．ここでは，圧縮の際に系の状態が何であるかわからないことがポイントである．もう 1 つは量子暗号で伝送する量子系の次元の圧縮である．この場合では，送信者がどのような量子状態を伝送しようとしているかわかっていることがポイントで，前者よりも圧縮の際の手段が多くある．もちろん，圧縮された系から，元の系に復

付録

極限及び線形代数特論

A.1 極限について

このテキストでは準備される系の数 n が十分大きくなったときの漸近的な振る舞いを扱うことが多くなる．そのため，$n \to \infty$ での極限操作を取ることが多い．以下，簡単に極限についてまとめておく．一般に数列 $\{a_n\}$ を考えたとき，その極限値 $\lim a_n$ が存在するとは限らない．a_n が $+\infty$ や $-\infty$ に発散する場合などがその例であるがその場合は，$\lim a_n = +\infty$ または $\lim a_n = -\infty$ と記すことにする．だが，a_n が n が偶数のとき 0 で奇数のとき 1 と定義されている場合などは，$n \to \infty$ で a_n は振動するので，$+\infty$ や $-\infty$ を許してもその極限値は存在しない．この場合に存在するのは $\underline{\lim} a_n$ や $\overline{\lim} a_n$ であり，$\underline{\lim} a_n = 0$，$\overline{\lim} a_n = 1$ となる．もう少し正確に $\underline{\lim} a_n$ 及び $\overline{\lim} a_n$ の定義を与えると，

$$\underline{\lim} a_n \stackrel{\text{def}}{=} \sup\{a | \forall \epsilon > 0, \exists N, \forall n \geq N, a \leq a_n + \epsilon\},$$
$$\overline{\lim} a_n \stackrel{\text{def}}{=} \inf\{a | \forall \epsilon > 0, \exists N, \forall n \geq N, a \geq a_n - \epsilon\}$$

となる．もちろん $\underline{\lim} a_n = \overline{\lim} a_n$ となるときには，$\lim a_n$ は存在し，それは $\underline{\lim} a_n = \overline{\lim} a_n$ と一致する．そして極限に関して以下の 3 つの補題が成り立つ．

補題 A.1 実数列 $\{a_n\}_{n=1}^{\infty}$ が

$$a_n + a_m \leq a_{n+m} \tag{A.1}$$

を満たし，$\sup_n \frac{a_n}{n} < \infty$ となるとき，極限値 $\lim \frac{a_n}{n}$ が存在し，

$$\lim \frac{a_n}{n} = \overline{\lim} \frac{a_n}{n} = \sup_n \frac{a_n}{n} \tag{A.2}$$

が成立する．もちろん，$-a_n$ を考えることで，$a_n + a_m \leq a_{n+m}$ を満たし，$\inf_n \frac{a_n}{n} > \infty$ であれば，$\lim \frac{a_n}{n} = \underline{\lim} \frac{a_n}{n} = \inf_n \frac{a_n}{n}$ が成り立つことも確認できる．

証明 はじめに m を固定すると，各 n に対して，l_n と r_n が $0 \leq r_n \leq m-1$ と $n = l_n m + r_n$ を満たすように一意に取れ，

$$\frac{a_n}{n} = \frac{a_{l_n m + r}}{l_n m + r} \geq \frac{a_{l_n m}}{l_n m + r} + \frac{a_r}{l_n m + r} \geq \frac{l_n a_m}{l_n m + r} + \frac{a_r}{l_n m + r}$$

主要参考文献

量子計算を含めた量子情報科学のテキストとしては以下が挙げられる．[N-C] は量子計算から，量子情報理論にわたる量子情報科学全般に渡ってバランスよく書かれたテキストである．本書では扱えなかった代数的な符号の構成について書かれている．[Helstrom],[Holevo] は今となっては古いが，当時の量子情報理論の最先端のテーマを扱っている．[番] は番雅司氏個人の web 上で公開されている現在更新中のテキストである．分量は 1000 ページを超え，かなりの分野を網羅しているが，やや計算機科学的な内容は弱い．また，[広田 1] は当時の量子情報理論の最先端をコンパクトにまとめたテキストであり，[広田 2] は近年のそれをコンパクトにまとめている．[信学会] はこの分野の最先端の話題を概観した特集号である．他は，量子計算のみに限って書かれたテキストである．

[**N-C**] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).

[**Holevo**] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, (North-Holland, Amsterdam, 1982). ロシア語版は 1980 年．

[**Helstrom**] C. W. Helstrom, *Quantum Detection and Estimation Theory,* (Academic Press, New York, 1976).

[**細谷**] 細谷暁夫，量子コンピュータの基礎，臨時別冊・数理科学 SGC ライブラリ-4, (サイエンス社，1999).

[**西野**] 西野哲朗，量子コンピュータ入門，(東京電機大学出版局，1997).

[**上坂**] 上坂吉則，量子コンピュータの基礎数理，(コロナ社，2000).

[**Gruska**] J. Gruska, *Quantum Computing*, (McGraw-Hill, 1999) 邦訳 伊藤正美，今井克暢，岩本宙造，外山政文，森田憲一共訳，量子コンピューティング，(森北出版，2003).

[**広田 1**] 広田修，光通信理論，(森北出版，1985).

[**広田 2**] 広田修，量子情報科学の基礎，(森北出版，2002).

[**信学会**] 今井浩 編，電子情報通信学会誌 8 月号，小特集 量子情報科学 (2002).

[**番**] 番雅司，量子情報物理学,（更新中），http://physics.cside.com/

その他，量子情報理論でのテーマでこのテキストでは十分に触れることができなかった内容を扱った解説記事としては以下が挙げられる．7.1 節 7.2 節の内容についての歴史的な経緯については [小澤] を読んで頂きたい．また，量子暗号や量子誤り訂正への符号理論の適用については [浜田] が優れている．そして，量子推定の実験については [林] 及びその参考文献が参考になる．

[**小澤**] 小澤正直，不確定性原理・保存法則・量子計算，日本物理学会誌，3 月号，157-165 (2004).

[**浜田**] 浜田充，シンプレクティック幾何と量子情報理論，応用数理学会誌，Vol.14, No.1, 2-12 (2004).

[**林**] 林正人，量子系の統計的推測と量子相関，物性研究 **80-5**, 662-699 (2003).

量子力学のテキストはたくさんあるが，量子情報科学のために量子力学を学ぶのであれば，比較的量子力学の数学的構造に注目して書かれたテキストが良い．このようなテキストとして以下があり，これらのテキストは，このテキストで割愛した Bell の不等式についても書かれている．

[**Sakurai**] J. J. Sakurai, *Modern Quantum Mechanics*, (Addison-Wesley, Massachusetts, 1985). 邦訳 桜井明夫訳，現代の量子力学，(吉岡書店，1989).

[**清水**] 清水明，量子論の基礎，臨時別冊・数理科学 SGC ライブラリ-22, (サイエンス社，2003).
この新版：「新版 量子論の基礎」新物理学ライブラリ別巻 2（同社刊）が，2004 年 4 月に出版された．

一方，量子情報理論の研究に参考となる情報理論のテキストとしては以下がある．量子系において量子相関を用いた測定を行なった場合，それから得られるデータ系列は必ずしも独立ではない．そのような一般的なデータ系列に対する理論としては [韓] が最も詳しい．[C-T] は情報理論のテーマを幅広く集めた文献であり，多くの欧米の量子情報理論の研究者はこのテキストから情報理論を学んだと言われる．[C-K] は情報理論の中のタイプ理論について書かれたテキストで [植松] はそのテキストを要約した和書である．[有本] は情報理論の数学的理論を一通りきれいに要約している．

[**韓**] 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); 英訳: *Information-Spectrum Methods in Information Theory*, (Springer-Verlag, New York, 2002).

[**有本**] 有本卓，確率・情報・エントロピー，(森北出版，1980).

[**植松**] 植松友彦，現代シャノン理論，(培風館，1998).

[**C-T**] T. Cover and J. Thomas, *Elements of Information Theory*, (John Wiley & Sons, New York, 1991).

[**C-K**] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, (Academic Press, New York, 1981).

情報幾何については，以下がある．[甘・長 2] は [甘・長 1] の英訳ということになっているが，量子情報幾何の部分については [甘・長 2] の出版の際に大幅に書き加えられたため，別のテキストと見るべきであろう．[甘・長 2] は量子情報幾何についての最も充実したテキストである．

[**甘・長 1**] 甘利俊一・ 長岡浩司，情報幾何の方法，(岩波書店，1993).

[**甘・長 2**] S. Amari and H. Nagaoka, *Methods of Information Geometry,* (AMS & Oxford University Press, 2000).

数理統計学については以下の [統計] が基礎的な事項を含めて解説したテキストとして定評がある．量子暗号を含む情報理論的暗号については和書では以下の [岡・山] が優れている．

[**統計**] 竹内啓，数理統計学，(東洋経済新報社，1963); 竹村彰道，数理統計学の基礎，(創文社，1991); 野田一雄・宮岡悦良，数理統計学の基礎，(共立出版，1992).

[**岡・山**] 岡本龍明・山本博資，現代暗号，(産業図書，1997).

なお，紙数の都合で他の参考文献は下記のサポートページに載せることになった．必要に応じてダウンロードして頂きたい．

http://www.saiensu.co.jp/support.htm

量子情報科学での多くの論文は Los Alamos にあるプレプリントサーバーに登録されている．参考文献で，quant-ph/0301*** のように書かれているものは，全て下記のページからダウンロードできる．

http://xxx.lanl.gov/abs/quant-ph/

あとがき

著者が量子情報理論の研究を始めたのは著者が修士 1 年の学生であった 1994 年の 10 月末ごろであった．当時は既に Shor の素因数分解の論文は世に出ていたものの，私自身はそのような研究が存在することも知らず，また量子情報理論の研究は十分に認知されてはいなかった．そのような状況の中，著者がどのようにして量子情報理論に出会ったか，簡単に書いてみることにする．このようなことは著者の個人的な体験であるが，これから大学院に進み研究を志す方に参考になるかもしれないと思い書く次第である．そもそも，著者は京都大学の理学部に入学してから学科制が無いことを良いことに，数学と物理の両方を勉強していた．それは，著者自身の興味が物理という自然法則に興味があるものの，いわゆる物理の考え方には十分になじめず，思考方法としてはどちらかというと数学に向いていたためである．その結果，学部時代は数学についてはそれなりに理解できたが，物理の方は芳しくなかった．特に,（学部段階では）物理的な思考形態が最も現れる統計力学については散々であった．4 年生の段階では宇宙論の研究室に所属したものの，結局，大学院に進学する段階になって，自分の物理の理解のレベルでは院試にパスすることは難しいと判断し，数学の大学院を受け，なんとかギリギリのラインで合格できた．それでも，4 年生の終わりまでは，宇宙論の研究室で初期宇宙をテーマに卒業研究を行ったわけであるが，全く統計物理がダメだったため散々な出来であった．そんな中，大学院進学後からある塾で物理を教えることになったのであるが，そのことを，とある物理の教官に話したところ,「私だったら絶対，君に物理を教えさせない.」と言われ相当落ち込んだことを覚えている．それほど，私の当時の物理の出来は散々であった．卒業研究の単位は頂けたが，落第点を与えられたようなものであった．

そして，4 月になり，大学院に入学して，当時，興味を持っていた相対論の関係から数理物理の中でも Twistor 理論 [285] を上野教授の下で研究することになった．しかし，このテーマは多くの数理物理と同じように，題材そのものは，物理に起源があるものの，本質的に取り扱っているものは数学に他ならなかった．また，そこに現れる数学的概念の物理的必然性もほとんど理解できなかった．結局，私の興味に合わず，他のテーマを探すことになった．そもそも，著者はそれなりに数学的な思考はできたが，数学そのものには結局のところほとんど関心が無かったので，数学だけにのめり込んで研究生活を行うことは不可能であった．一方で，大学院入学後に塾で高校の物理を教えることで初めて物理が理解できたと感じることができた．難しい数学に目が行きがちであった著者はこのとき初めて，基本概念の積み重ねで理解することの意義が理解できたように思える．

そのような経緯から色々な研究テーマを探していた頃，大阪大学の藤原彰夫講師（当時）に出会い，Holevo のテキスト [Holevo] の存在を教えて頂き，量子情報理論の研究を始めることになった．それまで，著者は物理的対応の付かない抽象的な数学理論を勉強していたが，それとはうって変わって Holevo のテキストはさして抽象度が高くない概念で量子力学の基礎概念である測定が見事に数学的概念で表現されていることに感銘を受けつつ，読み進んだことを覚えている．今から思えば，Holevo のテキストもそれなりに分かりにくいが，それまで著者が読んできた数学書はそれ以上に難解であったため，さほど問題にはならなかった．

今から振り返ると，当時は特に物理の中では量子力学の観測に関係する問題は哲学的な問題に結びつくからやるべきでないという雰囲気が強かったため，物理の大学院に進学しなかったことは，

量子情報をやる上で良かったのかもしれない．このように考えてみると，学部学生のときから，修士課程の段階で色々と回り道をしたように思えるが，結局は今の研究テーマについては最短に近いルートを歩んだようにも思える．

ただ，研究を始めるにあたって，一つの問題があった．著者はそれまで，数学と物理しか勉強していなかったので，数理統計学などの情報科学を全く理解していなかったのである，特に，数理統計学は，履修する機会があったにもかかわらず，全く勉強しなかった．学部時代の著者は，統計学などは便宜的な学問であり，物質の本質を見極める物理学に比べて軽く見ていたところがあった．しかし，Holevo のテキストを読むことでそのような考えを改めることになった．なぜなら，物理の根本をなす量子力学を数学的に整理すると，測定値が確率的であるため，統計学的視点を持ち込むことなしに，観測者が得る情報というものを定量的に評価することができないからである．結局，大学院に入ってから学部時代に本来やっておくような数理統計学や情報理論の勉強を行うことになった．結局，修士論文の段階では，十分に数理統計学を理解することなく研究することになった．

このような研究テーマを選んだため，周囲に研究上のディスカッションの相手が居なかったことも自分にとっては大きな問題であった．そのため，自分で遠方の研究者とのディスカッションの機会をアレンジする必要があった．さらに，博士課程進学後は収入の面でも安定せず，塾や高校での非常勤講師のアルバイトの合間に研究しているような時期もあった．その上，博士課程の最初の半年間はうまくディスカッションの機会を設定することも出来ず，研究も滞りがちであったた．そのような中，1996 年 11 月からスタートした量子計算研究会（関西）は自分とは比較的近い研究の話題について話せる場であり，おかげで研究生活を継続することができた．この時期には東京大学の松本啓史助手（当時）から統計学について電話で色々と教わり，統計学の素養を身に着けることができ，感謝する次第である．一方でこのようなわがままな学生を理研に就職するまで，面倒を見てくれた上野健爾教授には感謝している．

振り返って見ると，10 年もしない間に量子情報理論を取り巻く状況が全く変わってしまった．そのようなことを踏まえ，量子情報理論を含む将来的展望について簡単に述べてみたい．

最近では，高度な量子操作も実現できるようになり，様々な量子プロトコルが実現できるようになった．今後の発展を動機づける意味でも比較的実現が容易なプロトコルの提案が必要であろう．そして，物理学の基礎付けにフィードバックすることも有意義であると思う．特に，量子情報理論を経て情報科学から吸収したノウハウは物理学の基礎付けには有効であると思われる．その他，実現に近付きつつある量子暗号についてはもっと，情報理論的に緻密に解析する必要があると思う．

多くの研究者の努力により量子情報理論もそれなりに認知されるようになったが，既存の学科の枠組みで運営されている大学では，その取り扱いに困っているのではないかと思っている．本来，学問には境界など無いはずであり，量子情報理論のように既存の学科の枠組で捉えきれない分野の取り扱いを考えることで，より柔軟に対応できる創造的な研究・教育体制について考えることができると不遜ながら思っている．

色々と身勝手なことを書いてしまったが，今後 1 人でも多くの既存の分野に満足できない方がこのテキストを読んで量子情報理論やそれに関わる研究分野で活躍することを期待しつつ筆を置くことにする．

記号一覧

索　引

ア

カ

サ

タ

ナ

ハ

マ

ヤ

ラ

欧字

著者略歴

林　正人
はやし　まさひと

1996年　京都大学大学院理学研究科数学・数理解析専攻（数学系）修士課程修了
1998年　日本学術振興会特別研究員
1999年　京都大学大学院理学研究科数学・数理解析専攻（数学系）博士後期課程修了，博士（理学）
理化学研究所脳科学総合研究センター研究員，
科学技術振興機構 ERATO 今井量子計算機構プロジェクト技術参事，
同 ERATO-SORST 量子情報システムアーキテクチャーグループリーダー，
東北大学大学院情報科学研究科准教授を経て，
現　在　名古屋大学大学院多元数理科学研究科教授
専　門　量子情報理論，量子系の統計的推測

臨時別冊・数理科学 SGC ライブラリ-32
『量子情報理論入門 An Introduction to Quantum Information』（電子版）

著　者　林 正人

2018年5月10日　初版発行　ISBN 978-4-7819-9953-1
この電子書籍は2004年5月25日初版発行の同タイトルを底本としています．

数 理 科 学 編 集 部　　発行人　森 平 敏 孝
TEL.(03)5474-8816
FAX.(03)5474-8817

ホームページ　http://www.saiensu.co.jp
ご意見・ご要望は　sk@saiensu.co.jp まで．

発行所　© 株式会社 **サイエンス社**　　TEL.(03)5474-8500（代表）
〒151-0051 東京都渋谷区千駄ヶ谷1-3-25

本誌の内容を無断で複写複製・転載することは，著作者および出版者の権利を侵害することがありますので，その場合にはあらかじめサイエンス社著作権担当者あて許諾をお求めください．

組版　三美印刷