クラスター状態を用いた量子計算への新たなアプローチ

西　野　哲　朗

A New Approach to Quantum Computation Using Cluster States

Tetsuro NISHINO

This article is a short introduction to the cluster-state model of quantum computation. In this model, quantum information processing is performed by a sequence of single-qubit measurements applied to a fixed quantum state that is called a cluster state. We also review the following interesting properties of the model: (1) the cluster state cannot occur as the exact ground state of any naturally occurring physical system, (2) measurements on any quantum state which is linearly prepared in one dimension can be efficiently simulated on a classical computer, and thus are not candidates for use as a substrate for efficient quantum computation, and (3) the differences between the model and quantum circuits have led to new insights into quantum circuit complexity.

Key words: quantum computation, cluster states, one-way quantum computer

量子コンピューター[1,2]は，未だ実現されていないが，完成すれば任意の物理システムを効率よく模倣できるものと期待されている．そこで，いかなる物理資源が，量子コンピューターを構築するうえで有効かを調べれば，どのような物理資源が他の物理システムを模倣するうえで本質的であるかを検討することができる．つまり，「どのような物理システムが，他の物理システムを効率よく模倣できるか？」というシミュレーションに関する基本問題についての検討が可能となる．

本稿の目的は，測定に基づく量子計算（measurement-based quantum computation）に関する最近の理論研究について概観することである．それは，すべての基本操作が量子測定であるにもかかわらず，（ユニタリー動力学を含む）任意の量子動力学を模倣することができるという，著しい性質をもった量子計算のモデルである．本稿では，量子測定に基づく量子計算のモデルのなかでも，特に，Raussendorf と Briegel によって提案されたクラスター状態モデル（cluster-state model），あるいは，1方向性量子コンピューター（one-way quantum computer）[3]について述べる．

クラスター状態モデルは，その性質がまだ完全には解明されていないが，従来の量子計算のモデルとは異なる性質をもっている．これらの相違から，量子回路計算量に対する新たな結果が導かれており[4]，さらに，量子計算に関する実験の提案を著しく単純化できると主張されている[5–7]．この方面の最新の研究成果については，本特集の他の解説記事を参照されたい．

測定に基づく量子計算への別のアプローチが，Nielsen によって提案され[8]，その関連研究も行われているが[9,10]，このアプローチについては本稿では取り扱わない．なお，これら2つのアプローチの関係については，文献 11–13）などで述べられている．測定に基づく量子計算の研究は，近年，急速に発展している．したがって，関連するすべての文献を網羅することは非常に困難である．そこで，より詳細な情報については，本解説の参考文献や，それらの文献の末尾に掲載されている参考文献等を参照されたい．

また，クラスター状態モデルについては，以下の2つの未解決問題が提示されている．

電気通信大学情報通信工学科（〒182-8585 調布市調布ケ丘 1-5-1）　E-mail: nishino@ice.uec.ac.jp

- いかなるクラスター状態が，ある自然な物理システムの基底状態として現れうるか？
- いかなるクラスター状態が，通常の古典コンピューター上で効率よく模倣できるか？

どちらの問題に対しても，まだ十分な解答は得られていないが，Nielsen により，初歩的な解答が与えられているので，本稿でも簡単に紹介する．

1. 量子論理回路

1985 年に，英国人物理学者 David Deutsch は，量子チューリング機械（quantum Turing machine，以下 QTM と略す）という量子力学的動作原理に基づく新たな計算モデルを提案した[1,2]．この QTM に基づくコンピューターが，量子コンピューターとよばれている．

通常のコンピューターのメモリーの一区画には，0 または 1 が保持できるが，QTM のメモリーの一区画には，0 と 1 の任意の重ね合わせ状態が保持できる．ここで，重ね合わせ状態とは，0 に対応する状態ベクトル $|0\rangle$ と 1 に対応する状態ベクトル $|1\rangle$ を，それぞれ，

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},\quad |1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$$

とするとき，$\alpha|0\rangle+\beta|1\rangle$ の形で表されるベクトルの和のことをいう．ただし，α と β は，条件式 $|\alpha|^2+|\beta|^2=1$ を満たす任意の複素数であり，振幅とよばれる．この重ね合わせ状態を観測すると，0（または 1）が確率 $|\alpha|^2$（$|\beta|^2$）で読めるものと仮定する．

QTM のテープの一区画が保持できる情報量を 1 量子ビット（quantum bit, qubit）という．QTM の動作は，量子ビットに対するユニタリー変換とよばれる線形変換の適用という形で表現できる．一方，QTM 上で実行されるアルゴリズムを量子アルゴリズムとよぶ．そこで以下では，量子アルゴリズムを量子ビットに適用されるユニタリー変換の系列として記述することにする．

1994 年に，AT & T の Peter Shor は，整数の因数分解を小さな誤り確率で高速に行う量子アルゴリズムの設計に成功し，世界的な注目を集めた．というのは，現在広く用いられている RSA などの公開鍵暗号が，因数分解問題の難しさを前提として設計されているからである．この Shor の結果に影響されて，量子コンピューターの物理的実現に関する研究が現在盛んに行われている．

通常の組み合わせ論理回路のアナロジーとして，Deutsch によって導入されたのが，量子論理回路である．一般に電気回路は，多数の論理ゲートから構成されている．通常のコンピューターを実現するのに用いられている論理ゲートとしては，AND，OR，NOT ゲートなどがある．

例えば，AND と NOT，または OR と NOT の 2 種類のゲートを用いれば，任意のチューリング機械の計算を模倣する回路を構成することができる．

一方，量子計算は量子ビットに適用されるユニタリー変換の系列で表現される．Deutsch や Yao らの研究によって，QTM の動作は量子回路で模倣できることがわかっている[14]．最近，量子回路を実現するための量子論理ゲートについて盛んに研究が行われているが，現在までに，例えば以下のような量子論理ゲートが考案されている．なお，量子論理ゲートの各入出力は，1 つの量子ビットに対応している．

① 制御 NOT ゲート： このゲートは 2 入力 2 出力である．最も単純な場合について説明すると，制御 NOT ゲートにおいては，入力の第 1 ビット x_1 の値が 0 ならば，入力の第 2 ビット x_2 の値がそのまま出力の第 2 ビット y_2 の値となるが，x_1 の値が 1 ならば，x_2 の値が反転された値が y_2 の値となる．すなわち，$x_1=1$ のときには，x_2 の否定が y_2 に代入される．なお，いずれの場合においても，$y_1=x_1$ である．制御 NOT ゲートは，以下のような 4 次の正方行列で表現される，2 量子ビットに対するユニタリー変換を実行する．

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

ここで，この行列の各行各列は，それぞれ順に，$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$ という状態に対応している．例えば，上の行列の第 3 行は $|10\rangle$ という状態に対応し，第 4 列は $|11\rangle$ という状態に対応するが，その第 3 行第 4 列成分が 1 であることは，以下のことを表している．制御 NOT ゲートへの入力が $x_1=1$，$x_2=0$ である場合には，その出力は $y_1=1$，$y_2=1$ となる．

② 制御位相ゲート： このゲートも 2 入力 2 出力であり，制御 NOT ゲートと同様，制御ユニタリーゲートの特殊な場合である．制御 NOT ゲートにおける変換は，

$$|x,y\rangle\Rightarrow(-1)^{xy}|x,y\oplus x\rangle$$

という形式で定義されるが，制御位相ゲートにおける変換は，

$$|x,y\rangle\Rightarrow(-1)^{xy}|x,y\rangle$$

という形式で定義される．

③ ユニタリー変換ゲート： このゲートは1入力1出力であり，入力に対して指定されたユニタリー変換 U を行う．ただし，このユニタリー変換 U は，行列式が1であるような，2行2列のユニタリー行列で表現されるものである．ユニタリー変換ゲートの具体例としては，以下に示すアダマールゲート H を参照されたい．

通常の組み合わせ論理回路の量子アナロジーとして，Deutsch によって導入されたのが，量子回路である．これは，フィードバックをもたない古典的回路の量子版である．量子回路を定義するために，ある基本ゲートの集合が基底として選ばれるが，ここでの各基本ゲートは，$2^k\times 2^k$ ユニタリー行列によって規定される k-入力 k-出力素子である．

以下では，$h=2^k$ とし，$\boldsymbol{C}^h$ で h-組の複素数から構成されるベクトル空間を表す．$u, v\in\boldsymbol{C}^h$ に対し，内積を $\langle u, v\rangle=\sum_{1\le i\le h}u_i^* v_i$ により定義し，ベクトル u の長さを $(\langle u, u\rangle)^{1/2}$ で定義する．また，$\langle u, v\rangle=0$ が成り立つとき，u と v は直交するという．ただひとつの成分のみが1で，その他のすべての成分が0であるような自然な単位ベクトルは，全部で h 個存在するが，それらは $\{0,1\}^k$ 内の要素と同一視できる．$2^k\times 2^k$ ユニタリー行列 U は，ベクトル $u\in\boldsymbol{C}^h$ を別のベクトル $u'\in\boldsymbol{C}^h$ に次のような方法で変換する：入力 $u=\sum_{x\in\{0,1\}^k}c_x x$ に対し，出力は $u'=\sum_{x,y\in\{0,1\}^k}c_x U_{x,y}y$ によって与えられる．ただし，x と y は $\boldsymbol{C}^h$ 内の単位ベクトルである．定義より，ユニタリー行列は，互いに直交する単位ベクトルの集合を，互いに直交する単位ベクトルの別の集合に変換することに注意する．

量子回路は，通常のブール回路と同様に，基本ゲートを適当な遅延時間を伴ってワイヤーで結合することにより構成される．量子回路は，何本かの入力ワイヤーと出力ワイヤーをもつ．何本かの入力ワイヤーには，繰り返しを許して変数の集合 $x_1, x_2, \cdots, x_n$ が対応し，残りの入力ワイヤーには定数0と1が対応する．一方，出力ワイヤーの何本かを，特定の時刻に測定される出力変数 $y_1, y_2, \cdots, y_m$ に対応させる．すべての m-入力 m-出力量子ゲートの集合を B_m で表す．

Deutsch は，$n\ge 3$ の場合に，n 個のブール変数により定義される $\boldsymbol{C}^{2^n}$ のすべてのユニタリー変換は，B_3 を基底とする量子回路によって計算できることを示した．回路からフィードバック・ループをなくすには，最初，定数0または1に設定されており，出力時にはその同じ定数値に戻されているような，補助ワイヤーを追加すればよいことが知られている[14]．

通常のブール回路においては，AND，OR，NOT の3種類のゲートがあれば（実際は AND と NOT，または OR と NOT の2種類で十分），任意のブール関数を計算する回路を構成することができる．このような性質があるため，ゲートの集合 {AND，OR，NOT} は万能基底とよばれる．量子回路に対しては，次のような万能基底が知られている[15]．すなわち，制御 NOT ゲートと，すべての1量子ビットユニタリー変換ゲートから成るゲートの無限集合 G_U は万能基底である．任意の k 量子ビットユニタリー作用素を，G_U に属する $O(4^k k)$ 個のゲートを用いて正確に模倣できることが知られている[15]．したがって，G_U から，局所的ユニタリー変換ゲートから成る別の万能基底（3量子ビットゲート全体の集合など）に切り替えても，対応する回路サイズは定数倍にしか増加しない．

2. クラスター状態モデル

本章では量子計算のクラスター状態モデルを紹介する．以下の記述は文献 3, 16-18）の記述を参考にしている．

クラスター状態計算は，クラスター状態とよばれる，エンタングルした多量子ビット状態を用意するところから始まる．その後，クラスター上における単一量子ビット測定が順次行われ，最後に，得られた量子ビットから計算結果を読み出す．

クラスター状態とは，単一量子状態ではなく，量子状態の集合のことを指す．任意の n 頂点グラフ G に対し，対応する n 量子ビットクラスター状態を定義することができる．そのためには，まず最初に，各頂点に量子ビットを対応させ，さらに，以下のような，グラフに依存した量子ビットの準備手続きを適用すればよい．グラフに付随したクラスター状態は，次の準備手続きを適用することにより定義される．

1. n 個の各量子ビットを，状態 $|+\rangle\equiv(|0\rangle+|1\rangle)/\sqrt{2}$ に設定する．
2. グラフ内の対応する頂点が接続されている量子ビット間に，制御位相ゲートを適用する．

制御位相ゲートの適用順序は可換なので，ゲートが適用される順序は考慮しなくてよい．また，上ではクラスターの準備の過程を，量子ゲートの適用を用いて説明したが，クラスター状態は，測定だけによって準備できることが知られている．したがって，クラスター状態モデルは，真に測定のみを用いた計算モデルと考えることができる．

クラスター状態が準備できたら，計算の次のステップは，その状態上で一連の測定を実行することである．これらの測定は，以下を満たす．

- 行われる測定は，すべて単一量子ビット測定である．
- 測定の基底の選択は，それ以前の測定の結果に依存してよい，すなわち，古典的測定結果の先送りが許されている．
- 測定結果を先送りされる際には，古典コンピューターで処理してもよい．したがって，基底の選択は，それ以前の測定結果の複雑な関数になるかもしれない．クラスター状態計算が効率的であるためには，この古典計算は多項式時間実行可能でなければならない．

クラスター状態計算の出力は，2つの異なる方法で定義できる．第一の定義では，計算の出力をある量子状態とみなす．それは，一連の測定が終了したときに得られた量子ビットの量子状態である．第二の定義では，いくつかの読み出しのための測定を付加する．すなわち，測定が終了したときに得られた量子ビットに適用される，単一量子ビット測定の系列が付加される．この場合，計算の出力は古典的なビット列となる．

この量子計算のクラスター状態モデルは，1ビット・テレポーテーションとよばれる回路に関する関係式を模倣することで，量子回路を効率的に模倣できることが知られている[18]．

1．模倣すべき回路から構成したクラスター状態モデル上で，測定を実行する．
2．模倣すべき回路の計算過程を1ビット・テレポーテーションの適用の過程に解釈し直す．
3．その回路の出力状態を整理すると，上記のクラスター状態モデルの出力と等価であることが確認できる．

次に，どのような場合に，クラスター状態は，ある量子系の基底状態となりうるかについて考える．実は，典型的なグラフに対しては，クラスター状態が，現実的な量子状態の基底状態となることは不可能であることが示されている．それでは，どのような量子状態の性質が，量子計算に役立つのだろうか．例えば，クラスター状態の二次元配列が重要であることが示されている．すなわち，クラスター状態モデルと類似の一次元モデルが，古典コンピューターで効率よく模倣できることが示されている[18]．したがって，これらの一次元配列から得られる状態は，効率的な量子情報処理の実現には役立ちそうもない．

一方，クラスター状態モデルをある方式で変換することで，量子ビットを追加しながら量子回路を並列化し，回路の段数を削減して，回路全体としての計算時間を短縮する方法論が提案されている[19]．このような方向性の研究の発展も期待できるため，クラスター状態モデルは，量子計算量理論研究の観点からも大変興味深い．

本稿では，量子計算のクラスター状態モデルと量子回路の基本的枠組みについて紹介した．クラスター状態モデルは，その性質がまだ完全には解明されていないが，従来の量子計算モデルとは異なる性質をもっている．これらの相違から，量子回路計算量に対する新たな結果が導かれており[4]，さらに，量子計算に関する実験の提案を著しく単純化できると主張されている[5–7]．今後，クラスター状態モデルの本質的性質の解明と，このモデルの応用に関するさらなる研究が重要となるであろう．

文　　献

1) D. Deutsch: “Quantum theory, the Church-Turing principle and the universal quantum computer,” Proc. R. Soc. Lond. A, **400** (1985) 97–117.
2) 西野哲朗：量子コンピュータ入門（東京電機大学出版局，1997）．
3) R. Raussendorf and H. J. Briegel: “A one-way quantum computer,” Phys. Rev. Lett., **86** (2001) 5188–5191.
4) R. Raussendorf, D. E. Browne and H. J. Briegel: “The one-way quantum computer: A non-network model of quantum computation,” J. Mod. Opt., **49** (2002) 1299–1306.
5) D. E. Browne and T. Rudolph: “Resource-efficient linear optical quantum computation,” arXiv:quant-ph/0405157 (2004).
6) M. A. Nielsen: “Optical quantum computation using cluster states,” Phys. Rev. Lett., **93** (2004) 040503.
7) P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger: “Experimental one-way quantum computing,” Nature, **434** (2005) 169–176.
8) M. A. Nielsen: “Quantum computation by measurement and quantum memory,” Phys. Lett. A, **308** (2003) 96–100.
9) D. W. Leung: “Two qubit projective measurements are universal for quantum computation,” arXiv:quant-ph/0111122 (2001).
10) D. W. Leung: “Quantum computation by measurements,” arXiv:quant-ph/0310189 (2003).
11) P. Aliferis and D. W. Leung: “Computation by measurements: A unifying picture,” arXiv:quant-ph/0404082 (2004).
12) A. M. Childs, D. W. Leung and M. A. Nielsen: “Unified derivation of measurement-based schemes for quantum computation,” Phys. Rev. A, **71** (2005) 032318.
13) P. Jorrand and S. Perdrix: “Unifying quantum computation with projective measurements only and one-way quantum computation,” arXiv:quant-ph/0404125 (2004).
14) M. A. Nielsen and I. L. Chuang: *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
15) R. Cleve: “An introduction to quantum complexity theory,” quant-ph/9906111 (1999).
16) M. A. Nielsen: Journal club notes on cluster-state quantum computation, http://www.qinfo.org/qc-by-measurement/, 2003.
17) M. A. Nielsen and C. M. Dawson: “Fault-tolerant quantum computation with cluster states,” arXiv:quant-ph/0405134 (2004).
18) M. A. Nielsen: “Cluster-state quantum computation,” arXiv:quant-ph/0504097 (2005).
19) A. Broadbent and E. Kashefi: “Parallelizing quantum circuits,” http://arxiv.org/abs/0704.1736 (2007).

（2008年9月17日受理）