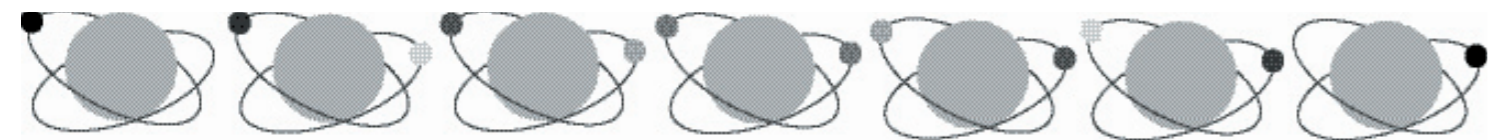


原理

原子などのミクロな粒子は時に波として振る舞うことがあります。そのような波は、水面にたつ波のようにいくつも重ね合わせることができます。波が重なり合ったとき、その粒子の粒子としての位置は不確定になります。このような粒子の状態を重ね合わせ状態といいます。



電子の軌道の重ね合わせ状態と0と1の重ね合わせ状態

さて、古典的なコンピュータのメモリの1ビットと呼ばれる一画素は、「0」か「1」のどちらかの値しか保持できません。それに対して、量子コンピュータのメモリの一画素は1量子ビットと呼ばれ、先に述べた量子力学的な性質を用いて、通常の「0」、「1」に加え、様々な「0と1の重ね合わせ状態」をとることができます。

威力

単純に、1量子ビットで「0」と「1」の両方の値を保持できると考えれば、たとえば2量子ビットの場合、メモリ全体で「00」、「10」、「01」、「11」の4つの値に関する計算を同時に実行できます。

もし、もっと量子ビットの数が多い量子コンピュータ、たとえば17量子ビットの量子コンピュータが実現できたなら、この量子コンピュータはメモリ全体で 2^{17} (約65,000)通りの値それぞれについての計算を、同時に行うことができます。これは2005年現在で世界最速のスーパーコンピュータBlueGene/Lに匹敵します。18量子ビットならさらにその2倍です。電子的なコンピュータが発明されて以来、一秒に一つのプロセッサが計算できる回数——周波数は年々向上してきました。これは基本的に回路の集積度(部品の詰まり具合)が技術の進歩により上がってきた為です。

しかし、ひとつひとつの部品を細かくするのにも限界があります。なぜなら、部品が原子数百個、数十個分と小さくなっていけば量子的な特性が無視できなくなるからです。

量子コンピュータは古典的なコンピュータの限界である粒子の量子的特性を逆手に取って、一度に行える計算の並列度を爆発的に高めるコンピュータです。

問題点

しかし、量子コンピュータは単純な並列計算機ではありません。実際には様々な量子力学的な制約が課せられます。そのため、どのような計算法(アルゴリズム)が量子コンピュータ上で威力を発揮するのか、量子コンピュータはどのような可能性を持っているのか、などを研究する必要があります。

歴史

- B.C. そろばんの発明
- A.D. 17 Pascal が歯車を用いた機械式計算機を発明した
- 1936 Church によって「計算」とは何か?が明らかにされた
- 1937 Turing によってチューリングマシンが考案された
- 1944 リレースイッチを使用した電子計算機 Mark- I が開発された
- 1946 真空管を使用した電子計算機 ENIAC が開発された

- 1985 Deutsch が量子チューリングマシンを考案した
- 1989 Deutsch が量子回路を定式化した
- 1993 Bernstein と Vazirani が効率的な万能量子チューリングマシンを構成した
- 1994 Shor のアルゴリズムが考案された
- 1996 Grover のアルゴリズムが考案された



量子コンピュータと古典的なコンピュータ

現在知られている主要なアルゴリズム

Grover のアルゴリズム

整列されていないデータベースの中から、所望のデータを高い確率で高速に探し出します。整列されていない100万個のデータからほしいデータを探す場合、現在のコンピュータで動く既存のアルゴリズムでは平均50万回調べなければ探し当てられませんが、このアルゴリズムを量子コンピュータ上で動かせば、1000回調べればほしいデータを発見することができます。

Shor のアルゴリズム

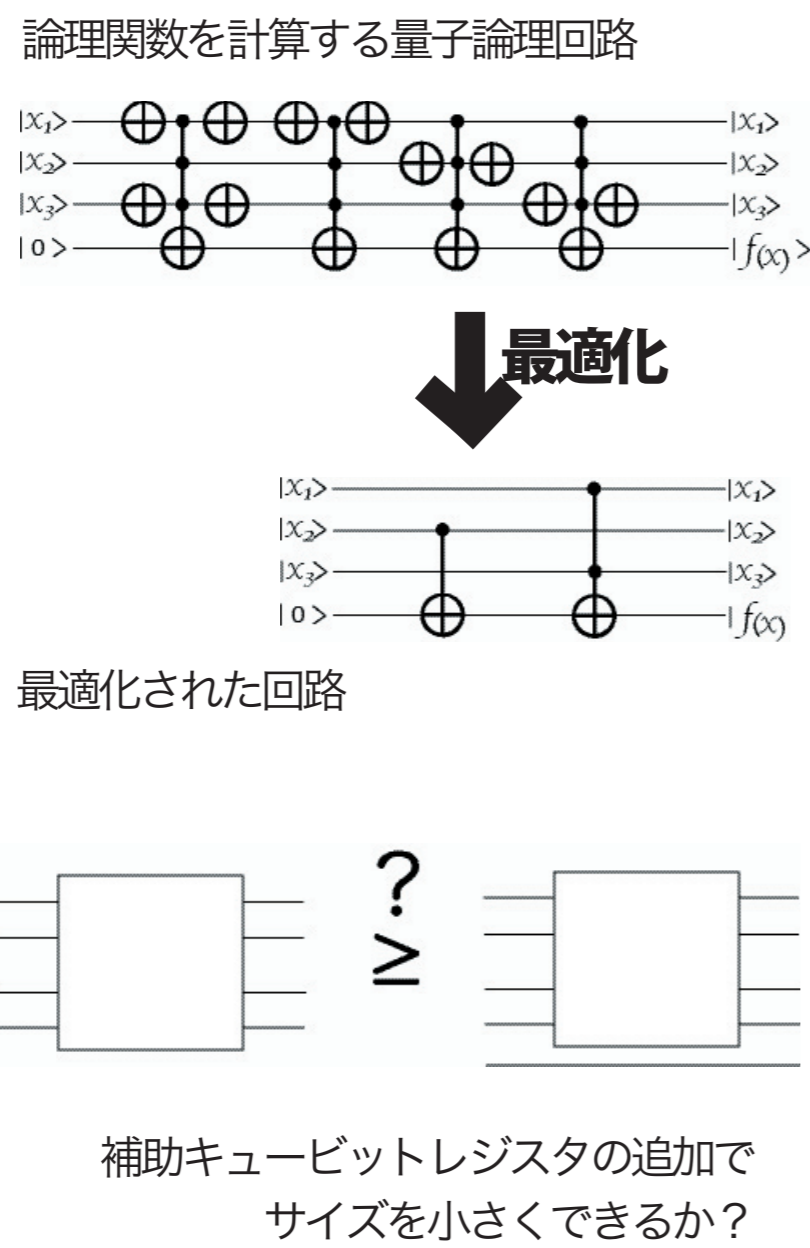
整数の因数分解を小さな誤り確率で高速に行うアルゴリズムです。一般に大きな整数の因数分解は現在のコンピュータでは非常に時間がかかります。500桁ほどの整数の因数分解には1000万年程度かかります。

この因数分解の困難さによってRSA公開鍵暗号など主要な暗号の安全性が保証されています。

つまり、もしこのアルゴリズムを実行できる量子コンピュータが実現されると、インターネット上での情報のやり取りの安全性が失われてしまいます。

量子回路

現在のコンピュータは基本的に論理回路で構成されています。量子コンピュータにおいても回路を考えることができ、それを量子回路と呼びます。特に論理関数を計算する回路を量子論理回路と呼びます。



量子論理回路の最適化

論理関数の計算は、量子コンピュータにとっても重要です。しかし量子論理回路は(演算が可逆でなければならないという量子力学の制約があるので)古典コンピュータとは異なる方法で実現しなくてはなりません。

また、量子コンピュータの状態は量子力学的に非常にデリケートなので、量子回路のサイズはなるべく小さくする必要があります。

当研究室では量子論理回路の設計法、および最適化の方法を研究しています。

量子回路における補助キュービットレジスタの効果の検証

量子コンピュータ上の計算において、使えるメモリの量を増やすことで量子回路のサイズを小さくすることができるのか、という問題を研究しています。

量子ゲーム理論

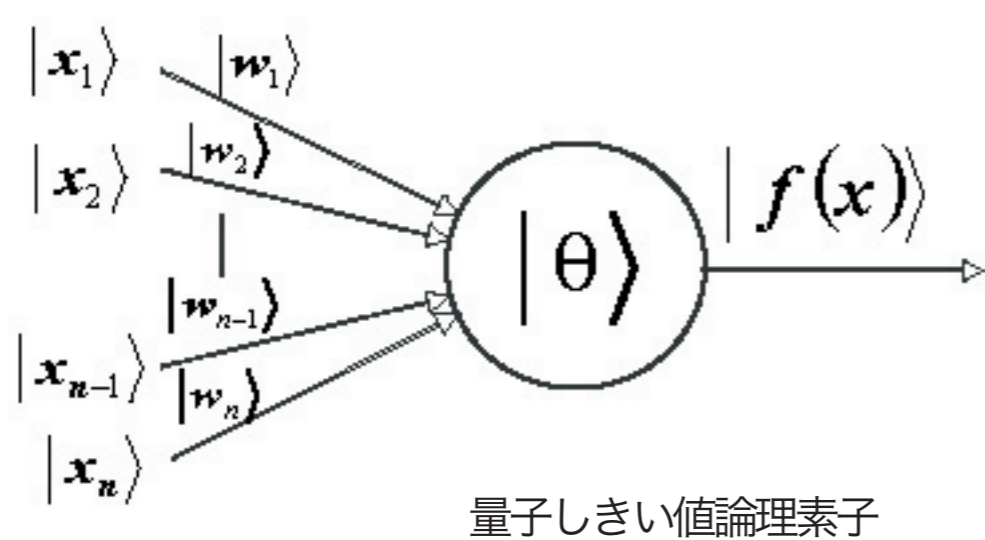
ゲーム理論は、経済学や心理学の分野と密接な関係を持つ理論です。あるルールのもとで最適な戦略を考える場合などに、応用されています。

また、量子ゲーム理論は、古典ゲームに量子力学的特性を考慮した物で、古典ゲームにおいて生じてしまう、いわゆる「囚人のジレンマ」などを解決できる場合があることが知られています。

当研究室では、量子ゲーム理論を用いて、古典的には説明することが難しい、さまざまな現象をシミュレーションすることができないか、研究を行っています。

種々の量子コンピュータ

現在、量子コンピュータの実現に向けて様々な方法が検討されています。しかし、その実現方法によって計算の特徴が異なると考えられます。そこで、それらの特徴を積極的に生かす方法を研究しています。



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です。基本の素子として「量子しきい値論理素子」を用います。これは既存のニューラルネットワークのしきい値論理素子の各入出力として0と1以外に、重ね合わせ状態を取ることができるような素子です。

これによってしきい値論理素子にはできない計算が行えます。たとえばNMR量子計算(後述)を用いて実現すれば排他的論理和を一層で計算できます。

当研究室では、量子しきい値論理素子の計算能力、および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。

NMR量子コンピュータ

NMR量子コンピュータは、「核磁気共鳴」を利用して動く量子コンピュータです。この方式の量子計算は比較的近い未来に実現可能だと考えられています。

当研究室では、計算量理論の立場から
NMR量子コンピュータ上で動作するアルゴリズム
NMR量子コンピュータ上でGroverのアルゴリズムの計算量の評価
通常の量子計算よりも高速である可能性の検証
などについて研究を行っています。

