量子コンピュータって
どんなもの？ 矢吹太朗[†], 伊庭斉志[†]

キーワード：量子計算, 量子チューリングマシン, 量子回路, ショアのアルゴリズム

表1 量子計算の特徴

1. 量子ビットは0と1の重ね合せ ($a|0\rangle + b|1\rangle$) を取る (このため並列計算が可能). 2キュービット系なら ($a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$).
2. 系の変化はユニタリ変換で記述される (例えば, 2キュービットの系なら, 上の $(a\ b\ c\ d)$ に対してユニタリ行列をかけることだと考えてください)
3. キュービットの値を読むと, 複数の状態のうちの1つが, ある確率 (重ね合せの係数の絶対値の2乗に比例) で得られる (例えば, 上の2キュービットの系を観測すると, 00, 01, 10, 11がそれぞれ $|a|^2$, $|b|^2$, $|c|^2$, $|d|^2$ の確率で得られる).

量子計算は1980年代に登場し, 今日大きな注目を集めている計算パラダイムです. 現在のコンピュータでは解くのが困難な問題を, 量子コンピュータなら容易に解くことができるかもしれないと期待されています.

1. 歴史

量子計算の研究が始まった背景には, 計算における情報処理量と消費エネルギーの関係についての研究や, 量子力学的システムのシミュレーションを従来のチューリングマシンをモデルにしたコンピュータで行うことが困難だというファインマンの指摘がありました. 現在のコンピュータもそのデバイスが量子力学的効果を利用しているという点では量子力学的です. しかし, 量子コンピュータはこの意味で量子力学的なのではなく, 1985年にドイツによって量子チューリングマシンとして定式化されたその情報処理方法ゆえに量子力学的なのです.

実用的な問題への応用が見つからず停滞していたこの分野が, 一躍脚光を集めるようになったきっかけは, 1994年のショアのアルゴリズムの発表です. もし量子コンピュータが実現すれば, 約数を高速に求めるこのアルゴリズムを使うことで, 現在広く普及している公開鍵暗号 (大きな整数の因数分解が困難だということに安全性の基盤がある) を破れるということも衝撃でした. にもかかわらず, 依然公開鍵暗号が使われているというのは, 誰も量子コンピュータの実現を本気で信じて

はいないせいなのか, 将来解説されても構わないようなことしか暗号化していないせいなのか興味深いところです. 以後, 物理学と情報科学の間で学際的にさまざまな研究が行われています. 1996年にはもう一つの重要なアルゴリズムである, グローバの検索アルゴリズムが発表されました.

2. 量子計算の実験

現在, 液体・固体中の原子核 (NMRを用いる), 電磁トラップ中に閉じ込めたイオン, 固体素子中のスピン, 光子などを用いて実験が行われていますが, 決定的なものはまだありません.

実験を困難にしている大きな要因の一つは, 量子ビット (キュービット) の重ね合せの状態が短時間で壊れてしまうことです. それを克服するための誤り訂正手法も考案されていますが, その実現には冗長性を持たせるためのキュービットを導入した大きな系が必要で, そこにもまた技術的な困難があります.

現在までに行われた最も大きな規模の実験は, NMRを用いた5キュービットの系で置換の位数を求めるアルゴリズム (ショアのアルゴリズムの一部に似ている) を実行したものです.

3. 量子チューリングマシン

チューリングマシンと量子チューリ

ングマシンは計算可能性の点では同等ですが, 計算複雑性は異なっていると考えられています. 量子チューリングマシンの性質で最も重要なのは, それを構成するキュービットが重ね合せの状態を持つことができるということです. これによって N キュービットの系は 2^N 個の状態を同時に持てるようになるのです.

今, 0から 2^N-1 までの入力に対し, ある関数 f を計算したいとしましょう. 古典的には明らかに f を 2^N 回呼び出さなければなりません. しかし量子計算においては, まず0から 2^N-1 の重ね合せを用意し (これは N 回の単純な操作でできます), それに対して f を1回だけ呼び出せばよいのです.

しかしながら, 今得られた状態 ($f(0)$ から $f(2^N-1)$ の重ね合せ) から実際に値を読もうとしてキュービットを観測しても, 重ね合せのうちのひとつ (例えば $f(5)$ など) が確率的に得られるだけです. つまり, せっかく並列計算を行っても, 素朴な方法ではその結果のうちのひとつしか知ることはできないのです. また, 系の時間変化はシュレディンガー方程式に従わなければならないので, キュービットに施す操作はユニタリ変換に限られています. このことは確率の和を不変に保たなければならないことから理解できます.

[†] 東京大学 大学院 新領域創成科学研究科
"What is Quantum Computer?" by Taro Yabuki and
Hitoshi Iba (Graduate School of Frontier Sciences,
The University of Tokyo, Tokyo)

図1 量子回路の例

図2 ショアのアлゴリズムの主要部

そこでアルゴリズムを工夫する必要がある出てくるのです。

4. 量子回路

具体的な量子アルゴリズムの前に、量子回路を紹介しましょう。量子回路とは図1のようなものです。1本の水平線が1つのキュービットに相当します。量子回路は左から右に向かって読み、例えば図1の回路は、1番目のキュービットに対して操作A、1番目が標的となる制御NOT、1番目に対して操作B、…という計算過程を表しています。

量子チューリングマシンと量子回路の関係は、チューリングマシンと論理回路の関係に似ています。また、ANDとNOTだけですべての論理回路ができるのと同様に、1キュービットに対するユニタリー変換と制御NOTの組合せからすべての量子回路を構成できることが示されています。

5. ショアのアлゴリズム

次に、ショアのアлゴリズムを例に、なぜ量子計算は速いと考えられている

かを説明しましょう。例えば、15の約数をショアのアлゴリズムによって求める過程は次のようになります。アルゴリズムの主要部の量子回路は図2のようになります。

- (1) 15より小さい整数 x を決める ($x=7$).
 - (2) 最大公約数 $\gcd(15,7) \neq 1$ ならば、約数が見つかったことになるため終了。
 - (3) $b=0,1,2,\dots$ について $f(b)=7^b \bmod 15$ を計算する。
($f(b)=1, 7, 4, 13, 1, 7, 4, \dots$)
 - (4) $f(b)$ の周期 r を求める ($r=4$).
 - (5) $\gcd(15, x^{r/2} \pm 1)$ を求める(3, 5).
- 以上で15の約数が求まる。

量子コンピュータが力を発揮するのは上の3, 4番目のステップです。量子コンピュータは、先に述べたように複数の b に対する $f(b)$ を同時に計算でき、(説明は省略しますが) 周期 r を求めるための離散フーリエ変換も効率よく行えるため、このアルゴリズムを高速に実行できるのです。並列計算した結果(先に述べたようにすべてを知るこ

とはできません)の周期さえ得られればよいことになっているのが要点です。

6. 今後の期待

量子計算について簡単に説明してきました。歴史の浅いこの分野には理論的にも実験的にも解決しなければならない問題が数多くあります。

何か問題が与えられたとしましょう。その問題のための単純な量子回路をどのように生成したらいいでしょうか。その問題において量子コンピュータは従来のコンピュータを上回ることができるのでしょうか。私たちは量子計算におけるこのような問題の研究を通じて、“ $P \neq NP$ 完全?”を初めとする計算複雑性の未解決問題への手がかりが得られるのではないかと期待しており、それを求める研究を進めています。

(2001年5月31日受付)

[文 献]

- 1) 細谷暁夫:“量子コンピュータの基礎”, サイエンス社 (1999)
- 2) C.P.ウィリアムズ, S.H.クリアウォータ:“量子コンピューティング”, シュプリンガー・フェアラーク東京 (2000)
- 3) 矢吹太郎, 伊庭斉志:“量子テレポテーション及びオラクル問題のための量子回路自動生成”, 情報処理学会シンポジウムシリーズ, 2000, 16, 新しい計算パラダイムシンポジウム2000論文集, p.73, 情報処理学会 (2000)

やぶき たらう
矢吹 太郎

1998年、東京大学理学部天文学科卒業。2001年、東京大学大学院新領域創成科学研究科基盤情報学専攻修士課程修了。現在、同専攻に所属し、進化システム・進化論的計算について研究している。

いば ひとし
伊庭 斉志

1985年、東京大学理学部情報科学科卒業。1990年、東京大学大学院工学系研究科情報工学専攻博士課程修了。同年、電子技術総合研究所入所。1998年から、東京大学大学院工学系研究科電子情報工学専攻助教授。進化システムおよび人工知能基礎の研究に従事。著書に、遺伝的アルゴリズムの基礎、遺伝的プログラミング、進化論的計算の方法など。工学博士。