工学者のための量子計算
基礎の基礎

慶應義塾大学理工学部
物理情報工学科

伊藤公平

目次

量子コンピュータとは何か？を学部レベルの知識でも理解できるよう説明し，量子コンピュータ開発にむけていかなる工学技術が必要か考える機会を提供する．

参考文献

本講義の内容は，最終章を除いて，以下の3冊の本の内容をまとめたものです．

1. 上坂吉則　量子コンピュータの基礎数理」コロナ社
2. ゲナディ・P・ベルマン，ゲーリー・D・ドーレン，ロンニエ・マイニエリ，ウラジミール・I・チフリノビッチ　「入門　量子コンピュータ」 訳 松田和典，パーソナルメディア社
3. Michael A. Nielsen and Isaac L. Chuang, “Quantum Computation and Quantum Information,” Cambridge University Press

計算のリソース

問題：N個の正整数を大きい順に並べる.

★古典的コンピュータ

最低　$L \approx N \log_2 N$ ステップ必要

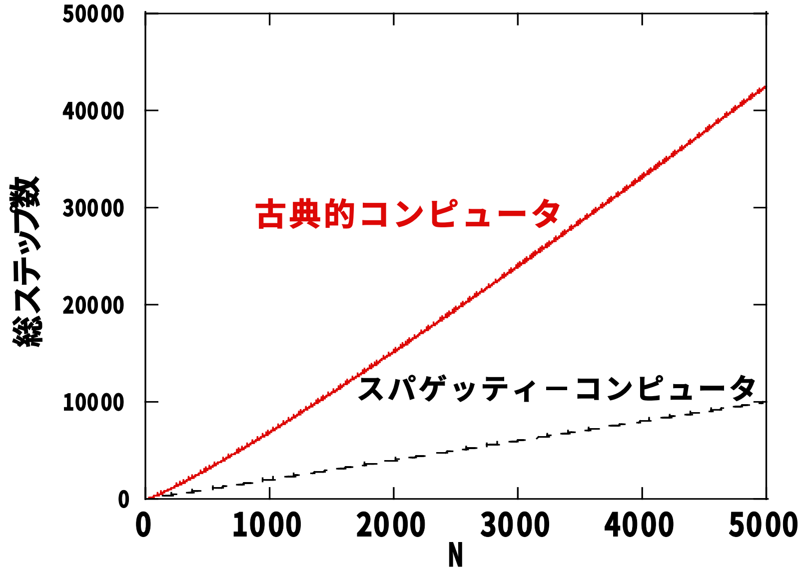
★スパゲッティー コンピュータ[西野哲朗 中国人郵便配達問題=コンピューサイエンス最大の難関，講談社(1999)]

スパゲッティーをN本用意し，正整数の大きさに切る（Nステップ）

束ねて机の上に立てる（ステップ）

長い順に取り出し机に並べる（Nステップ）

以上の総ステップ数は2N+1



なぜ，スパゲティーコンピュータ
は効率が良いのか？

量子コンピュータとは

時間に依存する
波動関数

$$i\hbar\frac{d\Psi}{dt}=H\Psi \qquad H=-\frac{\hbar}{2m}\left(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}+\frac{\partial^2}{\partial z^2}\right)+V(x,y,z) \tag{1}$$

Hが時間に対して不変の
場合 緩和時間が長い)

$$\Psi(t)=U(t)\Psi(0)$$

$$U(t)=e^{-iHt/\hbar}=I+\frac{(-iHt/\hbar)}{1!}+\frac{(-iHt/\hbar)^2}{2!}+\frac{(-iHt/\hbar)^3}{3!}+\cdots \tag{2}$$

ここで$U(t)$はユニタリ行列 $UU^*=I$

Ψをリソースとして，それらに何ステップものユニタリ演算をほどこすのが量子計算

Δt おきにユニタリ演算U を施すと

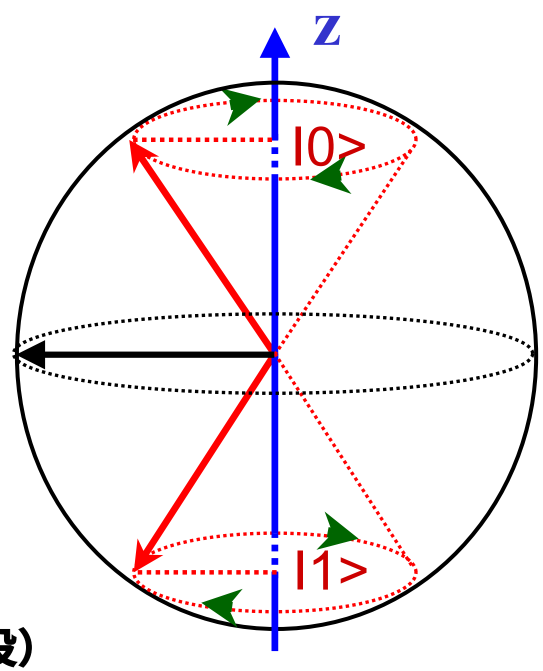
$$\Psi(\Delta t)=U(0)\Psi(0)$$
$$\Psi(2\Delta t)=U(\Delta t)\Psi(\Delta t)$$
$$\Psi(3\Delta t)=U(2\Delta t)\Psi(2\Delta t)$$
$$\vdots$$
$$\Psi_n=U_{n-1}U_{n-2}\cdots U_0\Psi_0$$
$$=U'\Psi_0$$

有限空間で考えると

Ψ を有限次元空間に属するベクトルと仮定する

$$\left.\begin{aligned} e_0 &= |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ e_1 &= |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{aligned}\right\} \text{基底}$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$



$$\boxed{\begin{aligned} \Psi(t) &= a(t)e_0 + b(t)e_1 \\ &= a(t)|0\rangle + b(t)|1\rangle \\ H &= -\hbar\omega_0 I^z \\ I^z &= \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned}}$$

I^Z はエルミート行列（複素共役）

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} = A^* = \begin{bmatrix} a_{00}^* & a_{10}^* \\ a_{01}^* & a_{11}^* \end{bmatrix}$$

$$U(t) = e^{-iHt/\hbar} = I + \frac{(-iHt/\hbar)}{1!} + \frac{(-iHt/\hbar)^2}{2!} + \frac{(-iHt/\hbar)^3}{3!} + \cdots \Longrightarrow \quad UU^* = I$$

ユニタリ演算の例（1）

例１ 一量子ビット回転ゲート(NOT演算)

（ユニタリかつエルミート）

$e_0 = \lvert 0 \rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
$e_1 = \lvert 1 \rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
基底

$U_R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ を $\begin{array}{l} \Psi^0 = 1e_0 + 0e_1 = 1\lvert 0 \rangle + 0\lvert 1 \rangle \\ \Psi^0 = 0e_0 + 1e_1 = 0\lvert 0 \rangle + 1\lvert 1 \rangle \end{array}$ にほどこすと

$U_R \lvert 0 \rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \lvert 1 \rangle$ と $U_R \lvert 1 \rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \lvert 0 \rangle$ のように反転（回転）させる．

$$\boxed{U_R \Psi(t) = a(t)\lvert 0 \rangle + b(t)\lvert 1 \rangle = a(t)\lvert 1 \rangle + b(t)\lvert 0 \rangle}$$

U_R はXゲート(I^X)とも呼ばれ重要である。

ディラック記法では、$U_R = \lvert 0 \rangle\langle 1 \rvert + \lvert 1 \rangle\langle 0 \rvert = \begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$\left\{ \begin{array}{l} U_R \lvert 1 \rangle = \lvert 0 \rangle\langle 1 \vert 1 \rangle + \lvert 1 \rangle\langle 0 \vert 1 \rangle = \lvert 0 \rangle \\ U_R \lvert 0 \rangle = \lvert 0 \rangle\langle 1 \vert 0 \rangle + \lvert 1 \rangle\langle 0 \vert 0 \rangle = \lvert 1 \rangle \end{array} \right.$$

$\langle 0 \rvert = \begin{bmatrix} 1 & 0 \end{bmatrix} \quad \langle 1 \rvert = \begin{bmatrix} 0 & 1 \end{bmatrix}$

$\langle i \vert k \rangle = \delta_{ik}$

$U_R \cdot U_R^* = \lvert 0 \rangle\langle 0 \rvert + \lvert 1 \rangle\langle 1 \rvert = I$

ユニタリ演算の例（2）

例２ 二量子ビット制御ノット(controlled NOT)演算 （$2^2\times 2^2$の行列が必要）

（ユニタリかつエルミート）

基底

$$e_0=|00\rangle=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\qquad e_1=|01\rangle=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$e_2=|10\rangle=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\qquad e_3=|11\rangle=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

標的ビット

制御ビット

$$U_{CN}|10\rangle=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=|11\rangle$$

テンソル積

$$|x_1\rangle\otimes|x_2\rangle=\begin{bmatrix}x_{1,0}\\x_{1,1}\end{bmatrix}\otimes\begin{bmatrix}x_{2,0}\\x_{2,1}\end{bmatrix}=\begin{bmatrix}x_{1,0}x_{2,0}\\x_{1,0}x_{2,1}\\x_{1,1}x_{2,0}\\x_{1,1}x_{2,1}\end{bmatrix}=|x_1x_2\rangle$$

$$|0\rangle\otimes|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=|00\rangle$$

まとめると

$$U_{CN}|00\rangle=|00\rangle,\quad U_{CN}|01\rangle=|01\rangle,$$

$$U_{CN}|10\rangle=|11\rangle,\quad U_{CN}|11\rangle=|01\rangle.$$

入力 $\psi_i=a_1|00\rangle+a_2|01\rangle+a_3|10\rangle+a_4|11\rangle$

出力 $\psi_f=U_{CN}\psi_i=a_1|00\rangle+a_2|01\rangle+a_3|11\rangle+a_4|10\rangle$

量子並列性 2準位系の2量子ビットで2^2状態が一度に計算できる。N量子ビットでは2^n状態を並列計算。

$$U_{CN}=|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 11|+|11\rangle\langle 10|$$

$$U_{CN}U_{CN}^*=|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 10|+|11\rangle\langle 11|=I$$

古典演算との違い－可逆性

可逆（古典、量子）

NOT演算

（回転ゲート）

$$b_f = \overline{a_i}$$

$$a_i, b_i = 0,1$$

a_i	b_f
0	1
1	0

不可逆（古典）

AND演算

$$c_f = a_i b_i$$

a_i	b_i	c_f
0	0	0
0	1	0
1	0	0
1	1	1

不可逆（古典）

XOR演算

$$c_f = a_i \oplus b_i = \overline{a_i} b_i + a_i \overline{b_i}$$

a_i	b_i	c_f
0	0	0
0	1	1
1	0	1
1	1	0

可逆（量子）

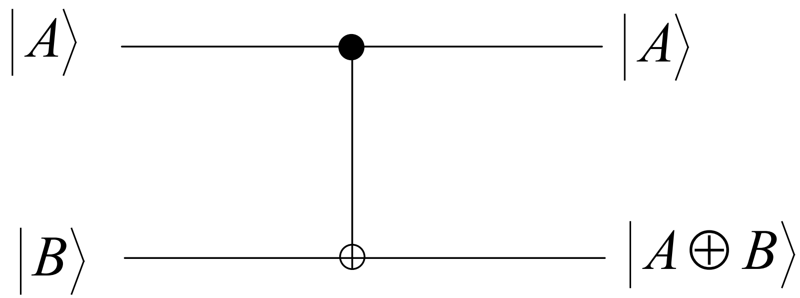
Controlled NOT

制御NOT

$$b_f = a_i \oplus b_i = \overline{a_i} b_i + a_i \overline{b_i}$$

a_i	b_i	a_f	b_f
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

量子回路



量子計算で利用される単一量子ビット操作

Hadamard gate （アダマードゲート）

$$\alpha|0\rangle+\beta|1\rangle \;—\boxed{H}—\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Pauli matrices （パウリ行列）

$$\alpha|0\rangle+\beta|1\rangle \;—\boxed{X}—\; \beta|0\rangle+\alpha|1\rangle$$

$$\alpha|0\rangle+\beta|1\rangle \;—\boxed{Y}—\; i\left(-\beta|0\rangle+\alpha|1\rangle\right)$$

$$\alpha|0\rangle+\beta|1\rangle \;—\boxed{Z}—\; \alpha|0\rangle-\beta|1\rangle$$

$$X=U_R\equiv\begin{bmatrix}0&1\\1&0\end{bmatrix}\qquad Y\equiv\begin{bmatrix}0&-i\\i&0\end{bmatrix}\qquad Z\equiv\begin{bmatrix}1&0\\0&-1\end{bmatrix}$$

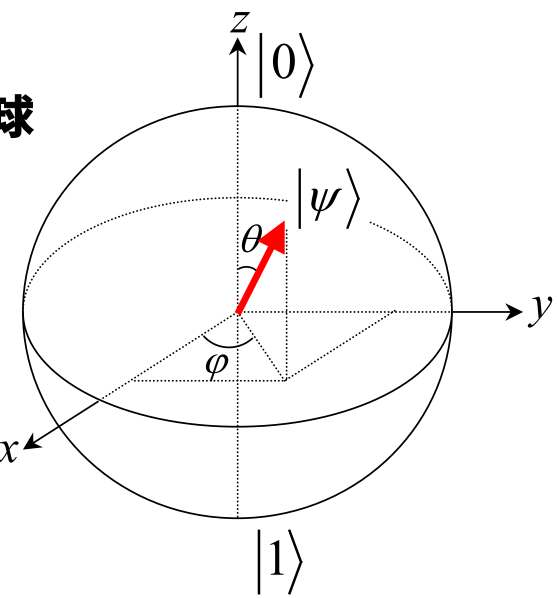
$$H\equiv\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\qquad I\equiv\begin{bmatrix}1&0\\0&1\end{bmatrix}$$

$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle,\quad |\alpha|^2+|\beta|^2=1$ より

$$|\psi\rangle=e^{i\gamma}\left[cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\,sin\frac{\theta}{2}|1\rangle\right]$$

$$|\psi\rangle=cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\,sin\frac{\theta}{2}|1\rangle$$

ブロッホ球

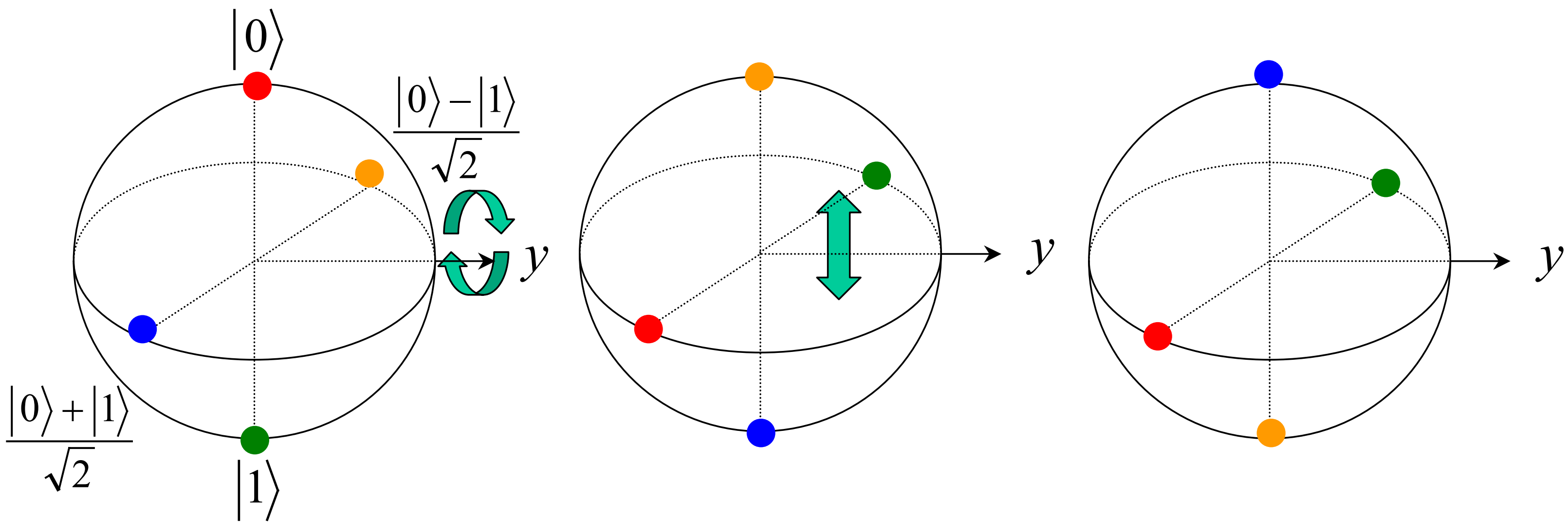


Hadamard gate

$$H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

H looks like a 'square-root of NOT' gate, though H^2 is not a NOT gate.

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad H\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = |0\rangle \quad H\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |1\rangle$$



回転操作

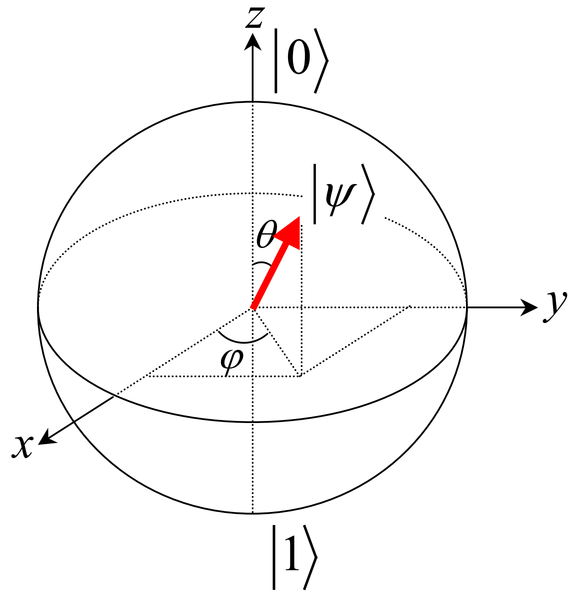
ブロッホ球のx, y, z軸それぞれを中心とした角度θの回転

$$R_x(\theta) \equiv e^{-i\theta X/2} = cos\frac{\theta}{2} I - i\,sin\frac{\theta}{2} X = \begin{bmatrix} cos\frac{\theta}{2} & -i\,sin\frac{\theta}{2} \\ -i\,sin\frac{\theta}{2} & cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = cos\frac{\theta}{2} I - i\,sin\frac{\theta}{2} Y = \begin{bmatrix} cos\frac{\theta}{2} & -sin\frac{\theta}{2} \\ -sin\frac{\theta}{2} & cos\frac{\theta}{2} \end{bmatrix}$$

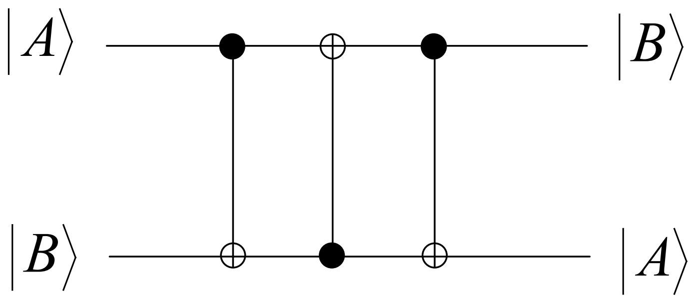
$$R_z(\theta) \equiv e^{-i\theta Z/2} = cos\frac{\theta}{2} I - i\,sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\,sin\frac{\theta}{2}|1\rangle$$

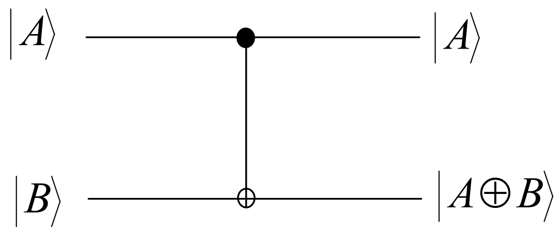


量子計算の例 ⑴ 交換回路

反転した三つの制御NOT



単一制御NOT

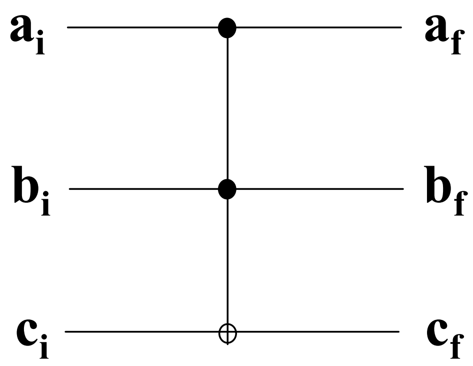


$$
\begin{aligned}
|A,B\rangle &\rightarrow |A, A\oplus B\rangle \\
&\rightarrow |A\oplus(A\oplus B), A\oplus B\rangle = |B, A\oplus B\rangle \\
&\rightarrow |B,(A\oplus B)\oplus B\rangle = |B, A\rangle
\end{aligned}
$$

$$
\begin{aligned}
|1,0\rangle &\rightarrow |1,1\oplus 0\rangle \\
&\rightarrow |1\oplus(1\oplus 0),1\oplus 0\rangle = |0,1\oplus 0\rangle \\
&\rightarrow |0,(1\oplus 0)\oplus 0\rangle = |0,1\rangle
\end{aligned}
$$

量子計算の例（2） 制御制御NOTゲート

制御制御NOT（controlled controlled NOT）



$$a_f = a_i,\quad b_f = b_i$$

$$c_f = \begin{cases} \overline{c_i}, & a_i = b_i = 1 \text{ の場合} \\ c_f & \text{その他} \end{cases}$$

または $c_f = a_i b_i \oplus c_i$

a_i	b_i	c_i	a_f	b_f	c_f
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

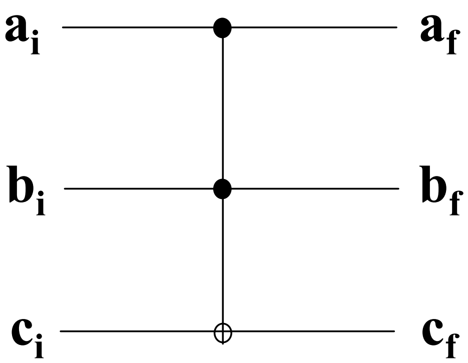
NOTゲート: $a_i = b_i = 1$ の場合 $c_f = \overline{c_i}$

制御NOTゲート: $a_i = 1$ の場合 $b_f = b_i, c_f = b_i \oplus c_i$

ANDゲート: $c_i = 0$ の場合 $c_f = a_i b_i$ 古典計算もできる！

制御制御NOTゲートは3量子ビットゲート

制御制御NOT（controlled controlled NOT）



$$
U_{CCN} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}
$$

$$a_f = a_i, \quad b_f = b_i$$

$$c_f = \begin{cases} \overline{c_i}, & a_i = b_i = 1 \text{ の場合} \\ c_f & \text{その他} \end{cases}$$

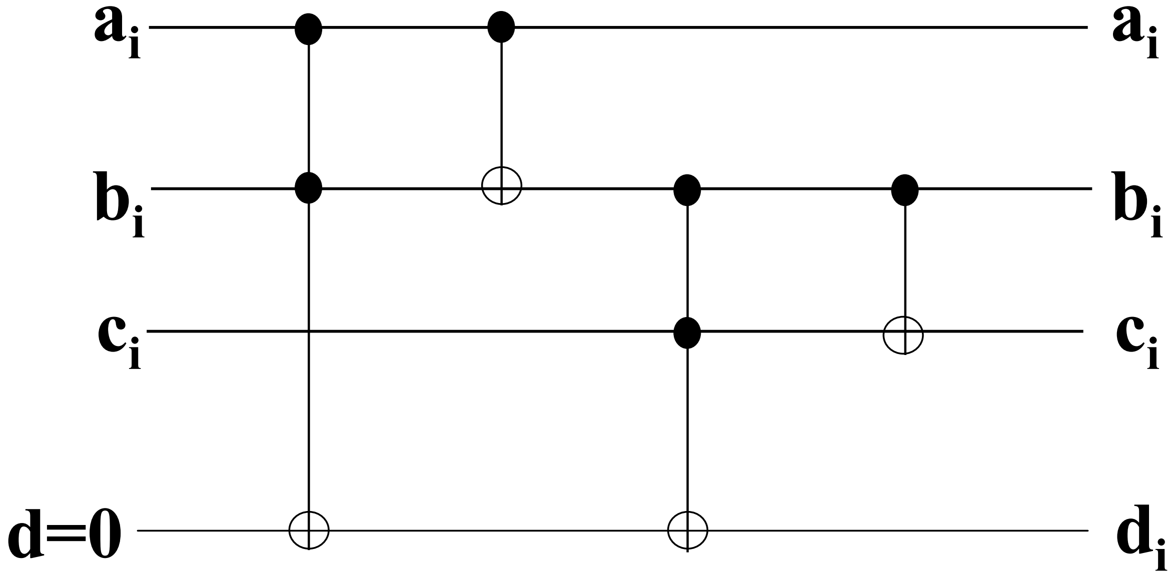
または $c_f = a_i b_i \oplus c_i$

$$
\begin{aligned}
CCN = {} & |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| + \\
& |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 111| + |111\rangle\langle 110|
\end{aligned}
$$

十進数表記で

$$
\begin{aligned}
CCN = {} & |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| + \\
& |4\rangle\langle 4| + |5\rangle\langle 5| + |6\rangle\langle 7| + |7\rangle\langle 6|
\end{aligned}
$$

宿題



この量子回路が加算器であることを示しなさい．

万能ゲートと観測問題

◎ 万能ゲート：すべてのユニタリー変換が、一量子ビット回転ゲート(U_R)と
二量子ビット制御ノットゲート(U_{CN})の組み合わせで実現
できる。または、三量子ビット制御制御ノットゲートのみの
組み合わせでもよい。
　量子並列性と矛盾？ 本来は100量子ビットの量子並列演
算には $2^{100}\times 2^{100}$のユニタリ行列が必要。

◎ 観測問題： 出力 $\psi_f = U_{CN}\psi_i = a_1|00\rangle + a_2|01\rangle + a_3|11\rangle + a_4|10\rangle$ を観測した場合

e_i (|00>, |01>, |10>, |11>) が確率 $\dfrac{|a_i|^2}{|a_1|^2+|a_2|^2+|a_3|^2+|a_4|^2}, \quad i=0,1,2,3$

で観測され、その後、波束はe_iの状態に収束する。
よって、正解の確率振幅を他より増大させる工夫が必要。

量子フーリエ変換（1）

◎入力ベクトルの確率振幅をフーリエ変換した結果が出力ベクトルの確率振幅となる.

$$\begin{cases} \tilde{f}(y) = \int_a^b K(y,x) f(x) dx \text{ で } K(y,x) = e^{-ixy}, a = -\infty, b = \infty \text{ だとフーリエ変換} \\ \tilde{f}(y) = \sum_{x=0}^{N-1} K(y,x) f(x) \text{ が離散フーリエ変換 } f(y) = \sum_{x=0}^{N-1} K^*(y,x) \tilde{f}(x) \text{ が逆変換} \end{cases}$$

量子離散フーリエ変換（ユニタリ変換） $U\left(\sum_{x=0}^{N-1} f(x)|x\rangle\right) = \sum_{y=0}^{N-1} \tilde{f}(y)|y\rangle$

選択的回転変換 $\tilde{f}(y) = \sum_{x=0}^{N-1} e^{i\theta_x} \delta_{xy} f(x) = e^{i\theta_y} f(y)$

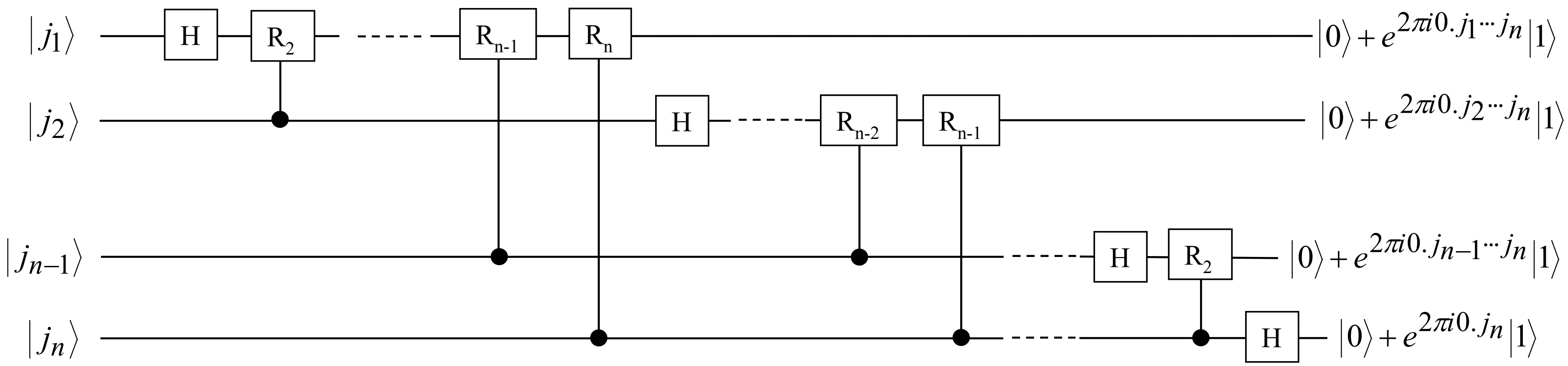
例：Hadamard gate（アダマードゲート）　1量子ビット離散フーリエ変換（可逆）

$$\alpha|0\rangle + \beta|1\rangle \; —\boxed{\mathrm{H}}— \; \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad \mathrm{H} \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle$$

量子フーリエ変換 (2)

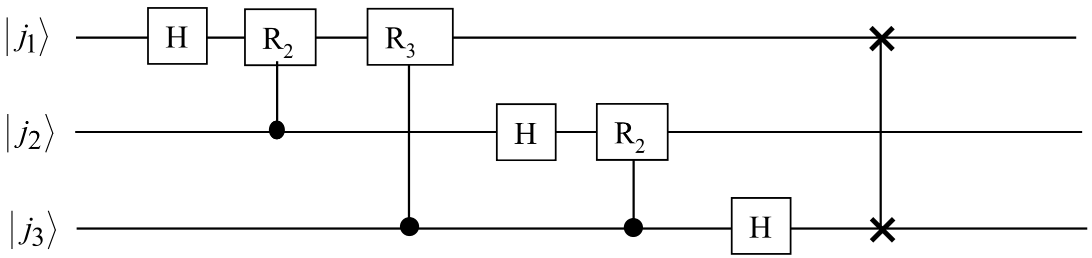
◎　n量子ビット量子フーリエ変換は以下の量子回路で実行できる．



位相ゲート　$R_{|j-k+1|} = |0_j0_k\rangle\langle 0_j0_k| + |0_j1_k\rangle\langle 0_j1_k| + |1_j0_k\rangle\langle 1_j0_k| + \exp\left(\frac{\pi}{2^{k-j}}\right)|1_j1_k\rangle\langle 1_j1_k|$

$$\mathrm{R}_{|j-k|+1} \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^{|j-k|+1}} \end{bmatrix}$$

3キュービット量子フーリエ変換の例



$$\mathrm{R}_2 \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{bmatrix}$$

$$\mathrm{R}_3 \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

入力 $|0\rangle_3 \otimes |1\rangle_2 \otimes |0\rangle_1 \equiv |010\rangle$

Step 1 $H_1|010\rangle = |0\rangle \otimes |1\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{\sqrt{2}}\left(|010\rangle + |011\rangle\right)$

Step 2 $R_{2(1-2)}|\ \ \rangle = R_{2(1-2)}\frac{1}{\sqrt{2}}\left(|010\rangle + |011\rangle\right) = \frac{1}{\sqrt{2}}\left(|010\rangle + \exp\left(i\frac{\pi}{2}\right)|011\rangle\right) = \frac{1}{\sqrt{2}}\left(|010\rangle + i|011\rangle\right)$

Step 3 $R_{3(1-3)}|\ \ \rangle = R_{3(1-3)}\frac{1}{\sqrt{2}}\left(|010\rangle + i|011\rangle\right) = \frac{1}{\sqrt{2}}\left(|010\rangle + i|011\rangle\right)$

Step 4 $H_2|\ \ \rangle = \frac{1}{2}\left\{|0\rangle\left(|0\rangle - |1\rangle\right)|0\rangle + i|0\rangle\left(|0\rangle - |1\rangle\right)|1\rangle\right\} = \frac{1}{2}\left\{|000\rangle - |010\rangle + i|001\rangle - i|011\rangle\right\}$

Step 5 $R_{2(2-3)}|\ \ \rangle = \frac{1}{2}\left\{|000\rangle - |010\rangle + i|001\rangle - i|011\rangle\right\}$

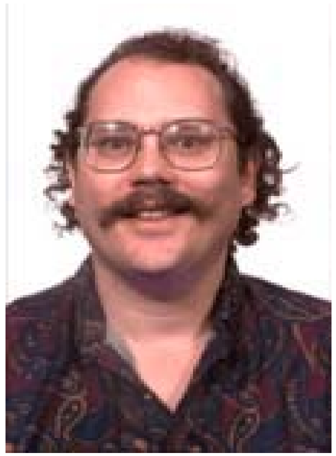
Step 6 $H_3|\ \ \rangle = \frac{1}{\sqrt{8}}\left\{|000\rangle + |100\rangle - |010\rangle - |110\rangle + i|001\rangle + i|101\rangle - i|011\rangle - i|111\rangle\right\}$

Step 7 逆転） $\frac{1}{\sqrt{8}}\left\{|000\rangle + |001\rangle - |010\rangle - |011\rangle + i|100\rangle + i|101\rangle - i|110\rangle - i|111\rangle\right\}$ **フーリエ変換終了**

$|hjk\rangle \to |kjh\rangle$

Quantum algorithms

- Deutsch-Jozsa algorithm
- Grover’s algorithm
- Shor’s algorithms



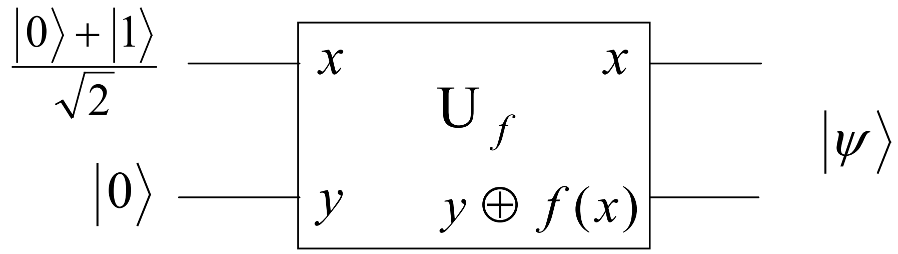
Deutsch-Jozsa algorithm （1）

補題１：量子並列性

$$f(x):\{0,1\}$$

$$U_f|x,y\rangle \to |x, y \oplus f(x)\rangle$$

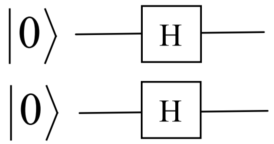
データ, ターゲット



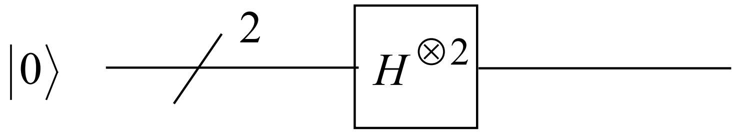
$$\boxed{\psi = U_f\left|\frac{|0\rangle+|1\rangle}{\sqrt{2}}, |0\rangle\right\rangle \to \frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}}$$

2関数を並列計算

Walsh-Hadamard transformを利用すると



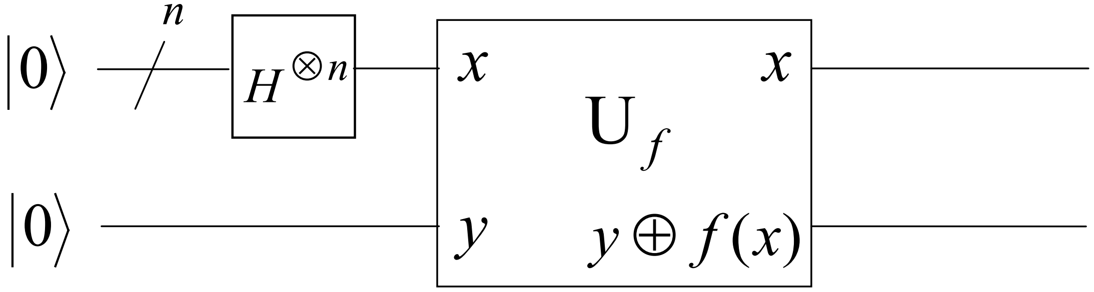
$$\psi = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$$



と記す

Deutsch-Jozsa algorithm (2)

補題1 (量子並列性 (つづき)



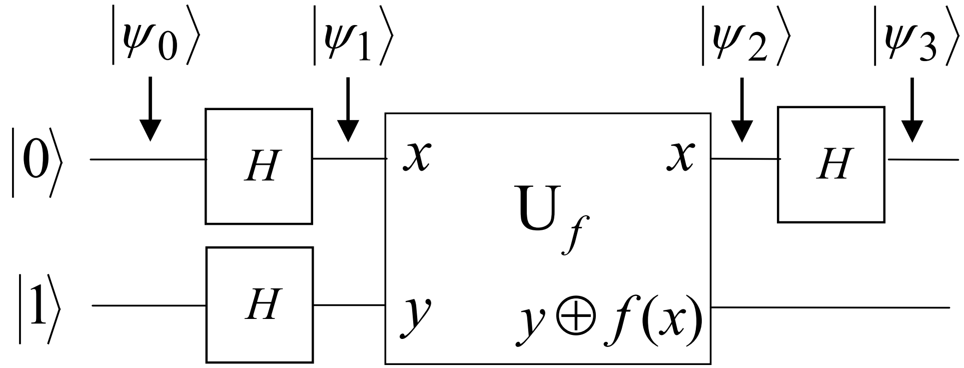
$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$$

入力 $|0\rangle^{\otimes n}|0\rangle$

出力 $\displaystyle \frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle = \frac{1}{\sqrt{2^n}}\left(|0,f(0)\rangle + |1,f(1)\rangle + |2,f(2)\rangle + \cdots\cdots + |x,f(x)\rangle\right)$

0〜xの入力を並列計算

Deutsch-Jozsa algorithm (3)



補題２:Deutschの問題

入力 $|\psi_0\rangle = |01\rangle$

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\begin{cases} |\psi_2\rangle = \pm\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if} \quad f(0) = f(1) \\ |\psi_2\rangle = \pm\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if} \quad f(0) \neq f(1) \end{cases}$$

$$\because U_f |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\begin{cases} |\psi_3\rangle = \pm|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if} \quad f(0) = f(1) \\ |\psi_3\rangle = \pm|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if} \quad f(0) \neq f(1) \end{cases}$$

$\Rightarrow$

$$\boxed{|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)}$$

$f(0) \oplus f(1)$ を1回で決定できる．

古典的には最低2回必要．

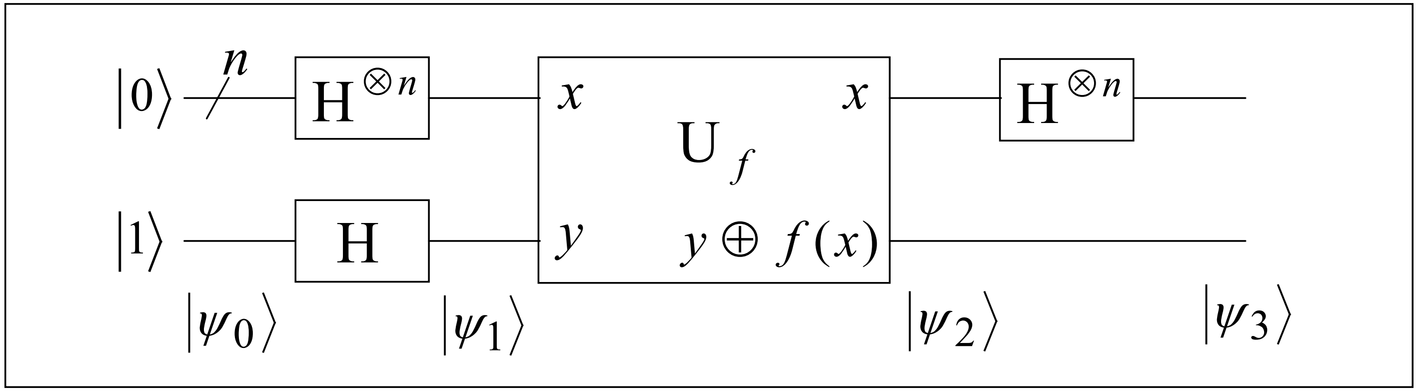
Deutsch-Jozsa algorithm （4）

本題

$f(x)$: $\{0,1\}$ $\quad (x = 0,1,\cdots,2^n - 1)$

- *constant* : **$f(x)$ is constant**
- *balanced* : **$f(x)$ is half 0 and half 1**

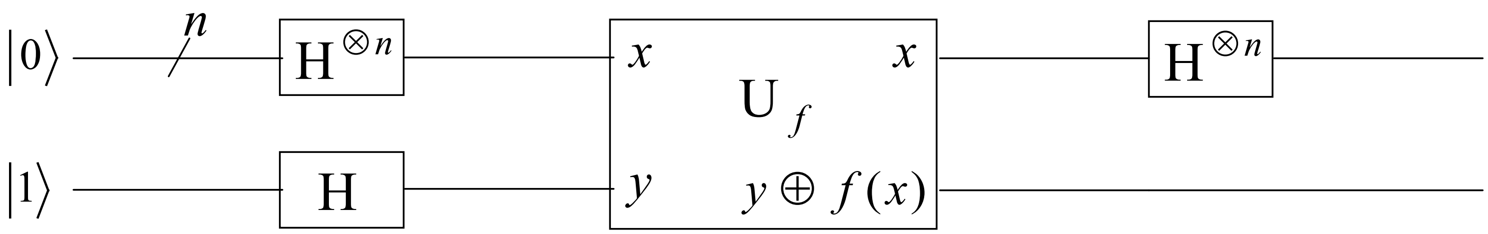
Mission : Judge whether $f(x)$ is constant or balanced.



$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle \qquad |\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \qquad |\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Example: n=2



Get 0 if $f(x)$ is constant.

$$|0\rangle \otimes |0\rangle \otimes |1\rangle$$

$$\downarrow$$

$$\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \otimes \mathrm{H}|1\rangle$$

$f(x) = (0,0,0,0)$ *or* $(1,1,1,1)$

$$\pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \otimes \mathrm{H}|1\rangle \rightarrow \pm|0\rangle \otimes |0\rangle \otimes \mathrm{H}|1\rangle \rightarrow 0$$

$f(x) = (0,0,1,1)$

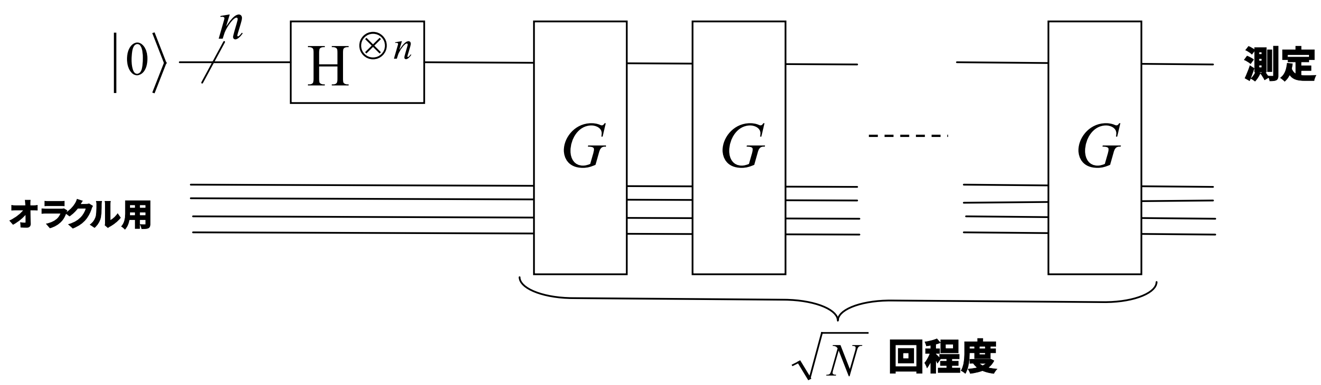
$$\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \otimes \mathrm{H}|1\rangle \rightarrow |1\rangle \otimes |0\rangle \otimes \mathrm{H}|1\rangle \rightarrow 2$$

$f(x) = (1,0,0,1)$

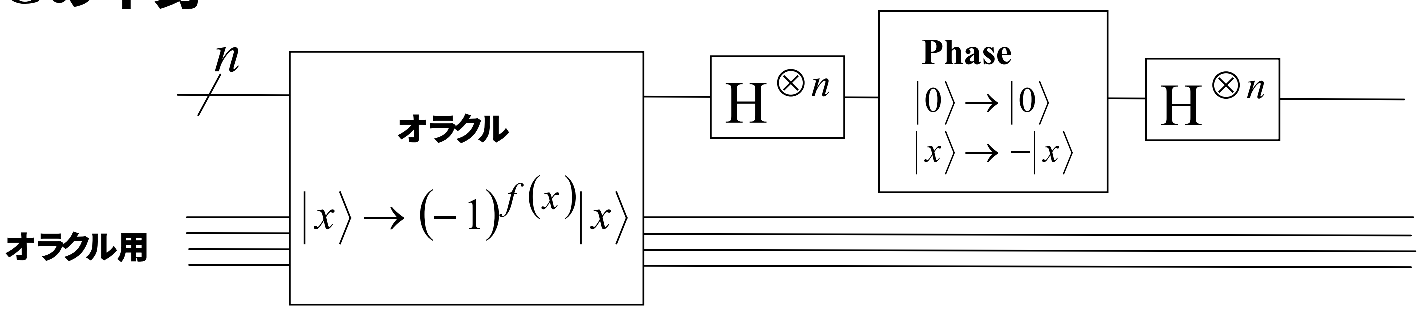
$$-\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \otimes \mathrm{H}|1\rangle \rightarrow -|1\rangle \otimes |1\rangle \otimes \mathrm{H}|1\rangle \rightarrow 3$$

Grover's algorithm (1)

データベース検索：N=2^n**個のファイルがあり，**0**から**N-1**までのアドレスがつけられている．指定された内容のファイルを少ないステップで見つけたい．古典的には**N**ステップ必要だが，グローバーの手法では**$\sqrt{N}$ **でよい．正解のアドレスでは** $f(x)=1$ **その他では**0**．**

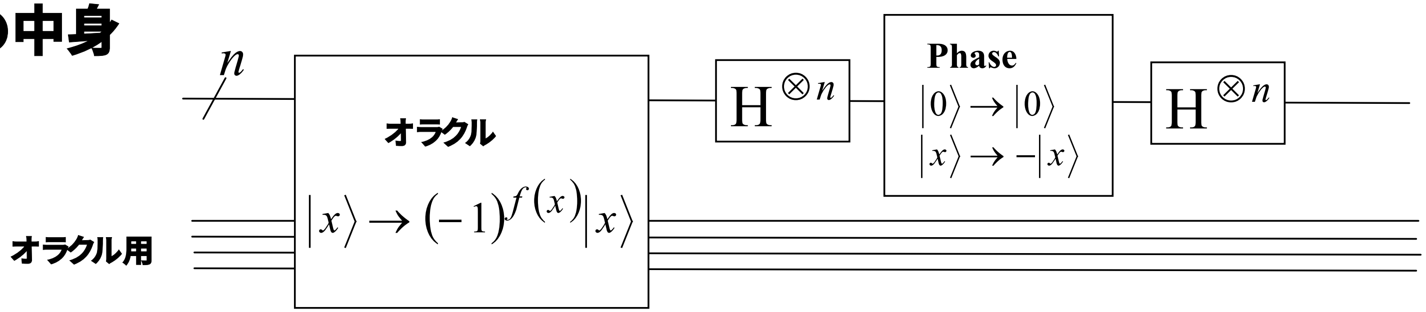


Gの中身



Grover's algorithm (2)

Gの中身



$|x\rangle \to (-1)^{f(x)}|x\rangle$ **, すなわちオラクルは正解**f(x)=1**のときのみに反転させる**

$$H^{\otimes n} P H^{\otimes n} = H^{\otimes n}\left(2|0\rangle\langle 0| - I\right)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

$$\left(2|\psi\rangle\langle\psi| - I\right)\sum_k \alpha_k |k\rangle = \sum_k \left(-\alpha_k + 2\langle\alpha\rangle\right)|k\rangle$$

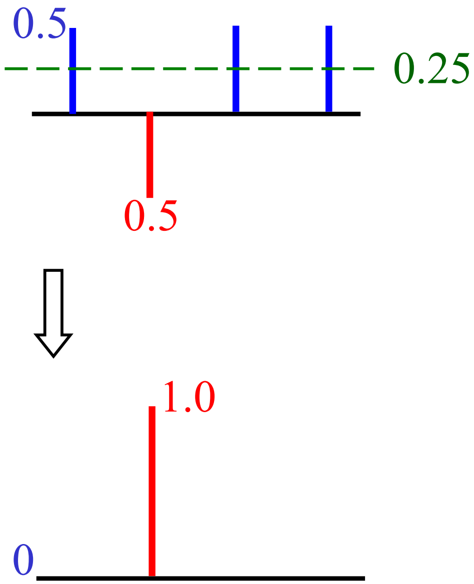
すなわち振幅の平均値<α>**を中心として反転させる**

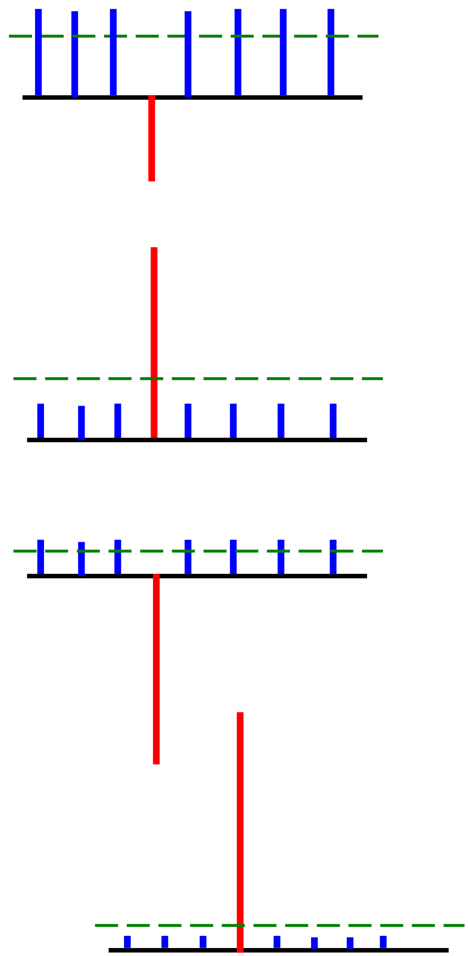
Grover's algorithm (3)

例：4量子ビットで正解が一つで
$|1\rangle$ の場合（2^nにおいてn=2に対応）

$x = |0\rangle \quad |1\rangle \quad |2\rangle \quad |3\rangle$

$\quad |00\rangle \quad |01\rangle \quad |10\rangle \quad |11\rangle$





素因数分解の計算（15=3×5の場合）

確定的モデル　　15÷2, 15÷3, 15÷4 ・・・・をつづけ
割り算の答えとあまりを求める

確率的モデル　乱数でためす）

$$F_n = m^n \pmod N$$

m^nをNで割ったあまり
を求める

$$F_n = 2^n \pmod{15}$$

例としてN=15, m=2を選ん
だ場合を考える

確率的計算　$F_n = 2^n \pmod{15}$

N=15, m=2	こたえ
$F_0=2^0$÷15のあまり	1
$F_1=2^1$÷15のあまり	2
$F_2=2^2$÷15のあまり	4
$F_3=2^3$÷15のあまり	8
$F_4=2^4$÷15のあまり	1
$F_5=2^5$÷15のあまり	2
$F_6=2^6$÷15のあまり	4
$F_7=2^7$÷15のあまり	8

周期 r= 4

$$m^{r/2}+1 = 2^{4/2}+1 = \underline{5}$$

$$m^{r/2}-1 = 2^{4/2}-1 = \underline{3}$$

確率的計算　例2)　$F_n = 11^n \pmod{15}$

N=15, m=11	こたえ
$F_0=11^0$÷15のあまり	1
$F_1=11^1$÷15のあまり	11
$F_2=11^2$÷15のあまり	1
$F_3=11^3$÷15のあまり	11
$F_4=11^4$÷15のあまり	1
$F_5=11^5$÷15のあまり	11
$F_6=11^6$÷15のあまり	1
$F_7=11^7$÷15のあまり	11

$\left.\begin{matrix} F_0 \\ F_1 \end{matrix}\right\}$ **周期** r=2

$$m^{r/2}+1=11^{2/2}+1=\underline{12}$$

$$m^{r/2}-1=11^{2/2}-1=\underline{10}$$

緑下線の数字とN=15の
最大公約数をとると<u>3</u>と<u>5</u>

古典的にrを求めるのが難しい

古典的計算機内での処理

$$F_n = 2^n(\mathrm{mod}15)$$

10進 | 2進

F_n	2^n(mod 15)
F_0	1
F_1	2
F_2	4
F_3	8
F_4	1
F_5	2
F_6	4
F_7	8

レジスターX (n)	レジスターY 2^n (mod 15)	
0 0 0 0	0 0 0 1	2^0
0 0 0 1	0 0 1 0	2^1
0 0 1 0	0 1 0 0	2^2
0 0 1 1	1 0 0 0	2^3
0 1 0 0	0 0 0 1	2^0
0 1 0 1	0 0 1 0	2^1
0 1 1 0	0 1 0 0	2^2
0 1 1 1	1 0 0 0	2^3

量子計算では

$$F_n = 2^n (\mathrm{mod} 15)$$

10進　　2進量子情報

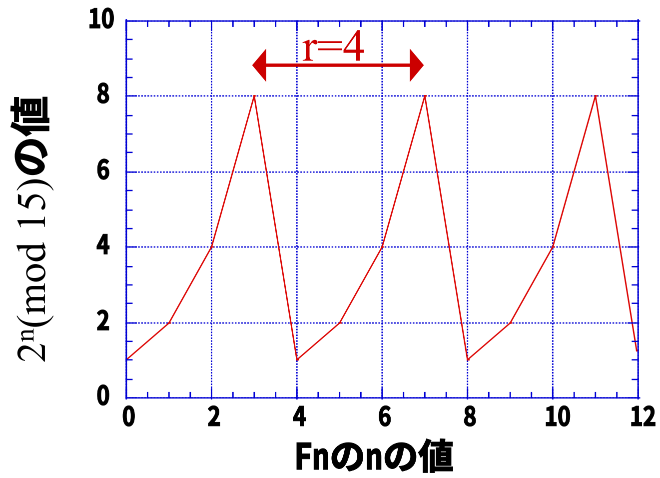
F_n	2^n(mod 15)
F_0	1
F_1	2
F_2	4
F_3	8
F_4	1
F_5	2
F_6	4
F_7	8

レジスターX (n)		レジスターY 2^n (mod 15)	
0 0 0 0	$\otimes$	0 0 0 1	2^0
0 0 0 1	$\otimes$	0 0 1 0	2^1
0 0 1 0	$\otimes$	0 1 0 0	2^2
0 0 1 1	$\otimes$	1 0 0 0	2^3
0 1 0 0	$\otimes$	0 0 0 1	2^0
0 1 0 1	$\otimes$	0 0 1 0	2^1
0 1 1 0	$\otimes$	0 1 0 0	2^2
0 1 1 1	$\otimes$	1 0 0 0	2^3

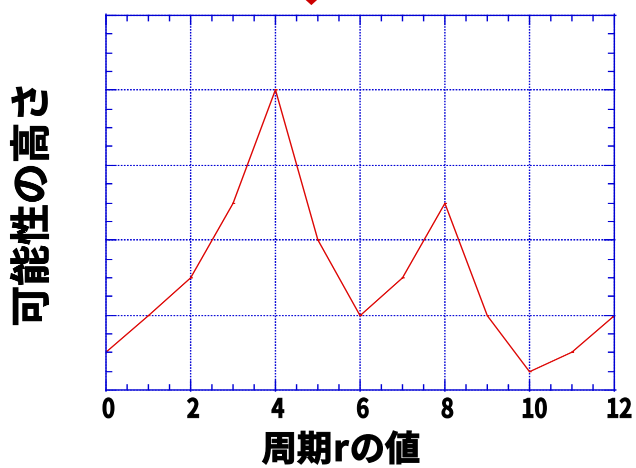
Xに重ね合わせ状態、Yに絡みあった状態をつくる　$\sum_x |x, f(x)\rangle$

量子計算では（2） $F_n = 2^n \pmod{15}$

レジスターX(n)		レジスターY 2^n (mod 15)	
0000	⊗	0001	2^0
0001	⊗	0010	2^1
0010	⊗	0100	2^2
0011	⊗	1000	2^3
0100	⊗	0001	2^0
0101	⊗	0010	2^1
0110	⊗	0100	2^2
0111	⊗	1000	2^3



フーリエ変換



Shor’s algorithm (1)

例 3量子ビットでf(x)の周期がr=2の場合を考える．

$$X : \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$

$$= \frac{1}{\sqrt{8}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\right)$$

$$X, Y : \psi = \frac{1}{\sqrt{8}}\sum_x |x, f(x)\rangle$$

離散フーリエ変換をψに適用する．知りたいのはf(x)の周期r）

$$\psi' = \frac{1}{\sqrt{8}}\sum_{x,k=0}^{7} e^{2\pi ikx/8}|x, f(x)\rangle = \frac{1}{8}|0\rangle\left\{|f(0)\rangle + |f(1)\rangle + |f(2)\rangle + \cdots + |f(7)\rangle\right\} +$$

$$\frac{1}{8}|1\rangle\left\{|f(0)\rangle + e^{2\pi i/8}|f(1)\rangle + e^{2\pi i2/8}|f(2)\rangle + \cdots + e^{2\pi i7/8}|f(7)\rangle\right\} +$$

$$\frac{1}{8}|2\rangle\left\{|f(0)\rangle + e^{4\pi i/8}|f(1)\rangle + e^{4\pi i2/8}|f(2)\rangle + \cdots + e^{4\pi i7/8}|f(7)\rangle\right\} +$$

・・・・・・

$$\frac{1}{8}|7\rangle\left\{|f(0)\rangle + e^{14\pi i/8}|f(1)\rangle + e^{14\pi i2/8}|f(2)\rangle + \cdots + e^{14\pi i7/8}|f(7)\rangle\right\}$$

Shor's algorithm (2)

f(x)も計算の結果，周期r=2であれば，f(0)=f(2)=f(4)=f(6)および f(1)=f(3)=f(5)=f(7)なので以下のようにくくれる．

$$\psi' = \frac{1}{2}|0\rangle\{|f(0)\rangle + |f(1)\rangle\} +$$

$$\frac{1}{8}|1\rangle\left\{|f(0)\rangle\left(e^{0} + e^{\pi i/2} + e^{\pi i} + e^{3\pi i/2}\right) + |f(1)\rangle\left(e^{\pi i/4} + e^{3\pi i/4} + e^{5\pi i/4} + e^{7\pi i/4}\right)\right\} +$$

$$\frac{1}{8}|2\rangle\left\{|f(0)\rangle\left(e^{0} + e^{\pi i} + e^{2\pi i} + e^{3\pi i}\right) + |f(1)\rangle\left(e^{\pi i/2} + e^{3\pi i/2} + e^{5\pi i/2} + e^{7\pi i/2}\right)\right\} +$$

$$\frac{1}{8}|3\rangle\left\{|f(0)\rangle\left(e^{0} + e^{3\pi i/2} + e^{3\pi i} + e^{9\pi i/2}\right) + |f(1)\rangle\left(e^{3\pi i/4} + e^{9\pi i/4} + e^{15\pi i/4} + e^{21\pi i/4}\right)\right\} +$$

$$\frac{1}{8}|4\rangle\left\{|f(0)\rangle\left(e^{0} + e^{2\pi i} + e^{4\pi i} + e^{6\pi i}\right) + |f(1)\rangle\left(e^{\pi i} + e^{3\pi i} + e^{5\pi i} + e^{7\pi i}\right)\right\} + \cdots\cdots$$

同色の色線で引かれた位相同士は干渉により弱めあい，ゼロとなる．
結果として生き残るのが

$$\psi' = \frac{1}{2}\left\{|0, f(0)\rangle + |0, f(1)\rangle + |4, f(0)\rangle + e^{i\pi}|4, f(1)\rangle\right\}$$

よってX測定では0か4を同確率でえる．

Shor’s algorithm (3)

ショアのアルゴリズムによると測定結果kは，$k=0, 2^n/r, 2\times 2^n/r, 3\times 2^n/r, \cdots (r-1)2^n/r$**をとる．**

⇩

前ページの例では$n=3$**，**$k=0,4$**から**$r=2$**が求まる．**

疑問：k**は，**$k=0, 2^n/r, 2\times 2^n/r, 3\times 2^n/r, \cdots (r-1)2^n/r$**と何種類の値をとれるため，周期**r**は決定できないのでは？**

7**量子ビットで**$r=8$**の例で考えると**$2^7=128$**．よって**X**の測定で**8**つの**$k=0, 16, 32, 48\ldots, 112$**のうちの**1**つが結果として得られる．たとえば**k**を測定して**80**が得られたとする．**

$$\frac{2^7}{k}=\frac{128}{80}=\frac{8}{5} \xrightarrow{\text{他のkでも同じようにすると}} \underline{\frac{2^7}{k}=8,4,\frac{8}{3},2,\frac{4}{3},\frac{8}{7}}$$

分子に注目すると正解$r=8$**が**50%**の確率で得られることがわかる．これで十分！**

入力に誤差がある場合の影響

◎例題：

f(x)=kx, k=0, 1, 2, ・・N-1が入力された場合の勾配kを知りたい。

方法： ユニタリ行列 $U=\lfloor U_{xy}\rfloor,\quad U_{xy}=\omega^{-xy}/\sqrt{N},\quad \omega=\exp(2\pi i/N),\quad x,y=0,1,....,N-1$

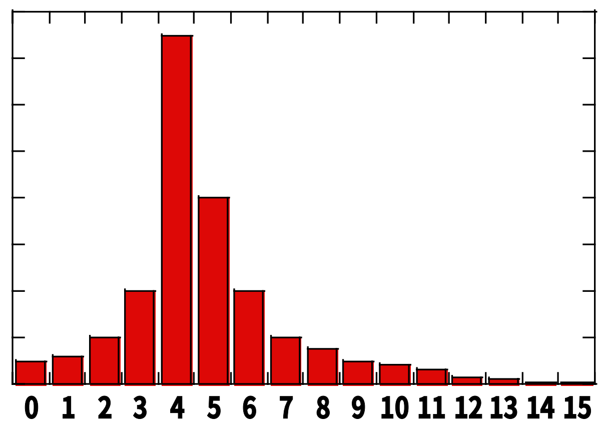
入力 $\psi_k=\left(\omega^{f_k(0)}e_0+\cdots+\omega^{f_k(x)}e_x+\cdots+\omega^{f_k(N-1)}e_{N-1}\right)/\sqrt{N}$

忠実に計算すると：$U\psi_k=e_k$ となり確率 1で正解が得られる。

例 ：N=2, k=1の場合

$$U\psi_1=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & e^{-\left(\frac{2\pi i}{2}\right)}\end{bmatrix}\frac{1}{\sqrt{2}}\left(\left(e^{-\left(\frac{2\pi i}{2}\right)}\right)^0\begin{bmatrix}1\\0\end{bmatrix}+\left(e^{-\left(\frac{2\pi i}{2}\right)}\right)^1\begin{bmatrix}0\\1\end{bmatrix}\right)$$

◎入力f_kが正確に行えず $g_k(x)=(k+\varepsilon)x,\ \left(|\varepsilon|<<1\right)$ が入力されると $U\psi_k=b_{k,0}e_0+\cdots+b_{k,x}e_x+\cdots+b_{k,N-1}e_{N-1}$ が出力される。N=16, k=4, ε=0.2では $g_4(x)=4.2x$ が高い確率で得られる。繰り返し測定が重要。



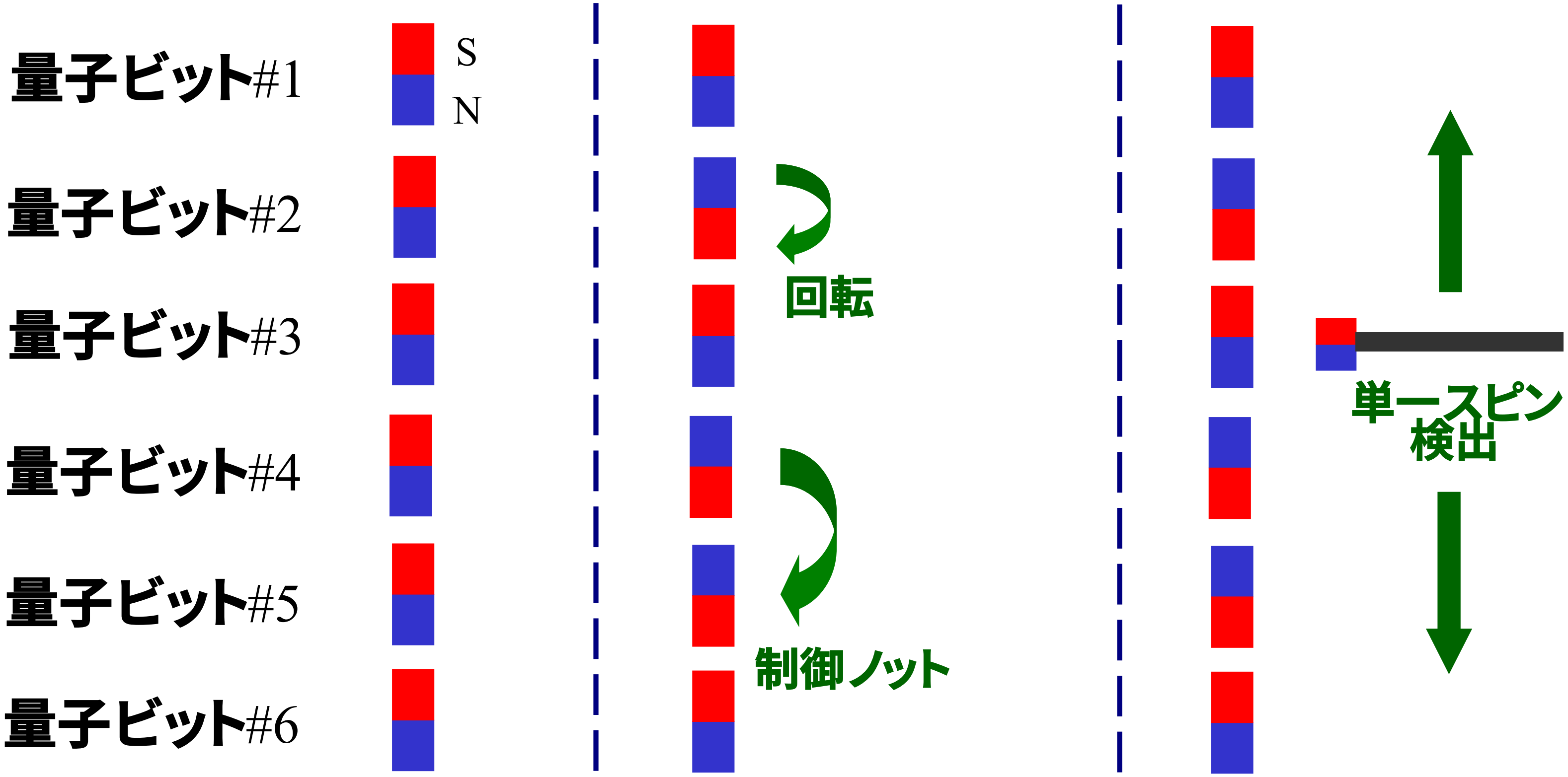
e_xが得られる確率(N=16, k=4, ε=0.2)

量子コンピュータの基本要素

1. 初期化

2. 量子演算

3. 読み出し



量子ビット数

総演算ステップ数

超並列計算

0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

2進数

10進数

2^n通りの数を一気に処理できる

量子ビットに必要な性質

1. 初期化が容易である.
2. 位相緩和時間が長い（Hが時間に依存しない）

   外界との相互作用が小さい
3. 1ステップに必要な演算時間が短い
4. 多量子ビット演算に充分な相互作用がえられる.

   他の量子ビットとの相互作用をon/offできる.
5. 単一ビットの状態測定（読み出し）が容易である.

量子コンピュータの実現にむけて

1. 量子ビット数(n)の増加 → 状態数 2^n

2. 総演算ステップ数≡ $\dfrac{\text{位相緩和時間 } T_2}{\text{スイッチ時間 } t_s}$

量子ビット	緩和時間 T_2 (秒)	スイッチ時間 t_s （秒）	総演算ステップ数
電子準位	10^{-9}	10^{-13}	10^{4}
電子スピン	10^{-6}	10^{-10}	10^{4}
イオン準位	10^{-1}	10^{-14}	10^{13}
核スピン	10^{3}	10^{-4}	10^{7}

光子

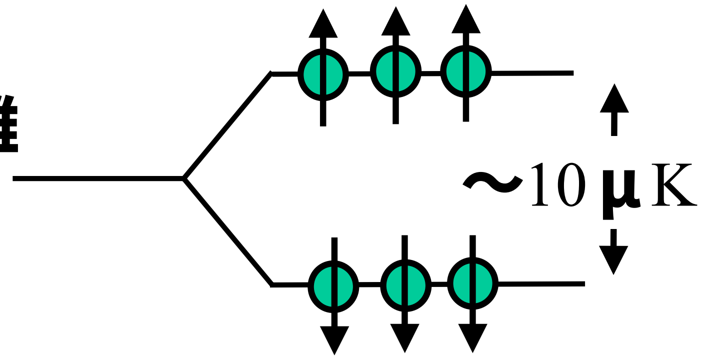
量子ビットのジレンマ 核スピンの例）

長所

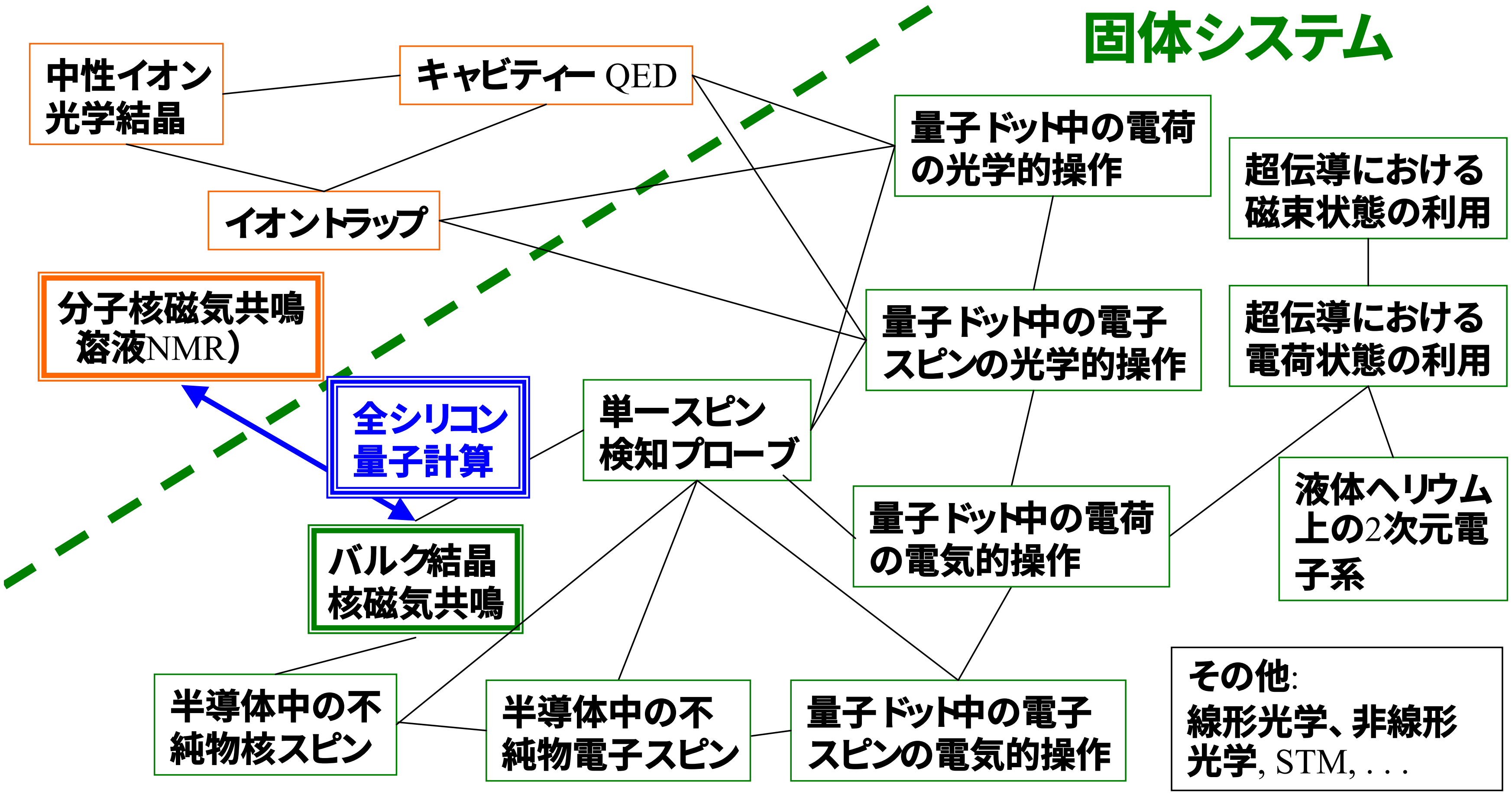
1. 外界との相互作用が小さい
   極めて長い緩和時間 T_2　1000秒?
2. スイッチ時間 t_s　0.0001秒
   核磁気共鳴周波数(KHz)の逆数）
3. 実現可能な演算ステップ数　10^7回

短所

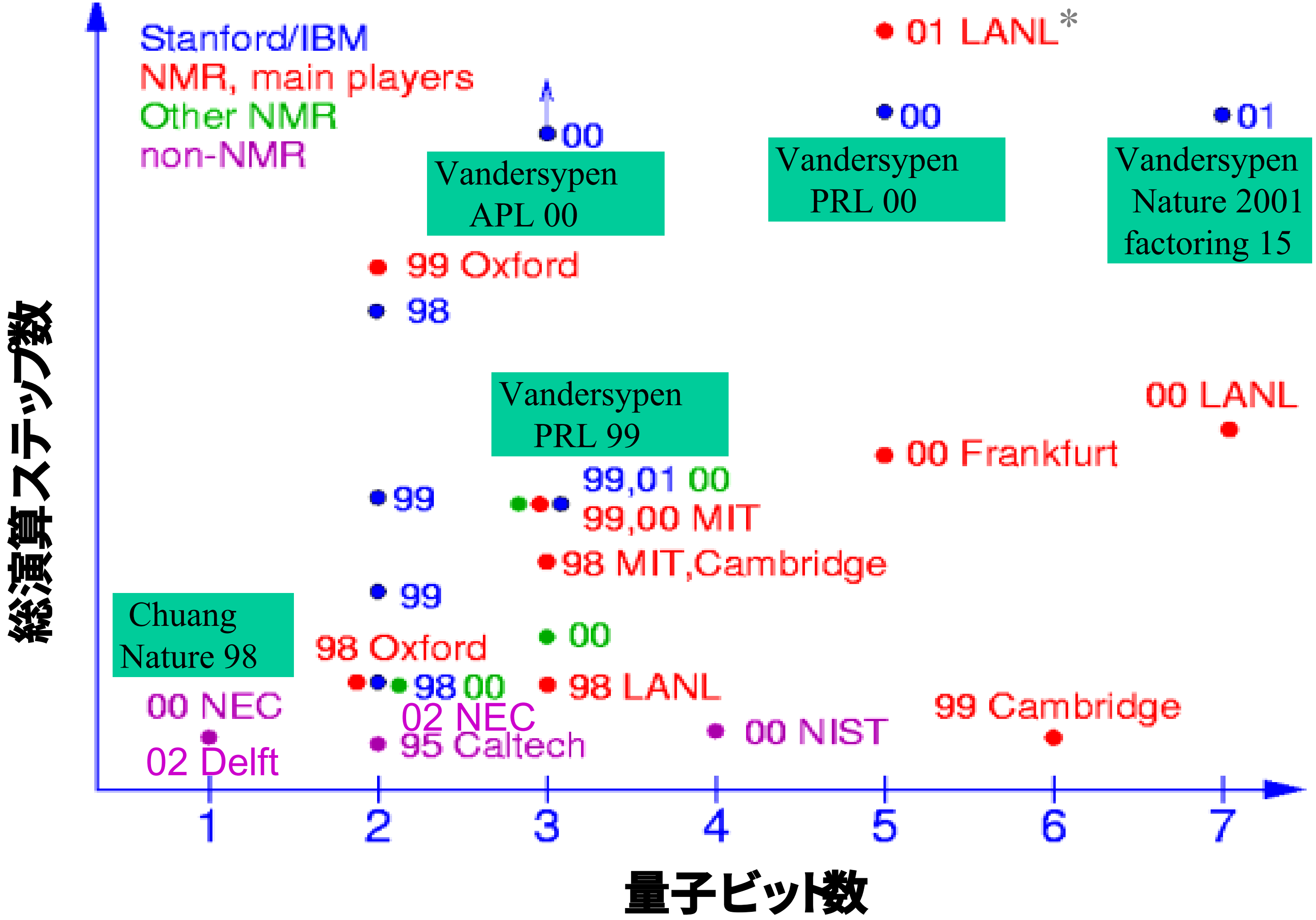
1. 外界との相互作用が小さい
   演算 •単一スピン測定が困難
2. 初期化が困難



実験による量子コンピュータの実現



量子ビット操作最前線



Stanford/IBM
NMR, main players
Other NMR
non-NMR
01 LANL*
00
00
01
Vandersypen APL 00
Vandersypen PRL 00
Vandersypen Nature 2001 factoring 15
99 Oxford
98
Vandersypen PRL 99
00 LANL
00 Frankfurt
99
99,01 00
99,00 MIT
98 MIT,Cambridge
99
Chuang Nature 98
00
98 Oxford
98 00
98 LANL
00 NEC
02 NEC
95 Caltech
00 NIST
99 Cambridge
02 Delft
1
2
3
4
5
6
7
総演算ステップ数
量子ビット数