１１情セ第２４０号

「量子計算機の研究動向に関する調査」

調　査　報　告　書

平成１２年２月

情報処理振興事業協会

量子計算に関する調査研究の報告書サマリー

本調査報告書は、量子計算の実験及び理論両面の現状と動向を調査し報告書をまとめたものである。

第 1 章で、量子計算機の研究動向に関する調査研究の目的と背景について述べる。

第 2 章では、量子計算の基本原理について説明する。ここでは量子計算機の演算処理の基本的な流れを説明し、特に量子力学の基本原理である重ね合せの原理が量子計算の仕組みであることを明らかにする。さらに超並列処理、干渉効果を利用した波束の集中、観測と読み出しについて説明する。そしてそれらの技術を使うことにより、ある種の問題に対して古典計算機よりも有効に働き、高速演算処理が可能なことを示す。またここで、簡単に量子アルゴリズムで使用する基本演算を数式で示す。

次に第 3 章では、量子計算機研究の実験の現状と将来の方向について述べる。まずは、量子計算を実現するための基本構成要素として何が必要かということに関して説明する。理論的には、1 キュービットの位相シフト演算と 2 キュービットの制御ノットが量子計算の演算を構成する基本要素となることがわかっている。またこれをふまえて、実際量子計算機を実現するいくつかの方式について簡単に説明し、代表的な方式である、線形光学素子方式、NMR 方式、イオントラップ方式を取り上げて詳しく記述する。各々利点と欠点を示す。また現段階で実現されているキュービット数、拡張性の点から将来性に関して調査する。

第 4 章では、量子計算機研究の理論の現状と将来の方向について説明する。

まず最初のセクションでは、量子アルゴリズムが古典計算機上のアルゴリズムと比較して有効となるアルゴリズムに関して、理論研究の歴史にそって記述する。量子アルゴリズムで最も衝撃的であったのは、Shor による素因数分解問題、離散対数問題に対する多項式時間アルゴリズムである。

次のセクションでは、量子計算の有効性を示した初期の研究である Deutsch-Jozsa のアルゴリズムを、また一般的な問題であるデータベース検索問題に対する Grover のアルゴリズムについて詳しく説明する。但し後者に関しては、古典計算機と比べて計算量が指数時

間から多項式時間に落せたわけではなく、平方根オーダまでしか高速化されていない。

次に、暗号の研究者に衝撃を与えた暗号解読に関する量子アルゴリズムに関して説明する。ここでは、Shor の素因数分解問題、離散対数問題に対する量子アルゴリズムを詳細に記述する。これらの問題は、古典計算機では準指数時間解読に要するものであるが、量子アルゴリズムで多項式時間の解法を与えたため、意義が大きい。また楕円曲線上の離散対数問題に関しても、Shor の離散対数問題に対する量子アルゴリズムの場合とほとんど同様に適用できることを説明する。

そしてこの章の最後では、理論の研究動向と将来の方向に関して説明する。具体的には、計算量クラスで分類し、NP 完全問題へのアプローチ、NPI(NP Intermediate)問題へのアプローチ、NP 困難な問題へのアプローチについて問題の定義なども含めて説明する。NP 完全問題とは、NP に属する問題で NP の全ての問題がこれに多項式時間還元できる問題である。このため NP 完全問題の代表的な問題である充足可能性問題(SAT)が積極的に研究されたが、現在のところ多項式時間で解ける量子アルゴリズムの発見はされていない。一方、NP 困難な問題である束内最短ベクトル探索問題に関しても、有効な多項式時間で解ける量子アルゴリズムは見つかっていない。しかし、この問題自身がいくつかの点で興味深いため、現在考えられている量子アルゴリズムを具体的に示す。

また暗号に関連した問題に関しては、いくつかの問題に対するアルゴリズムについて簡単に触れる。具体的には、アーベル群の固定部分群を求める問題や Hidden Subgroup 問題、Quantum Counting などである。

第 5 章では、量子計算研究に関する参考文献を論文、プレプリント、書籍からリストアップし、それらを分野別に分類してまとめる。具体的には、まず入門・解説文献を雑誌、書籍、講義ノートからピックアップする。そして量子計算の理論研究では、代表的論文やその他の研究論文、量子ゲートに関する論文を分類してまとめる。さらに量子計算の実験的側面に関する論文を示し、今回記述できなかった量子計算量理論に関する代表的な文献をまとめる。最後に関連有効サイトとして、ロスアラモス研究所のプレプリントサイトについても示す。

目次

1. 量子計算機に関する調査研究の背景と目的

この章では、最初に量子計算機に関する調査研究の背景と目的について述べる。

調査研究の背景

近年のインターネットに代表されるオープンなネットワーク上で暗号技術を応用した情報セキュリティシステムが電子商取引のシステムに利用され、また通信インフラ面でも次世代インターネット技術によるネットワーク構築が進められようとしている。一方、それらの技術とは別の分野の次世代研究で最近注目されている技術がある。その技術とは、ミクロの世界で日常生活レベルの常識とはかけ離れた現象が起こる「量子技術」である。ここでは電子や光子が主役となる。この技術を情報処理の分野に応用したものが、量子情報処理と呼ばれている。

量子情報処理の理論研究は、1970 年代から行われ、近年の実験技術の向上に伴い、理論での予言が実験的に検証されつつある段階にある。量子情報処理技術の暗号に関連する主なアプリケーションは、量子計算と量子暗号通信の 2 つである。これらの技術の実現可能性に関しては、量子計算では 1994 年に素因数分解アルゴリズム、1996 年にデータベース高速検索アルゴリズムといった理論的に大きな発見があったが、現在はこれらの物理的な実験がされ始めている。まだ研究段階ではあるが着実に実験面も発展している。一方、量子暗号通信に関しても、いくつかの基本プロトコルの物理的実現研究が進められている。

調査研究の目的

量子計算は、「量子力学的な重ね合せ状態」を利用して大規模な超並列計算を行うため、既存のコンピュータとは比較にならないほど高速処理が可能である。一方、量子暗号通信では、「量子状態は観測により影響される」という量子力学の基本原理を用いて、盗聴者の存在を必ず探知できるような通信方法である。両者とも潜在力を潜めた新しい技術の可能性がある。現在まで量子情報処理技術を殆ど考慮しないまま、既存の暗号技術の安全性評価や運用方式の研究が活発に研究されてきた。しかし、急速に進展する情報化社会では、将来次世代暗号関連研究が加速度的に進歩する可能性もあり、これらの次世代技術の現状を理解し、将来の方向性を見据える必要がある。そのため今回、量子計算の実験及び理論両面の現状と動向の調査を実施する。

2. 量子計算の基本原理[1-14]

量子計算機の特徴を説明するキーワードとして、重ね合わせ、超並列処理、干渉効果を利用した波束の集中、観測などが挙げられる。以下これらのキーワードを順に解説していくことで量子計算の処理の流れを説明する。

重ね合わせ

まず、量子計算機が古典計算機と違う点は、量子計算機においては可能な状態として 0 と 1 だけではなく、それらの重ね合わせ状態も取り得ることである。ここで状態であることを強調し、物理学で一般的に使用しているケットベクトル$|\ \rangle$の表記を用いると次の通り。すなわちαとβを複素数で、$|\alpha|^2+|\beta|^2=1$なる規格化条件を満たすものとして、

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$$

なる状態も量子チューリングマシン上のテープに書き込める点である。これが量子計算機の第 1 の特徴である重ね合わせ状態である。ここでα、βは確率振幅と呼ばれ、$|\alpha|^2$、$|\beta|^2$がそれぞれ$|0\rangle$、$|1\rangle$の状態を観測する確率となる。$|0\rangle$と$|1\rangle$の重ね合わせの状態を取り得るものをキュービット(qubit: quantum bit)と呼ぶ。

重ね合わせとは、複数の状態を確率的に取り得る状態であるが、実際状態を観測して見ると量子力学の原理によって、ある 1 つの状態に収縮する。このときその状態が観測される確率は、確率振幅の絶対値の 2 乗になる。またキュービットをn個用意すれば、2^n個の状態の重ね合わせを実現することができる。何故なら、各々のキュービットが 2 個の状態を取れて、それがn個あるからである。

実際には、基底状態から指数個（例えば、$N=2^n$）の状態の重ね合わせ状態を次に示した量子離散フーリエ変換QFT_Nを施して作りだせることが知られている。ここで、基底状態$|0\rangle$から指数個の重ね合わせ状態を多項式時間で作りだせること、すなわち量子離散フーリエ変換QFT_Nが多項式時間のステップで構成されるという事実が重要である。

量子離散フーリエ変換（ユニタリ変換）

一般の場合：　$$QFT_N|a\rangle = \frac{1}{\sqrt{N}}\sum_{c=0}^{N-1}\exp(2\pi iac/N)|c\rangle$$

上記で $a=0$ の特別の場合：　$$QFT_N|0\rangle = \frac{1}{\sqrt{N}}\sum_{c=0}^{N-1}|c\rangle$$

超並列処理

n キュービットの量子計算機は量子力学の原理に基づいて前述のように 2^n 個の状態の重ね合わせ状態をとれる。これはある関数 $f:a\to f(a)$ を考えたときに、2^n 個の入力変数を 1 つの物理状態として表せるということを意味する。そしてその状態に対してある物理演算（ユニタリ変換）を作用させて、関数 $f(a)$ の値を計算して、その関数値 $f(a)$ を入力値 a と関連づけた重ね合わせ状態に変換することが可能である。これは即ち、あるユニタリ変換が存在して、その操作を 1 回だけ施すことにより、$N=2^n$ の入力値に対して $f(a)$ をまとめて超並列計算できることを意味する。この超並列処理部分が量子計算機の利点の本質である。また、入力値 a とその入力に対する関数値 $f(a)$ が物理的に関係づけられた状態 $|a\rangle|f(a)\rangle$ になっていることも重要である。これが量子もつれあいと言われる。

関数 $f(x)$ の値を計算してレジスタに格納する演算 U_f （ユニタリ変換であり物理的に実現可能）が上で説明した物理演算に相当する。数式で表すと下記のとおり。

関数 $f(x)$ の値を計算しレジスタに格納するユニタリ変換 U_f

一般の場合：　$$U_f|a\rangle|b\rangle = |a\rangle|b\oplus f(a)\rangle$$

上記で $b=0$ の特別な場合：　$$U_f|a\rangle|0\rangle = |a\rangle|f(a)\rangle$$

実際の演算では次のようにして多項式時間で処理可能な演算を順次作用させて、ある関数 $f(a)$ の超並列処理を行う。

基底状態から多項式時間で重ね合わせ状態を作り出す

$$QFT_N|0\rangle|0\rangle = \frac{1}{\sqrt{N}}\sum_{c=0}^{N-1}|c\rangle|0\rangle$$

関数の超並列処理演算を多項式時間で行い、レジスタに格納する

$$U_f QFT_N|0\rangle|0\rangle = \frac{1}{\sqrt{N}}\sum_{c=0}^{N-1}U_f|c\rangle|0\rangle = \frac{1}{\sqrt{N}}\sum_{c=0}^{N-1}|c\rangle|f(c)\rangle$$

干渉効果を利用した波束の集中

演算結果は $N = 2^n$ 個の重ね合わせ状態にあるが、そこから必要な演算結果を得るには工夫が必要である。重ね合わせと超並列処理の特徴までは前述の説明のように簡単に行えるが、最終的に観測して得られるある物理量が問題の解に結びつくようにするために、一般にはさらに演算が必要である。今まで知られているのは、関数に周期性がある場合は、さらに量子離散フーリエ変換などの演算をすることで解に結びつく状態を取り出せる。具体的には、素因数分解問題や離散対数問題のような周期を求める問題などの場合である。一般には、干渉効果を利用して欲しい答えに対応する状態に波束を集中させる。

観測と読み出し

最後に状態を観測して結果を得る。詳しく説明すると、量子力学の原理により、状態としては複数の状態をある確率で取り得るが、実際に観測するとその中の 1 つの状態のみに収縮する。すなわち実際の物理的な観測を行うと、状態の収縮がおき、ある状態に対する物理量（観測値）が得られる。量子アルゴリズムでは、この観測値をもとに問題の解を算出することになる。

問題の解の算出に関しては、確実に正しい解が得られる場合と確率的に解が得られる場合の２つに分けられる。Deutsch-Jozsa のアルゴリズムは前者であるが、素因数分解問題や離散対数問題などに対する量子アルゴリズムは後者の確率的なアルゴリズムである。そのため誤った解答も得られるが、検算によってそれを排除する。

以上が量子計算の基本原理の説明である。

その他重要な演算として、物理学で一般的に使用されるパウリ演算子σ_zという演算も量子アルゴリズムで使用される。ここでは簡単に定義だけ示す。

パウリ演算子（ユニタリ変換）　σ_z

$$\sigma_z|a\rangle = (-1)^a|a\rangle$$

具体的に記述すると次の通りである。

$$\sigma_z|0\rangle = |0\rangle$$
$$\sigma_z|1\rangle = -|1\rangle$$

量子計算では、超並列処理が可能で、多項式時間で指数個の演算結果の重ね合わせが作り出せる。そのため、あとはそこから必要な情報をいかに取り出すかということが重要である。

3. 量子計算機研究の実験の現状と将来の方向

3.1 概要

Shor によって効率よく素因数分解ができる量子アルゴリズムが発見されて以来、量子計算機というものが注目を浴びている。それでは、素因数分解が実際できて、情報セキュリティの世界に衝撃を与えるような量子計算機は現に存在するのか、もしくは近い将来において実現できるのだろうか。残念ながら量子計算機はまだこれから黎明期を迎えつつあるという段階である。つまり、我々が日常用いているパソコン等の「古典計算機」が AND や OR のゲート素子から始まったように、基本的な量子ゲートを構成、もしくはいくつかのゲートを組合わせて簡単なアルゴリズムを検証しているという段階にある。この時点における量子計算機開発の指導原理とは、理論的に 1 キュービットの位相シフトと 2 キュービットの制御ノットが実現できれば物理的に量子計算機の回路が組める、即ちユニバーサルゲートであることが分かっていることである[35](図 3.1)。

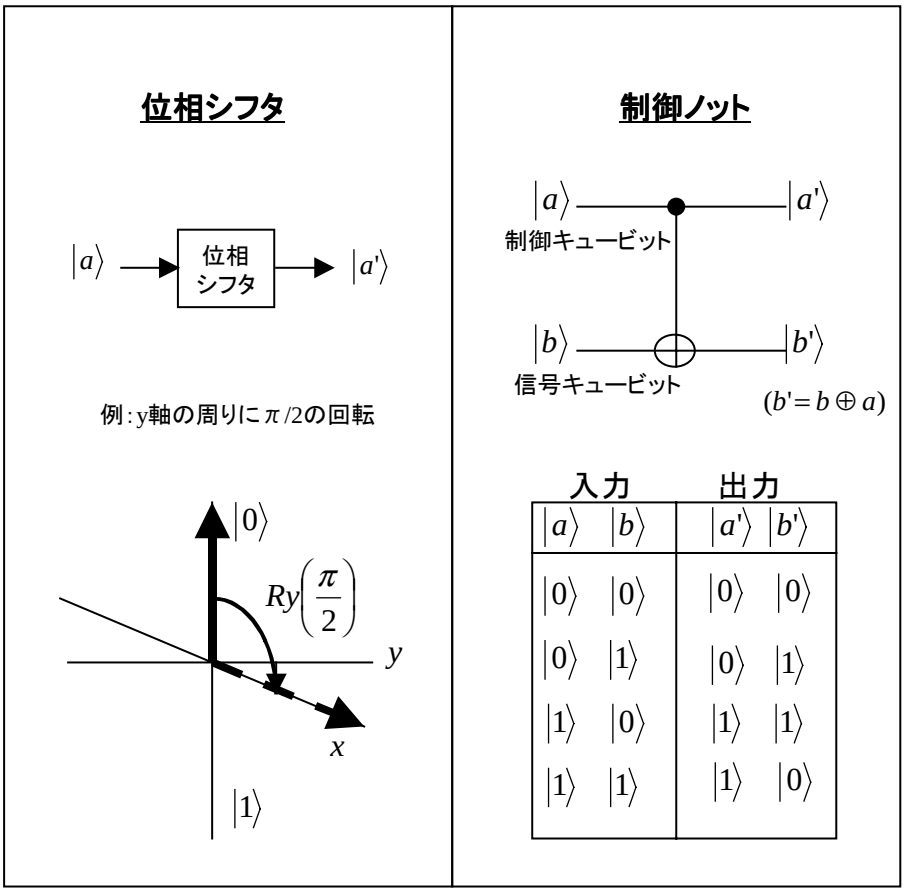


図 3.1 基本量子ゲート

従って、量子計算機を実現するためには、何をキュービットとして用い、どのようにゲートを構成するかを考えればよい。この構成方法により、様々な方式現在考案されている。表 3.1 はそのリストである。

表 3.1　量子計算機リスト（[3]より抜粋）

候補	方式	キュービット	現状	拡張性
線形光学素子[36,37]	弾道	単一	3 キュービットのアルゴリズムが実現	～10 キュービット
NMR 量子計算機[38]	固定	ﾊﾞﾙｸ	3 キュービットのアルゴリズムが実現	～10 キュービット
イオントラップ[39]	固定	単一	2 キュービット間のゲート操作	難
半導体不純物核スピン[44]	固定	単一	アイデアのみ	易
量子ドット(電子準位)[43]	固定	単一	重ね合わせ	易
フォトンロジック[40] (マイクロ波)	弾道	単一	2 キュービット間のゲート操作	難
フォトンロジック (可視)[41]	弾道	単一	制御ノットまであと少し	難
超伝導トンネル接合[42]	固定	単一	重ね合わせ	易

ここで、方式とは、キュービットおよびゲート操作の実現方法の観点からの分類である。大きく「弾道」方式と「固定」方式の 2 つに分類される。

固定型とは、キュービットを担う粒子を固定しておくことに由来する。ゲート操作は、レーザをあてる等の外力を加えることにより実現する。従って、プログラミングはレーザ光の照射順序、組合せにより表現される。これはプログラムの変更が容易にできるという利点を持っている。

弾道型とは、固定型とは逆にキュービット自身が量子計算機の中を移動しながらゲート操作を受けていく、ゲート素子の方が固定されている方式である。従って、プログラムはこのゲート素子の配列で表現される。

また、キュービットの種類で分類することもできる。但し、ここでの種類とは、キュービットが光子か、電子か、原子かという違いで分類するのではなく、キュ

ービットを担う「量子」自体を単一量子にするか、集団的な量子の振る舞いにするかという違いである。これをここでは「単一」と「バルク」と表現する。

このように様々なアイデアが提案されているが、量子計算機としての現状は、それぞれの方式により実現レベルは異なっている。これを簡単に表 3.1 にまとめてある。

量子計算機が現在注目を集めている理由の１つとして、多くの公開鍵暗号の安全性の基になっている因数分解や離散対数問題が簡単にとけるという理論上の成果があるが、これを実際の量子計算機で解くとなると、数キュービットではなく数千キュービットを扱えなければならない。このための拡張性についても、その難易度を表 3.１中に簡単に付した。

次のセクションで各方式の概要を述べる。

3.2 具体的な実現方式

ここでは代表的な量子計算機の実現方式として、線形光学素子方式、NMR 方式、イオントラップ方式の３つの方式について説明する。

線形光学素子量子計算機[3, 36,37]

この方式は既存の受動的光学素子（線形光学素子）を用いて量子計算回路を実現する。キュービットとしては単一光子の偏光や光路を用いる。このときの位相シフトは、偏光に対しては、2 軸性の結晶を用いた偏光回転板で、光路に対しては、ビームスプリッターによって実現できる(図 3.2)。

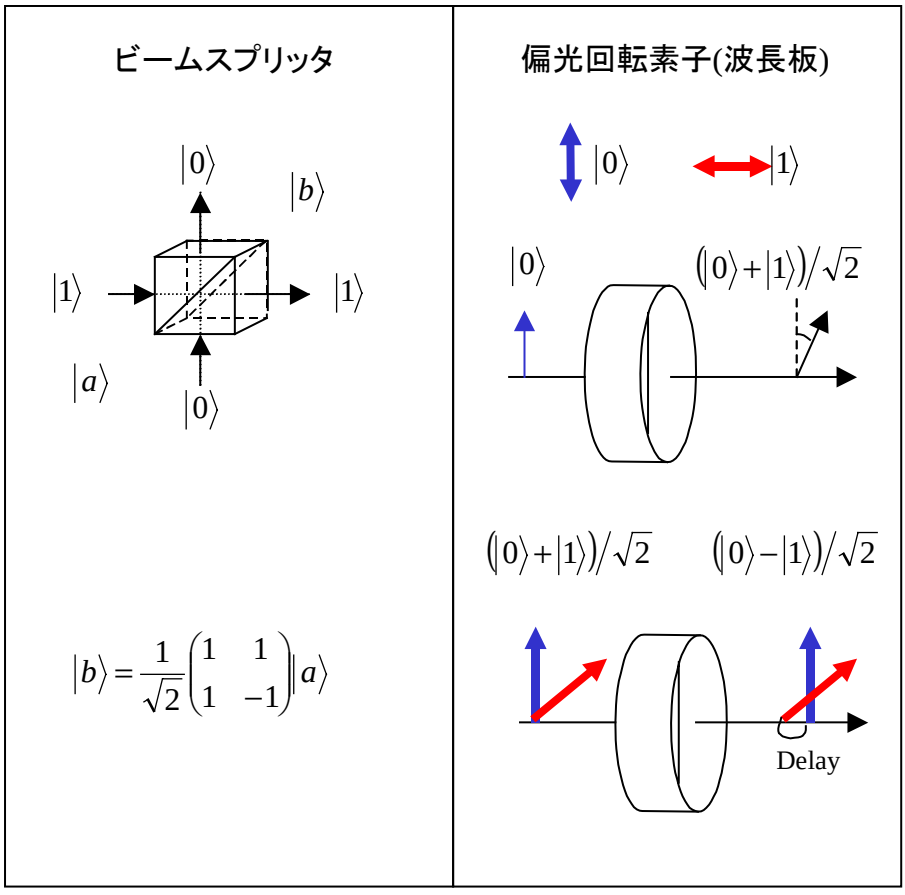


図 3.2　光学素子による位相シフタ

制御ノットは、キュービットとして偏光と光路の両方を用いる場合では、偏光ビームスプリッターによって可能である。キュービットとして光路のみで構成する場合は光路の交換で可能となる(図 3.3)。

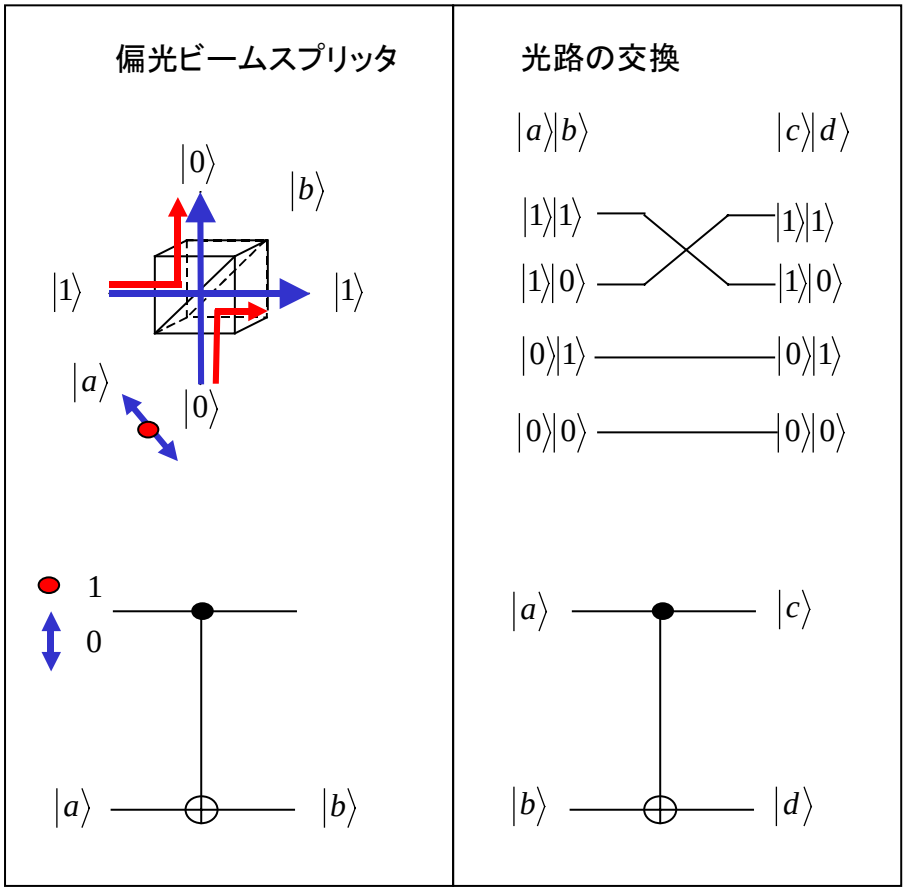


図 3.3 光学素子による制御ノット

これと併せて、線形光学素子により任意のユニタリ変換が実現可能であることが知られているので、線形光学素子を用いて任意の量子計算の実験を行うことができる。

従って、線形光学素子方式の利点として次の 2 点が挙げられる。

1) 任意の量子計算の実験が可能である点

2) 量子計算アルゴリズムを忠実に再現できるので NMR 量子計算機では実現できない「射影測定」という方法を用いるアルゴリズムも可能となる点。

欠点としては、n 個のキュービットで記述されるアルゴリズムを実行するためには、2^n 個の光路が必要になり、莫大なハード規模を要する。そのため、キュービット数が増えると実現可能性が乏しくなる点である。

実現アルゴリズム例としては、Deutsch-Jozsa アルゴリズム(図 3.4)がある。

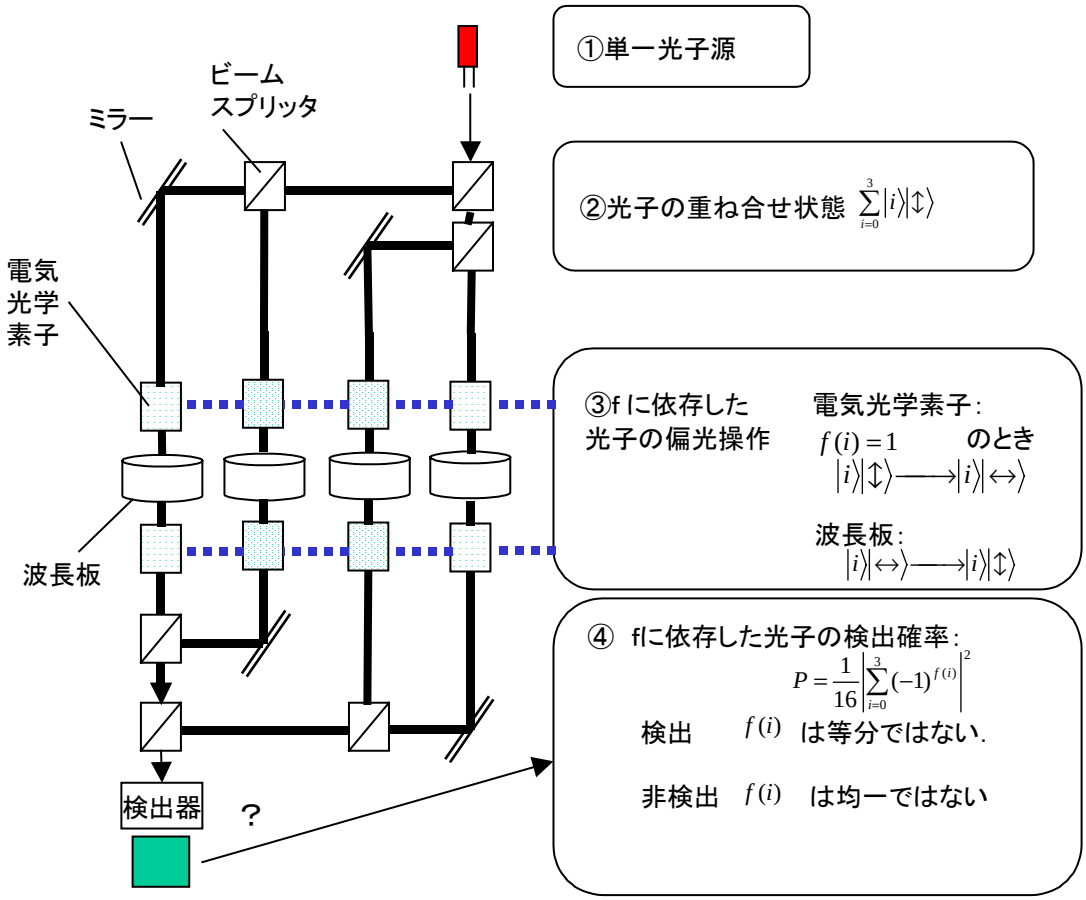


図 3.4 線形光学素子による Deutsch-Jozsa アルゴリズム

NMR 量子計算機[3,38]

この方式の特徴は、適当な溶媒にモルのオーダーで溶かしこまれた分子ひとつひとつが量子計算機として働く点である。この方式では、各分子中にある原子の核スピンがキュービットとなる(図 3.5)。I. L. Chuang の実験では、クロロホルム（$^{13}CHCl_3$)分子中の水素原子(H)と炭素原子(^{13}C)の核スピンをキュービットとして用い 2 キュービットの量子計算を実現した。

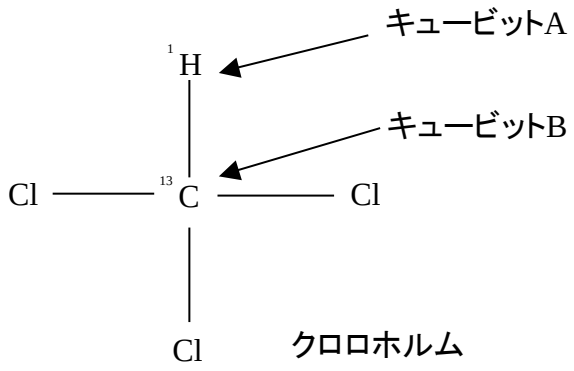


図 3.5 NMR 計算機のキュービット

この核スピンはいずれも 1/2 の値をもつ(炭素原子が同位体^{13}Cを用いているのはこの理由からである)ので、上向きと下向きという 2 つの状態がある。この 2 つの状態は通常縮退しているが、磁場を印加すると縮退がとけて 2 準位状態になる。一般に 2 準位状態を制御する手法としてラビ振動という現象を用いることができる。

ラビ振動という現象は、2 準位間の共鳴を利用するもので、2 準位のエネルギー差に等しい電磁場を印加する(具体的には、この NMR 計算機では高周波を、後述のイオントラップ計算機ではレーザを用いる)と、量子状態がこの 2 つの準位の間を時間的に振動する現象である。電磁場の印加時間に対して正弦関数的に遷移し、状態の位相因子もそれに伴って変化することで、位相シフタ、制御ノットを実現するのに使用される。

NMR 計算機の場合、具体的にはこのキュービットである核スピンの制御を、適当な高周波パルスを試料に印加することで実現している。核スピン状態の読み出しは、試料の発生するマイクロ波をパルス印加に用いたコイルでピックアップして行われる。従って、計算結果は常に単一のキュービットではなく、全分子の平均値として得られる。これがバルク型の由来である。

位相シフトは、磁場中での原子の核スピンのエネルギー準位がゼーマン分裂を起こしているので、このゼーマン分裂に共鳴する高周波を一定時間試料に照射して、スピンの上向き下向きを入れ替えることで実現できる。更にキュービットの読み出し操作も、このスピン制御を応用して、キュービットを位相シフト操作により横向きに倒すことで実現できる。つまり、このスピンの回転に伴い放出される高周波信号を解析するのである。

この方式の利点は、現在分析器として広く用いられている NMR の装置を用いて量子計算が実行できるため、特殊な実験装置を付け加える必要がない点である。

具体例として、Chuang による図 3.6 NMR 計算機の Deutsch-Jozsa アルゴリズム・フローチャートを下に示す（[3]より引用）

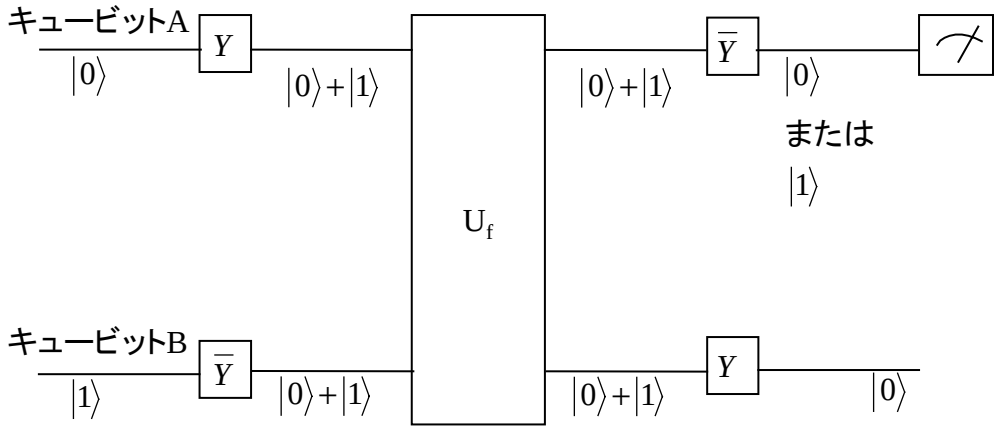


図 3.6 NMR 量子計算機用 Deutsch-Jozasa アルゴリズム

ここで、Y は位相シフタである。$\overline{Y}$ はその逆変換をあらわす。U_f はアルゴリズム依存の量子操作に対応する。

イオントラップ量子計算機[3,39]

イオントラップの技術を利用して直線状に個々のイオンを並べ、量子計算を行う方式である。キュービットは個々のイオンの電子状態である。つまり、各イオンで生じた電子状態の微細構造準位を利用するのである。従って、イオンの量子状態操作は、個々のイオンにねらいを定めたレーザービームによって行われる。この方式の利点は次の 2 点である。

1）微細構造準位を利用しているので緩和時間が長い点(時間スケールはエネルギーの逆数に比例する)。

2）後述するが、イオンの集団運動の励起状態(フォノン)を制御ノット操作の仲介役として用いるので、隣接していない遠く離れたキュービット間でも制御ノット操作が可能な点。

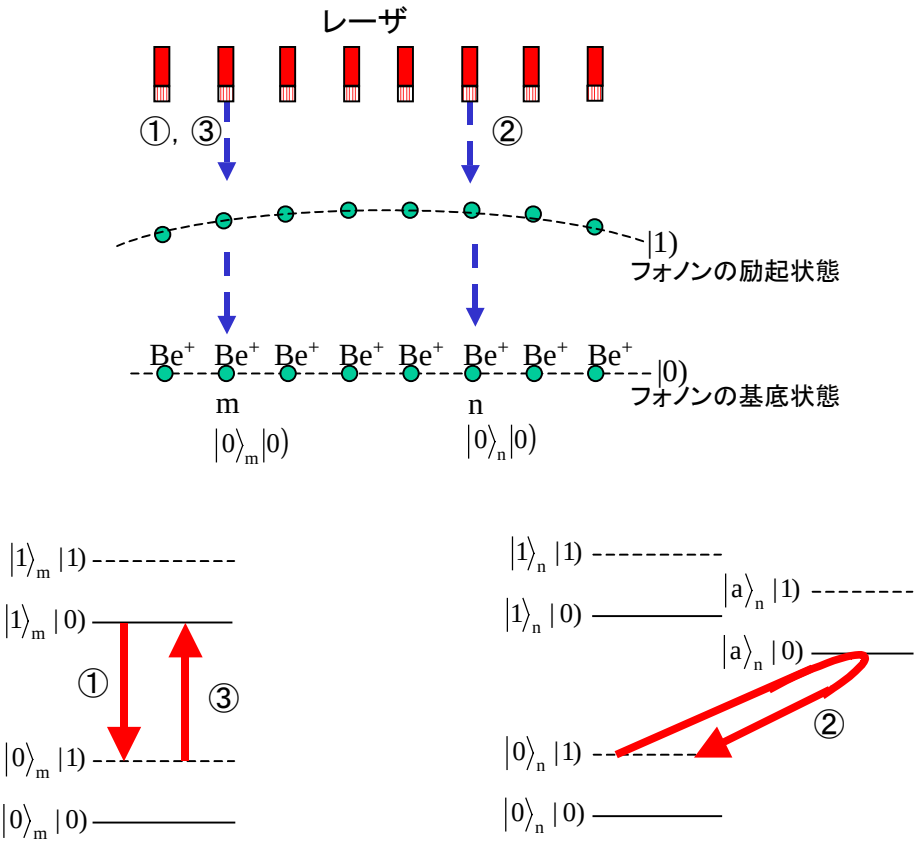


図 3.7 イオントラップ量子計算機

この量子計算機では N 個のイオンが直線状にトラップされている。個々のイオンには異なるレーザビームが照射される(図 3.7)。

各イオンは、その重心運動のフォノンの量子化準位が十分に分離できるほど冷却されているとする(フォノンの量子状態を丸括弧“ |) ”で表す)。このとき、キュービットは個々のイオンの微細構造準位のうち適当な 2 つの準位を用いる。ここで、m番目のイオンの基底状態を$|0\rangle_m$、励起状態を$|1\rangle_m$とすると、位相シフトは、この 2 準位間に相当するエネルギー差の波長をもつレーザを照射すれば実現できる。

制御ノットは、さらにフォノンと別の補助準位$|a\rangle_m$を用いて実現する。ここで、フォノンの重心運動の量子化準位の基底状態を$|0)$、励起状態$|1)$とする。

以下に、この方式の特徴をなす制御ノットの実現手順を図 3.7 に従い述べる。

①：m 番目のイオンにレーザを照射する。条件は、$|1\rangle_m|0)$と$|0\rangle_m|1)$のエネルギー差に相当しラビ振動を 4 半周期引き起こすだけの時間射する(π/2 パルス)こと。

従って、

$$|1\rangle_m|0) \longrightarrow i|0\rangle_m|1)$$

もしくは

$$|0\rangle_m|1) \longrightarrow i|1\rangle_m|0)$$

のようにのみ遷移が生じる。

②：n 番目のイオンにレーザを照射する。条件は、$|0\rangle_n|1)$と$|a\rangle_n|0)$のエネルギー差に相当しラビ振動を半周期引き起こすだけの時間照射(πパルス)すること。

従って、

$$|0\rangle_n|1) \longrightarrow -|0\rangle_n|1)$$

のようにのみ遷移が生じる。補助状態があらわれないことに注目。

③：m 番目のイオンにレーザを照射する。条件は、$|1\rangle_m|0)$ と $|0\rangle_m|1)$ のエネルギー差に相当し、ラビ振動を 4 半周期引き起こすだけの時間照照射する(π/2 パルス)こと。

従って、

$$|1\rangle_m|0) \longrightarrow i|0\rangle_m|1)$$

もしくは

$$|0\rangle_m|1) \longrightarrow i|1\rangle_m|0)$$

のようにのみ遷移が生じる。

このプロセスを m 番目と n 番目のイオンの状態のみに着目して整理すると(フォノンの状態はもとに戻っている)、表 3.2-a のようにm番目とn番目両方のイオンが励起状態にあるときのみ位相が反転していることがわかる。ここで、n 番目イオンの状態表現を、

$$\begin{pmatrix}|0\rangle\\|1\rangle\end{pmatrix} \longrightarrow \begin{pmatrix}|+\rangle\\|-\rangle\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}|0\rangle+|1\rangle\\|0\rangle-|1\rangle\end{pmatrix}$$

のように表現しなおすと表 3.2-b のようになり、制御ノットを実現していることがわかる。

表 3.2 イオントラップ制御ノット

a)"0，1"表現

入力 $\|m\rangle\|n\rangle$	出力 $\|m'\rangle\|n'\rangle$
$\|0\rangle_m\|0\rangle_n$	$\|0\rangle_m\|0\rangle_n$
$\|0\rangle_m\|1\rangle_n$	$\|0\rangle_m\|1\rangle_n$
$\|1\rangle_m\|0\rangle_n$	$\|0\rangle_m\|1\rangle_n$
$\|1\rangle_m\|1\rangle_n$	$-\|1\rangle_m\|1\rangle_n$

b)"+，-"表現

入力 $\|m\rangle\|n\rangle$	出力 $\|m'\rangle\|n'\rangle$
$\|0\rangle_m\|+\rangle_n$	$\|0\rangle_m\|+\rangle_n$
$\|0\rangle_m\|-\rangle_n$	$\|0\rangle_m\|-\rangle_n$
$\|1\rangle_m\|+\rangle_n$	$\|0\rangle_m\|-\rangle_n$
$\|1\rangle_m\|-\rangle_n$	$\|1\rangle_m\|+\rangle_n$

その他の量子計算機[3]

半導体核スピン量子計算機

この方式はシリコンウェファーの中に不純物としてドープされた ^{31}P イオンの核スピン(I=1/2)をキュービットとして用いる。周囲のシリコン原子の核スピンが I=0 なので、核スピン同士で生じる相互作用がなく、大きな緩和時間が見込めることが利点である。欠点としては、シリコンウェファー中の不純物の完全な除去や単一イオンをドーピングする技術などの課題を解決していかなければならない点である。

量子ドット量子計算機

エネルギーギャップの異なる半導体を積層したときに生じる量子井戸中の電子準位をキュービットとして用いる方式である。欠点は緩和時間が短いことである。利点は、原理的にシンプルなため制御ノットの構成が理解しやすい点である。

まとめ

これまでに述べてきた各量子計算機の利点・欠点をまとめる。

表 3.3 量子計算機の各方式の利点・欠点比較表

	利点	欠点
線形光学素子 量子計算機	任意の量子計算アルゴリズムを実現可能	回路規模がキュービットの数の増加につれて膨大となる
NMR 量子計算機	既存の NMR 分析器を用いることができる	計算結果が全分子の平均値としてしかえられない
イオントラップ 量子計算機	緩和時間が長い 隣接キュービット以外でも 制御ノットが可能	拡張性に難あり
半導体核スピン 量子計算機	緩和時間が長い	未解決の課題技術多し
量子ドット量子計算機	原理がシンプル	緩和時間が短い

4. 量子計算機研究の理論の現状と将来の方向

4.1 概要

量子計算が古典計算より完全にすぐれているかどうかはまだわかっていない。現在量子計算に関してわかっていることは、周期性がある問題に対して古典計算機より効率の良いアルゴリズムを構成できるということである。それでは、量子計算機が有効となる問題とは、いったいどのような問題であるのか。現在までに見つかっている量子アルゴリズムを、理論研究の歴史にそって簡単にふりかえる。

初期に考えられたアルゴリズムは、かなり特殊な（意図的な）問題であったが量子計算の可能性を示すに十分であった。1992 年に Deutch と Jozsa が、ある関数が均一か等分かどちらの性質を持つかを判定する問題を解こうとするとき、量子計算が有効に働くことを発見した。これは Deutch-Jozsa のアルゴリズムと言われる[15]。

しかしその後、実際に量子計算が脚光を浴びたのは、1994 年に Shor によって素因数問題と離散対数問題に対する多項式時間アルゴリズムが発見されてからである[17]。これらの問題は、古典計算機では準指数時間アルゴリズムしか得られておらず、公開鍵暗号の安全性の根拠として使用されている問題である。計算量クラスの観点から言うと、この２つの問題は、NP 完全でもなく P でもないクラスを NPI(NP Intermediate)と呼ぶならば、この NPI クラスに属する問題である。古典計算機では、多項式時間アルゴリズムが見つかっていない問題であったため、Shor による量子アルゴリズムの発見の意義は非常に大きい。

Shor による素因数分解問題、離散対数問題に対する量子アルゴリズムの発見後、当然 NPI のその他の問題であるグラフ同型性判定問題（GI）や、充足可能性問題（SAT）などの NP 完全問題に対して、量子計算多項式時間アルゴリズムの研究がなされた[23,30]。そんな中、1996 年 Grover が充足可能性問題の量子アルゴリズムを研究中、データベースの高速検索アルゴリズムの発見をした[18]。但し、これに要する計算量は、多項式時間ではなく、要素数の平方根オーダの計算量にまで高速化できるというものであった。このアルゴリズムは Shor のアルゴリズムほどは高速性がないが、ランダムなデータベースを対象としているため、汎用性があ

るという点で意味がある。Shor のアルゴリズムは、関数に周期性がある問題に対するアルゴリズムであったからである。

現在、その他の NPI の問題や NP 完全問題などの問題に対しては、多項式時間アルゴリズムは発見されていないが、NP 完全問題に対してはどうやら量子計算では解けないのではないかという否定的な見解を持っている研究者が多い。

4.2 量子計算アルゴリズム

この章では、量子計算機が古典計算機より高速に解くことが可能な主な問題を以下にまとめる。

Deutsch の問題[12]

$f:\{0,1\}\to\{0,1\}$ なるある関数 $f(x)$ が、$f(0)=f(1)$ かそうでないかを判定するアルゴリズム。即ち均一か等分かを判定する。

Deutsch-Jozsa の問題[15]

外部から与えられる 0、1 のビット列が、均一（すべて 0 かすべて 1）か、等分（0 と 1 が同数含まれている）かを判定するアルゴリズム。

Simon の問題[16]

次のような関数 $f(x)$ を考える。$f:\{0,1\}^n\to\{0,1\}^m$ で $n\le m$。また、ある 0 でない $\xi\in\{0,1\}^n$ が存在して、すべての $x\in\{0,1\}^n$ に対して、$f(x)=f(x+\xi)$ なる周期性を持つとする。このとき 0 でない周期 ξ を探すアルゴリズム。

素因数分解問題[17]

2 つの大きな素数の積からなる合成数 n の素因数分解を行うアルゴリズム。計算量は $\log n$ に関する多項式時間で可能となる。ちなみに古典計算機では $O(\exp(\log n\log\log n)^{1/2})$ の計算量を要する。すなわち準指数時間要する。

離散対数問題[17]

素数 p、$F_p^{\times}$ の生成元 g、$y(=g^x \bmod p)$ が与えられた時、離散対数 x を求めるアルゴリズム。計算量は $\log p$ に関する多項式時間である。古典計算機では、$O(\exp(\log p\log\log p)^{1/2})$ の計算量を要する。すなわち準指数時間要する。

Grover のデータベース検索問題[18]

N 個のランダムに並んだデータベースから、ある条件を満たす要素を高速に検索するアルゴリズム。この場合、計算量のオーダは$O(N^{1/2})$となる。一方、古典計算機の場合、検索必要ステップ数は約$N/2$であり、すなわち計算量のオーダでいうと$O(N)$となるため、古典計算機より高速な検索が可能となる。

但し、古典計算機での通常のデータベース検索問題を考える場合、データベースはインデックス順に並べられているため、ランダムとは言えず、バイナリソートを適用することで$O(\log N)$の計算量のみで検索可能である。このため、ランダムなデータベースという点が重要である。

最小値検索問題[19]

N 個の要素から最小値を見つけるアルゴリズム。Grover のアルゴリズムを単純にサブルーチンとして使用することによって、最小値検索に必要な計算量を$O(N^{1/2})$のオーダに落すことができる。古典計算機だと、最小値検索に必要な計算量のオーダは一般に$O(N)$必要となる。Grover のデータベース検索問題と同様、古典計算機より高速検索が可能となる。

拡張した Simon の問題[22]

次のような関数$f(x)$を考える。$f:\{0,1\}^n \to \{0,1\}^m$で$n \le m$。また、ある$\xi \in S \subseteq \{0,1\}^n$が存在して、すべての$x \in \{0,1\}^n$に対して、$f(x)=f(x+\xi)$なる周期性を持つ。このとき周期$\xi$の属する集合の生成元を探すアルゴリズム。Simon の問題を Brassard、Hoyer が拡張した。

以上量子計算が有効な主な問題を列挙したが、それらを大きく分類すると下記の３つに分けられる。

(1)関数にある周期性などがあり、抽出したい情報を確率的に取り出す
Simon の問題、素因数分解問題、離散対数問題、
拡張した Simon の問題

(2)汎用的な関数が与えられたとき、ある条件を満たす変数を高速に検索する

Grover のデータベース検索問題、最小値検索問題

(3)その他

Deutch の問題、Deutsch-Jozsa の問題

それではここでは、量子計算の有効性を示す初期に発見された Deutsch-Jozsa のアルゴリズムと Grover のデータベース検索問題について詳しく説明する。

Deutsch-Jozsa のアルゴリズムの説明[6,8,15]

問題

いま $a = 0,1,\cdots,2N-1$ の $2N$ 個の数に対して、0 と 1 の値を持つ関数 $f(a)$ があるとする。Deutch-Jozsa の問題とは、次の 2 つのどちらが正しいかを判定する問題である。

(1) $f(a)$ の値として、N 個の 0 と N 個の 1 があることはない。

(2) $f(a)$ の値として、$2N$ 個の 0 あるいは $2N$ 個の 1 があることはない。

前述の問題とは少し定義が異なるが、上記の問題もよく良く引用される。

アルゴリズム

Step 1　量子離散フーリエ変換 QFT_{2N} を基底状態 $|0\rangle|0\rangle$ に作用させて、重ね合わせ状態 $|\psi_{init}\rangle$ を作り出す

ここで一般に離散フーリエ変換は、$QFT_q|a\rangle = \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle$ で与えられる。

$$QFT_{2N}:\ |0\rangle|0\rangle \ \rightarrow\ \ |\psi_{init}\rangle = \frac{1}{\sqrt{2N}}\sum_{a=0}^{2N-1}|a\rangle|0\rangle$$

Step 2　$f(a)$ の値を計算して、第 2 レジスタに格納する

（ここで、$f(a)$ の値を計算するユニタリ変換 U_f を作用させる）

$$U_f|\psi_{init}\rangle = \frac{1}{\sqrt{2N}}\sum_{a=0}^{2N-1}|a\rangle|f(a)\rangle$$

Step 3　第 2 レジスタにパウリ演算子 σ_z を作用させて、$f(a)$ を-1 の指数にのせる

$$(I\otimes\sigma_z)U_f|\psi_{init}\rangle = \frac{1}{\sqrt{2N}}\sum_{a=0}^{2N-1}|a\rangle\sigma_z|f(a)\rangle = \frac{1}{\sqrt{2N}}\sum_{a=0}^{2N-1}|a\rangle(-1)^{f(a)}|f(a)\rangle$$

Step4　再度ユニタリ変換 U_f を作用させて、状態を $|\psi_{final}\rangle$ にする

（ユニタリ変換 U_f を 2 度作用させることで第 2 レジスタを 0 に戻す）

$$U_f(I\otimes\sigma_z)U_f\left|\psi_{init}\right\rangle=\frac{1}{\sqrt{2N}}\sum_{a=0}^{2N-1}(-1)^{f(a)}U_f\left|a\right\rangle\left|f(a)\right\rangle$$

$$=\frac{1}{\sqrt{2N}}\sum_{a=0}^{2N-1}(-1)^{f(a)}\left|a\right\rangle\left|f(a)\oplus f(a)\right\rangle$$

$$=\frac{1}{\sqrt{2N}}\sum_{a=0}^{2N-1}(-1)^{f(a)}\left|a\right\rangle\left|0\right\rangle=\left|\psi_{final}\right\rangle$$

Step 5　物理量を観測する

このとき、$\left|\psi_{init}\right\rangle$の状態を観測する確率 Pr は下記で与えられる。

$$\Pr=\left|\left\langle\psi_{init}\left|\psi_{final}\right\rangle\right\rangle\right|^2=\left|\frac{1}{2N}\sum_{a=0}^{2N-1}(-1)^{f(a)}\right|^2$$

ここで、常に条件の(1), (2)の少なくとも一方は真であることに注意する。

$\Pr=\left|\frac{1}{2N}\sum_{a=0}^{2N-1}(-1)^{f(a)}\right|^2=1$ のとき、即ち$\left|\psi_{init}\right\rangle$の状態を観測するとき、(2)が偽、(1)が真といえる

$\Pr=\left|\frac{1}{2N}\sum_{a=0}^{2N-1}(-1)^{f(a)}\right|^2=0$ のとき、即ち$\left|\psi_{init}\right\rangle$の状態を観測しないとき、(1)が偽、(2)が真といえる

以上が Deutsch-Jozsa のアルゴリズムである。

Deutsch-Jozsa の問題を古典計算機で判定しようとすると、$f(a)$の値を順番に$f(0), f(1), f(2),\cdots$と調べていき、N 個みて初めて条件(1),(2)のどちらを満たしているか判定できる。即ち古典計算機で判定に必要な計算量のオーダーは$O(N)$である。

それに対して、いま説明した量子計算アルゴリズムでは、すべての演算、操作は$\log N$ の多項式時間でできるため、古典計算機のアルゴリズムより高速判定が可能となる。

Grover のデータベース検索問題の説明[6,8,18]

問題

いま $N=2^n$ 個の変数があって各々 $x_1, x_2, x_3, \cdots, x_N$ とラベルされている。この変数の中で、ただ 1 つ $f(x)=1$ なる条件を満たす変数 x_μ があり、それ以外の変数に対しては、 $f(x)=0$ が成立する。このとき変数 x_μ を検索する問題。

アルゴリズム

Step 1　基底状態 $\left|00\cdots0\right\rangle$ を N 個の重ね合せ状態にする

$$\left|00\cdots0\right\rangle \rightarrow \quad \left|\psi_{init}\right\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\left|x\right\rangle$$

Step 2　次の操作を繰り返す

なお繰り返し回数は、検索したい状態の確率振幅が 1/2 以上になるまで。

(1)検索したい状態の位相を変化させる

・ $f(x)=1$ のとき、位相を π 変化させる

すなわち　$\left|x\right\rangle \rightarrow \quad e^{i\pi}\left|x\right\rangle = -\left|x\right\rangle$

・ $f(x)=0$ のとき、位相は変化させずそのまま

すなわち　$\left|x\right\rangle \rightarrow \quad e^{i0}\left|x\right\rangle = \left|x\right\rangle$

物理的解釈ではこの操作は、検索したい状態の確率振幅を反転させることに相当する。

(2)拡散変換(Diffusion Transform)を作用させる

この変換は検索したい状態の確率振幅を増幅させるために行う。物理的解釈では、各々の確率振幅をすべての確率振幅の平均値について折り返すという操作に相当する。行列表現で D とすると D の要素は下記の通りに書ける。

$$D_{ij} = -\delta_{ij} + \frac{2}{N}$$

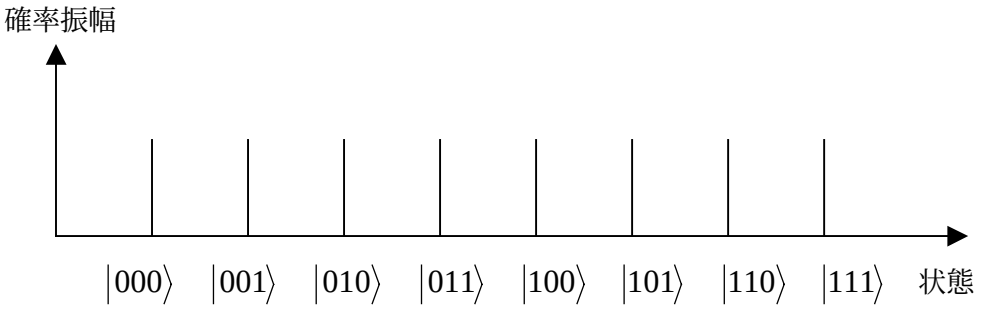
また、この行列 D は回転行列 R とウォルシュ・アダマール変換（Walsh-Hadamard 変換）行列 W によって、$D = WRW$ と記述できる。

Step 3　Step2 の繰り返し処理後（Step2 を $O(\sqrt{N})$ 回繰り返して）、物理的に観測する。取り出したい状態の確率振幅が増幅されているため、1/2 以上の確率で取り出したい状態が観測できることになる。検索終了。

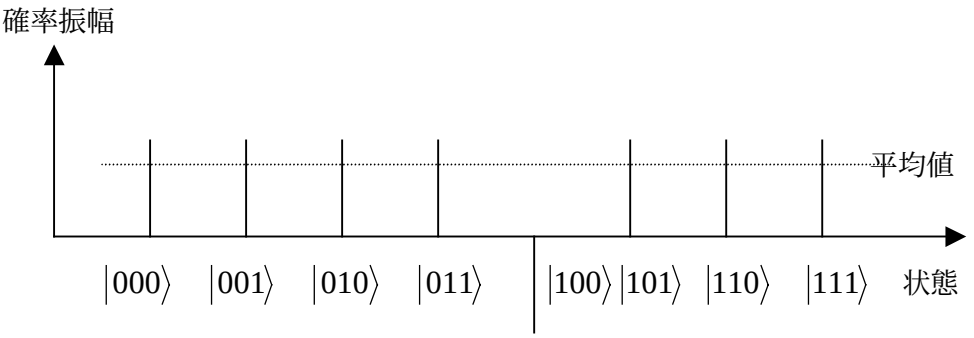
Grover のデータベース検索問題の簡単な例

$n=3$、$N=2^n=2^3=8$で、検索したい状態がx_4のとき。即ち$f(x_4)=1$のとき。

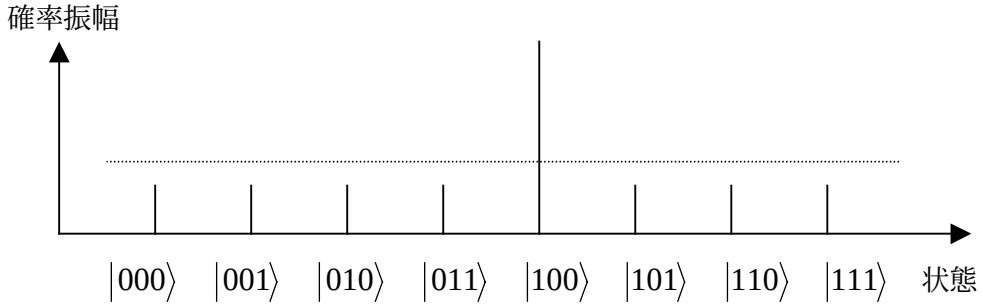
重ね合わせ状態（Step1 に対応）



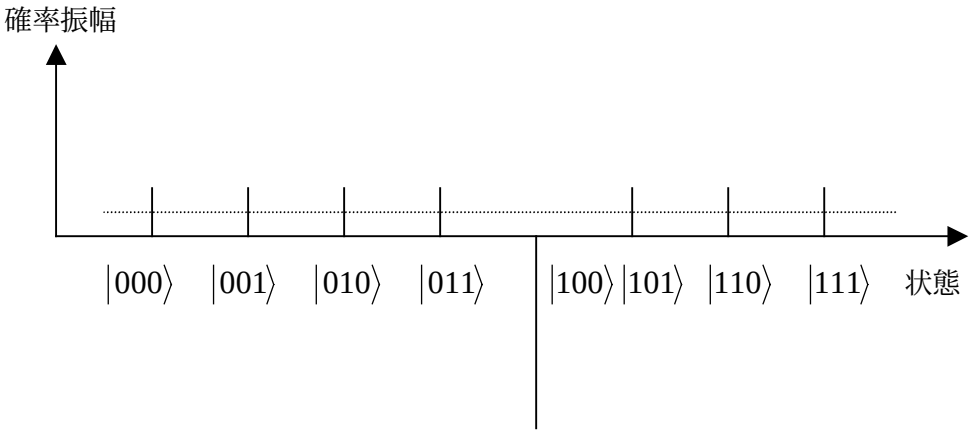
取り出したい状態の確率振幅を反転させる（1 回目の Step2(1)の操作に対応）



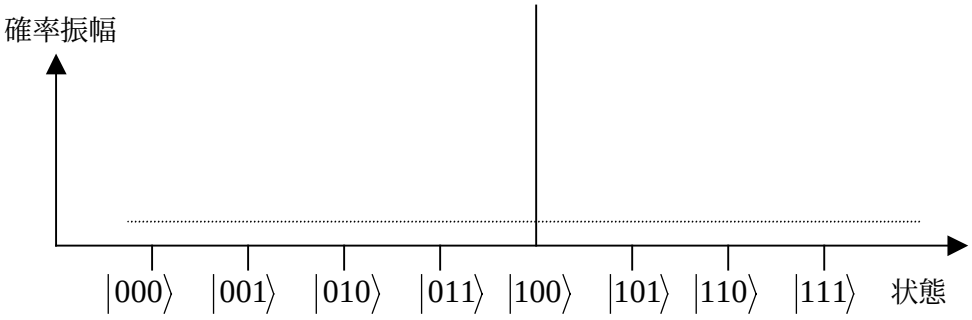
平均値に対して折り返し操作を行う（1 回目の Step2(2)の操作に対応）



取り出したい状態の確率振幅を反転させる（2 回目の Step2(1)の操作に対応）



平均値に対して折り返し操作を行う（2 回目の Step2(2)の操作に対応）



上記のように演算処理を続けていくことにより、検索したい状態の確率振幅のみを増幅させていく。

基本的に Grover のデータベース検索アルゴリズムは、上記操作からわかるように取り出したい状態の確率振幅は大きくなるが、一般にはその他の確率振幅は小さいが値として残る。すなわち、最後に観測して検索したい状態を取り出す操作を行う際に、別の状態を取り出してしまう確率は非常に小さく落せるが、一般に 0 にはならない。

繰り返し処理を $O(\sqrt{N})$ 回繰り返すと、取り出したい状態の確率振幅が増幅され 1/2 以上となる。計算量のオーダは $O(\sqrt{N})$ となる。

4.3 暗号解読に関係するアルゴリズム

ここでは、暗号解読に関係する量子アルゴリズムとして、素因数分解問題、離散対数問題、及び楕円曲線上の離散対数問題に対する多項式時間アルゴリズムを説明する。

素因数分解問題に対する量子アルゴリズムの説明[17]

問題

整数 $n = pq$（p、q は素数）を素因数分解する

アプローチ

次の２つのステップで素因数分解を行う。量子アルゴリズムは(1)の部分のみ。

(1)量子計算を用いた高速な 周期（period）の計算（Shor のアルゴリズム）

次の関数の周期 r を計算する。$f_{x,n}(a) = x^a \bmod n$。

(2)周期から因数を古典的な高速な手法で計算（Euclid アルゴリズム）

n の因数（i.e. p, q)を、$\gcd(x^{r/2}-1, n)$ と $\gcd(x^{r/2}+1, n)$ を計算して得る

数論的説明

(1)素因数因数分解したい整数 n が与えられたとき、次の関数 $f_{x,n}(a)$ を構成する

$f_{x,n}(a) = x^a \bmod n$

但し、 x は n と互いに素でランダムに選ばれた整数とする。

(2) 周期 r（すなわち $x^r \equiv 1 \bmod n$ なる r）を見つける

(3) もし 周期 r が偶数の場合、$(x^{r/2}-1)(x^{r/2}+1) \equiv 0 \bmod n$ となる。

この時、もし $x^{r/2} \equiv \pm 1 \bmod n$ でなければ、少なくとも上式の左辺の少なくとも一方は、n の非自明な因数を持たなくてはいけない。

(4)よって、$\gcd(x^{r/2}-1, n)$ and $\gcd(x^{r/2}+1, n)$ を計算することによって n の因数を見つけることができる。

アプローチの(1)のみ量子計算であるため、この部分の量子アルゴリズムを説明する。

量子計算を用いた高速な周期の計算（Shor のアルゴリズム）

周期rを計算する。 即ち $f_{x,n}(a) = x^a \bmod n$ として、 $f(a+r) = f(a)$ なる周期rを計算する。xとnが与えられたとき、上記のような周期rを見つけるため 次のアルゴリズムを実行する。

アルゴリズム

Step1. $2n^2 \le Q < 4n^2$ を満たすスムーズ（smooth）なQを見つける。

スムーズなQを選んだ理由は、あとの step で、多項式時間で構成される量子離散フーリエ変換QFT_Qを使用するため。

Step2 量子離散フーリエ変換QFT_Qを基底状態$|00\rangle$に作用させて、重ね合わせ状態$|\psi_{init}\rangle$を作り出す

ここで離散フーリエ変換は$QFT_Q|a\rangle = \frac{1}{\sqrt{Q}}\sum_{c=0}^{Q-1}\exp(2\pi iac/Q)|c\rangle$で与えられる。

$$QFT_Q:\ |00\rangle \ \rightarrow \quad |\psi_{init}\rangle = \frac{1}{\sqrt{Q}}\sum_{a=0}^{Q-1}|a\rangle|0\rangle$$

Step3 $x^a \bmod n$の値を計算して、第 2 レジスタに格納する。

（ここで、$f(x) = x^a \bmod n$と考えればよく、ユニタリ変換U_fを作用させる）

$$U_f|\psi_{init}\rangle = \frac{1}{\sqrt{Q}}\sum_{a=0}^{Q-1}|a\rangle|x^a(\bmod n)\rangle$$

Step4 周期rを取り出すために離散フーリエ変換QFT_Qを作用させる。

$$QFT_Q \cdot U_f|\psi_{init}\rangle == \frac{1}{Q}\sum_{c=0}^{Q-1}\sum_{a=0}^{Q-1}\exp(2\pi iac/Q)|c\rangle|x^a(\bmod n)\rangle$$

Step5 第 1 レジスタの物理量 c を観測する。

このとき、 $\left|c, x^k \pmod n\right\rangle$ の状態を観測する確率 Pr は下記で与えられる。

$$\Pr = \left| \frac{1}{Q} \sum_{x^a \equiv x^k \bmod n} \exp(2\pi i a c / Q) \right|^2$$

この確率は、周期 r が下記の条件のときに大きなピークを持つ。すなわち(1)の条件を満たすか、ほぼその関係を満たす状態しか観測にかからないといえる。

(1) $Q \mid A = \lfloor (Q-k)/r \rfloor$ なら、r_i が $r_i \cdot c = k \cdot Q$ を満たすとき

(2) (1)でないときは、r_i が $r_i \cdot c = k \cdot Q$ を満たす値の近傍のとき

Step6 観測した値 c から周期 r を得る

このような観測（c を得る）を $\log N$ 回の繰り返すと、周期 r が得られる（$r_i \cdot c \cong k \cdot Q$ なる関係を考慮して求める）

以上が Shor の周期 r を多項式時間で求める量子アルゴリズムである。周期 r を求めると古典計算機上の Euclid アルゴリズムから、多項式時間で n の因数 p, q が確率的に求めることができる。

古典計算機で素因数分解問題を解く場合、計算量が $O(\exp(\log n \log\log n)^{1/2})$ の準指数時間アルゴリズムまでしか知られておらず、量子計算アルゴリズムの方が高速処理できることになる。

離散対数問題に対する量子アルゴリズムの説明[17]

問題

素数 p 、 $F_p^{\times}$ の生成元 g 、 $y(=g^x \bmod p)$ が与えられた時、離散対数 x を求める

但し、これから説明するアルゴリズムは、 $p-1$ がスムーズ（smooth）の時の場合を説明する。この場合を easy case という。

アルゴリズム

Step1 量子離散フーリエ変換 QFT_{p-1} を基底状態 $|0\rangle|0\rangle$ に作用させて、重ね合わせ状態 $|\psi_{init}\rangle$ を作る

ここで、離散フーリエ変換は $QFT_{p-1}|a\rangle = \frac{1}{\sqrt{p-1}}\sum_{a=0}^{p-2}\exp(2\pi iac/(p-1))|c\rangle$,

で与えられる。

$$QFT_{p-1}\otimes QFT_{p-1}:\ |0\rangle|0\rangle\ \rightarrow\ |\psi_{init}\rangle = \frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a\rangle|b\rangle$$

Step2 $g^a y^{-b} \bmod p$ の値を計算して、第 3 レジスタに格納する

（ $f(x) = g^a y^{-b} \bmod p$ と考えればよく、ユニタリ変換 U_f を作用させる）

$$U_f:|\psi_{init}\rangle\ \rightarrow\ \frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a\rangle|b\rangle|g^a y^{-b} \bmod p\rangle$$

Step3 量子離散フーリエ変換 QFT_{p-1} を第 1 レジスタ、第 2 レジスタに作用させる

その結果下記の状態となる

$$QFT_{p-1}\otimes QFT_{p-1}\otimes I:$$

$$\frac{1}{(p-1)^2}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}\sum_{c=0}^{p-2}\sum_{d=0}^{p-2}\exp(\frac{2\pi i}{p-1}(ac+bd)|c\rangle|d\rangle|g^a y^{-b} \bmod p\rangle$$

Step4 第 1 レジスタの物理量 c、第 2 レジスタの物理量 d を観測する

このとき、$\left|c,d,y \equiv g^k \bmod p\right\rangle$ の状態を観測する確率 Pr は下記で与えられる。

$$\Pr = \left| \frac{1}{(p-1)^2} \sum_{\substack{a,b \\ a-xb \equiv k \bmod(p-1)}} \exp(\frac{2\pi i}{p-1}(ac+bd)) \right|^2$$

$$= \left| \frac{1}{(p-1)^2} \sum_{b=0}^{p-2} \exp(\frac{2\pi i}{p-1}(kc+b(d+xc))) \right|^2$$

Step5 観測すると、 $\left|c\right\rangle\left|-xc(=d)\right\rangle\left|y\right\rangle$ という状態が確率 $\frac{1}{(p-1)^2}$ で得られる

$d+xc \neq 0 \bmod(p-1)$ のとき、確率 Pr は 0、即ち観測されない

$d+xc \equiv 0 \bmod(p-1)$ のとき、確率 Pr は 0 でない値となり観測される

Step6 c と $p-1$ が互いに素のとき、x は観測値 c と d より、それらの逆元演算と乗算で求められる。

すなわち x、c、d は、$d \equiv -xc \bmod(p-1)$ なる関係式を満たしているため、

$x \equiv (-d)\cdot c^{-1} \bmod(p-1)$ の計算をすることで離散対数 x が求まる。

なお Step6 では、観測値 c が $p-1$ と互いに素のとき逆元 $c^{-1} \bmod(p-1)$ が存在して、離散対数 x が求まる。観測値 c が $p-1$ と互いに素となるような確率は、Euler 関数 Φ 及びその性質から次のように評価できる。

$$\Phi(p-1)/(p-1) \cong e^{-\gamma}/(\log\log p) > 1/\log p$$

すなわち、$\log p$ 回操作を繰り返すと、c が $p-1$ と互いに素となり x が求まる。

但し上記のアルゴリズムは easy case の説明である。この時、古典計算機上でも多項式アルゴリズムが存在する(Pohlig-Hellman 法)。easy case ではなく、一般の場合も Shor により同様にして多項式時間アルゴリズムが示されている[17]。

古典計算機では、離散対数問題を解くアルゴリズムの計算量のオーダとしては、$O(\exp(\log p \log\log p)^{1/2})$ の準指数時間要し、量子アルゴリズムの方が高速である。

Boneh-Lipton の論文[27]より、容易に一般の群の離散対数問題にも量子アルゴリズムは適用可能である。すなわち例えば楕円曲線暗号に関しても多項式時間で解読が可能であることが言える[27]。次に示す。

楕円曲線上の離散対数問題に対する量子アルゴリズムの説明[27,29]

問題

E を下記で定義される楕円曲線とする。

$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ （$a_1, a_2, a_3, a_4, a_6 \in F_q$）

F_q（但し、$q = p^m$、p は素数）は有限体である。またここで、$P \in E(F_q)$ を大きな素数 n を位数にもつ base point として、R を $R = rP$ なる楕円曲線上の r 倍点とする。このとき、楕円曲線上の離散対数問題とは、R と P が与えられたとき、$R = rP$ なる r を求める問題である。

アルゴリズム

Step1 $n \le Q < 2n$ を満たすスムーズ（smooth）な Q を見つける

但し、n は位数で $n = \#< P >$ である。また、スムーズな Q を選んだ理由は、あとで多項式時間で構成される量子離散フーリエ変換 QFT_Q を使用するため。

Step2 第 1 レジスタと第 2 レジスタのそれぞれに重ね合わせ状態 $|\psi_{init}\rangle$ を作り出す

$$|\psi_{init}\rangle = \frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}|a\rangle|b\rangle$$

但し P は basepoint。

Step3 $aP - bR$ の値を計算して、第 3 レジスタに格納する

（$f(x) = aP - bR$ と考えればよく、ユニタリ変換 U_f を作用させる）

$$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}|a\rangle|b\rangle|aP - bR\rangle \qquad \text{但し } R = rP$$

Step4 量子離散フーリエ変換 QFT_Q を第 1 レジスタ、第 2 レジスタに作用させる

ここで、離散フーリエ変換は

$QFT_Q|a\rangle = \frac{1}{\sqrt{Q}}\sum_{a=0}^{n-1}\exp(2\pi iac/Q)|c\rangle$ で与えられる。

$$QFT_Q \otimes QFT_Q \otimes I : \frac{1}{qn}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}\sum_{c=0}^{Q-1}\sum_{d=0}^{Q-1}\exp(\frac{2\pi i}{Q}(ac+bd)|c\rangle|d\rangle|aP-bR\rangle$$

Step4 第 1 レジスタの物理量 c、第 2 レジスタの物理量 d を観測する

このとき、$|c,d,K=kP\rangle$ の状態を観測する確率 Pr は下記で与えられる。

$$\Pr = \left|\frac{1}{nQ}\sum_{\substack{a,b \\ a-rb\equiv k}}\exp(\frac{2\pi i}{Q}(ac+bd))\right|^2$$

以下 Shor の離散対数問題アルゴリズムの議論と同様にこの値を評価し、$R=rP$ なる r を多項式時間で得ることができる。

また暗号解読に関連して Grover のデータベース検索アルゴリズムを秘密鍵暗号に適用することを考えると、全数探索の平方根の計算量で解読できる。すなわち例えば鍵が 64bit のブロック暗号の場合は、2^{32} の探索で解読できる。128bit ブロック暗号の場合は、2^{64} の探索で解読できることになる。

4.4 最近の研究動向と将来の方向

最近量子計算で解こうと試みられている問題として NP 完全問題、NPI の問題、NP 困難な問題がある。ここではその他のトピックも含めて簡単に最近の量子計算の研究動向を紹介する。

NP 完全問題へのアプローチ

NP 完全の定義は、NP に属する問題でかつ NP の全ての問題がこれに多項式時間還元される問題のクラスである。すなわち NP に属する問題の中で一番難しい問題である。そして定義より、NP 完全に属する問題がどれか 1 つ解ければ、NP に属する問題がすべて解けることになる。ここでは NP 完全問題の最も代表的な充足可能性問題(SAT)を取り上げる。充足可能性問題とは次のような問題である。

充足可能性問題

任意のブール式が充足可能か否かを決定する問題である。
ここで、ブール式とは $\{0,1\}$ を値とする変数 $x_1, x_2, \cdots$ と論理演算子 $\wedge$（論理積）、$\vee$（論理和）、$\neg$（論理否定）と括弧から構成される式である。充足可能とは、式の値を 1 とするような変数への割り当てが存在することをいう。

量子計算で充足可能性問題を解こうとする試み[30]は当然行われているが、現在では、計算量理論研究者は量子計算機を使っても多項式時間で解ける問題のクラスは NP 完全には届かないと予想している。

NP 完全を扱う場合、Grover のデータベース検索アルゴリズムが 1 つの道具と考えられる。このアルゴリズムは前述のように、ランダムに並んでいる要素数 $N = 2^n$ のデータベース検索において、計算量 $O(\sqrt{N})$ が最適だと示されている。そのため NP 完全問題を多項式時間で解こうと考える場合、直接充足可能性問題のような周期性のない問題を扱おうと試みるのではなく、まず NP 完全問題で周期性や構造のあるものを見つけ、次にそれを量子計算で解けないかと考えた方がよいという考えもある。

NPI(NP Intermediate Problem)へのアプローチ

計算量理論研究者はさまざまなトライアルの結果、現在では量子計算機を使っても解ける問題のクラスは NP 完全には届かないという印象を持っている。そのため、素因数分解問題や離散対数問題が属するクラス NPI の他の問題に注目して、多項式時間アルゴリズムが見つけられないかと研究の方向を変えている。
これらの問題として、主に次の２つが考えられた。

NPI で量子計算アルゴリズムが研究されている主な問題

(1)グラフの同型性判定問題 (GI: Graph isomorphism problem)

(2)束内最短ベクトル探索問題 (SVLP: Shortest vector in lattice problem)

但し、実は(2)の束内最短ベクトル探索問題が 1998 年に Ajtai によって NP 困難な問題であることが証明された[25]。このためこの問題はかなり難しいことが分かった。それゆえ代表的な NPI の問題はグラフ同型性判定問題となる。この問題はアメリカで活発に研究されている[23]。

なおここで簡単にグラフの同型性判定問題の定義を述べる。

<u>グラフの同型性判定問題</u>

任意のグラフ $G_1 = (V_1, E_1)$、 $G_2 = (V_2, E_2)$ がに対して

$[u, v] \in E_1 \quad \Leftrightarrow \quad (f(u), f(v)) \in E_2$

となるような 1 対 1 関数 $f : V_1 \to V_2$ が存在するか否かを決定する問題である。

グラフ同型性判定問題は、P と NP の間に分類の線を引こうとする場合、それに反する重要な問題である。この問題は明らかに NP に属するが、NP 完全であるかどうかも知られていない。また P や co-NP、BPP に属するかどうかも知られていない問題である。

NP 困難な問題へのアプローチ

量子計算による NP 困難の問題の研究例は、束内最短ベクトル探索問題である。このきっかけは、素因数分解問題や離散対数問題に対する量子アルゴリズム発見後、計算量理論的に NPI のグラフ同型性判定問題、束内最短ベクトル探索問題に注目が集まり、前述のように後者が最近になって NP 困難であることが証明されたことにある。束内最短ベクトル探索問題が NPI でなく、NP 困難であると判明してもこの問題を研究することは次の 2 点で興味深い。

(1)N 次元の束内最短ベクトル探索問題は、Ajtai-Dwork 暗号[26]のベースとなっている

(2)N 次元の束内最短ベクトル探索問題は average case で問題の難しさが証明されている唯一の問題である

なお、例えば素因数分解問題や離散対数問題の場合は worst case で難しいということになり、average case で難しいと証明されているのはこの問題だけである。

また量子計算による束内最短ベクトル探索問題の研究に関しては、古典計算機上でも考えるように、近似解を量子アルゴリズムで見つけるという方向が考えられている。今まで量子計算による近似解を求めるアルゴリズムはなく、新しい研究の方向と考えられる。

束内最短ベクトル探索問題の定義は次の通り。

束内最短ベクトル探索問題[24]

束内最短ベクトル探索問題とは n 次元束 L 内の 0 でない最短ベクトルを見つける問題である。ここで R^n 内の束は以下で与えられる形の集合である。

$$L = L(b_1,\ldots,b_n) = \{\sum_{i=1}^{n} \lambda_i b_i \mid \lambda_i \in Z, i = 1,\ldots,n\}$$

但し、$b_1,\ldots,b_n$ は R^n の基底であり、$(b_1,\ldots,b_n)$ を L の基底という。また $\|x\|$ と表記されるベクトル $x = (x_1,\ldots,x_n)$ の長さは $({x_1}^2 + \ldots + {x_n}^2)^{1/2}$ である。

暗号に関連した問題へのアプローチ

Shor の素因数分解問題、離散対数問題に対する多項式時間で解ける量子アゴリズムの発見以降、暗号に関連した比較的最近の研究がいくつかなされている。ここでは簡単に下記に４つ示す。

(1)Hidden linear structure[27]

ある関数 $f(x_1, x_2, \cdots, x_k)$ に、$f(x_1, x_2, \cdots, x_k) = h(x_1 + \alpha_2 x_2 + \cdots + \alpha_k x_k)$ なる関係式を満たすような、周期性を持つ関数 $h(x)$ と整数 $\alpha_1, \alpha_2, \cdots, \alpha_k$ が存在するとき、その関数は hidden linear structure をもつという。Hidden linear structure の厳密な説明は[27]を参照のこと。その構造に基づいた暗号は多項式時間で量子計算機によって解かれる。これを適用すると一般化された離散対数問題も直ちに多項式時間で解けることが言える。

(2)Abelian Stabilizer 問題[28]

アーベル群の固定部分群を求める問題。離散対数問題や位数を求める問題（素因数分解問題に関係）はこの問題の特別な場合である。また Abelian Stabilizer 問題自身は Hidden Subgroup 問題に含まれる。

(3)Hidden Subgroup 問題[31,32]

ある集合の部分群が存在するかどうかを問い、存在すればその部分群を求める問題。Simon の問題、離散対数問題、Abelian Stabilizer 問題などは Hidden Subgroup 問題の一例である。

(4)Quantum Counting[34]

長い数列の周期を求める Shor のアルゴリズムと、集合からある条件を満たすデータを抽出する Grover のデータベース検索アルゴリズムを組み合わせることにより得られた、集合からある条件を満たす部分集合の数を数え上げるアルゴリズム。計算量のオーダーは Grover と同じ $O(\sqrt{N})$ である。

暗号に関連した問題へのアプローチとしては基本的なものはセクション 4.3 で説明したが、ここでもう一度今説明した問題なども考慮して、公開鍵暗号、秘密鍵暗号に関してまとめる。

公開鍵暗号系では、素因数分解問題、離散対数問題、楕円曲線暗号などが量子計算で多項式時間で解読できる。公開鍵暗号は解読を関数問題と考えるとこの関数には周期性がある。そのため量子アルゴリズムが効率的に作用する。ここで興味深い問題として、Hidden Subgroup 問題があり、量子計算で有効な問題を考えたり統一的解釈およびその構造を理解する上で鍵となると考えられる。

一方、秘密鍵暗号ではまだ量子計算で多項式時間で解くアルゴリズムの発見はなされていない。現在知られている Grover のデータベース検索アルゴリズムを単純に適用すると、全数検索と比べて 1/2 乗のオーダーにまでは計算量は落ちる。秘密鍵暗号をある関数と見た場合その関数の周期構造を見つけて、それを利用して既存の量子アルゴリズムを適用して多項式時間に結びつけることなどが考えられる。

最近研究されている具体的な量子アルゴリズム例

束内最短ベクトル探索問題[24]

問題

束内最短ベクトル探索問題とはn次元束L内の 0 でない最短ベクトルを見つける問題である。ここでR^n内の束は以下で与えられる形の集合である。

$$L = L(b_1,\ldots,b_n) = \{\sum_{i=1}^{n} \lambda_i b_i \mid \lambda_i \in Z, i = 1,\ldots,n\}$$

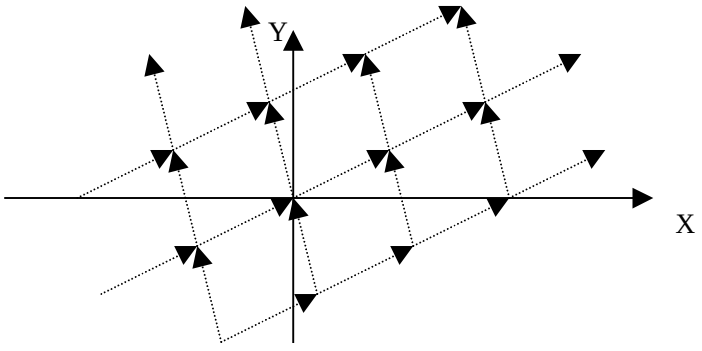
但し、$b_1,\ldots,b_n$はR^nの基底であり、$(b_1,\ldots,b_n)$をLの基底という。また$\|x\|$と表記されるベクトル$x = (x_1,\ldots,x_n)$の長さは$({x_1}^2 + \ldots + {x_n}^2)^{1/2}$である。

つまり束内最短ベクトル探索問題とは、基底$(b_1,\ldots,b_n)$を与えられたとき、$\|\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n\|$の値が$(\lambda_1,\ldots,\lambda_n) = (0,\cdots,0)$を除いて最小となる組合せを見つける問題である。

ここでは、簡単のため$n = 2$の場合を説明する。

問題

R^2の基底ベクトルb_1、b_2（但し、$\|b_1\| \le \|b_2\|$かつb_1とb_2は平行でない）が与えられたとき、最短ベクトルを与える$v = \lambda_1 b_1 + \lambda_2 b_2$（$\lambda_1, \lambda_2 \in Z$）の組$(\lambda_1, \lambda_2)$を見つける。



アルゴリズム

Step1. 探索範囲の限定

λ_1, λ_2 の値は現在 $-\infty$〜∞ まであり範囲を限定する必要あり

(1) $\|b_1\| \le \|v\|$ のとき　→　必ず最短ベクトルは b_1　→　解発見、探索必要なし

(2) $\|b_1\| > \|v\|$ のとき　→　この範囲に限定して探索必要

この(2)の条件のとき λ_1, λ_2 の条件は $b_1 = (b_{11}, b_{12})$ と $b_2 = (b_{21}, b_{22})$ とすると、下記の通りになる。

$$(b_{11}{}^2 + b_{12}{}^2)\lambda_1^2 + 2(b_{11}b_{21} + b_{12}b_{22})\lambda_1\lambda_2 + (b_{21}{}^2 + b_{22}{}^2)\lambda_2^2 - (b_{11}{}^2 + b_{12}{}^2) \le 0$$

上式は、どんな基底 b_1、b_2 を与えても楕円でその楕円の内部を意味する。よって探索範囲として λ_1, λ_2 を軸とする 2 次元空間内の楕円の内側のみを探索すればよい。

楕円が通常の楕円から角度 θ 傾いているとして、λ_1, λ_2 の範囲を再度計算すると次のようになる。

$$|\lambda_1| \le \alpha = \left\lceil \sqrt{\frac{C}{A}}|\cos\theta| + \sqrt{\frac{C}{B}}|\sin\theta| \right\rceil 、\ |\lambda_2| \le \beta = \left\lceil \sqrt{\frac{C}{A}}|\sin\theta| + \sqrt{\frac{C}{B}}|\cos\theta| \right\rceil$$

但し、

$$A = (b_{11}\cos\theta + b_{21}\sin\theta)^2 + (b_{12}\cos\theta + b_{22}\sin\theta)^2$$

$$B = (b_{11}\sin\theta - b_{21}\cos\theta)^2 + (b_{12}\sin\theta - b_{22}\cos\theta)^2$$

$$C = b_{11}{}^2 + b_{22}{}^2$$

よって、探索するべき範囲（λ_1, λ_2）は、長方形の内側で、検索すべき要素数は、$N = \alpha\beta$ 個の要素に対して最短ベクトルの探索を行えばよい。

Step2. （λ_1, λ_2）と各要素のインデックスの対応付け

（λ_1, λ_2）は $(-\alpha, -\beta)$ から (α, β) まで(0,0)を除いて調べればよい。

探索すべき要素は、$T[0], \cdots, T[N-1]$ の N 個で、これらの要素は各々下記のように関係づけられた（λ_1, λ_2）に対するベクトルの長さを値として持つ。

$T[0], \cdots, T[N-1]$ のインデックスが $0, \cdots, N-1$ として、これらと（λ_1, λ_2）の関係を次のようにする。

$$(-\alpha, -\beta), \cdots, (\alpha, -\beta), (-\alpha, -(\beta - 1)), \cdots, (-\alpha, \beta), \cdots, (\alpha, \beta) = 0, \cdots, N-1$$

Step3. 最小値探索アルゴリズム（Grover のアルゴリズムの拡張）の適用

(1)閾値のインデックス $y(0 \le y \le N-1)$ を一様にランダムに選択

(2)次の処理を繰り返す（但しこの繰り返し回数は $O(\sqrt{N})$ ）

a)メモリを $\sum_j \frac{1}{\sqrt{N}} |j\rangle |y\rangle$ に初期化

b) $T[j] < T[y]$ を満たすすべての要素 j に印をつける

c) 量子インデックス探索アルゴリズムを適用する

Grover のデータベース検索アルゴリズムをサブルーチンとして使用

i. $m = 1$ に初期化し、 $\eta = 6/5$ とする

ii. k を m より小さい非負整数とし、一様にランダムに選ぶ

iii.初期状態 $\sum_i \frac{1}{\sqrt{N}} |i\rangle$ から Grover のデータベース検索を k 回繰り返す

iv.レジスタを観測して、インデックス i が得られる

v. $T[i]$ が印をつけられた要素なら、ループを終了し、step (2)の d)へ

そうでない場合は、 m を $\min(\eta m, \sqrt{N})$ とし、step(2)の c)の ii)へ

d)最初のレジスタを観測し、結果を y' とする。

もし $T[y'] < T[y]$ なら、新たに $y := y'$ とする

(3)インデックス y を返す

この y が最小値のインデックスで、最短ベクトル v のインデックスとなる

以上が束内最短ベクトル探索問題に対する量子アルゴリズムである。このアルゴリズムは、束内最短ベクトル探索問題の検索範囲を有限にして、単純に最小値探索アルゴリズム（Grover のデータベース検索アルゴリズムがベース）を適用しただけである。そのため、計算量は要素数を N とするとオーダは $O(\sqrt{N})$ となっただけで、多項式時間のオーダまでは高速なアルゴリズムではない。

5. 量子計算に関係する文献調査

量子計算研究に関する参考文献を、論文、プレプリント、書籍からリストアップしてそれらを分野別に分類してまとめる。なお文献名で quant-ph/数字または cond-mat/数字は、ロスアラモス国立研究所(LANL)のサーバー[54]に登録されているプレプリントである。また ECCC とは計算量理論関係の研究レポートのことである[55]。

入門・解説文献

[1]特集：量子コンピュータ量子計算---理論と実験の最前線、数理科学 10 月号(サイエンス社 1998)

[2]量子情報理論とその応用論文小特集、電子情報通信学会論文誌 A Vol.J81-A No.12(1998)

[3]竹内、21 世紀、量子猫は計算をするか？、日本物理学会誌 54, 263-273(1999)

[4]特集：量子情報処理・量子コンピュータ、Computer Today11 月号(1999)

[5]細谷、量子計算機への招待、パリティ 12 月号(1996)

[6]西野、量子コンピュータ入門（東京電機大学出版局、1997）

[7]大矢、量子コンピュータの数理（パリティ物理学コース、丸善、1999）

[8]細谷、量子コンピュータの基礎--Lectures on Quantum Computation（サイエンス社、1999）

[9]R.P. Feynman, Feynman Lectures on Computation, Addison-Wesley(1996)

[10]M.Brooks, Quantum Computing and Communications(Springer-Verlag New York 1999)

[11]C.P.Williams and S.H.Clearwater, Explorations in Quantum Computing(Springer-Verlag, New York, 1998)

[12]Preskill and A. Kitaev, Caltech Lecture Note--Advanced Mathematical Methods of Physics (http://www.theory.caltech.edu/people/preskill/ph229)

[13]E.Rieffel and W.Polak, "An Introduction to Quantum Computing for Non-Physicists",quant-ph/9809016(1998)

[14]A.Ekert and R.Jozsa, "Shor's Quantum Algorithm for Factoring Numbers", Rev. Mod. Phys. 68, 733(1996)

量子計算の理論研究

主な量子アルゴリズム

[15]D.Deutsch and R.Jozsa, "Rapid solution of problems by quantum compuation", Proc.R.Soc. Lond., A 439, pp553-558(1992)

[16]D.R.Simon, "On the power of quantum computation" SIAM J. Comput., 26, pp.1474-1483, 1997

[17]P.W.Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", 35th FOCS ,116-123(1994)

[18]L.K.Grover, "Quantum Mechanical Helps in Searching for a Needle in a Haystack", Phys.Rev.Lett. 79, 325-328(1997)

[19]C.Durr and P.Hoyer, "A quantum algorithm for finding the minimum", quant-ph/9607014(1999)

[20]G. Brassard and P.Hoyer, "On the power of exact quantum polynomial time", quant-ph/9612017 (1996)

[21]G. Brassard and P.Hoyer, "An exact quantum polynomial time algorithm for Simon's problem", quant-ph/9704027 (1997)

[22]S.C.Sung and T.Mihara, "A Quantum Polynomial Time Algorithm for Extended Simon's Problem", QIT99-3(1999)

[23]M.Ettinger and P.Hoyer, "A Quantum Observable for the Graph Isomorphism Problem", quant-ph/9901029(1999)

[24]西野、與語、最短ベクトル探索問題の効率的量子アルゴリズムの設計について、QIT99-2(1999)

[25]M.Ajtai, "The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions", ECCC TR97-047, 1997

[26]M.Ajtai and C.Dwork, "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence", Revision 01 of ECCC TR96-065, 1997.

その他の量子アルゴリズム

[27]Boneh and Lipton, "Quantum Cryptanalysis of hidden linear forms", Crypto'95 Springer-Verlag.

[28]A.Y.Kitaev, "Quantum measurements and the Abelian Stabilizer Problem", quant-ph/9511026(1995)

[29]J.Shikata, J.Suzuki, H.Imai, "A Remark on Solving the ECDLP Efficiently by Quantum Computing", ISEC99-39 (1999)

[30]Ohya and N.Masuda, "NP Problem in Quantum Algorithm", quant-ph/9809075(1998)

[31]M.Mosca and A.Ekert, "The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer", quant-ph/9903071(1999)

[32]M.Rotteler and T.Beth, "Polynomial-time Solution to the Hidden Subgroup Problem for a Class of non-abelian Groups", quant-ph/9812070(1998)

[33] T.Hogg and C.Mochon, "Tools for Quantum Algorithms", quant-ph/9811073(1998)

[34]G.Brassard, P.Hoyer, A.Tapp, "Quantum Counting", quant-ph/9805082(1998)

量子ゲート

[35]B.Barenco, C.H.Bennet, R.Cleve, D.P.DiVincenzo, N.Margolus, P.Shor, T.Sleator, J.A.Smolin and H.Weinfurter, "Elementary gates for quantum computation", Phys. Rev. A52,pp 3457-3467(1995)

量子計算の実験的側面

[36]S.Takeuchi, "A Simple Quantum Computer: Experimental Realization of the Deutsch Jozsa Algorithm with Linear Optics", Proc.4th Workshop on Physics and Computation, PhysComp96 (1996)

[37]竹内、線形光学素子を用いた量子計算アルゴリズムの実現、電子情報通信学会論文誌 A J81-A, 1644 (1998)

[38]N.A.Gershenfeld and I.Chuang, "Bulk Spin-Resonance Quantum Computation", Science 275, 350 (1997)

[39]J.I.Cirac and P.Zoller, "Quantum Computations with Cold Trapped Ions", Phys.Rev. Lett. 74, 4091(1995)

[40]M.Brune, P.Nussenzveig, F.Schmidt-Kaler, F.Bernardot, A.Maali, J.M.Raimond, S.Haroche, "From Lamb Shift to Light Shift: Vaccum and Subphoton Cavity Fields

Measured by Atomic Phase Sensitive Detection", Phys.Rev.Lett. 72, 3339 (1994)

[41]Q.A.Turchette, C.J.Hood, W.Lange, H.Mabuchi, H.J.Kimble, "Measurement of Conditional Phase Shifts for Quantum Logic", Phys. Rev. Lett. 75, 4710 (1995)

[42]Y.Maknlin, F.Schoen, A.Shnirman, "Josephson-Junction Qubits with Controlled Couplings", cond-mat/9808067(1998)

[43]A.Barenco, D.Deutch, A.Ekert, R.Jozsa, "Conditional Quantum Dynamics and Logic Gates", Phys.Rev. Lett. 74, 4083 (1995)

[44]B.E.Kane, "A Silicon-Based Nuclear Spin Quantum Computer", Nature 393, 133(1998)

[45]中村、蔡、微小ジョセフソン接合を用いた量子ドット、QIT99-4(1999)

計算量理論(古典、量子)

[46]C.H.Papadimitriou, Computational Complexity, Addison-Wesely(1995)

[47]Bernstein and Vazirani, “Quantum Complexity Theory”, SIAM J.Computing, 26, No.5(1997)

[48]Cleve, “An Introduction to Quantum Complexity Theory”, quant-ph/9906111(1999)

その他

量子計算研究機関の主なサイト

[49]Oxford University, the Centre for Quantum Computation
http://www.qubit.org/

[50]Caltech, Clatech Quantum Optics Group
http://www.cco.caltech.edu/~qoptics/

[51]Caltech MIT-USC, Quantum Information and Computation(QUIC)
http://theory.caltech.edu/~quic/index.html

[52]Los Alamos, Qunatum Computation/Cryptography at Los Alamos
http://quantum-computing.lanl.gov/

[53] The Stanford-Berkley-MIT-IBM Quantum Computation Research Project
http://squint.stanford.edu/

プレプリントサーバー

[54]Los Alamos National Laboratory

http://xxx.lanl.gov/archive/quant-ph

[55]Electronic Colloquium on Computational Complexity

http://www.eccc.uni-trier.de/eccc/