観測に基づく量子計算

博士(理学) 小柴　健史
博士(工学) 藤井　啓祐 共著
博士(学術) 森前　智行

コロナ社

ま　え　が　き

約 20 年前，ショア (P.W. Shor) の素因数分解アルゴリズムやグローバー (L.K. Grover) の量子探索アルゴリズムなど，量子コンピュータの高い能力を示す量子アルゴリズムが発見されて以来，量子情報科学は脚光を浴びるようになり順調に発展してきた。そこで用いられている量子コンピュータのモデルは，ある意味で従来のコンピュータモデルからの拡張であった。従来の量子コンピュータモデルにおいて，計算プロセスは「量子的な演算」と「状態を取り出すための観測」の系列で表現されるが，観測操作はむしろ脇役として捉えられていたことと思う。

21 世紀になり，すぐに，ラッセンドルフ (R. Raussendorf) とブリーゲル (H.J. Briegel) により従来の量子コンピュータモデルとは異なる測定型量子計算モデルが提案された。測定型量子計算は，最初に準備フェーズとして特殊な量子状態を用意し，計算フェーズとしてその量子状態に対して適応的に観測を繰り返すことにより任意の計算を行うことができる。測定型量子計算の登場により，脇役であった観測操作が重要な役割を果たすことが明らかになったばかりでなく，計算プロセスを物理的操作の観点からも性質の異なる準備フェーズと計算フェーズに分離できるという事実は，量子計算に関して新しい見方をもたらしてくれたといっていいだろう。この新しい見方により，従来の議論からは見出しにくかった量子計算に関するさまざまな性質を追究し易くなった。本書において，測定型量子計算を理解する上で必要な知識についてトピックごとに解説を与えている。また，測定型量子計算モデルの登場によって明らかになった量子計算の諸性質について扱っている。

将来に実現されると期待できる量子コンピュータの実装を考えた場合，測定型量子計算モデルに基づいた方式は有望な量子コンピュータアーキテクチャであると思われる。将来量子コンピュータが実現するに先立って，本書を通じて測定型量子計算の魅力を感じ取っていただければ幸いである。

2017 年 1 月

小柴健史，藤井啓祐，森前智行

目　　次

1. 量子コンピュータモデル

2. 測定型量子計算の基礎

3. テンソルネットワーク上での測定型量子計算

4. 測定型トポロジカル量子計算

5. イジング模型分配関数と測定型量子計算

6. ブラインド量子計算（セキュアなクラウド量子計算）

7. 測定型量子計算と計算量理論

1 量子コンピュータモデル

物理学に慣れ親しんでいる方にとっては，量子力学的な効果を巧みに利用する計算メカニズムである量子計算はさほど突飛な存在ではないだろう。情報学を背景に持つ方にとっては，通常利用しているコンピュータが計算を行う対象であり，量子コンピュータの考え方はかなり異質な存在に感じるかもしれない。そもそも量子力学の概念を自然の摂理として受け入れるだけの準備が整っていないと思われる。量子計算の可能性や限界を計算機科学の一分野として研究している研究者も数多くいるが，その他の分野の計算機科学に関わっている方にとって量子計算は摩訶不思議な存在であり，測定型量子計算と呼ばれる従来から考えられている量子計算とは異なる特殊な量子計算モデルは視野にさえ入っていないと思われる。

本書は，測定型量子計算と呼ばれる特殊なモデルを紹介することを目的としている。目的以前に，なぜ測定型量子計算を考えるのかということについて触れておくべきであろう。測定型量子計算モデルの最大の利点は量子計算に対する新しい見方を提供することである。それにより，従来の量子計算モデルでは見出せてこなかった新しい事実が次々と発見されている。本書の各章において，そういった新しい事実を一つひとつ紹介している。その技術的な詳細は次章以降で解説することにして，本章では，コンピュータの歴史という観点から測定型量子計算の立ち位置を眺めてみることにする。

1.1 量子コンピュータのアイデア

コンピュータは計算を行う機械であるが，計算とはなにかということを論ずる計算論と呼ばれる分野がある。計算について論じるための妥当な計算モデルとしていくつかあるが，代表的なものとしてチューリングが提案したチューリング機械 (1936 年，A.M. Turing) がある。チューリング機械の秀逸な点は，万能チューリング機械を構築できるということであり，万能チューリング機械に別のチューリング機械の記述（プログラム）を与えることで任意のチューリング機械の動作を模倣できることにある。その他にもラムダ計算 (1936 年，チャーチ (A. Church)) や帰納的関数などがほぼ同時期に提案され，見かけ上まったく異なるにも関わらず，計算可能性という観点からは等価であることが証明されている。これらの等価性は計算可能性という概念の普遍性の顕れとして考えられており，Church-Turing の提唱は「計算することができる関数」という直観的な概念をチューリング機械などで議論するのがよいとしている。現在のコンピュータはフォンノイマン型コンピュータ（1946 年）とも呼ばれるが，チューリング機械という単純な計算モデルをベースにしてコンピュータアーキテクチャを構成したものになっている。

フォンノイマン (J. von Neumann) はまた，量子力学的な効果を利用したコンピュータの可能性についても着想している。その後，ドイッチ (D. Deutsch)[1)†] により，1985 年に量子チューリング機械モデルが定式化され，計算可能性という観点からは通常のチューリング機械との等価性が示された。ただし，計算ステップ数が，ある多項式で抑えられるといった計算資源を限定した場合の扱いに問題があり，その問題点はその後 1993 年になってバーンスタイン (E. Bernstein) とヴァジラーニ (U.V. Vazirani)[2)] によって修正された。

その一方で，量子チューリング機械はその扱いの不便さから，量子チューリング機械を用いて量子アルゴリズムが議論されることは少ない。量子アルゴリズ

† 肩付き数字は，各章末の文献番号を表す。

ムやその計算の複雑さを議論する際には，一般的に量子回路モデルが用いられる。この量子回路モデルはヤオ (A.C.C. Yao)[3] により 1993 年に提案された。

1.2　一様計算モデルと非一様計算モデル

ここで，回路モデルとチューリング機械の違いについて言及しておこう。チューリング機械が与えられたとき，入力がどんな長さであれ，その動作はチューリング機械の遷移関数によってのみ規定される。つまり，入力長が 10 ビットであっても 100 ビットであっても，チューリング機械は入力長とは独立にあらかじめ定められた遷移関数にしたがって動作する。それに対して回路（論理回路）の記述は，入力長を一つに定めてしまう。入力長が 10 ビットの場合の回路と入力長が 100 ビットの場合の回路とではその記述は異なる。そこで，論理回路を入力長ごとに定義する論理回路の族を導入することで可変長の入力に対応する。

入力長の多項式時間で終了するチューリング機械 M は基本ゲート数が多項式的に増加する論理回路族 $\{C_n\}_{n\geqq 1}$ に対応するが，逆は必ずしも真ではない。ここで，C_n は入力ワイヤー数が n の論理回路のこととする。つまり，論理回路族 $\{C_n\}_{n\geqq 1}$ が与えられたとき，それに対応するチューリング機械 M が存在しない場合もある。そのギャップを埋める概念が一様性と呼ばれるものである。あるアルゴリズム A が存在して 1^n を入力としたとき C_n の記述（用いられているゲートとその配線レイアウト）を出力する場合，$\{C_n\}_{n\geqq 1}$ は一様論理回路族と呼ばれる。アルゴリズム A の（計算時間等の）能力に依存して一様性にもいくつかのレベルが存在するが，一般的には多項式時間アルゴリズムを考える。また，上のような（計算時間非限定の）アルゴリズム A が存在しないとき，$\{C_n\}_{n\geqq 1}$ は非一様論理回路族と呼ばれ，チューリング機械と比較して能力が高いことが知られている。量子計算の場合，論理素子ではなく，別の基本ゲートを用いて量子回路が構成される。Yao が提案した量子回路モデルは一様回路族であり，量子チューリング機械と等価となっている。

1.3　量子アルゴリズム

量子計算の最大の特徴は，計算途中の状態が量子重ね合わせ状態と呼ばれる複数の状態が同時に存在できる状態を保持できることであり，その量子重ね合わせ状態に対して演算を適用させることができる点にある。特に，計算結果を得る上で望ましくない場合を存在しにくくなるように制御できることが，従来のアルゴリズムと大きく異なる点である。確率的な乱択アルゴリズムでは，内部状態が望ましくない状態に遷移した場合は，それは取り消せない事象であるが，量子アルゴリズムにおいてはその限りではない。

さて，量子計算が脚光を浴び始めたのは，アルゴリズム的なブレークスルーがあったからであろう。まず，1994 年にショア[4)] が量子コンピュータを用いれば素因数分解および離散対数問題は効率的に計算できることを示した。これらの問題は通常のコンピュータでは非常に計算が困難である問題として知られている。現在の情報セキュリティ技術は，これらの問題の困難性を利用して安全性が保証されている暗号プロトコルに大きく依拠しており，量子アルゴリズムが現実的に動作するようになると，それらの暗号プロトコルは完全に解読されてしまうことになる。また，1996 年にはグローバーアルゴリズム[5)] と呼ばれるデータベース探索アルゴリズムが提案された。構造がない N 個のデータから所望のデータを取り出すには通常のコンピュータでは $\Theta(N)$ ステップが掛かるのに対して，グローバー量子探索アルゴリズムでは $\Theta(\sqrt{N})$ ステップで十分であることが示された。これらの二大量子アルゴリズムの発見により量子情報科学という研究分野が大きく発展し今に至っているといっても過言ではない。

暗号分野においては，ショアのアルゴリズムが脅威として登場する以前の 1984 年に，ベネット (C.H. Bennett) とブラッサール (G. Brassard)[6)] により，量子鍵共有プロトコル（BB84 プロトコル）が提案されている。これは，二者（慣例にしたがってアリスとボブと呼ぶことにする）の間で鍵として用いるランダムなビット列を共有する方法であり，その無条件安全性がその後証明されている。

量子力学的な効果を利用しない方法では，無条件安全な鍵共有を行う方法は見出されていないため，BB84 プロトコルは量子力学的効果がポジティブに活用されている好例である。暗号分野においては，量子力学的な効果は，恩恵を享受する側面と損害を被るという負の側面がある正邪併せ持つ存在であり，暗号分野は量子情報科学を牽引する大きな役割を担っている。

1.4　測定型量子計算の登場

2001 年にラッセンドルフとブリーゲル[7] は量子回路計算モデルとはまったく異なる量子計算モデルを提案した。まず，クラスター状態（あるいはグラフ状態）と呼ばれる特殊な量子状態を用意し，その後は適応的に 1 キュービット測定だけを繰り返すことにより所望の計算ができるというものであり，一方向量子計算とも呼ばれる。ここで，適応的 (adaptive) というのは，ある一つのキュービットを測定する際に，その測定角度は，これまでの測定結果に依存する，というものである。ほぼ同時期に同種な計算モデルも提案されている。アリスとボブの間に量子もつれ合い状態（量子エンタングルメント）を事前に用意しておくことにより，アリスがボブに任意の量子状態を転送できるという量子プロトコルを量子テレポーテーションという（1993 年, ベネットら[8]）。量子テレポーテーションはベル測定と呼ばれる測定を行うことで量子状態がアリスからボブへ転送されるが，ゴッテスマン (D. Gottesman) とチュアン (I.L. Chuang)[9] は量子テレポーテーションが万能計算の基本要素になることを見出し，2003 年にニールセン (M.A. Nielsen)[10] がそれを利用してテレポーテーション型量子計算を提案した。一方向量子計算もテレポーテーション型量子計算も事前に特殊な量子状態を用意しておき，その後に測定を行うことで所望の計算を行うことができる。

測定型量子計算の最大の特徴は，最初に特殊な量子状態を用意するフェーズと用意された量子状態に対して適応的に観測を繰り返すというフェーズに分けられる点である。ある意味で，前者は量子的な操作であり，後者は古典的な操

索　　引

—— 著 者 略 歴 ——

小柴　健史（こしば　たけし）

1990 年　東京工業大学工学部情報工学科卒業
1992 年　東京工業大学大学院博士前期課程修了（情報工学専攻）
2001 年　東京工業大学大学院博士後期課程修了（数理・情報科学専攻）
　　博士（理学）
2005 年　埼玉大学助教授
2015 年　埼玉大学教授
　　現在に至る

藤井　啓祐（ふじい　けいすけ）

2006 年　京都大学工学部物理工学科卒業
2008 年　京都大学大学院工学研究科博士前期課程修了（原子核工学専攻）
2011 年　京都大学大学院工学研究科博士後期課程修了（原子核工学専攻）
　　博士（工学）
2011 年　大阪大学特任研究員
2013 年　京都大学特定助教
2016 年　東京大学助教
　　現在に至る

森前　智行（もりまえ　ともゆき）

2004 年　東京大学教養学部基礎科学科卒業
2006 年　東京大学大学院総合文化研究科博士前期課程修了（広域科学専攻）
2009 年　東京大学大学院総合文化研究科博士後期課程修了（広域科学専攻）
　　博士（学術）
2010 年　リール第一大学（フランス）　博士研究員
2011 年　パリ東大学（フランス）　博士研究員
2012 年　インペリアルカレッジロンドン（イギリス）日本学術振興会海外特別研究員
2013 年　群馬大学助教
　　現在に至る

観測に基づく量子計算

Measurement-based Quantum Computing

2017 年 3 月 10 日　初版第 1 刷発行　★

検印省略

著　者　小柴健史
　　藤井啓祐
　　森前智行

発行者　株式会社　コロナ社
　　代表者　牛来真也

印刷所　三美印刷株式会社

112–0011　東京都文京区千石 4–46–10

発行所　株式会社　コロナ社

CORONA PUBLISHING CO., LTD.

Tokyo Japan

振替 00140–8–14844・電話(03)3941–3131(代)

ホームページ　http://www.coronasha.co.jp

ISBN 978–4–339–02870–6　（森岡）　（製本：愛千製本所）

Printed in Japan