量子コンピューティング

未来の計算機への挑戦

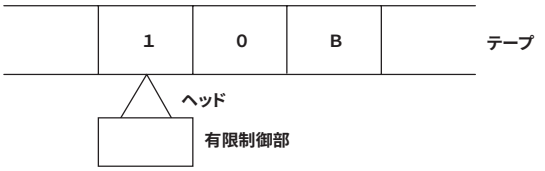
情報通信工学科
西野研究室

量子コンピュータとは

量子コンピュータとは、現在のコンピュータの仕組みに量子並列化の概念を導入したまったく新しい仕組みのコンピュータです。量子コンピュータを用いると、現在では解くのに非常に時間がかかると思われている問題を高速に解くことができます。このようなコンピュータに対する研究として、西野研ではShorの因数分解アルゴリズム、Groverのデータベース検索アルゴリズム、非線形量子計算、NMR量子計算などの研究を行っています。

Turing 機械

Turing 機械とは A.Turing が提唱した計算モデルであり、「ヘッダ」「無限に伸びたテープ」「有限制御部」からなっている図のような機械です。ここで、ヘッドは読み書き装置、テープは記憶装置にあたります。ヘッドは状態遷移関数に従って、１区画の読み書きを行ない、１区画ずつ左右に移動することができます。



状態遷移関数

現状態	現記号	次状態	書き込む記号	移動方向
c_0	1	c_0	1	R
c_0	0	c_1	1	R

単純なモデルですが対象の本質を抽象化しており、これが今の計算機の標準的なモデルとなっていて、同時に計算の定義も与えています。

量子計算のしくみ

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

今までのコンピュータでは1bitで0または1の一方しか扱えませんでしたが、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。たとえば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 2 qubit なので4通りですが、100qubit では 2^{100}= 1267650600228229401496703205376 通りと爆発的に量子並列度が上がることを用いて計算の高速化を図っています。

量子計算の簡単な歴史

1985 D.Deutsch が量子 Turing 機械を提唱。
1994 P.W.Shor が因数分解の量子多項式時間誤り限定アルゴリズムを発見。
1996 D.K.Grover がデータベース検索アルゴリズムを発見。

http://www.ice.uec.ac.jp/tnlab/

量子コンピューティング

未来の計算機への挑戦

情報通信工学科
西野研究室

因数分解に関する量子アルゴリズム

1994 年に P. 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を提案し、大きな注目を集めました。というのは、現在広く用いられている RSA公開鍵暗号系においては、既存のコンピュータが因数分解に膨大な時間を要することが、その安全性の拠り所になっているからです。つまり、もし量子コンピュータが物理的に実現できた場合には、RSA 暗号はその安全性の根拠を失うことになります。

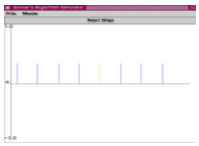
そこで、私たちは、既存のコンピュータ上で可能な限りシミュレーションを行なうことにより、Shor のアルゴリズムの振舞いや種々の性質を明らかにすることを目指しています。

Grover のアルゴリズムの応用

Groverのアルゴリズムは Shorのアルゴリズムと並ぶ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ことができます。

概念的な動作原理は以下の図のようになっています。

Grover 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、西野研究室では最短ベクトル探索問題などに対するアルゴリズムへの応用を研究しています。



全ての状態が
等しい振幅を
持つように初期化

所望の状態の
振幅を反転

振幅の平均について
折り返し演算を行うと
所望の状態を発見する
確率が高くなる

非線形量子計算のシミュレーション

D.S.Abrams と S.Lloyd は非線形量子力学の効果を使い、NP 完全問題という難しいと考えられている問題を効率的に解くためのアルゴリズム(AL アルゴリズム)を示しました。

私たちは、このアルゴリズムを Turing 機械でシミュレーションできることを示しました。この結果と量子 Turing 機械は Turing 機械と同じ計算ができるという定理より、線形な量子Turing機械を用いてある種の非線形効果をシミュレーションできることがわかりました。現在は AL アルゴリズムをシミュレーションするときに必要な資源について研究しています。これまでに、シミュレーションには AL アルゴリズムに比べて大きな領域が必要であることがわかりました。

NMR(核磁気共鳴)量子計算

NMR装置は原子一つ一つのエネルギーを測定する装置です。NMR 量子計算では、0 と 1 を分子の回転の向きに対応させて、量子ビットを構成します。NMR装置は、一般的に普及した装置であり、比較的手軽に研究できるため、世界初の量子コンピュータの実現に向けて盛んに研究が行なわれています。私たちは、計算量理論の立場から NMR 量子計算の理論の構築を行なっています。

- Bulk 量子 Turing 機械の定義と決定問題、関数問題の計算量クラスの構築
- NMR 装置の初期設定法
- Bulk 量子 Turing 機械上のアルゴリズム

http://www.ice.uec.ac.jp/tnlab/