量子コンピューティング
Quantum Computing

# 計算機 ： The Next Generation

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に量子力学的動作原理を導入した新しい仕組みのコンピュータです。

量子コンピュータが実現すれば、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。

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、理論計算機科学の側面からおこなっています。

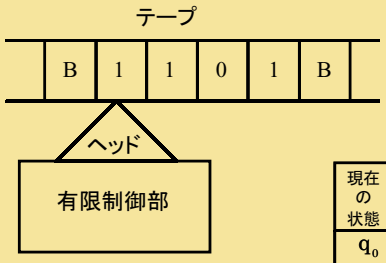
## 量子計算の簡単な歴史

1985 D.Deutsch が量子 Turing 機械を提唱。
1993 E.Bernstein and U.Vazirani が効率的な万能量子 Turing 機械を構成。
1994 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 D.K.Grover がデータベース検索アルゴリズムを発見。

## Turing 機械

現在の計算機の数学的モデルは、A.Turing が提唱した Turing 機械です(右図参照)。テープは記憶装置にあたり、区画分けされた各領域には記号をひとつ書くことができます。ヘッドはこの記号を読み書きします。

Turing機械は状態遷移関数に従って動作します。有限制御部は状態を保持し、動作の各ステップにおいて、現在の状態とヘッドが読んでいる記号に応じてテープのヘッド位置の記号を書き換え、現在の状態を変更し、ヘッドを右または左に１区画移動します。




| 現在の状態 | 現在の記号 | 書きこむ記号 | 次の状態 | ヘッドの移動方向 |
|---|---|---|---|---|
| $q_0$ | 0 | 0 | $q_0$ | R |
| $q_0$ | 1 | 1 | $q_0$ | R |
| $q_0$ | B | B | $q_1$ | L |
| $q_1$ | 0 | 1 | $q_F$ | L |
| $q_1$ | 1 | 0 | $q_1$ | L |
| $q_1$ | B | 1 | $q_F$ | L |

右表はテープ上の二進数に1を足すTuring機械の状態遷移関数です。初期状態は $q_0$ で、最終状態 $q_F$ になると停止します。B は空白記号です。

## 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の一方しか表現できませんでしたが、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ります。このことを用いて計算の高速化を図っています。

量子コンピューティング
Quantum Computing

# 計算機 ： The Next Generation

情報通信工学科
西野研究室

## 因数分解に対する量子アルゴリズム

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ました。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になっています。

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。

## 非線形量子計算の模倣

D.S.Abrams と S.Lloyd は非線形量子力学の効果を使い、難しいと考えられているNP完全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 機械で模倣できることを示しましたが、量子Turing機械はTuring機械を効率的に模倣できるので、線形領域の量子 Turing 機械を用いてある種の非線形効果を模倣できることがわかりました。

ただし、量子Turing機械を使用した模倣では、ALアルゴリズムよりも大きな領域が必要となります。

## NNR 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。現在までに 5 qubit NMR 量子計算の実験が成功しています。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。

## Grover のアルゴリズムの応用

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。

概念的な動作原理は以下の図のように示されます。

全ての状態が等しい振幅を持つように初期化

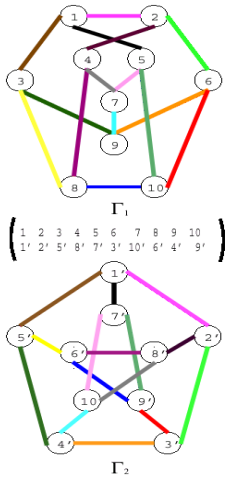
所望の状態の振幅を反転

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

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、西野研究室でも以下の問題への応用を研究しています。

### グラフの同型性判定問題

右図は 2 つの同型なグラフを示しています。2つのグラフ $\Gamma_1$ と $\Gamma_2$ が同型か否かを判定するのがグラフの同型性判定問題です。




### 最短ベクトル探索問題

最短ベクトル探索問題とは、n本の基底ベクトルを与えられ、それらを整数倍して足し合わせて得られるベクトルのうち、最短のベクトルを求める問題です。

### 衝突問題

写像先が同じ要素となる組(collision)を探索する問題です。