量子計算

情報通信工学科
情報メディア学講座　西野研究室

未来のコンピュータ

コンピュータの誕生から今日までの約50年間、その計算速度は年を重ねるごとに高速になり、サイズは小型化されてきました。しかし、このような急速な進歩もついに限界に直面していると言われており、将来、コンピュータの更なるミクロ化を目指すのならば、まったく新しい計算理論に基づく新技術が必要となります。

そこで、1985年にD.Deutschが「量子チューリング機械」という新しい計算モデルを提案しました。この、量子チューリング機械をモデルとするコンピュータのことを「量子コンピュータ」と呼びます。量子コンピュータは未来のコンピュータと言われ、現在のコンピュータでは時間がかかりすぎて解けない問題を、高速に解くことができると考えられています。

量子計算の簡単な歴史

1985年　D.Deutschが量子Turing機械を提唱

1993年　E.BernsteinとU.Vaziraniが効率的な万能量子Turing機械を構成

1994年　P.W.Shorが因数分解の誤り限定多項式時間量子アルゴリズムを発見

1996年　L.K.Groverがデータベース検索アルゴリズムを発見

Turing機械

チューリング機械は、図1に示すようにテープ、ヘッドと有限制御部から構成されています。おおまかに言うと、テープは現在のコンピュータのメモリ（記憶装置）に対応し、ヘッドはメモリへの読み書き装置、有限制御部はCPU（中央処理装置）に対応しています。図1はチューリング機械のハードウェアを図示したものです。

一方、チューリング機械のソフトウェア（プログラム）は状態遷移関数と呼ばれる関数で指定され、図2のような表形式で表現されます。この表において、SとTが有限制御部の状態。0、1、Bはテープの各区画に記入できる記号。R、Nはヘッドの移動方向をそれぞれ表しています。ここでRは「ヘッドを1区画右に動かす」ことを、Nは「ヘッドを動かさない」ことをそれぞれ表しています。

図1：チューリング機械の構成

現在の状態	現在の記号	次の状態	新記号	移動方向
S	0	S	0	R
S	1	S	1	R
S	B	T	1	N

図2：状態遷移関数

量子計算のしくみ

量子コンピュータのモデルとなっている量子チューリング機械は、チューリング機械のテープの1区画に、0が書き込まれている状態と、1が書き込まれている状態の「任意の重ね合わせ」を保持することができます。

量子並列化は量子力学の以下のような基本原理に基づいています。

・重ね合わせの原理
・状態のユニタリ時間発展
・確率解釈

今のコンピュータでは1bitで0または1の一方しか表現できません。しかし、量子コンピュータでは1qubit（1量子bit、現在の1bitに対応）として、0と1の重ね合わせ状態を扱うことができます。

例えば、1qubitどうしの足し算では

$0 + 0 = 0$　$0 + 1 = 1$

$1 + 0 = 1$　$1 + 1 = 0$

の4通りの計算を量子コンピュータは一度に行うことができます。上の例では2qubitなので4通りですが、100qubitでは $2^{100} = 2676506002282294014967032053760$通りと爆発的に量子並列度が上がります。この事を用いて計算の高速化を図っています。

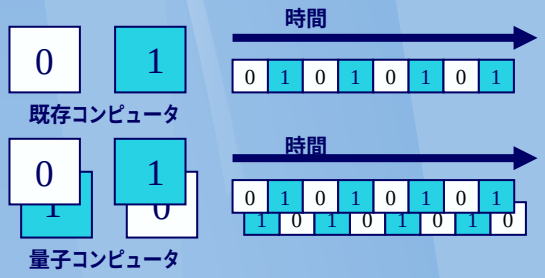


図3：ビットの重ね合わせ

Shorのアルゴリズム

現在のコンピュータは因数分解に膨大な時間を必要とし、このことはRSA公開鍵暗号系の安全性の拠り所となっています。

しかし、1994年にP.W.Shorは量子チューリング機械上で、大きな整数の因数分解を小さな誤り確率で高速に行えることを示しました。これにより、もし量子コンピュータを実際に作ることができれば、インターネット上でのセキュリティを確保することができなくなります。具体的に、500桁の「因数分解」を解くときに費やす時間を比較してみると、現在のコンピュータでは1000万年かかるのに対し量子コンピュータでは数十秒で解けてしまいます。

Groverのアルゴリズム

Groverのアルゴリズムは有名な量子アルゴリズムの1つで、ソートされていないデータベースの中から所望の要素を高い確率で発見するために用いられます。例えば、10万個のデータからほしいデータを探し出すとき、平均5万回調べなくてはなりませんが、量子コンピュータでは1000回調べればほしいデータを発見することができます。また、このアルゴリズムは、本来の機能よりもその汎用性が注目されており、西野研究室でも最短ベクトル問題や衝突探索問題、グラフの同型性判定問題、また、暗号解読などに応用して研究を進めています。

研究テーマ

情報通信工学科
情報メディア学講座　西野研究室

NMR量子計算

NMR量子計算とは？

- 量子計算の物理的実現方法の一つ
- 核磁気共鳴を利用して量子計算を実行
- 比較的近い未来に実現可能と考えられている

しかし、通常の量子計算とは枠組みが違う！

- 動作するアルゴリズムは？
- 通常の量子計算との計算能力の違いは？

西野研では、計算量理論の立場から

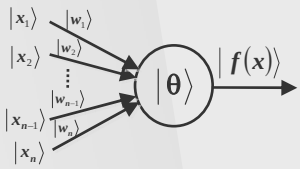
- 計算モデル Bulk Quantum Turing Machineの提案
- 正しく 動作するアルゴリズムの提案
- Grover のアルゴリズムの計算量の評価
- 通常の量子計算より高速である可能性の検討

などについて研究を行っています

量子ニューラルネットワーク

量子ニューラルネットワークとは？

- ニューラルネットワークに量子計算の概念を導入したもの
- 量子しきい値素子を基本素子として用いる。
  - しきい値論理素子の各入出力に重ね合わせ状態を取れる
  - しきい値論理素子では行えない計算を行える
  - NMR量子計算で実現すれば、XORを1層で計算できる！



西野研究室では、

- 量子しきい値素子の計算能力の解明
- 量子ニューラルネットワークの構成方法

に関して研究を行っています。

断熱量子計算

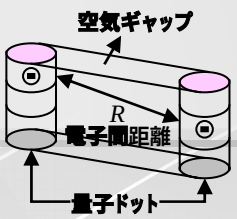
量子計算機の汎用機を作るのはとても難しい。

- 物理的実現可能性が高い専用計算機を考えよう！
  - → 断熱量子計算
- 専用量子計算機の理論モデルのひとつ。
- 現在のコンピュータでは困難な問題の解決を期待。

西野研では、

- 量子ドットを用いたシステムによる3彩色問題の解法
- そのシステムによる断熱量子計算の実現可能性の検証
- 現在のコンピュータとの計算能力の比較

などについて研究しています。



NMR量子アルゴリズムのシミュレータ作成

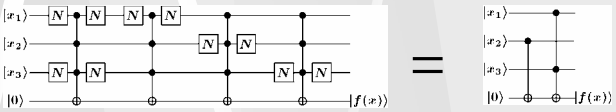
NMR量子コンピュータ上で動作する、量子探索アルゴリズムが提案されている。
そこで

1. 量子ビット数を節約できる可能性のある、ある探索アルゴリズムに注目し、そのアルゴリズムを実装したシミュレータを作成する。
2. Groverのアルゴリズムを用いて解く量子アルゴリズム　の動作を、解析しやすいように通常のコンピュータを用いてミュレータを作成する。

研究をそれぞれ行い、アルゴリズムが実行される際の問題点を明らかにしていきたいと考えています。

量子論理回路の最適化

- 論理関数の設計は、量子計算においても重要。
- 演算の可逆性を保つために、古典計算とは異なる方法で実現。



西野研では、

- 論理関数を計算する量子回路の設計法
- その回路のコストを最適にする方法の提案

に関して研究を行っています。

量子計算と暗号解読

多くの暗号の安全性は、解読に非常に時間が掛かることに依存している。
量子計算で高速に解けると、安全性が揺らぐ！

- どんな暗号の信頼性が無くなるのか？
- どの程度の速度で解けるのか？
- どうやって解けばよいのか？
- どんな暗号なら量子計算に耐性があるのか？

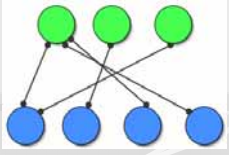
西野研では、特に衝突問題と最短ベクトル探索問題に注目して

研究を行っています（太田・國廣研との共同研究）

パーマネントの計算

- 量子コンピュータでは真の乱数を用いることができる。
- 乱数の質が重要なモンテカルロ法という近似計算を量子コンピュータ上で実行することで、高い精度のパーマネントを求めることができる。
- パーマネントの計算は応用例の多い2部グラフの問題に置き換えられる。

2部グラフのマッチング



- 緑と青の組をどれだけ多く作れるか？
- ただし、選んでいいのは線で結ばれているペアのみ