跡見学園女子大学マネジメント学部紀要　第 32 号　（2021 年 7 月 25 日）

量子情報科学へのアプローチ

Approach to Quantum Information Science

深　町　浩　祥
Hiroyoshi FUKAMACHI

要　旨

本稿では、量子コンピュータ論のファッション化にともない、一般にも注目されている量子情報科学の歴史と基礎概念について考察した。近年、人工知能（AI）などに続く革新的技術として期待されるものに量子コンピュータの実用化が挙げられている。米法人は 2019 年理論上の概念だった性能を実証し、最先端のスーパーコンピュータで 1 万年かかる問題を瞬時に解く実験に成功したと発表した。その後、量子コンピュータへの期待やリスクについての言説が流行している。

量子コンピュータの可能性への理解のためには、量子コンピュータを実現するために研究されている量子情報科学と、その理論的基礎となっている物理学と数学の知識が必要である。しかし、その内容は直観的な日常世界の常識とは異なる要素を含んでいる。

そこで本稿では、量子情報科学を理解するために必要な量子力学、情報科学そしてコンピュータの歴史的な経緯を考察した。続いて、量子情報科学を理解する上で必要な物理学と数学の基本概念を概観した。古典力学が成立しない量子力学的世界の概念、そして、古典力学の世界観では生じなかった多数の問題を解決するための基本的数理概念について整理した。

キーワード：量子情報科学、量子力学、情報科学、量子コンピュータ

はじめに

本稿の目的は、量子情報科学が誕生するまでの歴史的経緯を考察するとともに、量子情報科学の特殊性を基本的な物理学および数学を用いて明らかにすることにある。

2019 年 10 月に米グーグルは、理論上の概念だった性能を実証し、最先端のスーパーコンピュー

タで１万年かかる問題を瞬時に解く実験に成功したもようだと報じられた[1]。その後、インターネットなどで使う暗号が解読されかねない[2]ため危険であるという言説や、桁違いの計算速度により、製造現場や都市交通の問題を解決するだけでなく、将来の様々な分野のイノベーションも期待されるという言説[3]など、量子コンピュータへの過度な期待とリスクが取り上げられるようになった。量子コンピュータを語ることがファッション化し、基礎概念や現実の研究成果を反映していない言説が流布しており混乱を招いていると考えられる。

現代の情報科学はノーバート・ウイナー[4]（Norbert Wiener）やクロード・シャノン[5]（Claude Shannon）らによって創設された通信と情報に関する数理理論を基盤としている。そして、シャノンらの理論体系に量子力学の原理を統合する理論の体系化が研究された。量子情報科学は、量子論の中でも情報理論に関する研究領域である。しかし、量子情報科学は、量子力学と情報理論との単純な組み合わせではないので、両者の知識を組み合わせれば理解できるというものではない。一方、量子コンピュータは、コンピュータの概念に量子力学を融合するものであり、その研究は、アラン・チューリング[6]（Alan Turing）、リチャード・ファイマン[7]（Richard Feynman）、デイビット・ドイチュ[8]（David Deutsch）、ピーター・ショア[9]（Peter Shor）など多くの研究者により蓄積がある。量子情報科学や量子コンピュータの理解には、量子力学、情報理論、数学、物理、光学、エレクトロニクスと様々な分野を横断する知識が求められる。したがって、量子情報科学には様々な背景をもった研究者がおり、術語の用いられ方や解釈が統一されていないため、

1　「量子コンピュータで「超計算」人類の手中に」日本経済新聞 2019 年 10 月 19 日 https://www.nikkei.com/article/DGKKZO51143200Y9A011C1MM8000/（2021.01.23 閲覧）

2　「量子計算機の衝撃　新たな暗号で解読防げ」日本経済新聞 2019 年 11 月 13 日 https://www.nikkei.com/article/DGXMZO52100640S9A111C1X90000/（2020.01.23 閲覧）

3　「量子コンピューター先駆け D ウェーブが描くスゴい未来」日本経済新聞 2021 年 1 月 19 日 https://www.nikkei.com/article/DGXZQOGR18BTM0Y0A211C2000000/（2021.01.25 閲覧）

4　Norbert Wiener “*Cybernetics, Science and Society*”, Mit Pr 1986. 通信工学と制御工学を融合し、生理学、機械工学、システム工学を統一的に扱うことを意図して作られた学問であるサイバネティックスの提唱者。

5　Claude Shannon, “*A Mathematical Theory of Communication*”, Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, 1948. 情報を定量的に扱えるように定義し、情報理論という新たな数学的理論を創始した。

6　後に「チューリングマシン」とよばれる想像上のコンピュータが初めて示された「計算可能数とその決定問題への応用」という論文を 1936 年に発表。

7　R. P. Feynman, “*Simulating physics with computers*”, International Journal of Theoretical Physics, 21, pp. 467-488, 1982. 量子力学のルールで動作するコンピュータの必要性を指摘。

8　D. Deutsch, “*Quantum theory, the Church—Turing principle and the universal quantum computer*”, In Proceedings of the Royal Society of London A, 400 (1818), pp. 97-117, 1985. チューリングマシンを定式化。

9　P. W. Shor, “*Algorithms for quantum computation: Discrete logarithms and factoring*”, In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994. 素因数分解アルゴリズムを発見。

理解することが難しい部分がある。そこで本稿では、できる限り専門知識の背景がなくとも量子情報科学への導入部分を理解できるように、量子力学と情報科学の基本的な概念を中心に整理する。

初めに、量子情報科学の歴史について、量子力学、情報科学そしてコンピュータの側面からそれぞれ概観する。次に、量子情報科学を理解する上で必要な、不確定性関係や重ね合わせ状態など、量子力学の基本概念を整理する。そして、物理現象を記述するための数学的な基本概念を整理する。最後に、以上の考察を踏まえて、量子情報科学の現代的な意義と将来性について検討することにしたい。

1　量子情報科学小史

量子情報科学について考察するにあたり、その基礎となる量子力学誕生までの物理学[10]、コンピュータおよび情報理論の歴史を概観する。

1－1　量子力学の誕生

量子情報科学を理解する前提として、はじめに量子力学誕生までの物理学の歴史を概観する。

物理学の世界ではこれまでに、ガリレオ・ガリレイ（Galileo Galilei）[11]による天体の円運動の発見、アイザック・ニュートン（Isaac Newton）[12]による運動方程式の定式化や万有引力の発見、さらにジェームス・クラーク・マクスウェル（James Clerk Maxwell）[13]による電磁気学の確立など、粒子の運動と波の運動という重要な規則が発見されてきた。これらの力学と電磁気学は古典物理学[14]と呼ばれ、現在でも有効に機能している[15]。

しかし、物質を構成している原子や電子を観測する技術が成熟すると、古典物理学で説明できない現象が観測されるようになった[16]。いわゆる、二重スリット実験[17]を電子で行ったところ、予想に反して干渉縞が現れた。電子は、波と粒子の両方の性質も持つようにふるまったのである。

10 「物」のふるまいを支配する「理」を探求する学問が物理学である。
11 Galileo Galilei “*Dialogo sopra i due massimi sistemi del mondo*”, 1632.
12 参考：山本義隆（1997）『古典力学の形成―ニュートンからラグランジュへ』日本評論社
13 Maxwell JC “*On reciprocal figures and diagrams of forces*”, Philos Mag 26: 250-261, 1864.
14 「古典」とは消極的な意味合いではない。現在でも、ある一定の条件では自然現象を理解する上で有効である。
15 藤井啓祐（2019）『驚異の量子コンピュータ』岩波書店、2-5 頁。
16 同上、6 頁。
17 光の波動性を示したトマス・ヤングの実験が知られている。

このような、電子のふるまいは波と粒子を別のものと捉える古典物理学では説明できない[18]。そこで、古典物理学では別ものと考えられていた波と粒子という性質は、それらを超越した何かの別の側面であると考えられるようになった[19]。

ドイツのマックス・プランク（Max Planck）[20] は、これまで波と思われていたものに決まったエネルギーをもった粒子のような性質を発見した。そして、電磁波のエネルギーは連続的なエネルギーを取りうるのではなく、最小のエネルギー単位があり、離散値[21] をとるというプランクの量子仮説を 1900 年に提唱した[22]。このエネルギーの最小単位のことを量子という。1905 年にはアルバート・アインシュタイン（Albert Einstein）が物質に照射した光による電子の放出を説明する中で光が粒子のようなふるまいをすることを指摘していた[23]。一方、フランスの物理学者ルイ・ド・ブロイ（Louis de Broglie）[24] は、物質も波であるという物質波の概念を導入する。そして、1925 年にドイツの理論物理学者ヴェルナー・ハイゼンベルグ（Werner Heisenberg）は、粒子の運動を拡張する行列力学を定式化した[25]。また、1926 年にオーストリアの理論物理学者エルヴィン・シュレーディンガー（Erwin Schrödinger）は波の運動の理解を拡張する波動力学を定式化した[26]。この二つの定式化は等価であることがわかり、波と粒子を統一した新たな概念である「量子」の力学が確立した。量子力学以前の古典力学では量子のもつ波と粒子の二つの性質のうち、片方の性質だけしか見えていなかったことになる[27]。

量子力学では、電子の波と粒子の二重性をどのように捉えるのかが問題となる。現実的には、電子のふるまいを追跡することはできない。そこで、量子力学では、どこに粒子があるのかを確認しない限り粒子の位置は確定せず、空間的な広がりをもった曖昧なものであると考える。当時の物理学者たちは、粒子がどの位置にどれくらい存在するかという可能性の大きさが波に対応していると考えたのである。そのような考えは、いろいろな位置に粒子が存在する可能性が重なっているので「重ね合わせの原理」と呼ばれる[28]。ひとつの電子であっても、曖昧な広がりをもち

18　藤井・前掲注（15）7 頁。

19　同上、9 頁。「ネッカーの立方体」ずっと見ていると、どちらの面が手前になっているかが入れ替わる。そして、その二つの性質を同時に見ることはできない。

20　Planck, Max. “*On the Law of Distribution of Energy in the Normal Spectrum*” Annalen der Physik 309 (3): 553-563, 1900.

21　非連続な値。

22　Planck, Max “*Ueber das Gesetz der Energieverteilung im Normalspectrum*” Annalen der Physik 309 (3): 553–563, 1900. 藤井・前掲注（15）10 頁。

23　藤井・前掲注（15）11 頁。

24　“*Recherches sur la théorie des quanta Thesis*”, Paris, 1924, Ann. de Physique (10) 3, 22, 1925.

25　Heisenberg, W. “*Über quantentheoretishe Umdeutung kinematisher und mechanischer Beziehungen*”. Zeitschrift für Physik. 33 (1): 879-893,1925.

26　Schrödinger, E. “*An Undulatory Theory of the Mechanics of Atoms and Molecules*” Physical Review. 28 (6): 1049-1070,1926.

27　藤井・前掲注（15）11 頁。

ながら様々な場所に存在し、可能性の波として伝わると考えるのである。電子は観測するまでは可能性の波が広がり、観測する（電子を見る）ことにより可能性の波の強弱に依存して電子の位置がはじめて確定する（可能性の収縮）。このように電子の二重スリット実験の結果を解釈することで、途中までは波であり、観測によって粒子となる、という電子の二つの要請を取り込むことができたのである[29]。

この解釈には量子に関する重要な三つの性質が含まれている。第一の性質は、観測するまでは電子の所在が確定せず、曖昧に様々な可能性が重ね合わさっていること（重ね合わせの原理）。第二に、その可能性は波としてふるまうため、干渉して強め合ったり弱め合ったりすること（波動性）。第三に、電子の位置を観測すると可能性は収束し一粒の粒子になること（波束の収縮）、である[30]。

量子力学は、古典力学では説明のできなかった微視的な世界の物理現象を解明し、現代の物理学の基礎となっている。

1－2　量子情報科学の誕生

続いて、量子情報科学誕生までのコンピュータと情報科学の歴史を概観する。

初期のコンピュータと呼ばれるもので代表的なものとしては、イギリスの数学者チャールズ・バベッジ（Charles Babbage）が発明した蒸気機関で動く歯車を利用した階差機関が挙げられる。歯車の歯という離散的な量を整数に対応させているバベッジの発明はデジタルコンピュータである。しかし、バベッジの階差機関はその複雑さにより実現しなかった。

現在のコンピュータでは計算が抽象化され、計算することと計算を行う物理系（半導体素子）とが切り離されている。そのため、そのアルゴリズムを理解するために半導体素子などの物理学を理解する必要はない。この現代のコンピュータの原型を提案したのが、イギリスの数学者アラン・チューリングである[31]。

チューリングによって、現代のコンピュータと互換性のあるチューリングマシンが 1936 年に提唱された[32]。チューリングマシンの概念で重要な点は、数値を離散的な整数値で表現するデジタル方式であったことである。これにより、計算を実行する機械に誤差があっても離散化した各整数の範囲を越えなければ同じ値を表現できるようになり、情報の正確さを確保できるようになった。デジタル情報を表現する具体的な物理系（連続的な値）とその上で実行される計算（デジタ

28　藤井・前掲注（15）13 頁。
29　同上、14 頁。
30　同上、14-15 頁。
31　同上、21 頁。
32　参考：Morten Tyldum (2014) movie “*The Imitation Game*”.

ル＝離散的な値）を切り離して議論することが可能となったのである [33]。

一方、情報理論の発展に寄与したのが米国の電気工学者・数学者クロード・シャノンである。シャノンは 1937 年にスイッチング回路 [34]（リレー）を用いた計算を数学的に定式化した [35]。続いてシャノンは、情報量を測るという課題に取り組み、シャノンエントロピーと呼ばれる情報量を測るための尺度を定義し、情報理論（シャノン理論）を創設した。チューリングにはじまる計算理論とシャノンにはじまる情報理論が、情報科学の二つの大きな流れとなっている [36]。

ドイツにおいて電気的に動作するコンピュータ（Z3）がスイッチング回路を用いて製作された。しかし、消費電力が大きく、スイッチの動作速度に計算速度が制限される問題があった。コンピュータの動作速度を測るには、クロック数 [37] という単位が用いられる。Z3 のクロック数は 5Hz であり、1 秒間に 5 回程度の計算しかできないものであった [38]。この計算速度の問題を解決するため、電気的な制御で演算を行える真空管を用いたコンピュータが 1946 年に開発された [39]。その後、新しい演算素子トランジスタの登場によりコンピュータの歴史は大きく変わる。トランジスタは小さな素子で高速な計算を可能にした。さらに、1960 年代には膨大な数のトランジスタを一つのチップ上に並べることができるようになり、集積回路（IC: integrated circuit）の時代となる。そして、1970 年代にはデータの入出力の制御やそのデータに対する演算など、コンピュータが行う処理の中心部分（CPU: central processing unit、中央処理装置）をまとめて一つのチップで行うマイクロプロセッサが登場する [40]。

この後、1 枚のチップに微細にトランジスタを搭載する技術が進歩し、性能の向上と微細化が進んだ [41]。しかし現在、マイクロプロセッサの微細化が限界を迎え、配線に流れる電流が量子的にふるまうことで演算が困難になってきている。その原因は、電子が量子的にふるまう領域に入

33　藤井・前掲注（15）23 頁。
34　電流が流れているか否かによってスイッチのオン・オフが変わる回路。
35　スイッチはオン・オフの 2 種類の状態しかないので、0 と 1 の二つの状態のみを用いて計算を行う。このような二つの状態をもつ変数のことを情報の最小単位としてビット（bit: binary digit の略）という。このような、0 と 1 だけの演算は論理演算と呼ばれる。シャノンよりも先に研究していたのが日本人として、日本電気（NEC）の中嶋章がいる。参考：山田昭彦（2010）「スイッチング理論の原点を尋ねて」『Fundamentals Review Vol.3 No,4』IEICE 電子情報通信学会 基礎・境界ソサイエティ 9-17 頁。藤井・前掲注（15）24 頁。また、1 ビットは 1 シャノンである。シャノン（shannon）は、IEC 80000-13 で定められた情報量およびエントロピーの単位である。
36　藤井・前掲注（15）24 頁。
37　1 秒間に基本的な演算を何回実行できるかという値。
38　現在私たちが使っているコンピュータのクロック数は数ギガ Hz（1 秒間に数十億回の演算）である。
39　エニアック（ENIAC）：真空管 17,000 本搭載。クロック数は約 100kHz（1 秒間に 10 万回の基本演算）。
40　世界初の商用マイクロプロセッサ i4004 はインテル社が開発。これにより、個人でも所有できる小型のコンピュータの製造が可能になった。スティーブ・ジョブズらによる Apple I の発売が 1976 年。藤井・前掲注（15）27-28 頁。

り、配線を飛び越えることで発熱[42]と消費電力増加が起こり、さらにクロック数を上げることが難しいと考えられた[43]。そこで、発熱しないコンピュータの実現が志向された。計算のためのエネルギー消費問題については、情報科学の知見だけでは解決できないため、情報処理を行う物理系に注目する必要がある。そこで、1920年代の量子力学の確立に始まる現代物理学と1930年代に始まった情報科学、それぞれが独立して発展した物理学と情報科学が1980年代に入り融合することになる。

IBMフェローであったロルフ・ランダウア（Rolf Landauer）は「情報は物理である（Information is physical）[44]」と考え、1961年にランダウア情報消去の原理[45]を提案した。これは、情報消去にはエネルギー消費[46]を伴う、いいかえれば、情報を消去しなければエネルギー消費がないというものである。

一般に、計算においては情報の消去が行われている。例えば、NOT演算[47]におけるビット[48]の反転（0と1が入れ替わる）では、反転された結果から反転される前の状態が推測可能であり（可逆計算）、情報は消去されていない。しかし、AND演算（掛け算）[49]では、入力1,1→出力1＊1=1以外の演算結果はすべて0が出力されるため、もとの入力状態（1,0）、（0,1）、（0,0）は特定できない（不可逆計算）。つまり、情報が消去されたことになり、ランダウア情報消去の原理により計算途中でエネルギーが消費され発熱することになる[50]。これらのことから、可逆な基本演

41　ムーアの法則（Moore's law）：インテル創業者の一人であるゴードン・ムーアが、1965年に自らの論文上で唱えた「半導体の集積率は18か月で2倍になる」という半導体業界の経験則。

42　情報を処理するためには、脳内のシナプスやノートのメモなど何らかの物理装置に記憶される必要がある。計算をする場合には、その情報をなんらかの物理法則にしたがって操作しなければならないため、物理法則から逃れることはできない。また、CPUの熱問題は、ノートに書いた鉛筆のメモを消すためには紙と消しゴムの摩擦により熱が発生し消しゴムが消費されることに近い。藤井・前掲注（15）30-31頁。

43　同上、29頁。

44　古田彩（2004）「二人の悪魔と多数の宇宙：量子コンピュータの起源」『日本物理学会誌 5巻8号』日本物理学会、512頁。Rolf Landauer, "*Phys.Today*" 44 (5) 23-29,1991.

45　Rolf Landauer, "*Irreversibility and heat generation in the computing process*", IBM Journal of Research and Development, 5 (3): 183–19,1961.

46　エントロピー増大の過程と言い換えることができる。エントロピーは、熱力学において断熱条件下での不可逆性を表す指標である。（一方、情報理論におけるエントロピーは、そのできごとの起こりにくさを表す尺度であり、確率によって決まるものである。）

47　NOT演算は単項演算であり、1つの値を反転する演算である。（真）⇄（偽）。

48　情報の基本単位であり、二進数の1桁のこと。Binary digit。

49　AND演算は論理積と呼ばれる。1と1のAND演算結果だけが1になる。演算する2つの値の両方が1（真）なら演算結果が1（真）すなわち、「aかつbが真なら結果は真」となる。二進数では1でなければ0であるから，その他の演算結果は0になる。

50　計算の論理状態の数が計算によって減少すると、熱力学第二法則によりエントロピーを減少させないように、各論理的状態に対応する物理的状態の数がそれを補完するだけ増加し、結果として熱が発生する。

算だけを用いてコンピュータを構成すればエネルギーが消費されず、発熱を抑えることになる [51]。

上記のことから、演算そのものは可逆に行うことができて、そこにエネルギー消費はないのであれば、すべて可逆計算すればよいことになる。そこで、1 ビットの AND 演算を可逆化するためには、3 ビットを入力として 3 ビットを出力する演算を利用する。これにより、3 ビット中の 2 ビットは入力をそのまま出力して、残りの 1 ビットに計算結果を格納することで可逆性を実現できる [52]。

NOT 演算と AND 演算を組み合わせれば、ビット列を入力とするすべての計算ができる。しかし、AND 演算を可逆化する際、入力を出力として書き出すため、計算終了後に求める結果以外の計算履歴が残ることになる。この履歴を消去するために計算サイズにともなってエネルギーが消費されては可逆化した意味がなくなる。そこで、この問題を解決したのが、エドワード・フレドキン（Edward Fredkin）[53] とトマッソ・トフォリ（Tommaso Toffoli）[54] である。求める結果だけを書き出し（コピー）し、それ以外の履歴を消すために可逆性を利用して逆計算をするアンコンピューテーションを行う [55]。これにより、計算の履歴は初期状態に戻り、原理的に発熱しない可逆操作のみから計算結果だけを取り出すことができるコンピュータを構成できることになった。

このように、エネルギーを消費しない計算として可逆計算が研究されてきた。しかし、熱力学第二法則が教えるように、多くの物理操作は不可逆的な現象であるため、可逆計算のためには可逆な物理プロセスの発見が必要であった。そのような状況下で、1980 年にアメリカの物理学者ポール・ベニオフ（Paul A. Benioff）は、可逆計算を可能にする物理系として、可逆性を潜在的にもつ量子力学を提案した [56]。なぜならば、量子力学の方程式は時間の向きを入れ替えても同じ形になっていることが知られており、量子力学に従う系は必ずある時刻の状態から過去の状態へと戻すことが原理的に可能である [57] ためである。このようにして、情報科学（計算）と量子力学が接近したが、その目的は古典コンピュータを可逆にするために、可逆性をもつ量子力学を利用

51　藤井・前掲注（15）33 頁。

52　XOR 演算（足し算）について考える。XOR 演算も同じ出力となる入力がある（0,0 → 0、1,1 → 0、0,1 → 1、1,0 → 1）ので可逆的でない。XOR 演算の場合は入力を二つとも残す必要はなく（0,0 → 0,0、1,1 → 1,0、0,1 → 0,1、1,0 → 1,1）、2 ビット演算で可逆化することができる。

53　アメリカの計算機科学者、物理学者。可逆計算（フレドキン）ゲートを考案。

54　アメリカのコンピュータ科学者、物理学者。可逆論理（トフォリ）ゲートを提案。Toffoli, Tommaso “*Reversible Computing*”Technical Report MIT/LCS/TM-151 an adapted and condensed version 1980.

55　Fredkin, Edward, Toffoli, Tommaso “*Conservative Logic*” International Journal of Theoretical Physics. 21 (3–4): 219-253, 1982.

56　Paul Benioff, “*The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines*”, Journal of Statistical Physics, 22, 563, 1980.

57　藤井・前掲注（15）37 頁。

するものであり、古典コンピュータをこえるコンピュータをつくるというものではなかった。

1－3　量子コンピュータの誕生

本節では、量子情報科学誕生までの量子コンピュータの歴史を概観する。

古典コンピュータから量子コンピュータの構築へ貢献したのはアメリカの物理学者のリチャード・ファインマン（Richard Feynman）[58] である。ファインマンは 1981 年 5 月、アメリカのマサチューセッツ工科大学で開かれた会議「物理と計算（Physics and Computation）」において、「結局、自然は古典力学的ではないから、古典的な解析はうまくいかないものである。もし自然をシミュレートしたいのなら、量子力学的にやる必要がある」と述べた [59]。このファインマンの講演は、その後、量子コンピュータの有用性を最初に予言したものとして、長く記憶されることとなる [60]。1980 年代当時、コンピュータでシミュレーションをすることによって物理を理解するというアプローチが発展する中、量子力学に従って運動する物理系を古典コンピュータでシュミレーションすると、必要なメモリーや計算時間が物理系のサイズに対して指数関数的に大きくなることがわかっていた。ファインマンは物理系シミュレーションのためには量子力学の原理を取り込んだコンピュータの構築が必要だと唱えた。

同時期にイギリスの物理学者デイビット・ドイチュは計算の原理は従来の古典的な論理計算に限定される必要はないと考え、量子力学で動くコンピュータの原型、量子版のチューリングマシンを定式化した。これが、現在につながる量子コンピュータの起源である [61]。ドイチュは実際に量子チューリング機械があらゆる量子力学過程を表せることを証明し、これを汎用量子コンピュータと名づけた [62]。

米国の理論物理学者のベンヤミン・シューマッカー（Benjamin Schumacher）は量子情報を定量化する量子ビット（キュービット）を提唱 [63] し、アメリカの理論物理学者ウィリアム・ウッタース（William Wootters）はランダウアと長年共に研究したチャールズ・ベネット（Charles Bennett）らとともに量子テレポーテーションの基礎理論を構築した [64]。

量子コンピュータの誕生に間接的ながら主要な役割を演じたランダウアはその後、量子コン

58　1965 年、量子電磁力学の構築により、ジュリアン・S・シュウィンガーや朝永振一郎とともにノーベル物理学賞を共同受賞。
59　古田・前掲注（44）516-517 頁。
60　同上、517 頁。
61　藤井・前掲注（15）40 頁。
62　D. Deutsch: Proc. R. Soc. London A 400 97-117, 1985.
63　B. Schumacher: Phys. Rev. A 51 (4) 2738-2747, 1995.
64　C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters: Phys. Rev. Lett. 70 (13) 1895-1899, 1993.

ピュータ批判の急先鋒となる。量子コンピュータは計算を進めるにつれてエラーが積み重なり、それを訂正する術がない。ゆえに物理的に実現できず、そんなコンピュータの計算理論など意味がない、と繰り返し指摘した[65]。彼の鋭い舌鋒はドイチュら若手を奮起させ、最初のエラー訂正アルゴリズム[66]の考案など、量子コンピュータを実現するための研究を大いに加速した[67]。

人間の指から集積回路まで、これまで人間が使ってきた計算の道具は、すべて我々の目に見える世界にある[68]。しかし、量子コンピュータは計算の道具を、私たちの目に見えない世界、つまりヒルベルト空間[69]に拡張した初の計算機である。ヒルベルト空間は実空間よりもずっと多様で大きいので、従来よりも速く、多彩な計算が可能になる[70]。

次章以降では、量子情報科学における物理学と数学の基本的な概念について整理する。

2　量子力学からのアプローチ

量子力学は、微視的世界の現象を高精度で記述する物理学の基礎理論である[71]。従って、量子情報科学にアプローチするためには、情報理論と量子力学を理解することが必要となる。しかし、量子力学を厳密に理解することよりも、「ある状態の下で、ある（物理量の）測定を行ったとき、どのような確率で測定値が得られるか？」[72]という命題（確率規則）を基本軸として、量子系の状態[73]や測定[74]の理論的記述、さらに状態の時間発展[75]の法則および合成系[76]の記述を理解すれば、量子力学の基本的理論構造の準備としては十分である[77]。本章では、不確定性原理と重ね合

65　古田・前掲注（44）518 頁。

66　A. Barenco, A. Berthiaume, D. Deutsch, A. K. Ekert, R. Jozsa and C. Macchiavello: SIAM J. Comput. 26 (5) 1541-1557,1997.

67　古田・前掲注（44）518 頁。

68　同上、17 頁。

69　完備な内積空間をヒルベルト空間という（後述）。

70　古田・前掲注（44）517 頁。

71　石坂智ほか（2020）『量子情報学入門』共立出版、15 頁。

72　石坂・前掲注（71）16 頁。

73　“状態”は物理学では重要な術語。情報理論としては、「あらゆる物理量の測定に対する応答を定めるもの」といえる。測定の確率的な予言を行う量子力学においては、「あらゆる物理量の測定を行ったときの測定値の確率分布を定めるもの」として定義される。量子力学では、状態と物理量（あるいは測定）を、それぞれベクトルや行列などの数学で表現してから、確率規則を通じて測定に対する応答を定めることになる。なお、量子系の状態を量子状態と呼ぶこともある。同上、18 頁。

74　物理系には、物体の物理的性質を表す様々な物理量がある。例えば、（粒子の）位置、運動量、エネルギー、（スピン）角運動量、また、（光子の）偏光などである。物理量は（原理的に）測定可能なものである必要がある。同上、17-18 頁。

75　時間の経過による状態の変化。

76　複数の物理系をまとめて対象とする場合の物体の把握の仕方。

わせの原理を中心に整理する。

2－1　不確定性原理

ハイゼンベルクは1927年に、ある特別な関係を持つ二つの物理量は完璧な精度で観測することが原理的にできないことを示した[78]。そして、一方を精度よく観測しようとすると他方はますます不正確になるとして、その精度には次のような関係が成り立つことを示した。

$$\Delta x \times \Delta p \approx h$$

ただし、Δは誤差を表す。これが不確定性原理または不確定性関係とよばれる量子的な特徴である[79]。量子力学では、このような不確定性原理を物理学に導入する。

古典力学では、物体自体がどの瞬間でもある確定した状態にあることを前提にしている。これに対して、量子力学は確定した状態にある物体は実在しないと考えなければならない。しかし、位置あるいは運動量のうち、どちらか一方の物理量が確定した状態は許される。その場合、他方の物理量は完全に不確定（値を持たない）となる。このように、不確定性原理は物体の存在に関しても次の関係を与える。

$$\Delta x \times \Delta p \geq \frac{\hbar}{2}\text{定数}\quad \hbar = \frac{h}{2\pi}\ \text{(換算プランク定数)}$$

ここで、Δは系統誤差や測定の精度などによる誤差ではなく、物体の存在（物理量の測定値）に関する不確定性である[80]。この式は、位置と運動量が同時に確定している状態はないことを示している。

以上のように、古典力学では自然法則として物体の存在が確定しているが、不確定性原理は自然界にある物体の存在に関する不確定性と観測の限界を規定している[81]。

微視的世界における物体は波動関数[82]をもっている。波動関数は電子であれば位置と運動量に対応する物理量の関数である。シュレーディンガーによって、この波動関数が従うべき方程式が

77　石坂・前掲注（71）16頁。

78　広田修（2002）『量子情報科学の基礎：量子コンピュータへのアプローチ』森北出版、24頁。「ガンマ線顕微鏡」とよばれる思考実験で、量子の位置xと運動量pは本質的な意味で不確定で、その測定値には必ずその不確定性程度のばらつきがある。そして、位置の不確定性と運動量の不確定性の積にはプランク定数hに比例する下限があることを示した。松浦壮（2020）『量子とはなんだろう』講談社、109頁。

79　hはプランク定数であり、量子論を特徴づける基本的な普遍定数。その値は$h \cong 6.626 \times 10^{-34}[J \cdot s]$。後述の$\hbar$は、換算プランク定数（ディラック定数ともいう）であり、$\hbar \cong 1.054 \times 10^{-34}[J \cdot s]$。

80　Δx：位置の広がり（不確定性）、Δp：運動量の広がり（不確定性）。

81　広田・前掲注（78）25頁。

82　波動関数$\psi(x, t)$は系の状態を表す（ψは複素数）。

導出されたが、その波動関数の意味に関して、デンマークの理論物理学者ニールス・ボーア（Niels Bohr）、ドイツの理論物理学者マックス・ボルン（Max Born）、ハイゼンベルグらが一つの回答を与えた。それは、コペンハーゲン解釈[83]とよばれるもので、「量子系の物理量（位置あるいは運動量）を表す演算子の固有値の関数として表現される波動関数の絶対値の2乗はその固有値が観測される確率を表す。」というものである。この解釈によれば、不確定性原理における不確定性は観測される値の確率的な分散として定量化することができる[84]。これらをまとめると、量子力学の成立過程は次のようになる。

(1) 記述したい物理系の物理量は量子規則[85]と実験事実に、矛盾しないように対応させられた演算子で表される。
(2) その物理量がどのような状態にあるかを表すのは波動関数である。
(3) その波動関数はシュレーディンガー方程式[86]に従って運動する。
(4) 実際に物理量がどのような値を持っているのかを知るために観測しようとすれば、対応する演算子の固有値の関数として表現される波動関数の絶対値2乗が測定値の確率分布を与える。
(5) この確率は観測者の知識不足を表すのではなく、量子の世界が必然として持っている不確かさが、観測によって具現化したものである[87]。

このように量子力学は、波動関数の運動に関する理論体系と測定過程をもつのである。

2－2　量子測定過程

本節では、量子の測定過程[88]を記述するための理論である量子測定理論について整理する。

コペンハーゲン解釈にもとづけば、測定値は確率変数となり、まったく同じ波動関数であっても観測ごとに測定値は異なった値をとる。さらに、量子力学の理論構成において、ある測定値が得られれば、その物理系の波動関数は測定値に対応する波動関数になっていなければならないことが要請される。したがって、測定過程の構造は次のようになっている。

83　量子力学の初期段階では、このコペンハーゲン解釈と、アインシュタイン、ド・ブロイやシュレーディンガーらによる実在解釈が主導権を争っていた。

84　広田・前掲注（78）25頁。

85　ボルンの規則。

86　“確率を表す波”が満たす方程式（シュレーディンガー方程式）

$$i\hbar\frac{\partial\psi(x,t)}{\partial t}=\left[-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}+V(x,t)\right]\psi(x,t)\quad \text{略記 } i\hbar\frac{\partial\psi}{\partial}=\hat{H}\psi\quad \hat{H}\text{ は演算子ハミルトニアン。}$$

87　広田・前掲注（78）25-26頁。

88　ここで、観測とは観測する行為のことを表し、測定とは観測という行為を実行するための手法とする。波動関数が満たすシュレーディンガー方程式では、測定過程は記述することはできない。

（1）ある波動関数をもつ物理量を観測すると仮定する。

（2）物理量はエルミート演算子[89]で表され、測定値はその演算子の固有値で表される。

（3）測定値（固有値）は波動関数の絶対値の2乗で表現される確率にしたがって測定結果として出現する。

（4）測定値が確定した瞬間、波動関数はその測定値（固有値）に対応する固有関数になる。このような状況を“波束の収縮”という。

（5）固有関数になるというのは、そのような状態でもう一度同じ観測をしたら確率1で同じ値を得ることを意味する[90]。

波束の収縮のような瞬間的な変化を数学的に記述するためには、波動関数を抽象空間の量子状態ベクトル $|\psi\rangle$ として表現し、物理量を表すエルミート演算子を抽象空間上の自己共役作用素として扱う理論が有用である[91]。

1932年にハンガリー生まれのアメリカの数学者ジョン・フォン・ノイマン（John von Neumann）は、ヒルベルト空間[92]と自己共役作用素を用いて、量子力学の数学的基礎を達成した。その本質的な論理は下記のとおりである。

89　$A=A^{\dagger}$ を満たす A はエルミート演算子（または自己共役演算子）とよばれる。石坂・前掲注（71）304頁。

90　広田・前掲注（78）26-27頁。

91　演算子・作用素はいずれも英語のoperatorの訳である。伝統的に物理学では演算子と訳され、数学では作用素と訳されている。河東泰之（2004）「演算子・作用素というパラダイム」『数理科学No.490』サイエンス社、5頁。広田・前掲注（78）27頁。

92　ヒルベルト空間：以下の性質(1)-(3)を満たす演算 $|\psi\rangle$、$|\phi\rangle\in V\rightarrow\langle\psi|\phi\rangle\in\mathbb{K}$ を持つベクトル空間を内積空間とよぶ。(1) $\langle\psi|\phi\rangle\geq 0$（正値性）ただし等号成立は $|\psi\rangle=0$ のときに限る（正定値性）、(2) $\overline{\langle\psi|\phi\rangle}=\langle\phi|\psi\rangle$（対称性）、(3) $\langle\psi|a\phi+b\xi\rangle=a\langle\psi|\phi\rangle+b\langle\psi|\xi\rangle$（線形性）。$\langle\psi|\phi\rangle$ をベクトル $|\psi\rangle, |\phi\rangle$ のエルミート内積または単に内積とよぶ。(3)より零ベクトルと任意の内積は零である。(3)を繰り返し用いると、内積の線形性 $\langle\psi|\sum_i a_i\psi_i\rangle=\sum_i a_i\langle\psi|\psi_i\rangle$ を得る。$\mathbb{K}=\mathbb{C}$（$\mathbb{K}$ は、実数の集合 $\mathbb{R}$ または複素数の集合 $\mathbb{C}$）のとき、(2)と(3)より左側の要素に関しては、共役線形であることに注意する $\langle a\phi+b\xi|\psi\rangle=\overline{a}\langle\psi|\phi\rangle+\overline{b}\langle\psi|\xi\rangle$。

2つのベクトル $|\psi\rangle$、$|\phi\rangle$ は $\langle\psi|\phi\rangle=0$ を満たすとき直交するという。内積空間には自然なノルム（ベクトルの大きさ）$\|\psi\|:=\sqrt{\langle\psi|\psi\rangle}$ が定義される。ノルムが1のベクトルを単位ベクトルとよぶ。零ベクトルでない任意の $|\psi\rangle$ に対し、$|\tilde{\psi}\rangle:=|\psi\rangle/\|\psi\|$ は（$|\psi\rangle$ と同じ向きの）単位ベクトルである。$|\psi\rangle$ から $|\tilde{\psi}\rangle$ を求める操作を規格化（あるいは正規化）とよぶ。互いに直交する単位ベクトルの集合 $\{|\psi_i\rangle\}_{i=1}^{n}$ を正規直交系とよぶ（正規直交条件は、クロネッカーのデルタ記号（$\delta_{ii}:=1, \delta_{ij}:=0(i\neq j)$）を用いて $\langle\psi|\phi\rangle=\delta_{ij}$. 正規直交系は一次独立である。よって d 次元内積空間 V において d 個の正規直交系 $\{|\psi_i\rangle\}_{i=1}^{d}$ は基底となる。これを正規直交基底という。

ベクトルの列 $(|\psi_n\rangle)_{n\in\mathbb{N}}$ は、$n, m\rightarrow\infty$ のとき $\|\psi_n-\psi_m\|\rightarrow 0$ を満たすとき、コーシー列とよばれ、あるベクトル $|\psi\rangle\in V$ が存在して、$n\rightarrow\infty$ のとき $\|\psi-\psi_n\|\rightarrow 0$ を満たすとき、収束列と呼ばれる。任意のコーシー列が収束列となる内積空間を完備であるといい、完備な内積空間をヒルベルト空間（Hilbert space）と呼ぶ。ただし、$\mathbb{K}$（実数または複素数の集合）上の有限次元内積空間は自動的に完備となるので、有限次元の場合、内積空間とHilbert空間と同一視することができる。石坂・前掲注（71）296-299頁。

（1）シュレーディンガー方程式はヒルベルト空間上で量子状態ベクトルの発展過程（ユニタリ過程）を表す。

（2）量子測定過程はヒルベルト空間の量子状態ベクトルをそのヒルベルト空間の直交基底（物理量の固有状態ベクトル）への射影として記述される。

（3）両者を一つの力学系として融合させることはできない[93]。

量子力学の先駆者であるシュレーディンガーやハイゼンベルクの理論に加えて、量子測定過程を数学的に表現するためには新たな理論が必要となった。フォン・ノイマンによるヒルベルト空間と自己共役作用素を用いた公式化は、それ以後の量子力学および量子情報理論の発展の基礎を与えた[94]。

先述のとおり、量子力学の原理の中で最も重要な概念のひとつは重ね合わせの原理である。量子力学では、物理量を表す作用素（あるいは行列）とその状態を記述するための量子状態（あるいは波動関数）が用いられる。そして、量子状態を関数空間におけるベクトルとして表す。この量子状態ベクトルは古典力学には存在しない量子独特なものである。ここで量子状態ベクトルに対し線形性を与える。これが重ね合わせの原理である。

2－3　量子情報科学に向けての基礎

量子情報科学ではスピンを量子情報の基本ユニットとしてモデル化するため、物理学におけるスピンの知識が必要となる。電子は原子内の軌道角運動以外に自転による換算プランク定数の半分 $\hbar/2$ の大きさの固有角運動量をもつという仮説が提案され、スピンと名づけられた。その後、ディラックの相対論的電子論によってスピンは電子の自転と解釈する必要はなくなり、現在スピンはある種の磁気モーメントの数学的な記述と理解される[95]。

スピンは空間における x、y、z の方向に関係づけて定義される。すなわち、それぞれが物理量として次のような作用素で表される。

93　フォン・ノイマン、井上健他訳（1957）『量子力学の数学的基礎』みすず書房。河東・前掲注（91）8頁。広田・前掲注（78）27頁。

94　広田・前掲注（78）27頁。1948年に先述のリチャード・ファインマンが、ハイゼンベルグの行列力学ともシュレーディンガーの波動力学とも異なる、「経路積分」をもちいた量子力学の一形式を発案した。その発想の原点は、「粒子があらゆる経路を同時に通る」というもので、量子力学とはプランク定数程度に幅をもった古典力学ともいうべき体系である。松浦・前掲注（78）160-175頁。L. M. Brown 編 "*Feynman's Thesis-A New Approach to Quantum Theory*", World Sci. 2005. R. P. Feynman, "*Space-time approach to non-relativistic quantum mechanics*", Rev. Mod.Phys., 20 (1948), 367-387.

95　R. P. ファインマン、A. R. ヒッブス著、D. スタイヤー校訂、北原和夫訳（2017）『量子力学と経路積分　新版』みすず書房、15頁。広田・前掲注（78）30頁。

$$S_x = \frac{\hbar}{2}\sigma_x, S_y = \frac{\hbar}{2}\sigma_y, S_z = \frac{\hbar}{2}\sigma_z \tag{2.1}$$

ここで、それらを行列で表現すると、下記のように表すことができる。

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.2}$$

上の三つのスピンの固有値はすべて $\hbar/2$ と $-\hbar/2$ となるので、簡略化のため $\hbar$ を単位にすれば電子のスピンの角運動量は 1/2 と −1/2 となる。(2.2) はパウリ (Pauli) 行列とよばれる。パウリ行列のσ_x は古典計算におけるビット反転の操作を、σ_z は位相反転とよばれる操作を行い、量子計算において量子ビットを操作する量子回路モデルで利用される。

二つの直交する固有状態を持つような物理系では、その物理量が取り得る量子状態は二つの固有状態の線形和、すなわち重ね合わせ状態である。

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.3}$$

ここで α, β は任意の複素数である。観測者にとってその量子状態に関する知識がまったくない場合、この物理系は無限の可能性をもつ、すなわち、この量子状態を同定するためには無限の情報が必要になる。この物理系は無限のシャノン情報のメモリーとはなり得ない[96]。古典力学の世界では、同定に要する情報とそれを有効なメモリーとして活用できることとは等価でありうる。なぜなら、蓄積した情報は原理的に抽出可能だからである。しかし、量子の世界では、量子測定理論が間に入り、抽出できる情報は有限であり、また一度測定すれば、その量子系の量子状態は破壊される。したがって、量子状態の世界と人間の世界（古典力学）に差が存在し、同定とメモリーは等価ではない。この等価でない現象を情報理論として体系化する理論を量子情報理論という[97]。

一方、量子状態は測定しなければ量子状態の形態のまま制御可能であり、そのような処理系を考えることが可能である。このとき量子状態自身を通常の情報（シャノン情報）として扱うことは意味がない。このような無限の可能性をもつ 2 次元量子状態系の物理量を一つの情報ユニットと考えるなら、無限の量子状態を含んだ空間を情報ユニットとすべきである。このように、2 次元ヒルベルト空間で記述される物理系を 1 量子情報ユニットと定義する。多くの文献ではこれを量子ビットと名づけるが、誤解を生む可能性がある。ビットはシャノン情報であり、明確な情報測度の理論にもとづいて定義されている。しかし、ここで述べているユニットは情報ではなく、量子状態の集合というリソースである[98]。

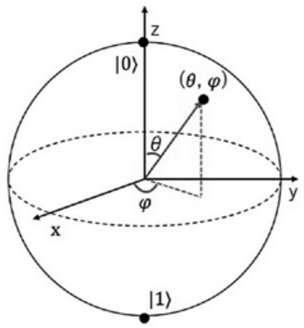
ここで、1 量子情報ユニット（量子ビット）とは 2 次元ヒルベルト空間のベトル（量子状態）で

96　広田・前掲注（78）31 頁。
97　同上、31 頁。
98　同上、32 頁。石坂・前掲注（71）23-27 頁。

記述される一つの物理系である。このような量子情報ユニットは図に示すような一つの球で表すことができる。なぜなら量子状態のノルム[99]は1であるので$|\alpha|^2+|\beta|^2=1$でなければばならない。このとき式（2.3）は

$$|\psi\rangle = cos\theta|0\rangle + e^{i\varphi}sin\theta|1\rangle \tag{2.4}$$

と表すことができる。



図：ブロッホ球

このような球表現は、ブロッホ球（Bloch sphere）とよばれる。量子状態をユニタリ変換で操作するとき、結果としての量子状態はこの球の中の運動としてみることができる。

3　数学的アプローチ

本章では、量子情報科学の諸問題において最も関係する数学的記述の基本を整理する。

3－1　ディラックの表記法

量子力学の理論では、実験結果がうまく説明できるという理由で、ベクトルや行列といった数学を利用する。しかし、数学では使用されないディラック[100]の表記法を用いる。本節では、複素ユークリッド空間（ユークリッド内積付きの複素列ベクトル空間）$\mathbb{C}^d$に関する表記法を整理する。

以下本節では、a、b、c（$a_1, a_2\cdots$なども含む）は複素数（スカラー）を、Aは行列を表す。単にベクトルという場合は、$\mathbb{C}^d$の列ベクトルを表すものとする。また、列ベクトルにおいては転置記号^{T}を用いて$(a_1, ..., a_d)^T := \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$と表すこともある。

ディラックの表記法では、ベクトルを$|\psi\rangle$のように表す。記号$|\rangle$をケット[101]といい、（列）ベ

99　状態自身の内積。石坂・前掲注（71）297頁。

100　物理学者のディラックにより導入された。P. A. M. Dirac, “*The Principles of Quantum Mechanics*” Oxford, 1958. 朝永振一郎（1969）『量子力学Ⅰ, Ⅱ』みすず書房。

クトルをケットベクトルとよぶ[102]。

ベクトル $|\psi\rangle=(a_1, a_2, \ldots a_d)^T\in\mathbb{C}^2$ に対し、記号 $|\rangle$ を逆向きにした $\langle\psi|$ は、以下で定義される複素共役な行ベクトルである。

$$\langle\psi|:=(\overline{a_1}, \overline{a_2}, \cdots \overline{a_d}) \tag{3.1}$$

（本稿では、複素数 $c=x+iy\,(x, y\in\mathbb{R})$ の複素共役を $\overline{c}=x-iy$ で表す。）

記号 $\langle|$ をブラといい、$\langle\psi|$ を（$|\psi\rangle$ に対応する）ブラベクトルとよぶ[103]。

以下、ケットベクトルとブラベクトルの組み合わせによる内積と行列を説明する。

ベクトル $|\psi\rangle=(a_1, \ldots, a_d)^T$ と $|\phi\rangle=(b_1, \ldots, b_d)^T\in\mathbb{C}^d$ の複素ユークリッド内積を $\langle\psi|\phi\rangle$ と記す。

$$\langle\psi|\phi\rangle=\sum_{i=1}^{d}\overline{a}_i b_i \tag{3.2}$$

（3.2）から、$\langle\psi|\phi\rangle\geq 0$ であり、等号は $|\psi\rangle=0$ のとき、またそのときに限る。これにより $|\psi\rangle=(a_1, \ldots, a_d)^T$ の大きさを

$$||\psi||:=\sqrt{\langle\psi|\psi\rangle}=\sqrt{\sum_i |a_i|^2} \tag{3.3}$$

で測ることができる。これを（ユークリッド）ノルムという。また、$\overline{\langle\phi|\psi\rangle}=\langle\psi|\phi\rangle$、ならびに、内積の右側成分に関する線形性 $\langle\psi|a\phi_1+b\phi_2\rangle=a\langle\psi|\phi_1\rangle+b\langle\psi|\phi_2\rangle$ が成立する[104]。

ベクトルの集合 $\{|\psi\rangle\}_{i=1}^{m}$ が正規直交系[105]であることは、クロネッカーのデルタ記号[106]を用いて $\langle\psi_i|\psi_j\rangle=\delta_{ij}\,(i, j=1, \ldots, m)$ と書ける。

内積の表記（3.2）は、ケットベクトル（d 次元列ベクトル）とブラベクトル（d 次元行ベクトル）は、それぞれ（$d\times 1$）と（$1\times d$）の行列とみなせるので、それらの行列積を考えることができる[107]。

特に、ベクトル $|\psi\rangle=(a_1, \ldots, a_d)^T$ と $|\phi\rangle=(b_1, \ldots, b_d)^T\in\mathbb{C}^d$ とに対し、$\langle\psi|$ と $|\phi\rangle$ の順番の行列積を考えると、

$$\langle\psi||\phi\rangle=(\overline{a_1}, \ldots, \overline{a_d})\begin{pmatrix} b_1 \\ \vdots \\ b_2 \end{pmatrix}=\sum\nolimits_{i=1}^{d}\overline{a}_i b_i\in\mathbb{C} \tag{3.4}$$

を得る[108]。右辺はユークリッド内積の値と一致するので、

101　英語で括弧を意味するブラケット（bracket）から。

102　石坂・前掲注（71）19 頁。

103　同上、20 頁。

104　$\langle\psi|\phi\rangle\geq 0$、$\overline{\langle\phi|\psi\rangle}=\langle\psi|\phi\rangle$、$\langle\psi|a\phi_1+b\phi_2\rangle=a\langle\psi|\phi_1\rangle+b\langle\psi|\phi_2\rangle$ は内積の一般的定義となる。同上、20 頁。

105　大きさが 1 で互いに直交するベクトルの集まり。

106　$\delta_{ij}:=\begin{cases}1 & i=j \\ 0 & i\neq j\end{cases}$

107　石坂・前掲注（71）21 頁。

$$\langle\psi||\phi\rangle=\langle\psi|\phi\rangle \tag{3.5}$$

となる。これより、記号 $\langle\psi|\phi\rangle$ は「ベクトル $\langle\psi|$ と $|\phi\rangle$ の内積」または「ブラ $\langle\psi|$ とケット $|\phi\rangle$ の行列積」とみなしてもよい[109]。

次に、ケットとブラの順番を変えた行列積を考える。

$|\psi\rangle=(a_1,\cdots,a_d)^T$ と $|\psi\rangle=(b_1,\cdots,b_d)^T\in\mathbb{C}^d$ に対し、$|\phi\rangle$ と $\langle\psi|$ の順番の行列積は、

$$|\phi\rangle\langle\psi|=\begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}(\overline{a_1},\ldots,\overline{a_d})=\begin{pmatrix} b_1\overline{a}_1 & \cdots & b_1\overline{a}_d \\ \vdots & \vdots & \vdots \\ b_d\overline{a}_1 & \cdots & b_d\overline{a}_d \end{pmatrix} \tag{3.6}$$

となる[110]。

記号 $\langle\psi|\phi\rangle$ はスカラー（数）であり、記号 $|\psi\rangle\langle\phi|$ は行列である[111]。

ディラックの表記法を用いると、ケットやブラがかかわる複雑な式も簡単に計算できるようになる。特に、ブラ×ケットの組み合わせは（内積となって）数になるので、この組み合わせを先に計算する。例えば、ベクトル、$|\xi\rangle=(c_1,\cdots,c_d)^T$ に、(3.6) の行列 $|\phi\rangle\langle\psi|$ を掛けるものとする。これを直接計算すると、

$$|\phi\rangle\langle\psi|\xi\rangle=\begin{pmatrix} b_1\overline{a}_1 & \cdots & b_1\overline{a}_d \\ \vdots & \vdots & \vdots \\ b_d\overline{a}_1 & \cdots & b_d\overline{a}_d \end{pmatrix}\begin{pmatrix} c_1 \\ \vdots \\ c_d \end{pmatrix}=\begin{pmatrix} \left(\sum_i \overline{a}_i c_i\right) b_1 \\ \vdots \\ \left(\sum_i \overline{a}_i c_i\right) b_d \end{pmatrix}=\langle\psi|\xi\rangle|\phi\rangle \tag{3.7}$$

を得る。

しかし、左辺を（ケット $|\phi\rangle$ とブラ $\langle\psi|$ とケット $|\xi\rangle$ の）行列積とみなせば、ブラ×ケットの組み合わせを先にすれば良いので、(3.7) の結果は直ちに得られる。

$$|\phi\rangle\langle\psi||\xi\rangle=\langle\psi|\xi\rangle|\phi\rangle \tag{3.8}$$

このような計算の形式化が可能となるのは、行列の積（演算子の積）が結合法則を満たすからである[112]。

3－2　量子確率論

量子力学においては波動関数の集合で構成される関数空間に確率理論を構築しなければならない。以下に量子力学固有の現象を含めた完全な確率論、いわゆる量子確率論の基本構造を整理する。

108　$(1\times d)$ の行列と $(d\times 1)$ 行列の積は数（1×1 行列）である。
109　石坂・前掲注（71）21頁。
110　$(d\times 1)$ と $(1\times d)$ の積は $(d\times d)$ との行列である。同上、21頁。
111　同上、22頁。
112　同上、22頁。複数の行列の積は、並び順さえ変えなければ、どの組み合わせから積を計算してもよいので、ケットとブラのどの組み合わせで計算しても良い。

フォン・ノイマンは、δ 関数[113]を議論することなしに量子力学はヒルベルト空間と非有界線形作用素の理論によって、その数学的バックグラウンドを構成できることを示した[114]。ヒルベルト空間と線形作用素の理論はそれだけでは単に数学の一形式であるが、フォン・ノイマンはこれらを用いて、いくつかの公理論的手続きを導入して量子力学を定式化したのである。ヒルベルト空間は線形空間の任意の要素に対して内積が定義され、その内積を距離とすれば内積に関して完備である空間である。このような抽象空間は、ユークリッド空間のように特に座標軸などがあるわけではない。座標軸を設定するためには、その要素の中から線形独立なものを選んで直交系を作らねばならない。もし、その直交系が、空間を構成しているすべての要素を表現できれば、それは完全正規直交系とよばれる。そのような直交系を決めれば、任意の要素（関数あるいはベクトル）はそれらの線形和で表現される。このとき直交系は座標軸の働きをする[115]。ヒルベルト空間の要素の部分集合でそれらがまた演算規則に対して閉じている（線形多様体）なら、それは部分空間である。ある部分空間$\mathcal{H}_1$の要素に対し、もう一つの部分空間$\mathcal{H}_2$の要素がすべて直交していれば、$\mathcal{H}_2$は$\mathcal{H}_1$は直交補空間とよばれる[116]。

ある線形多様体の要素（この集合は定義域とよばれる）を他の要素に変換する作用素で、線形の条件を満たすものを線形作用素という。線形作用素による定義域の像は値域とよばれる。ヒルベルトとドイツの数学者エルハルト・シュミット（Erhard Schmidt）はすでに有界な線形作用素の理論を完成させていた。それは、有界線形作要素のエルミート共役とはヒルベルト空間の要素のすべて[117]に対し

$$\langle \varphi, A\psi \rangle = \langle A^{\dagger}\varphi, \psi \rangle \tag{3.9}$$

を満たす一義的な作用素 $A^{\dagger}$である[118]。$AA^{\dagger} = A^{\dagger}A = I$ であれば A はユニタリ作用素とよばれる。I は恒等作用素[119]である。有界線形自己共役作用素でかつ、ベキ等律すなわち、$E^2 = E = E^{\dagger}$ であれば射影作用素とよばれる[120]。最も重要な定理の一つは、有界線形自己共役作用素がその固有値 λ_i と固有関数（あるいは固有ベクトル $|\lambda_i\rangle$）によって表現できるとするスペクトル定理である。

113　δ（デルタ）関数とは、空間の一点にだけ存在する粒子を数式中に表現するためにディラックによって発明された関数である。

114　1927 年にヒルベルト（D. Hilbert）、ノルデハイム（L. Nordheim）との共著「量子力学の基礎について」を出版。広田・前掲注（78）77 頁。

115　同上、77 頁。

116　同上、77-78 頁。

117　$A \in L(H) L$ は線形作用素の集合。石坂・前掲注（71）300 頁。

118　広田・前掲注（78）78 頁。

119　引数として用いた値と同じ値を常にそのまま返すような写像。

120　石坂・前掲注（71）305 頁。任意の $|\psi\rangle \in H$ に対し、$\langle \psi | P\psi \rangle = \langle \psi | P^2 \psi \rangle = \langle P^{\dagger}\psi | P\psi \rangle = \langle P\psi | P\psi \rangle = ||P\psi||^2 \geq 0$ より、射影作用素は正値作用素である。

$$A=\sum_i \lambda_i \boldsymbol{E}(\lambda_i) \tag{3.10}$$

ここで、λ_i は固有値、$\boldsymbol{E}(\lambda_i)$ は固有値λ_i に属する固有ベクトル上への射影作用素である。直交射影子は固有ベクトルを用いて次のように定義される

$$\boldsymbol{E}(\lambda_i)=|\lambda_i\rangle\langle\lambda_i| \tag{3.11}$$

この射影子が量子力学における測定過程を表現することになる。フォン・ノイマンは先述のとおり、数理体系を非有界線形作用素に一般化した。次にその一般化により数学的に疑いのない量子力学の基礎付けをおこなったのである。特にフォン・ノイマンは非有界な作用素の定義域や共役作用素を明確に規定し、自己共役 A と $A^\dagger$が同じ定義域をもち、かつそこで同じ作用をする作用素であればスペクトル分解可能であることを証明した。このような成果を基礎として、彼は以下のような量子力学の形式の公理論的表現を提案した。

公理Ⅰ. 任意の系にヒルベルト空間が対応し、それに属する量子状態ベクトルの $|\psi\rangle$ は、その系の状態を規定する。

公理Ⅱ. 可観測量（物理量）は自己共役作用素で記述される。

公理Ⅲ. 状態ベクトルの時間発展はシュレーディンガー方程式で決定される。

公理Ⅳ. ある状態ベクトルにある物理量 A を測定したとき測定値は A の固有値 λ_i で、それが測定される確率は $p_i=|\langle\psi|\lambda_i\rangle|^2$。測定値が λ_i のとき測定後の系の状態は、固有状態 $|\lambda_i\rangle$ になる [121]。

古典力学の法則は、量子測定で得られる測定値の平均値に対して適用される。すなわち、

$$\langle A\rangle=\mathrm{TrA}|\psi\rangle\langle\psi|=\textstyle\sum_i\lambda_i|\langle\psi|\lambda_i\rangle|^2 \tag{3.12}$$

ここで、Tr はトレースとよばれ、作用素や行列の対角成分をすべて加える操作を意味する。量子状態を表すベクトルは純粋に量子の世界を代表するものである。純粋状態を書き下すことは、観測者にとって知り得るすべての情報が明らかにされていることになる。それにもかかわらず、測定の結果が確率的になるというのが量子力学の本質である。このように、コペンハーゲン解釈に対して数学的に完結した量子確率論が構成される、フォン・ノイマンの量子確率論は関数解析的な確率論であるが、これ以後、量子確率過程の体系化がおこなわれ、古典論と同等な理論が展開されている。

一方、量子の世界でも古典的なゆらぎや不確定さがある。このような状態を数学的に記述するためフォン・ノイマンは統計作用素（密度行列ともいわれる）を導入した [122]。すなわち、物理系が古典的な確率：$\{p_i\}$ でいくつかの純粋状態が現れるような状況にあるとき、その物理系状態は

121　広田・前掲注（78）78-79 頁。

122　牧二郎（1992）「統計作用素の概念的基礎について」『科学基礎論研究 21 巻 1 号』科学基礎論学会、9-15 頁。

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i| \tag{3.13}$$

で記述される[123]。これは純粋状態 $|\psi_i\rangle$ が確率分布 $\{p_i\}$ である状態であり、これを混合状態とよぶ。この統計作用素は前もって準備された量子系の統計的性質を完全に規定する。統計作用素の導入によって量子力学を基礎とする量子統計力学の数学的基礎が確立した[124]。もっとも重要なエントロピーは以下のように定義される。準備された量子系のエントロピーを考察するために、その量子系に対する測定をおこない、そのときの量子系の状態の重み分布 p_i に対し

$$H = -\sum p_i \log p_i \tag{3.14}$$

を求める。そしてその最小値を探し、それをエントロピーとする。それが最小になる測定系は統計作用素の直交固有状態ベクトルに対応するものである。それらは次の固有値方程式で求めることができる。

$$\rho|\eta_i\rangle = \eta_i|\eta_i\rangle \tag{3.15}$$

ここで η_i は ρ の固有値で、$0 \le \eta_i \le 1, \sum \eta_i = 1$。したがって、量子統計力学においてエントロピーは次のように定義される。

$$S(\rho) = -k\sum_i \eta_i \log \eta_i = -k \mathrm{Tr}\rho \log \rho \tag{3.16}$$

k はボルツマン定数である。上式はフォン・ノイマンエントロピーとよばれる[125]。フォン・ノイマンエントロピーの性質は下記のとおりである。

ここで、状態が純粋状態ひとつしかないとすると、統計作用素は射影子となる。すなわち

$$\rho = |\psi\rangle\langle\psi| \tag{3.17}$$

このとき、量子状態に関わらずエントロピーはゼロでなければならない。上記の射影子の固有値は任意の量子状態に対し 1 である[126]。したがって、フォン・ノイマンエントロピーはゼロである。もし用意された純枠状態の集合が互いに直交しているとき、エントロピーはそれぞれの状態の重み確率に対する式（3.10）となる。したがって、重み確率が等確率のときに最大値をもつ。その最大値は $\log d$、ただし d はその量子状態を包含するヒルベルト空間の次元である。集められた量子状態が非直交状態ベクトルすなわち二つのベクトルの内積が

$$\langle\psi_i|\psi_i\rangle \neq 0 \tag{3.18}$$

であればフォン・ノイマンエントロピーは直交度に依存した値をもつ[127]。

123　広田・前掲注（78）78-79 頁。
124　同上、79 頁。
125　同上、80 頁。
126　同上、80 頁。
127　同上、80 頁。

フォン・ノイマン自身はフォン・ノイマンエントロピーと情報の関係にはまったく言及しなかった。しかし、約 50 年後、量子情報科学においてそれが脚光を浴びることになる[128]。

先述のとおり、量子状態と射影作用素によって確率が定義される。この確率は関数解析的ではあるが、定義される確率はコルモゴロフ[129]の測度論的確率に帰着されなければならない。確率測度の要請として次式が必要である。

$$\sum_i \mu(\boldsymbol{E}(\lambda_i)) = \mu\left(\sum_i \boldsymbol{E}(\lambda_i)\right) = \mu(\boldsymbol{I}) = 1 \tag{3.19}$$

1957 年にアメリカの数学者アンドリュー・グリーソン（Andrew Gleason）は 3 次元以上のヒルベルト空間に射影作用素を用いて導入可能な確率測度が $\mathrm{Tr}\rho\boldsymbol{P}(\lambda_i)$ の形であることを示した[130]。これをグリーソンの定理という。

以上のような考察によって量子確率論における確率測度は数学的に完備された[131]。

おわりに

本稿で考察したことを以下にまとめたい。

第一に、量子力学、情報科学そしてコンピュータのそれぞれが時に融合しながらも、別個の歴史をたどり、量子情報科学の分野において融合されたことを明らかにした。第二に、量子情報科学を理解する上で必要な、不確定性関係や重ね合わせ状態など、量子力学の基本概念を整理した。量子力学は、その存在が確率的によってのみ決まるという、我々の日常における直観とは異なる微視的な世界を取り扱う。そこで現れる不思議な現象を事実として受け入れ、現代物理学として成立していることが明らかとなった。第三に、物理現象を記述するための数学の基本概念を整理した。ヒルベルト空間、作用素、確率論など基本的な内容について整理した。

量子情報科学は、物理学、数学、工学など多くの分野の研究成果が集積して誕生した。物理学においては、素粒子・原子核・宇宙を取り扱う物理学と、物性（日常的な大きさ）を扱う物理学とに大きく分けられる。この両者にまたがるものが量子情報科学である。多くの場合、量子情報科学は情報を量子力学の数理体系において処理する学問であるため、量子力学の基礎数理を理解

128　広田・前掲注（78）80 頁。

129 「測度論に基づく確率論」「確率論の基礎概念」で公理主義的確率論を立脚させ、現代確率論の始まりとなった。

130　A. M. Gleason, “*Journal of Mathematics and Mechanics*”. **6**, 885, 1957.　2 次元を含む一般的な場合については、正作用素値測度を用いて 2003 年にドイツ生まれの数理物理学者ポール・ブッシュ（Paul Busch）によって証明された。P. Busch, “*Physical Review Letters*” **91**, 120403, 2003.

131　広田・前掲注（78）81 頁。

することが量子情報科学を理解するために必要不可欠になる。しかし、量子力学という物理学のための数学のみでは量子情報の学問を構成することはできない。そこで、物理現象の記述という立場を越え物理現象を制御するという立場からの数学が求められる。しかし、関連する数多くの数理概念は物理学者、数学者、工学者の間に概念的な混乱を生じさせているという課題がある。

本稿では、情報とは概念ではなく物理的実体をともなうものであることを指摘した。その情報を古典物理学ではなく量子力学の世界で考えるのが量子情報科学といえる。情報の概念から量子を理解し、多くの分野に応用することができると考えられる。情報というキーワードから私たちが存在する世界を把握しようとする研究分野といえる。

今後は各分野の専門性を横断する研究を進めることによって、分野横断的な学問である量子情報科学を発展させる必要があると考える。

参考文献等

石坂智ほか（2020）『量子情報学入門』共立出版

高水裕一（2020）『時間は逆戻りするのか—宇宙から量子力学まで、可能性のすべて　第4刷』講談社

竹内勇貴（2020）「量子コンピュータの原理と優位性」『現代思想2　量子コンピュータ』青土社、30-44頁

武田俊太郎（2020）『量子コンピュータが本当にわかる！』技術評論社

林正人（2009）「量子情報理論とその難しさ」『Fundamentals Review Vol.3 No,1』IEICE 電子情報通信学会 基礎・境界ソサイエティ 44-56頁

林正人（2014）『量子論への表現論　第2刷』共立出版

広田修（2002）『量子情報科学の基礎：量子コンピュータへのアプローチ』森北出版

古田彩（2004）「二人の悪魔と多数の宇宙：量子コンピュータの起源」『日本物理学会誌　59巻8号』日本物理学会、512-519頁

藤井啓祐（2018）「量子コンピュータの基礎」『オペレーションズ・リサーチ6月号　Vol.63　No.6』（公財）日本オペレーションズ・リサーチ学会、日科技連出版社、311-318頁

藤井啓祐（2019）『驚異の量子コンピュータ』岩波書店

J. J. サクライ、J. ナポリターノ著、桜井明夫訳（2014）『現代の量子力学（上）（下）第2版』吉岡書店

R. P. ファインマン、A. R. ヒッブス著、D. スタイヤー校訂、北原和夫訳（2017）『量子力学と経路積分　新版』みすず書房