連載講座

量子情報処理パラダイム
3. 量子情報科学

松本　啓史

概要

量子力学の観測の理論など，量子情報科学の基礎となる概念を説明し，この分野で現在どのような研究が行われているかを概観する．

1. はじめに

量子力学の世界観が日常の直感と著しく反することは広く喧伝されている通りである．一方，情報科学の諸分野では，その基礎的な概念は，日常的直感の成り立つ世界，古典力学的な世界観に無意識的に立脚している．もし，系の状態の記述や測定の概念を量子力学的なそれに置き換えたら，情報科学はどう変わるであろうか．これは，量子力学や情報科学の根本的問題への理解を深める上で，興味深い問いである．

量子情報ブームの主要な要因の一つとして，古典的な情報処理で不可能なタスクが実現可能になることが挙げられる．多項式時間での素因数分解，盗聴を確実に検出する鍵配布（量子鍵配布，量子暗号）などがそれである．量子鍵配布などは，実用を目指した本格的な実験がすでに行われている．ただし，このような派手な成果の陰には観測の理論の急速な整備や，量子情報科学の基礎理論の充実があることを忘れてはならない．

現在，量子情報科学は成熟期に入っており，専門分化が進んでいる．それとともに，量子○○理論の研究に古典の○○理論の深い知識と豊富な経験が必要とされるようになってきた．しかし，特に日本では，情報科学的背景を持った研究者の参入が遅れている．読者の方々が，各々の専門分野の知識を生かして量子情報科学に参入して頂けたら幸いである．

本稿では，量子情報科学の基礎と，先端の研究を簡単にレビューする．現在，一人の研究者で量子情報科学の全分野をカバーするのは難しくなってきているが，筆者の能力と紙幅の許す限り，バランスの取れたレビューをしたい．

まつもと　けいじ
科学技術振興事業団 今井プロジェクト
〒113-0033 文京区本郷5-28-3

2. 量子力学，状態，測定

この節の内容については，文献[23]のI-2章がよい解説である．また，文献[25]も大いに参考になるが，戦後の測定の理論の成果を文献[23]などで補う必要がある．数学的に緻密な議論は文献[24]やその参考文献を参照されたい．

2.1 状態と測定

量子力学では，系の状態，測定は複素行列を用いて表される．これらの行列が住むベクトル空間を**表現空間**という．ある物理系の理論を展開するとき，表現空間の次元をどうとるかは，物理的な考察によって決められる．例えば，電子などの粒子は，軌道運動の他に内部的な「回転」に対応する自由度（スピン）を持つと考えられている．この自由度に対応する表現空間は$\mathbb{C}^2$である[25]．

物理の慣習にならって，縦ベクトルを$|u\rangle=(u_1 u_2 \cdots)^T$，その複素共役転置を$\langle u|=(u_1^* u_2^* \cdots)$で表す．

量子力学は確率的な理論で，ある系に測定を行うと，その測定結果は確率的にのみ定まる．この確率分布は，系の状態と測定の関数である．系の状態は**密度行列（密度作用素）**という

$$\rho=\rho^*,\ \mathrm{tr}\,\rho=1,\ \rho\geq 0 \tag{1}$$

を充たす行列で表され，測定は，instrumentという行列の組$\{A_\omega\}_{\omega\in\Omega}$で表現される．ここで，＊は複素共役転置（disjoint）を表し，ωは測定値，Ωは可能な測定値全体の集合であり，A_ωは

$$\sum_{\omega\in\Omega} A_\omega^* A_\omega=\mathrm{Id} \tag{2}$$

を充たすとする（Id：単位行列）．

今，ρで表現される状態の系に，測定$\{A_\omega\}_{\omega\in\Omega}$を

施すと，確率 $\mathrm{tr}\, A_\omega^* A_\omega \rho$ で観測値 ω が得られ，このとき系の状態は

$$\frac{A_\omega \rho A_\omega^*}{\mathrm{tr}\, A_\omega^* A_\omega \rho} \tag{3}$$

へと変化する．先ほどの電子のスピンの場合，物理で'z 軸方向のスピンの測定'といわれる測定があるが，それは測定値として↑(upspin)，↓(downspin) を返し，対応する instrument は，

$$A_\uparrow = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad A_\downarrow = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

と書ける．この測定は，不均一磁場を通過した電子の軌道の曲がり方を観測することで実現できる[25]．

2.2 合成系

表現空間が $\mathcal{H}_A$，$\mathcal{H}_B$ となる二つの系をまとめて一つの系とみるとき，これを**合成系**といい，その表現空間は，以下に定義する，$\mathcal{H}_A$，$\mathcal{H}_B$ のテンソル積空間 $\mathcal{H}_A \otimes \mathcal{H}_B$ である．

ベクトル空間 $\mathcal{H}_A$，$\mathcal{H}_B$ の正規直交基底系を $\{|e_i^A\rangle\}$，$\{|e_j^B\rangle\}$ とする．そして，形式的な積 $|e_i^A\rangle \otimes |e_j^B\rangle$ を考え，正規直交基底系 $\{|e_i^A\rangle \otimes |e_j^B\rangle\}$ で張られる空間が $\mathcal{H}_A \otimes \mathcal{H}_B$ である．$\mathcal{H}_A \otimes \mathcal{H}_B$ の次元は $\dim \mathcal{H}_A \times \dim \mathcal{H}_B$ に等しい．

2.3 量子情報処理で可能な操作

量子情報科学の理論の発展の基礎として，量子力学で原理的に可能な状態操作が数学的に美しく特徴付けられているていることが挙げられる．つまり，情報処理の際に何が可能か，ということの必要十分条件が簡潔に呈示されているのである．

測定のように系から情報を取らない場合，次のような操作のみが許されることがわかっている．すなわち，ρ が ρ' に変化した場合，(2)を充たすある行列の組 $\{A_\omega\}_{\omega\in\Omega}$ を用いて，

$$\rho' = \sum_{\omega\in\Omega} A_\omega \rho A_\omega^* \tag{4}$$

と書けなければならない．ただし，この場合，ω には測定値という意味合いはなく，単に和をとるためのインデックスである．(4)の様に書ける行列から行列への写像を，TPCP 写像（Trace Preserving Compretely Positive Map）という．からである．符号化その他，状態に対して行う情報処理も，(4)の形に限らなければならない．さらに，状態から情報を引き出す操作，すなわち測定は小節 2.1 で述べた形のものに限られる．これらの理論は戦後の観測の理論の重要な成果であり，現代の量子情報科学はその基礎の上に成り立っている[24]．

2.4 古典系の記述

建前としては，古典力学は量子力学から導かれることになっている．実際にはこの導出はあまり成功していないと思うが，量子力学的な記述の枠組で，古典的な情報処理が記述できることは確かである．

まず，ある基底 $\{|e_i\rangle\}$ を固定する．そして，行う観測および操作は $A_j = \sum_i a_{i,j} |e_i\rangle\langle e_j|$ と書けるものに制限する．そして，状態は基底 $\{|e_i\rangle\}$ で対角化されているもののみを考える．すると，密度行列 $\sum_i p_i |e_i\rangle\langle e_i|$ は確率分布 $\boldsymbol{p} = (p_1, \cdots, p_{\dim\mathcal{H}})$ に，TPCP 写像 $\{A_j\}$ は確率遷移行列 $[|a_{i,j}|^2]$ を持つ Markov map に，それぞれ対応する．

つまり，量子情報科学は古典情報科学の拡張に（少なくとも形式上は）なっている．量子情報科学の理論研究の結果，新しい視点が情報科学に導入されることもある．特に，通信理論では量子通信理論から，古典通信理論の問題としても新しくて興味深い問題がいくつも呈示されている．

3. 量子情報処理の「からくり」

量子情報科学と古典情報科学とを根本的に分けるものは一体何なのであろうか．

まず，第一に量子力学では，測定はかならず状態の変化を伴う．これは実は量子鍵配布（量子暗号）などではこのことを積極的に利用する．量子統計推測や cloning ではこのことは逆に困難性として現れる．

第二に entanglement の効果である．entanglement は，古典確率では説明できない，量子系特有のある種の相関のことである．もしも，合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ の上の状態が $\mathcal{H}_A$ 上の状態 $\rho_{A,i}$，$\mathcal{H}_B$ 上の状態 $\rho_{B,i}$ を用いて

$$\rho = \sum_i p_{i,j} \rho_{A,i} \otimes \rho_{B,j} \tag{5}$$

と書けていなければ，ρ は separable であるといわれる．なぜなら，$\mathcal{H}_A$ と $\mathcal{H}_B$ の「相関」はは古典的確率分布 $p_{i,j}$ で決まるからである．separable でないとき，状態 ρ は entangle している，という．このとき，A と B の間に古典的には説明できない不思議な相関が現れる．

4. 量子情報科学の諸分野

4.1 Teleportation など

entanglement の不思議を最も端的に表すのが，

teleportationである．これは，AからBへの量子状態の伝送を古典的な情報の送信のみで行うプロトコルである．もしも，量子状態が既知のものであれば，その記述を送信することでBの側で再構成できる．しかし，この方法は膨大な情報を伝送する必要があるし，また状態が未知の場合には全く使えない．

今，AとBがあるengangleした状態を共有しているとしよう．この場合，わずか1ビットの古典的情報を送ることで未知の$\mathbb{C}^2$上の量子状態を相手に送れることが知られている（teleportation，文献[3]）．

その他，通信計算量の節約，古典情報伝送の効率化，wartermarking，information hidingなどで，entanglementを巧妙に用いたプロトコルが多く提案されている．

4.2 量子鍵配布

量子情報ブームの重要な要因は，古典的に不可能であったタスクが実現可能になるからである．Wiensnerそして後に独立にBenett-Brassardによって提案された量子鍵配布（量子暗号）はその代表的な例である．

量子鍵配布の目的は，暗号の秘密鍵を離れた二者間で，通信路を介して安全に共有することである．今，量子状態に鍵を符号化して送信する．伝送されている状態に盗聴者が測定を施したとすると，その状態は(3)式の様に変化してしまい，受信者はその変化から盗聴の事実を検知できる．もし盗聴が判明したら，その鍵は捨て実際の暗号通信では使用しない．このようにして，100%原理的に安全な暗号通信が可能となる．

この原理は直観的にはわかりやすいが，意味のある形で安全性の証明をするのはやさしくはない．なぜなら，状態をわずかに乱すだけで一定量の情報を盗聴することができるなら，実質上は盗聴可能とみなすのが自然だからである．現在は，この辺りの定量的評価がかなり緻密に行われており，如何なるアタックに対しても「指数的に安全」であることが証明されている[4, 14, 18, 20, 26]．このような証明が可能であるのは，盗聴者に可能な操作が小節2.3でのように明確に表現されているからである．

4.3 量子bit commitment，その他

AはBにある情報が封印された箱を送る．この箱は，Aが後に鍵を渡したときに初めて開けることができるようにつくられており，さらに，鍵で開けるまで，BもAも箱の中身を改変できないようになっているとする．これをbit commitmentといい，暗号で重要な概念である．bit commitmentを計算量的な意味ではなく，情報理論的な意味で実現しようという提案がBenett，Brassard[2]によってなされ，後に類似の提案があいついでなされた．しかし，後にそれらのプロトコルはentanglementを用いた巧妙なアタックで破られてしまった[12, 17]．のみならず，Lo and Chao，Mayersらにより，情報理論的bit commitmentの不可能性が証明されてしまった[13, 19]．この証明では，近似的なbit commitmentの可能性もまとめて否定されてしまっている．量子情報処理の限界が示されたことは残念なことではあるが，この強力な主張が厳密かつ簡潔に証明されたことは驚くべき達成である．

bit commitmentに関連した話題として，離れた二者間で通信路を介して偏りのないコイン投げが実現できるか，という問題がある．これはもしもbit commitmentができれば簡単に実現できる．しかし，その不可能性が証明された以上，コイン投げの成否を検討することは興味深い話題である．ただし，完全に公平なコイン投げの不可能性は，bit commitmentの証明と同様の議論で，Loにより証明されている[13]．近似的なコイン投げについては，Mayersら[21]の提案があるが，近年，このプロトコルが安全でないことを強く示唆する結果が得られてしまっている[11]．少なくとも，現在の所，εの偏りのコイン投げを実現するには，多数回$\left(O\left(\log\log\frac{1}{\varepsilon}\right)\text{回}\right)$の通信が必要であることがわかっている[1]．

このように色々とプロトコルやタスクが提案されると，量子情報処理でそもそも何が可能で不可能か，という問が自然に湧いてくる．この問題についての系統的なアプローチとしては，Koashi-Imotoの理論がある[10]．これは極めて強力な武器であり．例えば，暗号のプロトコルが成立するための条件が明らかになっているし，また，steganography（情報が埋め込まれている事実そのものを隠す技術）の実現のために必要な条件も導出に成功している[22]．その他，量子通信理論で重要な諸結果を簡潔に導出するのに用いられるなど，広い応用がある．量子情報処理は古典情報処理を含むから，Koashi-Imoto理論の結果は，古典の場合にもそのまま用いることができる．

4.4 量子通信理論

量子情報科学は1960年代のHelstromによる，量子光通信の研究にはじまる[7, 8]．このHelstromの

研究から直接派生した分野が量子通信理論と量子統計推測である．

量子通信理論は大まかに二つの問題設定がある．第一には，メッセージを量子状態を媒体としていかに効率よく伝送できるかを論じる．この問題設定では，媒体として用いた量子状態は著しく損なわれても構わないとする．それに対して第二の問題設定では，量子状態そのものの効率的な保存と伝送を論じる．例えば，ノイズのある通信路を通して量子的なプロトコルを行うためにはこのような問題を考えなければならない．また，同様の理論は量子計算のノイズに対する頑健さを増すためにも有望である．

メッセージの伝送/圧縮，そして量子状態の圧縮については，レートの限界はもちろん，強逆性，誤り指数，ユニバーサルコーディングなどの深い理論が発達している．しかし，量子状態の伝送については，レートの限界についても今だにきれいな一般論はない．

さて，量子状態の圧縮，伝送の古典での対応物は，確率分布列の圧縮，伝送である．これは新しい問題設定であり，とくに確率分布列の圧縮率の限界（正確にいうとvisible coding におけるそれ）は，mutual informationの新しい操作的意味を与えると予想されている[31]．そのほか，reverse Shannon theoremなど，古典通信理論からみても興味深い話題が多く生み出されている[30]．

4.5 量子統計推測

量子統計推測は，光通信の受信過程の解析から始まった．まず研究されたのは，与えられた未知の状態が，$\rho_1, \rho_2, \cdots, \rho_M$ のうちどれであるのかを判別する，という問題である（判別問題）．

これはある主の半正定値計画問題であり[27]，その一般論，特に相補性定理を適用することで最適な測定の必要十分条件を書き下すことができる（Holevo, Yuen-Kenedy-Lax[9, 29]）．判別問題で，未知の状態の候補が連続無限個ある場合を推定問題というが，この場合にも相補性定理が成立する[5]．

しかし，Holevo-Yuen-Kenedy-Laxの条件は非線形な連立行列方程式・不等式であるので，一般的にはこれを解くことは難しい．そこで，問題が群の作用により不変な構造を持つとか，または未知の状態のコピーが数多く与えられている（漸近論）などということを仮定したりする[6]（この辺りの事情は古典の統計推測でも同じである）．

古典統計と量子統計の決定的な差は，「非可換性」である．古典統計で複数の統計量を計算する場合，どの統計量を先に計算するかで答えは全く変わらない．量子統計で統計量に相当するものは測定であるが，これは行列の組で表され，行列の積は非可換である．「非可換性」が量子力学の最も顕著な特徴であることは古くから注意されてきたが，量子統計推測においては特にそれが顕著に表れる．そこで，量子統計推測の理論を押しすすめることで，「非可換性」に新しい角度から光をあてることができる[15, 16]．

量子情報処理を行うためには適切な量子状態を生成する必要があるが，その精度のチェックにも量子統計推測の応用が期待され，実験的研究も行われている．

量子情報，量子計算の理論において量子統計推測的な考察が必要になることがしばしばあり，ある意味で，量子情報全般の基礎となる分野である．

参考文献

[1] A. Ambainis, Proceedings of the 2001 Annual ACM Symposium on Theory of Computing, (2001).

[2] C. H. Bennett and G. Brassard, In Proceeding of IEEE Int. Conf. on Computers, Systems, and Signal Processings (Bangalore, India, 1984), IEEE, New York, (1984), pp. 175-179.

[3] C. H. Bennett, et. al., Phys. Rev. Lett., 70, (1993), pp. 1895-1899.

[4] E. Biham, et. al., In Proceedings of the 32 nd Annual ACM Symposium on Theory of Computing (ACM Press, New York, 2000), pp. 715-724.

[5] M. Hayashi, E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/9704044 (1997).

[6] 林　正人, 松本啓史, 応用数理, Vol. 11, No. 3, (2001), pp. 223-234.

[7] C. W. Helstrom, Physics Letters, **25A**, (1967), pp. 101-102.

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

[9] A. S. Holevo, *Journal of Multivariate Analysis*, Vol. 3, (1973), pp. 337-394.

[10] M. Koashi, N. Imoto, E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/0101144 (2001). E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/0103128 (2001). E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/0104001 (2001). E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/0203045 (2001).

[11] B. Leslau, E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/0104075 (2001).

[12] H. K. Lo and H. F. Chau, Phys. Rev. Lett., 78, (1997), p. 3410.
[13] H. K. Lo and H. F. Chau, Physica D, 120, (1998), pp. 177-187.
[14] H. K. Lo and H. F. Chau, Science, 26, (1999), pp. 2050-2056.
[15] K. Matsumoto, J. Phys. A, to appear.
[16] K. Matsumoto, E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/9711027 (1997). Quantum Communication, Computing, and Measurement 2 (edited by Kumar, P., D'ariano, G. M., and Hirota, O.), Plenum, New York, (2000), pp. 105-110. E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/0006076 (2000). A geometrical approach to quantum estimation theory, doctoral thesis, Graduate School of Mathematical Sciences, University of Tokyo, (1997).
[17] D. Mayers, E-print http://xxx.lanl.gov/abs/quant-ph/quantu-ph/9603015 (1996).
[18] D. Mayers, Proceedings of Crypto '96 (1996), pp. 343-357.
[19] D. Mayers, *Physical Review Letters*, **78** (1997), pp. 3414-3417.
[20] D. Mayers, J. ACM 48, (2001), pp. 351-406.
[21] D. Mayers, L. Salvail, Y. Chiba-Kohno, E-print http://xxx.lanl.gov/abs/quant-ph/quantu-ph/9904078 (1999).
[22] S. Natori, M. Koashi, K. Matsumoto, unpublished manuscript.
[23] M. A. Nielsen and I. L. Chuang, Quantum Computation and Information, Cambridge University Press, (2000).
[24] 小澤正直, 観測理論の数理, 数理物理への誘い 3 (江沢洋編), 遊星社, (2000), pp. 163-189.
[25] J. J. Sakurai, 現代の量子力学(上), 吉岡書店, (1985), pp. 2-30.
[26] P. W. Shor and J. Preskill, Phys. Rev. Lett., 85, (2000), p. 441.
[27] L. Vandenberghe and S. Boyd, Semidefinite Programming, *SIAM Review*, Vol. 38, No. 1, (1996), pp. 49-95.
[28] Wiesner Stefen, *Sigact News*, **15** (1983), pp. 77-88. unpublished manuscript written in 1970.
[29] H. P. Yuen, R. S. Kennedy and M. Lax, *IEEE Trans. Information Theory*, Vol. IT-21, No. 2, (1975), pp. 125-134.
[30] C. H. Bennet, et al., E-print http://xxx.lanl.gov/abs/quant-ph/quant-ph/0106052 (2001).
[31] W. Dür, et al., Phys. Rev. A, Vol. 64, 022308, (2001).