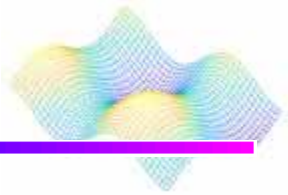
22171036

166ページ11行目～170ページ

複雑性クラス



複雑性理論

- 解決に多項式時間を要する問題
- 多項式をより必要とする問題

多項式時間アルゴリズム

非常に大きいnの値が実用的

非多項式時間アルゴリズム

大きいnの値では実行不可能

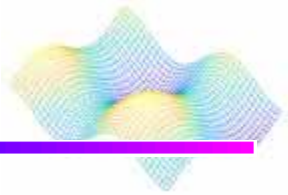
古典的なアルゴリズム

多項式時間で解くことができる
問題はPで表される

量子アルゴリズム

多項式時間で解くことができる
問題はQPで表される

複雑性クラス

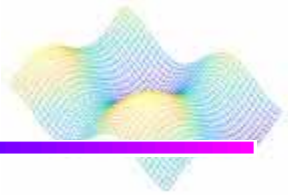


ドイッチュの問題

クラスPには属してなく、クエリの複雑さのために
QPに属している

ドイッチュの問題はPとQPを分離すると言われるが
クエリの複雑さのため、QPに属するがPに属さない
ことが問題である

複雑性クラス



n = 10 とする

10個の入力を受け取る関数を与えられ
バランスが取れているか、一定であるか

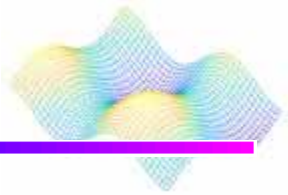
答えを推測できるまで、特定の入力で評価し続ける必要がある

ここで$2^{10} = 1024$通りの可能な入力

最悪な場合

関数のバランスが取れているが、最初の512個に対して同じ答えが
得られ、513番目の評価で他の値を得ることである

複雑性クラス



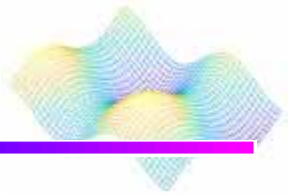
関数のバランスが取れている場合、各入力値が
0か1と等しくなる可能性がある

コインを512回投げて毎回表が出る確率は?

答えは $\left(\frac{1}{2}\right)^{512}$

この確率は1を1グーゴル (10の100乗) で
割ったものより小さくなる

複雑性クラス



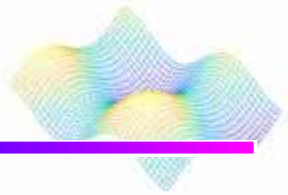
少なくとも99.9%の成功率、またはエラー率0.1%未満

関数のバランスが取れている場合、その関数を11回評価する
毎回1が得られる確率と毎回0が得られる確率は
ともに0.00049である

多項式時間とある範囲内のエラーの確率で解くことが出
来る古典的なアルゴリズムはBPPと表される

ドイッチュの問題はクラスBPPの中にある

複雑性クラス



サイモンのアルゴリズム

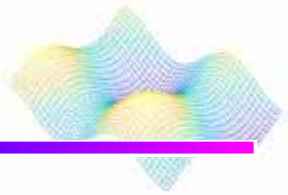
回路を通してn-1個の線形独立方程式ができるまで
キュービットを送り続ける必要がある

サイモンのアルゴリズムはクラスQPに属さない

Nが計算できるということで $\left(\frac{1}{2}\right)^N$ がエラーの範囲よりも小さい

回路を n + N 回実行するとシステム n − 1 線形独立方程式を
含む n + N 方程式の確率は $1-\left(\frac{1}{2}\right)^N$ よりも大きい

複雑性クラス



エラーの確率の範囲を決め、値Nの計算をする

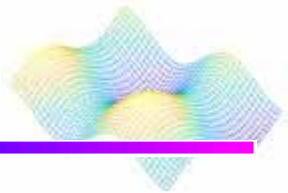
値 N は n に依存しない

サイモンの回路を n + N 回実行する

N は固定されて、n は線形関数

n − 1 の独立ベクトルを含む n + N 方程式のシステムを仮定する

複雑性クラス



古典的なアルゴリズムをn + Nの方程式を解く

かかる時間はn + Nの2次である

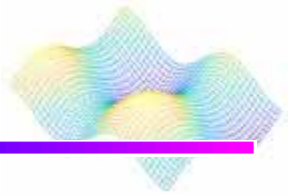
多項式時間とある範囲内のエラーの確率で解くことが出来る量子アルゴリズムはBQPと表される

サイモンのアルゴリズムはクエリの複雑さによってBPPに属さず、BQPに属する

最悪の場合、古典的なアルゴリズムは$2^{n-1}+1$の関数評価がかかることを示している

サイモンの問題はクエリの複雑さをBPPとBQPを分離する

量子アルゴリズム



量子アルゴリズムによって提供される高速化は
量子並列処理によってもたらされる

入力をすべての基本状態を含む重ね合わせに入れることが出来る

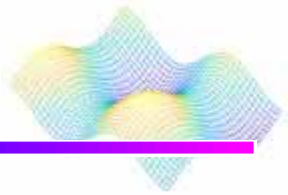
1985年ドイッチュは論文でアルゴリズムを発表した

1992年ドイッチュとジョサはアルゴリズムの一般化を発表した

ドイッチュの論文は、量子回路の図を使用しないことが現在標準になっている

1993年～1995年に重要なアルゴリズムの多くが発見された

量子アルゴリズム



直交行列は量子ゲートを表し、量子回路はゲートの組み合わせからなる

乗算直交行列に対応し、直交行列の積は直交行列の1つになり、
任意の量子回路は1つの直交行列で書くことが出来る

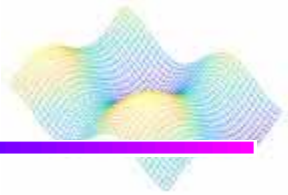
量子コンピューティングは、従来のコンピューティングよりも
問題を多くの方法で見ることが出来る

古典的なアルゴリズムより速い量子アルゴリズムを構築すること

2021/6/8　　p171-p174 14行目

9章　量子コンピューティングの影響

9章　量子コンピューティングの影響



量子コンピュータが完成すると起きる様々な影響を例を挙げて説明。

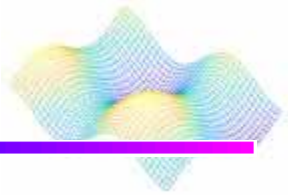
Shorのアルゴリズムと暗号解読

暗号解読に関する量子計算は主にShorの アルゴリズムを使用する。

Shorの アルゴリズム

- **オイラーの定理、数論、連分数展開、複素解析、離散フーリエ変換などを使用。**
- **サイモンのアルゴリズムと同様に古典的な部分と量子的な部分がある。**
- **RSA暗号の解読などに使用できる。**

RSA 暗号化



発明者である
Ron Rivest、Adi Shamir、Leonard Adleman
にちなんで命名

コンピュータ間で送信されるデータを暗号化するために、インターネット上で広く使用されており、インターネットバンキングやクレジットカードを使用した電子購入に使用されている。

RSA 暗号化

例：銀行とその利用者が個人情報などを共有していて、その情報を盗聴から守りたい

情報を暗号化

・情報を暗号化、復号化するためのキーも暗号化する必要がある。

キーを暗号化するときにRSA暗号化を使用

RSA 暗号化

利用者側

- **暗号化と復号化に使用されるキー(*K*)を生成。**

銀行側

- **ほぼ同じbit数の2つの大きな素数 *p* と *q* を決める。**
- **モジュラスと呼ばれる積 *N* = *pq* を求める。**
  (*N* は10進数で300桁以上)
- ***p* -1 または *q* -1 と、同じ因数を持たない比較的小さな数 e を決める。**

***p* と *q* は秘密に**

キー(*K*)を生成

RSA 暗号化

利用者側

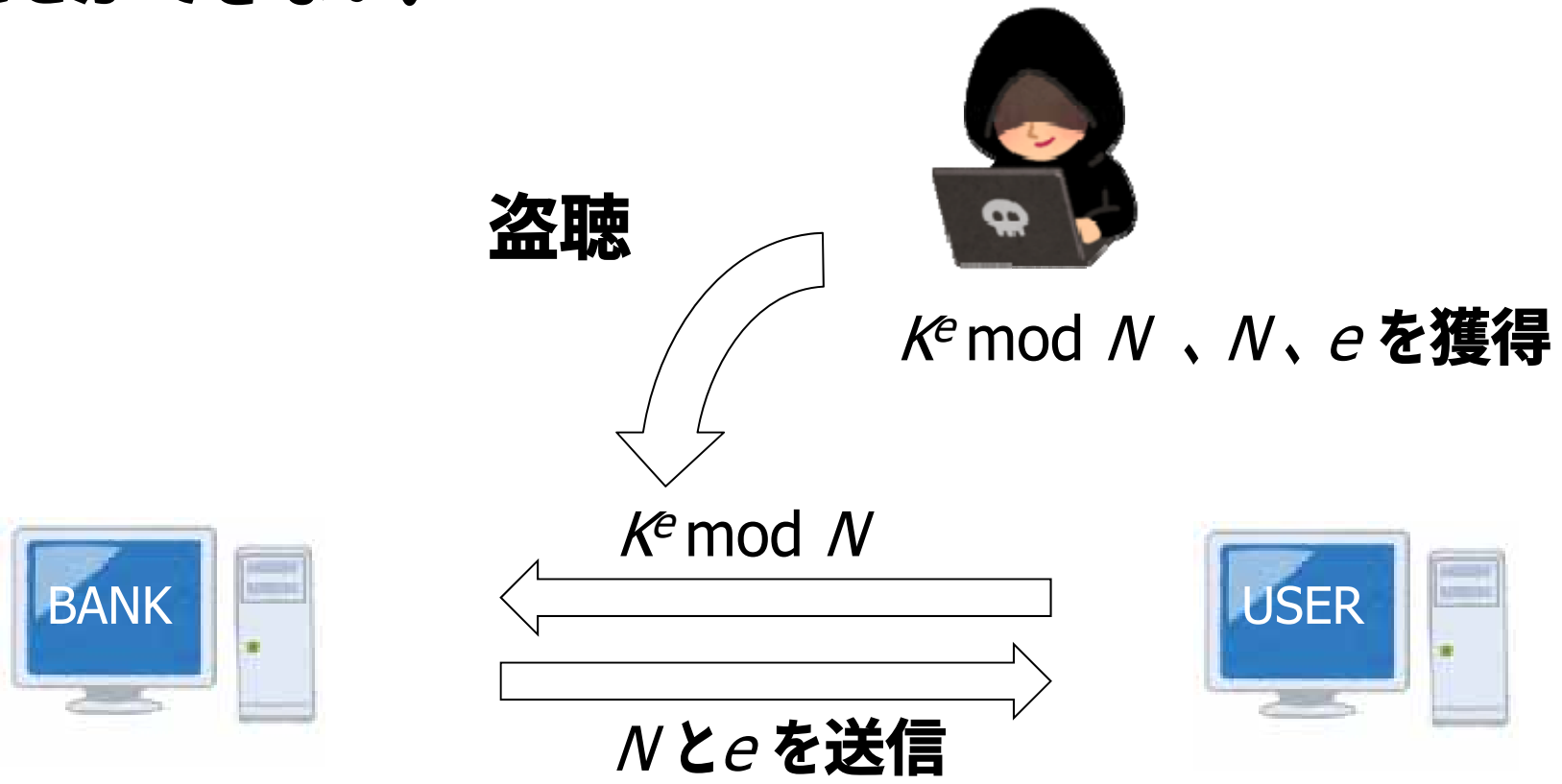
- **送信された N と e を使ってキー K を暗号化し暗号文 $K^e \bmod N$ を送信。**

銀行側は p と q を知っているためすぐに K を求めることができる

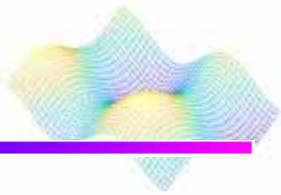
K を導出

RSA 暗号化

ハッカーがいた場合
$K^e \bmod N$ 、N、e **を知ることができるが**K **を求めることができない。**



RSA 暗号化



多項式時間に2つの大きな素数の積を考慮できる古典的なアルゴリズムを誰も発見していない。

- RSA暗号は p と q なしで計算することはできない。

量子コンピュータが完成すると…

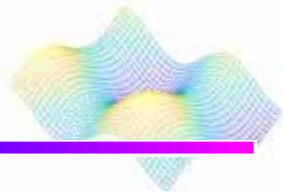
Shor が大きな素数の積を因数分解する量子アルゴリズムを構築。

- 複雑性クラスが BQP であり、高い確率で正答を返し多項式時間で実行可能。

RSA暗号は安全ではなくなってしまう。

P174-P178

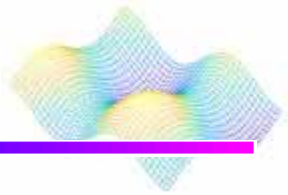
Shorのアルゴリズム



Shorのアルゴリズムには、かなりの量の数学が含まれる。アルゴリズムの重要な部分は、量子フーリエ変換ゲートと呼ばれるゲートである。これはHadamardゲートの一般化と考えられる。

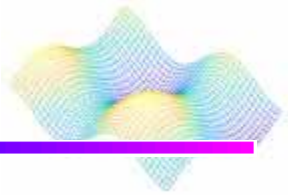
フーリエ変換行列と量子フーリエ行列の主な違いは、後者の場合のエントリは一般に複素数であるということである。

Simonのアルゴリズム



干渉を使用し、振幅は1または-1。
項を追加すると、ケットは互いにキャンセルまたは強化された。

Shorは同様のアイディアが量子フーリエ行列に
適用されたことにきずいた。現在、振幅は1と-1
だけでなく与えられる。
より多くの種類の周期を検出できる。



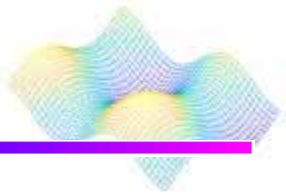
数Nがわかっていて2つの素数pとqの席に因数分解することを思い出すと、アルゴリズムは、1<a<Nとなる数aを選択する。

(aがNと何らかの因子を共有している場合)
→aがpまたはqの倍数であると推測できる。
(aがNと因子を共有していない場合)
→a mod (N)、a^2 mod (N)、　a^3 mod (N)などを計算する。

ここで、a^i mod (N)はa^iを計算することを意味しNで割ったときにあまりをとる。(N未満)

a^r mod (N)＝a mod (N)となる数値rは周期と考えられる。

Simonのアルゴリズムを一般化して未知の期間rを見つけられる！



実際に実装されている。

2001**年**→15**の因数分解**
2012**年**→300**の因数分解**

RSA**暗号化スキームが安全でなくなるのは時間の問題である**

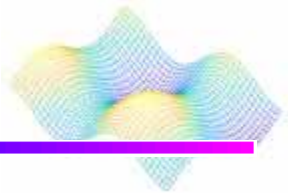
他の暗号化方法が開発されてきたが、Shor**のアルゴリズムはこれらの多くでも機能する。**

ポスト量子暗号は現在非常に活発な分野であり、新しい暗号化方法が開発されている。

量子コンピュータによる破壊に耐えられるようにするには・・・

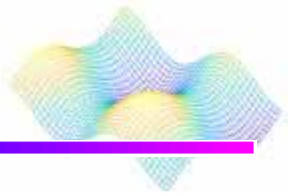
暗号化されたメッセージが必要である。

QKDシステム



- **２００７年に最初に使用される。**
- Micius**と呼ばれる衛星が使われている。**

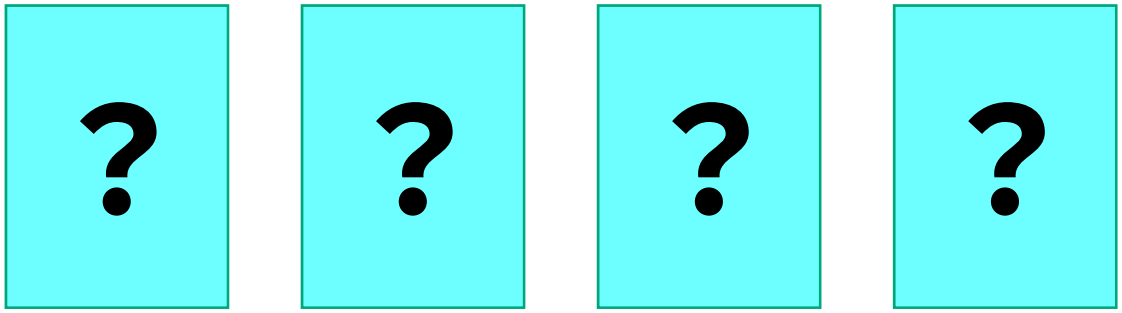
Groverのアルゴリズム



データ検索を高速化する。

従来のアルゴリズムより高速化されているのは、クエリの複雑さ。

ある問題



どこかにハートのエースがある。
どれがハートのエースか当てるためには何枚目くる必要がある？

A.平均すると2.25枚

言い換えると・・・

00、01、10、11の4つの2進数行列がある。これらの文字列のうち3つを0に送信し、もう1つを1に送信する関数fがあり、1に送られる2進数行列を求めたい。関数評価をいくつ行う必要があるか？

A.平均2.25

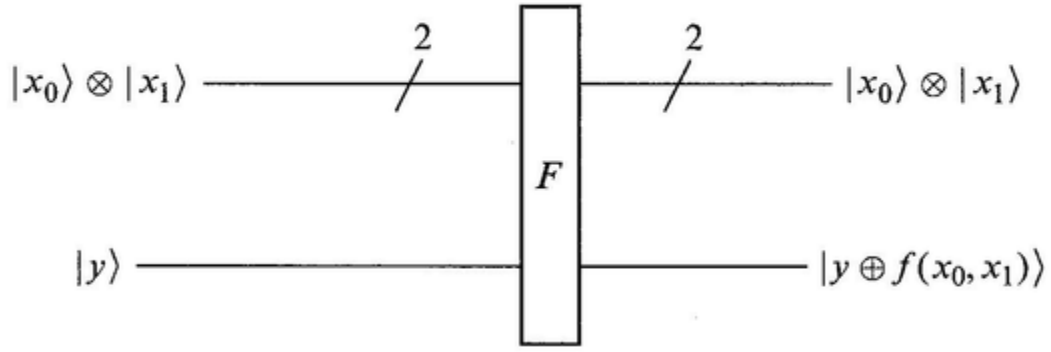


Figure 9.1

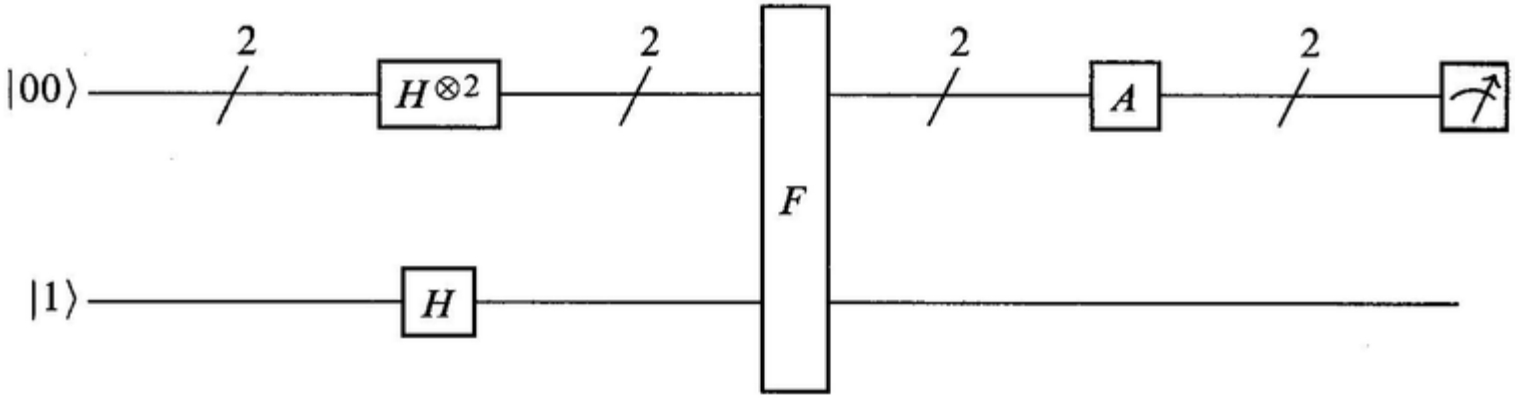


Figure 9.2

9.2はグローバーのアルゴリズムの回路

2つのステップがある。

1つ目は、見つけようとしている場所に関連する確率振幅の符号を変転すること。

2つ目は、この確率分布を増幅すること。

Hadamardゲートを通過した後、トップの2つの量子ビットの状態は

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

となり、下の量子ビットの状態は

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

となる。組合せ状態を

$$\frac{1}{2}\left(|00\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) + |01\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\right.$$
$$\left. + |10\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) + |11\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\right)$$

次にキュービットはFゲートを通過する。これにより検索しようとしている場所の3番目のキュービットの$|0\rangle$と$|1\rangle$が反転する。
$f(10)=1$の例を使用すると、次の様になる

$$\frac{1}{2}\left(|00\rangle\otimes\left(\frac{1}{\sqrt{2}}\left|0\right\rangle-\frac{1}{\sqrt{2}}\left|1\right\rangle\right)+|01\rangle\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)\right.$$
$$\left.+|10\rangle\otimes\left(\frac{1}{\sqrt{2}}|1\rangle-\frac{1}{\sqrt{2}}|0\rangle\right)+|11\rangle\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)\right)$$

これは次のように書くことができる

$$\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle)\otimes\left(\frac{1}{\sqrt{2}}\left|0\right\rangle-\frac{1}{\sqrt{2}}\left|1\right\rangle\right)$$

その結果、上の二つのキュービットは下のキュービットと絡み合っていないが、見つけようとしている場所に対応する確率振幅$|10\rangle$の符号を反転させました。

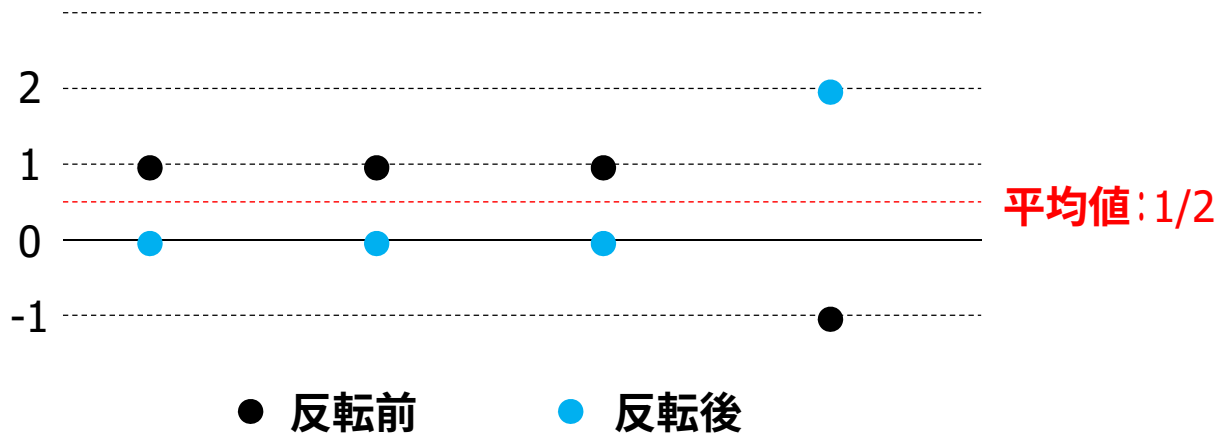
テキストp178下2行～p182下3行

量子振幅増幅

量子振幅増幅は，確率振幅を平均値に対して反転させることで機能する．

例）４つの数字　1，1，1，-1を用いる．

合計：2　　**平均**：1/2
次に各数値を平均値を軸に反転する．



→　0, 0, 0, 2

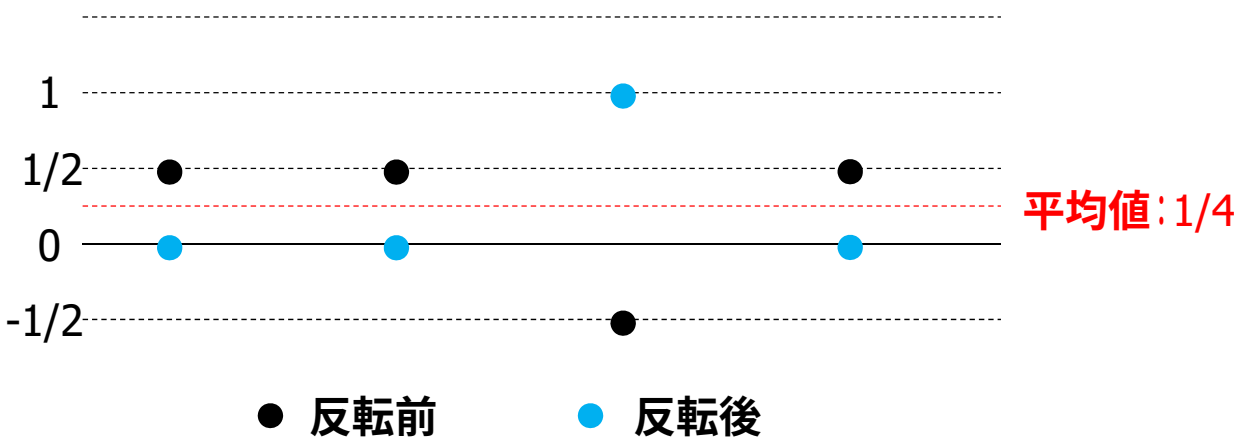
量子振幅増幅

現在の上2つの量子ビットは,

$$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

合計:1　**平均**:1/4

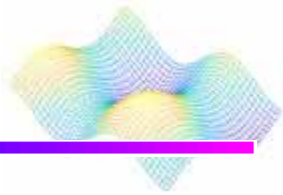
反転させる



$$0|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle = |10\rangle$$

これを測定すると確実に$|10\rangle$が求められるため,
我々が望んでいるとおりになることが分かる.

量子振幅増幅



平均に対して反転させることが可能なゲートが必要．
このゲートは，以下のように表せる．

$$A = \frac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

このゲートを前述の量子ビットに作用させると・・・

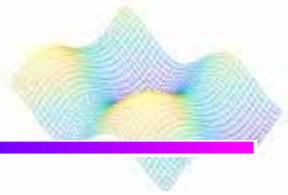
量子振幅増幅

$$A\left(\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right)$$

$$= \frac{1}{4}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

今回の例では，量子ビットが2つしか使われていないため，
オラクルは1回だけ使用すればよい．
しかし，同じことを古典的アルゴリズムで行った場合，平均して
2.25の質問が必要である．

量子振幅増幅



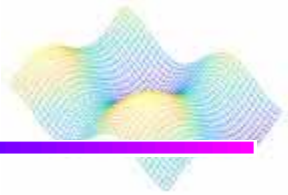
量子ビットがn個の場合でも同様に機能する.

n個の場所からある1つの場所を見つけたいとき・・・

古典的アルゴリズム	Groverのアルゴリズム
最悪の場合, n-1個の質問をする必要がある. このとき問題数はnと同じ割合で増える.	√n回で高確率で答えを導くことが出来る. このとき問題数は√nの割合で増える.

古典的アルゴリズムに対して, Groverのアルゴリズムは2乗のスピードアップをしているといえるが, 指数関数的なスピードアップ程劇的ではない.
しかし, Groverのアルゴリズムの利点はスピードアップではなく,
様々なことに応用できることである.

化学とシミュレーション



1929年　**Paul Dirac**

「物理学と化学の大部分の数学的処理に必要な基本法則は完璧に知られている．しかしこれらの方程式は解くことが難しすぎる．」

理論上，すべての化学物質には原子の相互作用と電子の配置が伴う．これらを方程式で書き表すことはできるが，解くことは難しい．

実際には，化学者は正確な答えを出すのではなく，近似を使用します．計算科学ではこの方法を使用し，大抵の場合，古典的コンピュータは良い答えを導き出す．

しかし，近似が不十分で現在の計算技術が機能しない場合もある．そこで現在必要なのが近似されてしまった細かい部分である．

量子コンピューティングの貢献が期待される分野

Feynman
「量子コンピュータの主なアプリケーションの1つは量子システムのシミュレーションである.」

①肥料を作るために使用される酵素であるニトロゲナーゼが実際にどのように機能するかを理解すること

現在の製造方法では，大量の温室効果ガスを放出し，莫大なエネルギーを消費する.
量子コンピュータは，この触媒反応やその他の触媒反応を理解するうえで重要な役割をすると考えられる.

量子コンピューティングの貢献が期待される分野

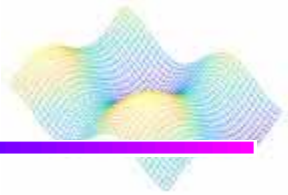
②光合成が行われるプロセスの理解

光合成による，太陽光から化学エネルギーへの変換は迅速かつ非常に効率的に行われるプロセスである．
これは量子力学的なプロセスであり，このプロセスを理解することで，太陽電池に使用できる可能性がある．

③超伝導と磁性の深い理解

超伝導と磁性は量子力学的現象であり，量子コンピュータがこれをより深く理解することに役立つ可能性がある．
目標の1つとして絶対零度近くまで冷却する必要のない超伝導体を開発すること

量子コンピュータの実際の構築



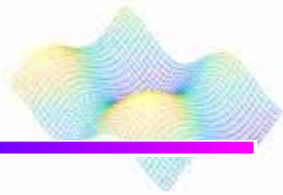
IBM (International Business Machines Corporation)

7量子ビットの量子プロセッサで水酸化ベリリウム (BeH2) の分子をシミュレートした.

・BeH2は原子が3つしかない比較的小さな分子
・近似は使用しない
・数量子ビットしか使用しないため, 古典的なコンピュータを用いてシミュレートできる

しかし, 量子ビット数が増えると, 古典的なコンピュータではシミュレートできなくなる.

まとめ



量子シミュレーションが従来のコンピュータの能力を超える
新しい時代に突入する.
ここまでは考えられるアプリケーションをいくつか挙げてきた.

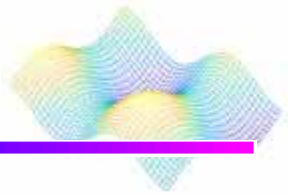
以降, 量子コンピュータの構築に使用されているいくつかの
方法について説明される.

2021年6月8日

ハードウェアと量子アニーリング

p.182-186

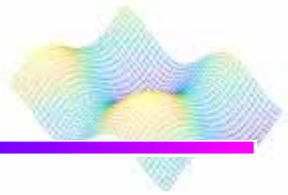
ハードウェア



最も重要なのはデコヒーレンス
（量子ビットが環境からの何かと相互作用することで量子上の情報が失われること）

量子ビットを初期状態に設定し、使用するまでその状態を維持することが必要であり、ゲートと回路を構築できることも必要

ハードウェア



フォトン

初期化が簡単で絡みやすく、環境とあまり相互作用しないため長期間一貫性を保つことができる。しかしフォトンを記録装置に記録し、必要な時に準備することは困難。

電子スピン

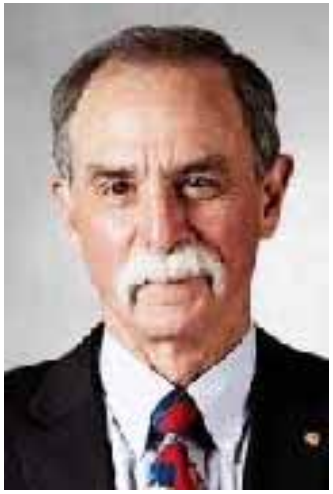
合成ダイヤモンドの電子を使用する。レーザーを照射することによって操作できる。1つまたは2つの量子ビットを構築できるが、現時点では、大きな数を生成することはできない。

有機エレクトロニクス

イオンのエネルギー準位

電磁場によって所定の位置に保持されるイオンを使用する。

すべてを絶対零度近くまで冷却すると、振動を最小限に抑えられイオンを維持することができる。量子ビットにエンコードし、レーザーで操作できる。



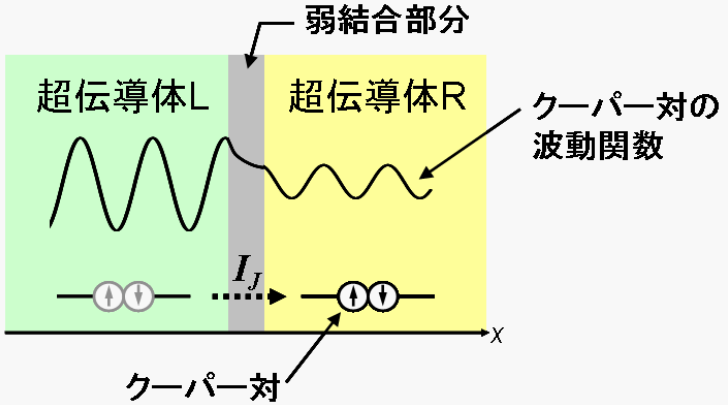
David Wineland は、1995年に最初のCNOT ゲートを構築するためにイオントラップを使用し、ノーベル賞を受賞した。2016年には、NISTの研究者が200を超えるベリリウムイオンを量子もつれにした。

クーパー対とジョセフソン接合

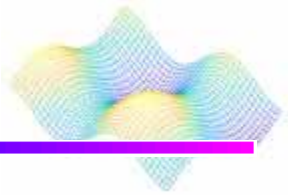
超伝導体の電子はクーパー対を形成する。超伝導体の薄層を絶縁体の薄層で挟むと、ジョセフソン接合になる。

ジョセフソン接合を含む超伝導ループ内のクーパー対のエネルギー準位は離散的であり、量子ビットのエンコードに使用できる。

弱く結合した2つの超伝導体の間に超伝導電子対（クーパー対）が量子トンネルすることによって超伝導電流が流れる現象



企業の動向

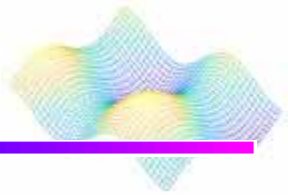


2016 年、IBM は 5 量子ビットのコンピューターを導入し、クラウド上で誰でも無料で利用できるようにした

目的は、超高密度コーディング、ベルの不等式、および水素原子のモデルをすべてこのマシンで実行するために、量子コンピューティングを幅広い回路に導入すること

2017 年末、IBM は 20 量子ビットのコンピューターをクラウドに導入した。

企業の動向



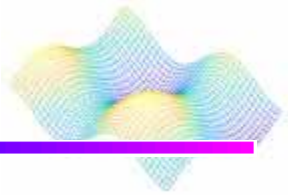
Google は近い将来、72 キュービットを使用するコンピューターを発表する予定。これは、古典的なコンピューターでは実行またはシミュレートすることが不可能なアルゴリズムを量子コンピューターで実行することが可能になったということ。

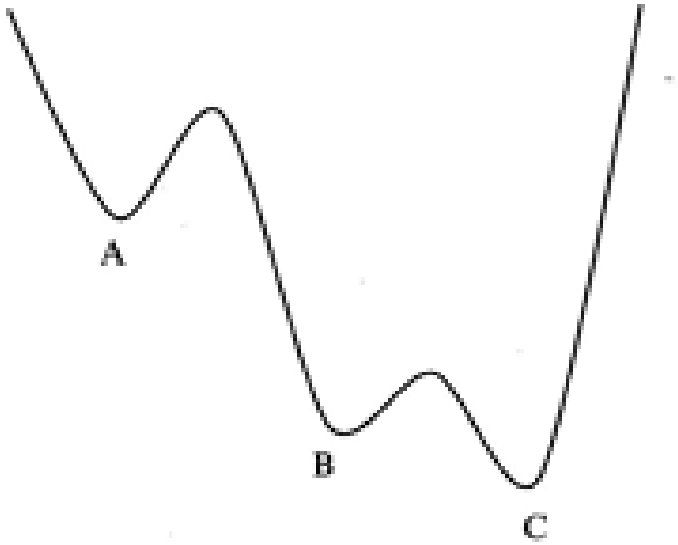
IBMのチームは、56 キュービット システムを古典的にシミュレートする方法を最近発見し、量子超越性に必要なキュービット数の下限を引き上げた。

量子アニーリング

- D-WaveのD-Wave 2000Q は、2,000 キュービットを備えている。
- 量子アニーリング専用で特定の最適化の問題を解決できる。

量子アニーリング





Cに行きたい

エネルギーを徐々に減らすことで、一方は移動できるがもう一方は移動できない

ボールベアリングは最下点で終わる

テキスト（p.186下7行～p.189）

量子超越性と並行宇宙①

3ビットの組み合わせ：000, 001, 010, 011, 100, 101, 110, 111

↓ キュービットに切り替えると、

基底ベクトルに関連付けられるため、ベクトル空間が8次元となる。

n個のキュービットがある場合、2^nの基底ベクトルがあり、
空間は2^n次元となる。

量子超越性と並行宇宙②

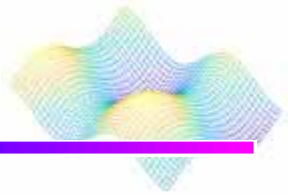
＜72キュービットの場合＞

基底要素の数＝2^{72}＝4,000,000,000,000,000,000,000

多数であり、古典的なコンピュータが量子コンピュータをシミュレートできない点である。

量子コンピュータが72キュービットもしくはそれを超えるキュービットを持つ場合、量子コンピュータが古典的なコンピュータの能力を超える計算を実行できるとき、量子超越性の時代に入る。

量子超越性と並行宇宙③



＜300キュービットの場合＞

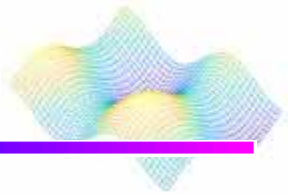
基底要素の数は2^{300}であり、既知の宇宙の素粒子の数よりも多い。

David Deutschは宇宙にある粒子よりも多くの基底要素を含む
このような計算を実行するには、

それぞれがお互いに協力し合う並行宇宙を導入する必要がある
と考えた。

David Deutschの目標の一つとして、量子計算の研究において、
並行宇宙を主張することである。

計算①



Alan Turing：**計算理論の父の一人。**

人間が計算を実行するときに何をしたのかを考え、最も基本的なレベルまで分解できる

チューリング機械と呼ばれる単純な理論的な機械を示した。

＜チューリング機械の特徴＞

- **ビットの操作を含む**
- **最も基本的な操作を示す**

しかし、

チューリングは人間の行動に基づいて計算を分析していたことを忘れないでください。

計算②

＜量子コンピュータと古典的コンピュータの違い＞

＜古典的コンピュータ＞

・量子コンピュータをシミュレートできない。 ⇒ 計算が人間中心主義である。

＜量子コンピュータ＞

・古典的なコンピュータをシミュレートできる。
・古典的な計算すべては、量子コンピュータで実行できる。 ⇒ 計算が人間を中心としてはいない。

計算はすべて量子コンピュータで実行でき、量子計算は真のパラダイムシフトを表す。

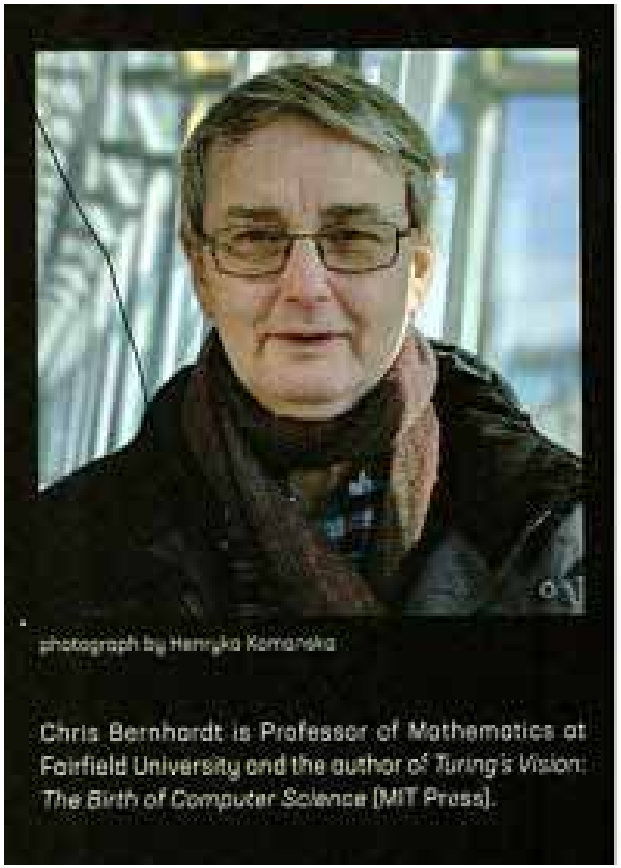
最後に

私たちが新しい方法を使い、新しいものを構築できるかを実験し確認することで、パラダイムシフトはこれからも起こるだろう。

今こそ探求と革新のときである!!

量子計算の最高の年は私たちの前にある!!

編集



「令和３年度電子デバイス工学特論
実行委員会」

担当　岡田　裕之

(第2.718版　2021.7.8)