

量子コンピュータって何？

ITCL研究会

2018年5月24日

高橋哲夫

報道

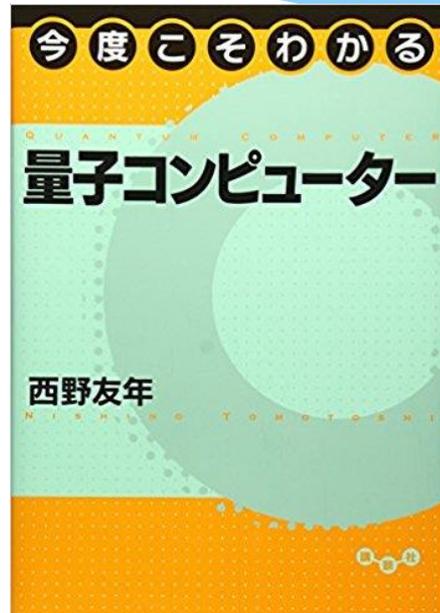
最近、量子コンピュータが新聞をにぎわしている

- 量子コンピュータって何？という素朴な疑問に答える
[量子コンピュータって何？毎日新聞2017年12月10日](#) まるで禅問答！
- 世界の研究機関・企業の動向を伝える
 - D-Wave Systems社は
「世界初の商用量子コンピュータ」D-Wave Oneを発表。2011年5月11日
https://ja.wikipedia.org/wiki/D-Wave_Systems#/
 - 量子コンピュータ市場を狙うIBM-慶大や日本企業も高い関心 2018年3月28日
<https://japan.zdnet.com/article/35116732/>
 - [グーグル、新チップで挑む量子コンピュータ2018年3月18日](#)
 - [量子コンピューター、巻き返しへ本腰 NECや富士通2018年1月22日](#)
 - [「スパコン超え」国産コンピューター2017年12月10日](#)
 - [量子ニューラルネットワークをクラウドで体験2017年11月20日](#)

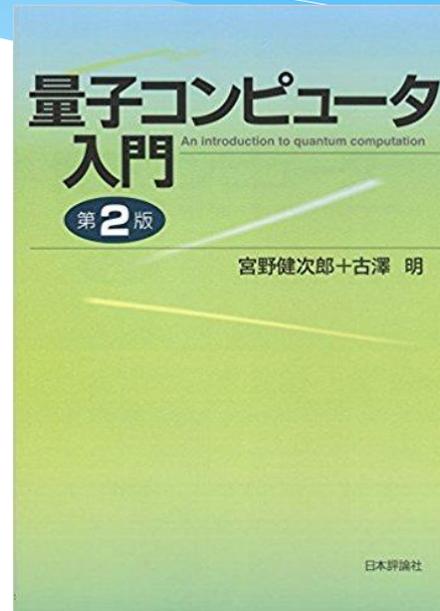
本を購入



アマゾンの評価:あまりよくない。
私の評価:読み返してだんだん良くなった。



アマゾンの評価:
専攻する学生は高評価
私の評価:大変良い。



アマゾンの評価:すこぶる高い
私の評価:これから。多分アマゾンの評価になる？



アマゾン評価:レビュー数が34と多く、高評価
私の評価:分かり易い良書

一般向けの量子コンピュータ関連の本を眺めていると、肝心のところが雲の向こう・・・

量子コンピュータの歴史

- 1900年 熱放射の理論、エネルギー量子の発見 マックス・プランク
- 1921年 光電効果の解明 アインシュタイン
- 1924年 物質波(あらゆる物質は波の性質をもつ)仮説 ド・ブロイ
- 1925年 ハイゼンベルクの運動方程式(粒子的な量子像、行列力学) ヴェルナー・ハイゼンベルク
- 1926年 シュレディンガー方程式(波動的な量子像、波動力学) エルヴィン・シュレディンガー
- 1927年 量子力学の数学的基礎 フォン・ノイマン
(ヒルベルト空間上でハイゼンベルクの運動方程式≡シュレディンガー方程式を明らかにした)
- 1929年 エルミート関数作用素の一般固有値理論 フォン・ノイマン
(この論文で量子力学の数学的理論を確立)
- 1980年 量子を使ったチューリング・マシンの理論と可能性 ポール・ベニオフ
- 1982年 「量子の世界のシミュレーションは量子の理屈で動くコンピュータが必要」 リチャード・ファイマン
(量子コンピュータを構想)
- 1985年 量子コンピュータの計算モデル(量子回路)を考案 デイヴィット・ドイチュ
- 1992年 ドイチュ=ジョサのアルゴリズムを考察 デイヴィット・ドイチュとリチャード・ジョサ
- 1993年 万能量子チューリング・マシン ウメシュ・バジュ、イーサン・バーンシュタイン
- 1994年 ショアのアルゴリズム(素因数分解) ピーター・ショア
- 1996年 グローバーのアルゴリズム(データ探索) ロブ・グローバー
- 1998年 ・量子コンピュータ用プログラミング言語 QCL ベルンハルト・オマール
・量子アニーリング法 西森秀稔、門脇正史

なぜ量子コンピュータなのか

1. 古典コンピュータの限界

- 超高性能コンピュータを必要とするアプリケーション領域の出現
- ムーアの法則がそろそろ限界
- エネルギー消費が膨大

2. 超高性能コンピュータを必要とするアプリケーション領域

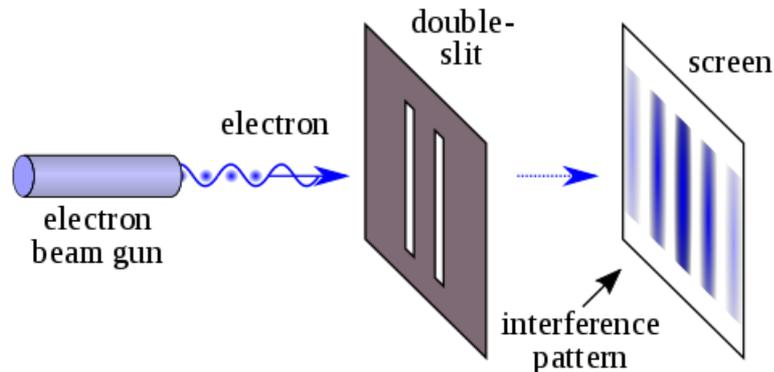
- 組み合わせ最適化
巡回セールスマン問題、渋滞を回避するルート、創薬 など
- 素因数分解
- ビッグデータ、機械学習

3. 理論的には古典コンピュータを実現できるのだそうである

⇒ 将来のコンピュータは量子コンピュータになるかもしれない

量子とは？

- 原子や分子、電子などと同様のモノではない。
- エネルギー量の最小単位
- 光や電子は粒子や波の性質を持つ。



Wikipedia 二重スリット実験

電子銃から電子を1発ずつ発射して、向こう側の乾板に到達させる。電子の通り道に2本のスリットがある衝立を置く。乾板には電子による感光で濃淡の縞模様が描かれる。電子が波の性質を持っている証である。

量子とは？

重ね合わせ



発射時と着弾時には粒子状態だが、飛んでいるときはもやもや状態。

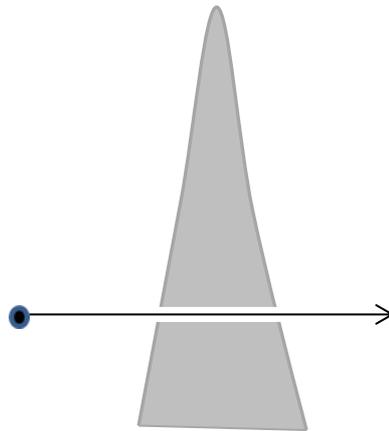
1つの電子が発射されると、複数の存在確率を持った電子になって、重ね合わさって存在している。(コペンハーゲン解釈)

量子コンピュータは重ね合わせの状態を利用して超並列計算を行なう。

量子とは？

トンネル効果

エネルギーの壁



トンネル効果

粒子がわずかな確率で壁(超えるべきエネルギー)の向こうに染み出して仕舞う現象

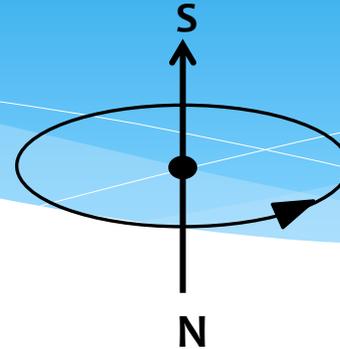
量子を取り出す候補

- * 電子スピン
- * 光の偏光
- * 磁束
- * エネルギー準位
- * 超伝導の位相
- * 超伝導の電荷
- * 原子核スピン

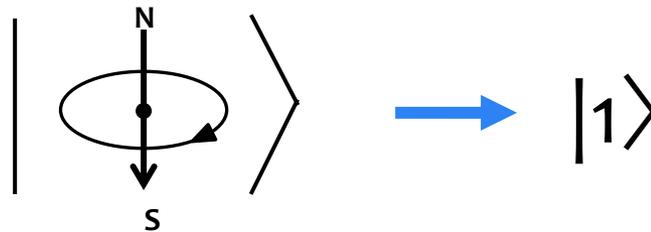
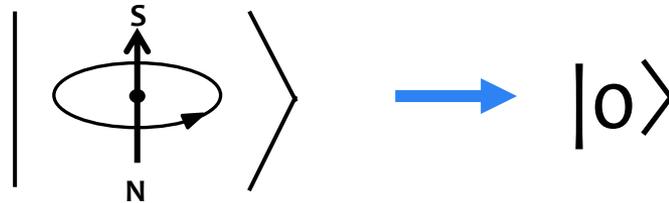
「電子情報技術の潮流」 独立行政法人科学技術振興機構 より

電子スピンによる量子ビット

電子はスピンしている小さな磁石である



電子の状態を“|”と“>”で囲んだケット記号で表わす



重ね合わせ

量子ビットは次の3つの状態をとる。

$|\psi\rangle = |0\rangle$ ブロッホ球(下図)のS極

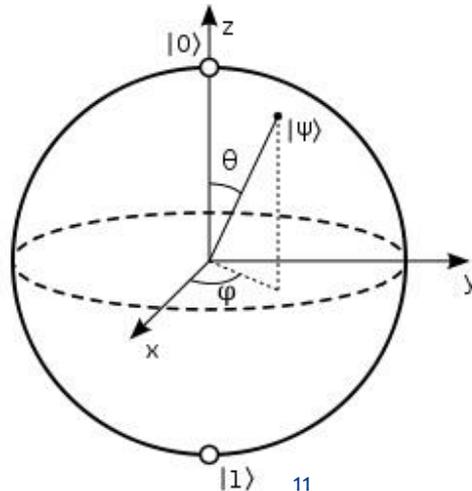
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

α 、 β は複素数で確率振幅という。 $|\alpha|^2 + |\beta|^2 = 1$

ブロッホ球面の任意の場所

$|\psi\rangle = |1\rangle$ ブロッホ球のN極

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ は $|0\rangle$ と $|1\rangle$ との重ね合わせを表わす。
観測すると $|0\rangle$ か $|1\rangle$ に収束する。



エンタングルメント 量子もつれ

どのような仕組みか説明できないらしいが、2つの光子や電子が絡まった状態が存在する。しかし、この状況を完全に記述する数学が存在する。数学的には、複数の量子ビットで表わされる量子状態がそれらを構成する個々の量子ビットの量子状態の単純な積で表せない時に存在。例えば、2量子ビットの量子状態が、2つの独立した1量子ビットの量子状態で表せない場合。つまり、2つのq-bitの直積にならない。

$$\Phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle_1 + \beta|1\rangle_1)(\gamma|0\rangle_2 + \delta|1\rangle_2)$$

(α , β , γ , δ をどうとつてもイコールにならない)

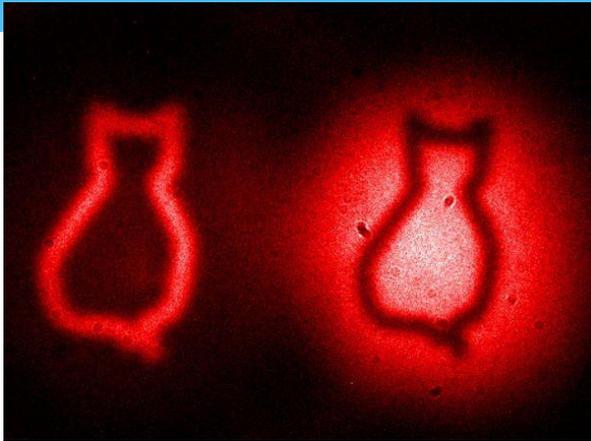
1番目の量子ビットを操作すると2番目の量子ビットに影響が出る。つまり、量子ビットは独立ではない状態。2量子ビットの場合をベル状態という。

GHZ状態: n 桁 ($n \geq 3$) の重ね合わせ状態で、

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\dots 0\rangle + |11\dots 1\rangle)$$

で与えるものをいう。

「量子もつれ」を視覚的に実証



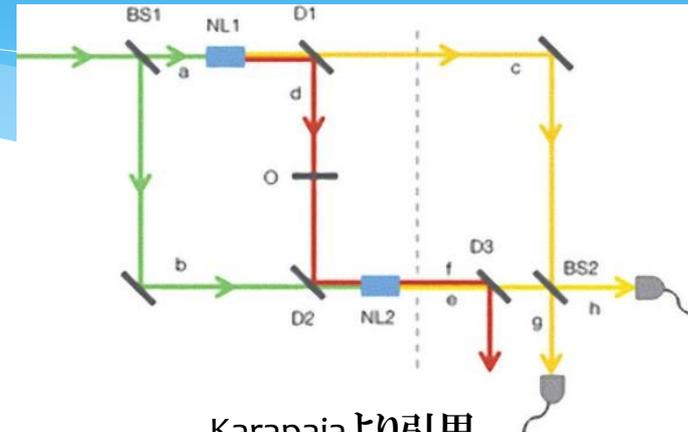
Photograph by Gabriela Barreto Lemos

オーストリアのウィーンの量子光学及び量子情報研究所のガブリエラ・バレット・レモス (Gabriela Berreto Lemos) 氏を中心とする研究チームがこのほど発表した実験では、対象物に当たっていない光の粒子(光子)が、小さな猫の画像を映し出している。

「Nature」誌のオンライン版の8月27日付けに掲載

日経BP記事2014.08.28より引用

<http://natgeo.nikkeibp.co.jp/nng/article/news/14/9651/>



Karapaiaより引用

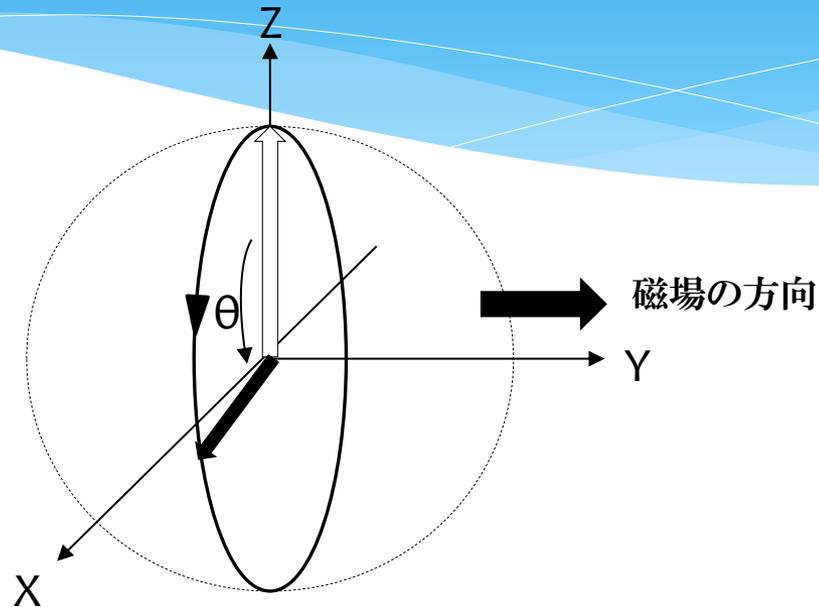
緑のレーザービームをスプリッターで2つに分ける。1つは結晶の中を通過して赤と黄の光子の合わさったものになる。そしてそれぞれに分けられ赤は猫型に切り抜かれたボードにぶつかり、黄色は最後のビームスプリッターに向かう。このスプリッターはその半分の黄色の光子を検出器に送り、残りを別の検出器に送る。

一方、初めに分けられた緑のレーザーの片割れは、猫型を通り抜けた赤と合流する。この赤と緑の光子の組合せは2つ目の結晶にぶつかり、赤と黄色に分けられる。その後赤の光子は除外される。ここに、最初に分かれた緑色レーザー由来の黄色い線の光と合流させ最後のスプリッターに通し2つの検出器に向かって分れる。

検出器では、研究者は猫の画像を見ることができた。

量子ビットの操作

1) 初期の量子ビット: S極 (Z方向) を向いている状態とする



2) Y軸方向に磁場をかけると量子ビットはX-Z平面をぐるぐると回る。

3) 一定時間かけると角度 θ を回る。

この性質を利用して、ブロッホ球上の任意の位置の量子ビットを操作する。

ブラ記号・共役・内積

量子力学による表現の追記

* ブラ記号

状態を表わす記号として、ケット記号 $|\psi\rangle$ に対応するブラ記号 $\langle\psi|$ を導入する。

この対応関係は共役である。

$$\langle\psi| = (|\psi\rangle)^\dagger = (\alpha|0\rangle + \beta|1\rangle)^\dagger = (\alpha|0\rangle)^\dagger + (\beta|1\rangle)^\dagger = \alpha^* \langle 0| + \beta^* \langle 1| \quad (\dagger \text{はダガー})$$

α, β は複素数 α^* は α の共役、 β^* は β の共役

例 $\langle 0| = (|0\rangle)^\dagger$ $\langle 1| = (|1\rangle)^\dagger$

* 内積

ブラ $\langle\Phi|$ とケット $|\psi\rangle$ をくっ付けたもの $\langle\Phi|\psi\rangle$ は数を与える。これを内積という。

内積は実数あるいは複素数である。

例 $\langle 0|0\rangle = 1, \langle 0|1\rangle = 0, \langle 1|0\rangle = 0, \langle 1|1\rangle = 1$

$$\langle 0|\psi\rangle = \langle 0|(\alpha|0\rangle + \beta|1\rangle) = \alpha\langle 0|0\rangle + \beta\langle 0|1\rangle = \alpha$$

$$\langle 1|\psi\rangle = \langle 1|(\alpha|0\rangle + \beta|1\rangle) = \alpha\langle 1|0\rangle + \beta\langle 1|1\rangle = \beta$$

例 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, |\Phi\rangle = \gamma|0\rangle + \delta|1\rangle$ とすると、内積 $\langle\Phi|\psi\rangle$ は、
 $\langle\Phi|\psi\rangle = (\gamma^*\langle 0| + \delta^*\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = \gamma^*\alpha + \delta^*\beta$ である。

同じ状態の内積 $\langle\psi|\psi\rangle$ をノルムという。

※ブラとケットを合わせてbracket

演算子

パウリ演算子 $\hat{\sigma}_x$, $\hat{\sigma}_y$, $\hat{\sigma}_z$

$\hat{\sigma}_x$, $\hat{\sigma}_y$, $\hat{\sigma}_z$ はそれぞれX軸、Y軸、Z軸の周りを回転

$$\hat{\sigma}_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad \hat{\sigma}_y = i|1\rangle\langle 0| - i|0\rangle\langle 1|, \quad \hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

例 $|0\rangle$ にパウリ演算子を操作

$$\hat{\sigma}_x |0\rangle = (|1\rangle\langle 0| + |0\rangle\langle 1|) |0\rangle = |1\rangle\langle 0|0\rangle = |1\rangle$$

$$\text{(ただし、} \langle 0|0\rangle = 1, \langle 0|1\rangle = 0, \langle 1|0\rangle = 0, \langle 1|1\rangle = 1 \text{)}$$

$\hat{\sigma}_x$ によって、状態 $|0\rangle$ が180度回転して $|1\rangle$ になっている

アダマール演算子 \hat{H}

座標軸以外の方向を向いた軸の周りを回転

$$\hat{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|)$$

例 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ としたとき、

$$\begin{aligned} \hat{H}|\psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|)(\alpha|0\rangle + \beta|1\rangle) \\ &= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle \end{aligned}$$

測定

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ を始状態とする実験で、終状態として $|0\rangle$ か $|1\rangle$ かを区別する測定を行う。測定後、元の $|\psi\rangle$ は消滅する。

同じ始状態が何度でも用意できる場合、用意される度に測定を繰り返すと、測定確率は、

確率 $P_0 = |\alpha|^2 = \alpha^* \alpha$ で終状態 $|0\rangle$ が測定される

確率 $P_1 = |\beta|^2 = \beta^* \beta$ で終状態 $|1\rangle$ が測定される

測定演算子としては例えば、 $\hat{M}_0 = |0\rangle\langle 0|$, $\hat{M}_1 = |1\rangle\langle 1|$ とすると、

$$\hat{M}_0 |\psi\rangle = |0\rangle\langle 0| (\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle\langle 0|0\rangle + \beta|0\rangle\langle 0|1\rangle = \alpha|0\rangle$$

$$\hat{M}_1 |\psi\rangle = |1\rangle\langle 1| (\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle\langle 1|0\rangle + \beta|1\rangle\langle 1|1\rangle = \beta|1\rangle$$

\hat{M}_0 、 \hat{M}_1 を射影演算子という。

ゲートと回路

- 始状態

$|\psi\rangle$ ———

- 測定

————— \hat{M} , $|\psi\rangle$ ——— \hat{M}

- パウリ演算子 $\hat{\sigma}_x$, $\hat{\sigma}_y$, $\hat{\sigma}_z$ に対応するゲート

————— \hat{X} ——— \hat{Y} ——— \hat{Z} ———

$$\begin{aligned} \hat{X} &: \hat{\sigma}_x = |1\rangle\langle 0| + |0\rangle\langle 1| & \hat{\sigma}_x|0\rangle &= |1\rangle & \hat{\sigma}_x|1\rangle &= |0\rangle \\ \hat{Y} &: \hat{\sigma}_y = i|1\rangle\langle 0| - i|0\rangle\langle 1| & \hat{\sigma}_y|0\rangle &= i|1\rangle & \hat{\sigma}_y|1\rangle &= -i|0\rangle \\ \hat{Z} &: \hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1| & \hat{\sigma}_z|0\rangle &= |0\rangle & \hat{\sigma}_z|1\rangle &= -|1\rangle \end{aligned}$$

- アダマールゲート \hat{H}

————— \hat{H} ———

$$\hat{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|)$$

ゲートと回路_{その2}

- 制御ユニタリー・ゲート \hat{U} がパウリ演算子

2つの量子ビット

1つ目の量子ビット:制御ビット

これに作用する射影演算子 $|0\rangle_1\langle 0|$ と $|1\rangle_1\langle 1|$

2つ目の量子ビット:ターゲット・ビット

これに作用する恒等演算子 \hat{I} またはユニタリー演算子 \hat{U}

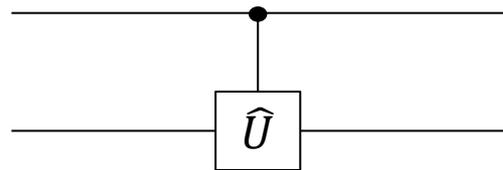
これらを組み合わせた

$$\hat{G} = |0\rangle_1\langle 0|\hat{I}_2 + |1\rangle_1\langle 1|\hat{U}_2$$

を制御 \hat{U} ゲートという。その回路図は下記。

制御ビット

ターゲット・ビット



ゲートと回路 その3

- 制御NOTゲート \hat{U} がパウリ演算子 $\hat{\sigma}_X$ のケース

$$\hat{G} = |0\rangle_1 \langle 0| \hat{I}_2 + |1\rangle_1 \langle 1| \hat{\sigma}_{X2}$$

この演算子が表わす量子ゲートを制御NOTゲート or C-NOTゲートという。
計算基底 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ への作用は次の通り。

$$\hat{G}|00\rangle = |0\rangle_1 |0\rangle_2$$

$$\hat{G}|01\rangle = |0\rangle_1 |1\rangle_2$$

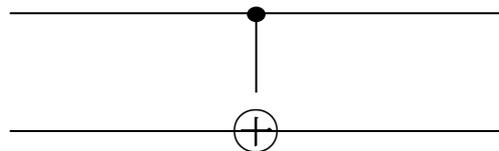
$$\begin{aligned} \hat{G}|10\rangle &= (|0\rangle_1 \langle 0| \hat{I}_2 + |1\rangle_1 \langle 1| \hat{\sigma}_{X2}) |1\rangle_1 |0\rangle_2 \\ &= |1\rangle_1 \hat{\sigma}_{X2} |0\rangle_2 = |1\rangle_1 |1\rangle_2 \end{aligned}$$

$$\hat{G}|11\rangle = |1\rangle_1 \hat{\sigma}_{X2} |1\rangle_2 = |1\rangle_1 |0\rangle_2$$

制御ビットが $|1\rangle$ のときターゲット・ビットを反転させている。
その回路図は下記。

制御ビット

ターゲット・ビット



⊕は $\hat{\sigma}_{X2}$ のこと

量子プログラミング言語

量子プログラミング言語 蓮尾一郎 星野直彦 情報処理 vol55 No.7 July2014 より

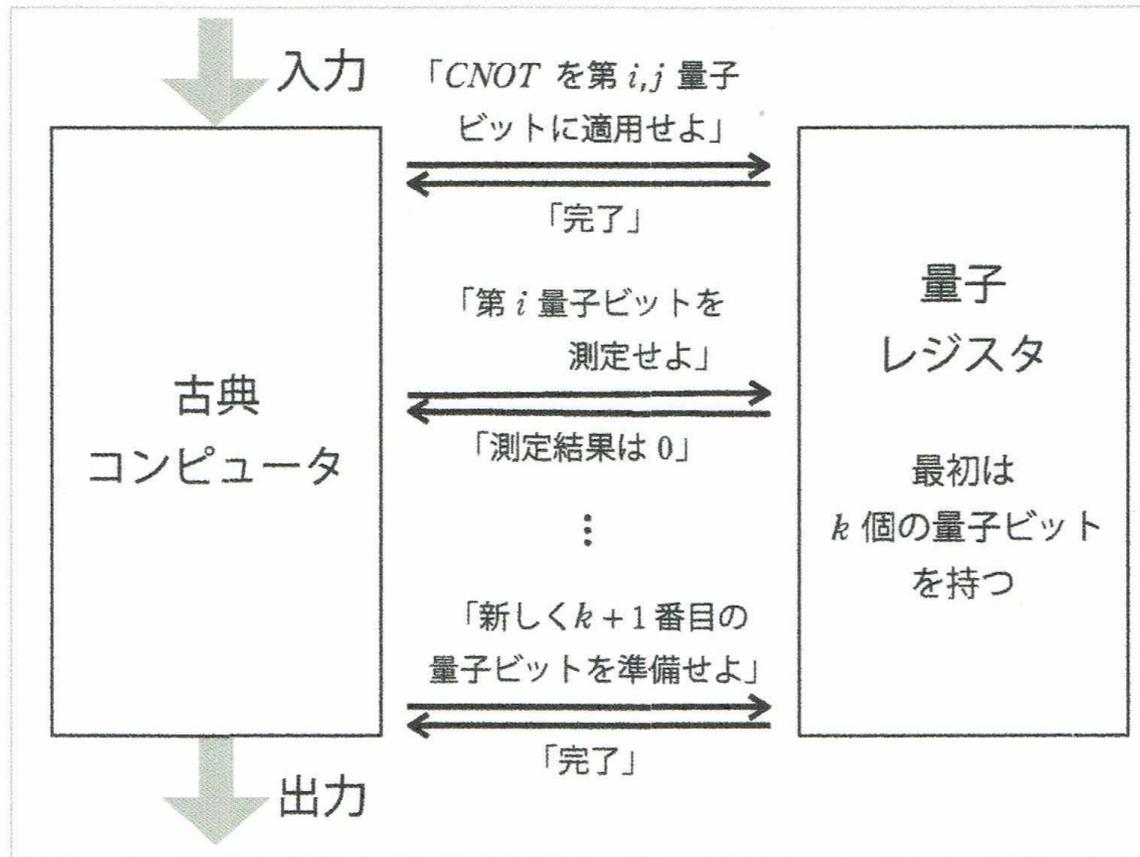


図-2 Knill の QRAM モデル Quantum Random Access Machine

量子プログラミング言語

量子プログラミング言語 蓮尾一郎 星野直彦 情報処理 vol55 No.7 July2014 より

```
procedure deutsch() {
  qureg x[1];           // レジスタの2つの量子ビットを
  qureg y[1];           // それぞれ変数 x, y に割り当て
  int m;
  {
    reset;              // ループ
    U(x,y);             // 量子レジスタをすべて|0>に初期化
    measure y,m;        // ユニタリ変換
  } until m==1;         // y を測定
  measure x,m;          // 測定結果 1 を得るまでくり返し
  print "g(0) xor g(1) =",m; // x を測定. これは
  reset;                // g(0) xor g(1) に一致するはず
                        // 量子レジスタ
}
```

図-3 QCLによる文献7)のアルゴリズム(文献8)による)

7) Deutsch,D. :The Church-Turning Principle and the universal Quantum Computer, Proceedings of the Royal Society of London A, Vol.400(1818):pp.97-117(2013)

8) Omer,B. : Structured Quantum Programming. PhD Thesis, Institute of Theoretical Physics, Technical University of Vienna(2000)

量子プログラミング言語

量子プログラミング言語 蓮尾一郎 星野直彦 情報処理 vol55 No.7 July2014 より

```
alice :: Qubit -> Qubit -> Circ (Bit, Bit)
alice q a = do
  a <- qnot a `controlled` q    // CNOT ゲートを適用
  q <- hadamard q
  (x,y) <- measure (q,a)
  return (x,y)

bob :: Qubit -> (Bit, Bit) -> Circ Qubit
bob b (x,y) = ...              // 略

teleport :: Qubit -> Circ Qubit
teleport q = do
  (a,b) <- bell100             // Bell 状態
  (x,y) <- alice q a
  b <- bob b (x,y)
  return b
```

4) Green, A., Lumsdaine, P., Ross, N., Selinger, P. and Valiron, B.: Quipper: A Scalable Quantum Programming Language, PLDI 2013:333-342(2013)

図-4 Quipper による量子テレポーテーション (文献4) による

$$\begin{aligned} \mathbf{EPR} &= \lambda s. \mathbf{CNOT} \langle H(\mathit{new} 0), \mathit{new} 0 \rangle \\ \mathbf{BellMeas} &= \lambda q_2. \lambda q_1. \mathit{let} \langle x, y \rangle = \mathbf{CNOT} \langle q_1, q_2 \rangle \mathit{in} \langle \mathit{meas}(Hx), \mathit{meas} y \rangle \\ \mathbf{U} &= \lambda q. \lambda (b_1, b_2). \mathit{if} b_1 \mathit{then} (\mathit{if} b_2 \mathit{then} U_{11}q \mathit{else} U_{10}q) \\ &\quad \mathit{else} (\mathit{if} b_2 \mathit{then} U_{01}q \mathit{else} U_{00}q) \\ \mathbf{telep} &= \mathit{let} \langle x, y \rangle = \mathbf{EPR} * \mathit{in} \\ &\quad \mathit{let} f = \mathbf{BellMeas} x \mathit{in} \\ &\quad \mathit{let} g = \mathbf{U} y \\ &\quad \mathit{in} \langle f, g \rangle \end{aligned}$$

5) Selinger, P. and Valiron, B.: A Lambda Calculus for Quantum Computation with Classical Control, Mathematical Structures in Computer Science 16(3):527-552(2006)

図-5 文献5) の量子ラムダ計算による量子テレポーテーション

量子コンピュータによる解は確率的

古典コンピュータは決定論的だが、量子コンピュータは確率的。

量子コンピュータは、量子力学を用いた量子回路を設計し、何度も試して、命題の正しさを確率的に検証する。

ショアのアルゴリズムの量子回路

因数分解したい数を n とする。簡単のため n は2つの素数の積 $n=pq$ のケースとする。この因数分解のアルゴリズムは次のように考えることができる。

1. $\{1, 2, \dots, n\}$ からランダムに1つを選び、その数を a とする。
2. $\gcd(a, n) = 1$ なら3. へ。 $\gcd(a, n) \neq 1$ なら1. へ。
3. a の $\text{mod } n$ に関する位数 r を求める。(= 量子コンピュータによる)
4. 得られた位数が偶数なら5. へ。奇数なら1. へ。
5. $p' = \gcd(a^{r/2} + 1, n)$ と $q' = \gcd(a^{r/2} - 1, n)$ を求める。
6. p', q' のいずれかが n なら1. へ。それ以外ならば p, q が求める因数。

$a^r \pmod n = 1$ を満たす最小の自然数 r を位数という

フェルマの小定理
 a が n の倍数でないとき
 $a^{n-1} \equiv 1 \pmod n$
 が成り立つ。

Shor の素因数分解アルゴリズムにおける計算量の精密な評価数理解析研究所講究録1452 巻2005 年206-214 より

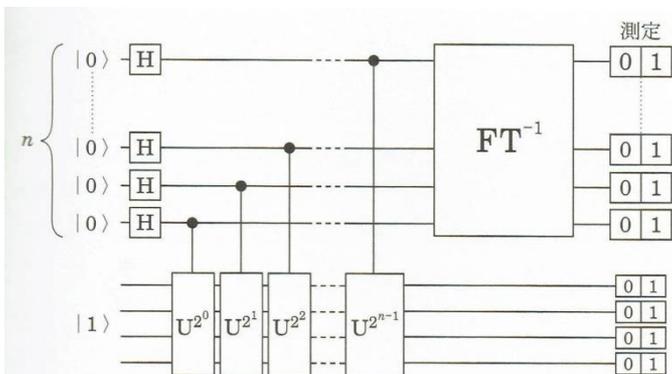


図 5.5 位数を計算する量子回路。図 5.4 の問題レジスタへの入力を $|u\rangle$ の代わりに $|1\rangle$ にしている。また、問題レジスタの測定を行う。

← 位数を求める量子回路

量子コンピュータ入門 第2版 (宮野健次郎+古澤明)より

量子検索

q-bitの並び $|00\dots 00\rangle, |00\dots 01\rangle, \dots, |11\dots 11\rangle$, 即ち $|0\rangle, \dots, |2^n-1\rangle$ なる 2^n 個の計算基底からQ番目の状態を探し出す問題。

検査器 $\hat{U}_Q = \hat{I} - |Q\rangle\langle Q|$ (演算子)

$$\hat{U}_Q |i=Q\rangle = -|Q\rangle$$

$$\hat{U}_Q |j \neq Q\rangle = |j\rangle$$

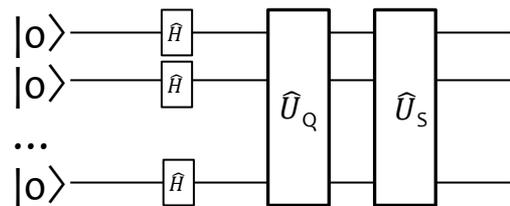
任意の $|i\rangle$ に対して期待値 $\langle i | \hat{U}_Q | i \rangle$ を求める測定を行い、 $i=Q$ の場合-1を得て、その他の場合1を得る。

すべての状態を等しい重みで重ね合わせた状態を

$$|S\rangle = 2^{-n/2} \sum_{i=0}^{2^n-1} |i\rangle \text{ とする。}$$

$|S\rangle$ は量子回路で、 n 個並んだ $|0\rangle$ にアダマールゲート \hat{H} を作用させておく。

$$\hat{U}_S = 2|S\rangle\langle S| - \hat{I} \text{ (演算子)}$$



グローバーの検索アルゴリズム

- (0) $|\psi_0\rangle$ を初期状態として用意
- (1) $\hat{U}_Q \hat{U}_S$ を作用させて
 $|\psi_1\rangle = \hat{U}_Q \hat{U}_S |\psi_0\rangle$ を作る
- (2) $\hat{U}_Q \hat{U}_S$ を作用させて
 $|\psi_2\rangle = \hat{U}_Q \hat{U}_S |\psi_1\rangle$ を作る
---以下同様---
- (m) 「適当な回数m」だけ繰り返すと
 $|\psi_m\rangle \approx |Q\rangle$ が成立する
- (m+1) $|\psi_m\rangle$ を射影測定して $|Q\rangle$ を知る

※何回繰り返せば良いかは計算できる

量子コンピュータのタイプ

- * 量子ゲート

汎用的でいかなる量子計算もできる。

量子イジングモデルでできる計算は本方式でもできるが、現時点では実用的な性能がでない。

量子ゲート:

アダマールゲート(\hat{H})、ユニタリーゲート(\hat{U})、制御NOTゲート(CNOT) など

- * 量子イジングモデル

既に商用レベルの実機がある

組合せ最適化問題以外は解けない

- 量子アニーリング方式

D-Wave社 ※NECも2023年度までに開発予定

- 量子ニューラルネットワーク

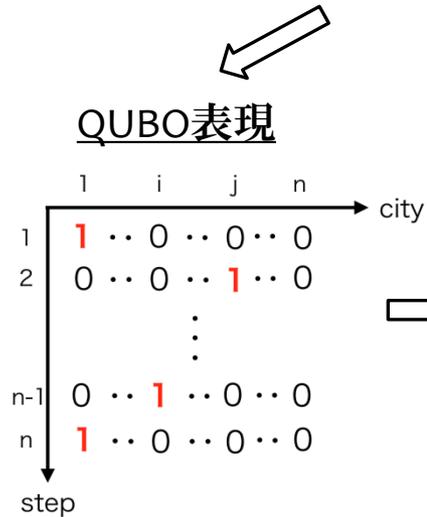
NTT QNN クラウドで公開

量子アニーリング方式

組み合わせ最適化問題に特化した方式

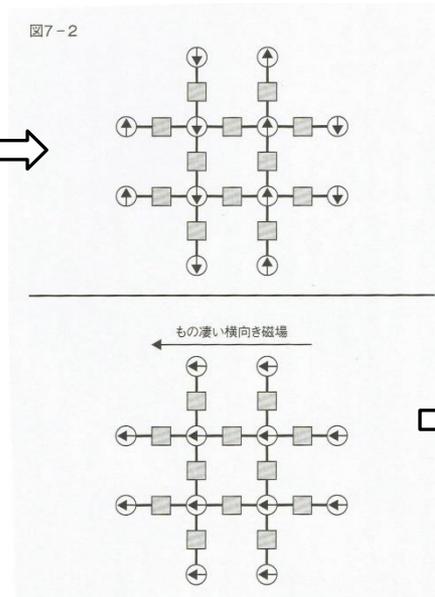
例 巡回セールスマン問題:セールスマンが複数の都市をそれぞれ1回だけ訪問する最短距離を求める。

都市の数を n とし、都市 i と j 間の距離を c_{ij} とすると、全ての都市を1回だけ訪問するときの距離 (目的関数) は $C = \sum_{i \neq j} c_{ij} x_{ij}$ である。

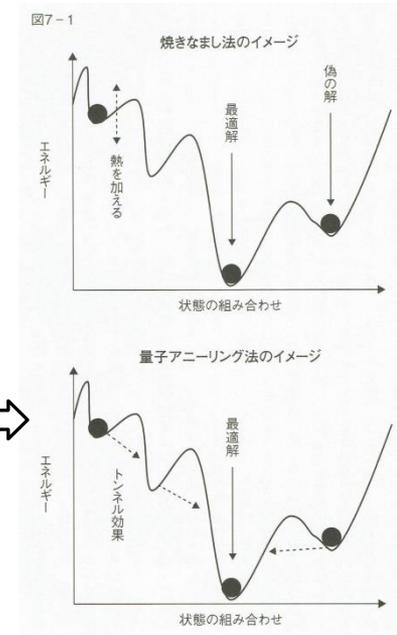


Quadratic unconstrained binary optimization (QUBO) is a pattern matching technique.

イジングモデル



量子アニーリング



量子コンピュータの使い道

* 素因数分解 既述

* 量子検索 既述

* 量子暗号

RSAなどの素数を使った暗号は量子コンピュータで解かれてしまうことが分かっている。それでも解読できない暗号を量子を使って作ろうとするのが量子暗号である。

* 組み合わせ最適化

巡回セールスマン問題、渋滞を回避するルート、創薬 など

* AI : 機械学習、ディープラーニング

* ビッグデータ

* 量子シミュレーション

生体、化学物質

量子コンピュータの課題

- * 量子ビットの数 なかなか増やせない
 - IBM 50量子ビット
 - D-Wave 2000 量子ビット 実際には使えるのは1000位といわれている
 - QNN 2000 量子ビット
- * 量子ビットの実現とエンタングルメント
- * 量子ビットの隔離・遮断 と 量子エラーコレクション

- * 特に量子ゲート方式の場合、有効なアプリケーション探し

ムーアの法則の限界を超える

半加算器 (1桁のたし算)

$0+0 = 00$
 $0+1 = 01$
 $1+0 = 01$
 $1+1 = 10$

量子コンピュータ入門 第2版
(宮野健次郎+古澤明)より

古典ゲート

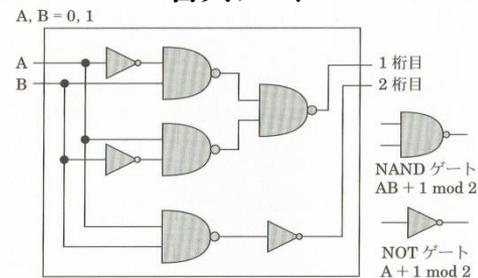


図 5.7 NAND ゲートで構成した半加算器。ただし、NOT ゲートは入力の方方を 1 とした NAND ゲートと考えることができる。

量子ゲート

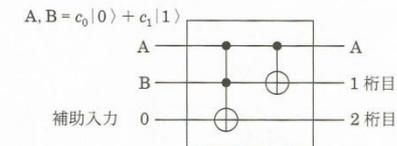


図 5.8 制御 NOT ゲートで構成した半加算器。ただし、左側の制御 NOT ゲートは二つの制御ビットが両方も 1 のときのみビットフリップ²⁷⁾操作を施す。

- 古典ゲートよりも量子ゲートの方がシンプルで圧倒的に速い
- 量子コンピュータは古典コンピュータに比べ消費電力が2桁少なくてできる
- シリコン中の電子スピンを用いた量子コンピュータ開発が進んでいる

☆ 私が期待するのは「古典コンピュータに代わって量子コンピュータにやらせる」
しかし、“量子コンピュータが人工知能を加速する”の著者西森秀稔・大関真之氏は本の「あとがき」で、それは「壮大なむだづかいである」と書いている

学習するには

- [IBM Quantum Computingで計算してみよう](#)
- [量子コンピュータ授業\(慶応大学\)](#)
- [All about Quantum 伊藤公平先生登壇](#)
<https://www.ibm.com/events/think/watch/playlist/244632/replay/113753028/>
26分20秒の辺り
- [日本生まれの量子コンピュータ - NTTがクラウドシステムとして一般に公開](#)
- [QNNCloudを試してみた](#)
[Quantum Neural Network](#)
- [S.Jordan:Quantum Algorithm Zoo](#)
300以上の量子アルゴリズム
<http://math.nist.gov/quantum/zoo/>