Introduction to Quantum Information Processing

Eisuke Abe (Keio University)
December 17, 2002
"Towards scalable quantum computation"
at RIEC, Tohoku University

KEIO UNIVERSITY
CALAMVS GLADIO FORTIOR
1858

目次

- Qubitと量子論理ゲート
- 量子計算としての量子テレポーテーション
- 量子アルゴリズム
  - Deutsch-Jozsaのアルゴリズム
  - Groverの検索アルゴリズム
  - Shorの素因数分解アルゴリズム
- Physical Realization

参考文献

- Quantum Computation and Quantum Information, M. A. Nielsen and I. L. Chuang, Cambridge University Press (2000)

BitからQubitへ

情報処理の単位として，0と1だけでなく，その重ね合わせ

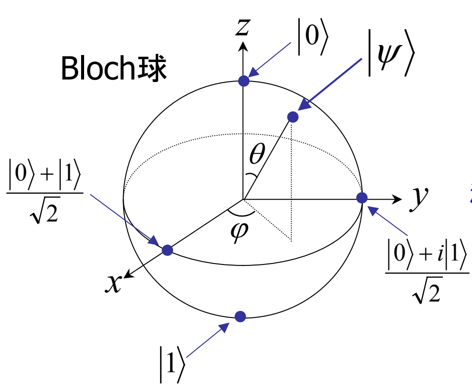
$$\alpha|0\rangle + \beta|1\rangle$$

も許されるとしたら，どんなことができるだろうか?

1-qubitの状態とBloch球

1-qubitの状態の標準基底

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



任意の重ね合わせ状態

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad (\alpha, \beta \in \mathbf{C})$$

複素2変数－1束縛条件＝実3変数

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

測定結果に影響しない

実2変数(物理的要請)

相対位相

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

Unitary演算

Schrödinger equation

$$\frac{\partial|\psi\rangle}{\partial t} = -i\,\mathcal{H}|\psi\rangle \qquad \begin{cases} \hbar = 1 & \text{(Planck定数)} \\ \mathcal{H} & \text{(系のHamiltonian)} \end{cases}$$

状態ベクトルの時間発展

$$|\psi\rangle \to \exp(-i\,\mathcal{H}\,t)|\psi\rangle = U|\psi\rangle$$

Sorry, not “dagger” but “dollar”!

U : unitary演算子 $\quad UU^{\$} = U^{\$}U = \mathbf{1}$

$$(AB)^{\$} = B^{\$}A^{\$} \qquad (U|\psi\rangle)^{\$} = \langle\psi|U^{\$}$$

1-qubitの量子状態の変化

$$|\psi\rangle = \alpha_0|0\rangle + \beta_0|1\rangle \xrightarrow{U_1} \alpha_1|0\rangle + \beta_1|1\rangle \xrightarrow{U_2} \alpha_2|0\rangle + \beta_2|1\rangle \xrightarrow{U_3} \cdots$$

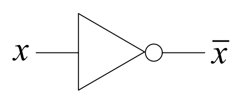
$$\Downarrow$$

$$U_n \cdots U_2 U_1|\psi\rangle$$

Time ←

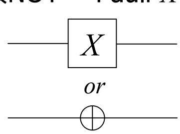
1-qubitの演算の例, Pauli行列

古典回路における1-bit演算 ⇒ NOTのみ



量子演算版NOT = Pauli-X ゲート

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



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

$$\begin{cases} X|0\rangle = |1\rangle \\ X|1\rangle = |0\rangle \end{cases} \Leftrightarrow X\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix},\ X\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$$

$$X = \begin{bmatrix} \boxed{\begin{matrix}0\\1\end{matrix}} & \boxed{\begin{matrix}1\\0\end{matrix}} \end{bmatrix}$$

→ $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ がどの状態になるかを表す

→ $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ がどの状態になるかを表す

Pauli-Y,Z ゲート

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \alpha|0\rangle + \beta|1\rangle \;—\boxed{Y}—\; -i\beta|0\rangle + i\alpha|1\rangle$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \alpha|0\rangle + \beta|1\rangle \;—\boxed{Z}—\; \alpha|0\rangle - \beta|1\rangle$$

回転操作

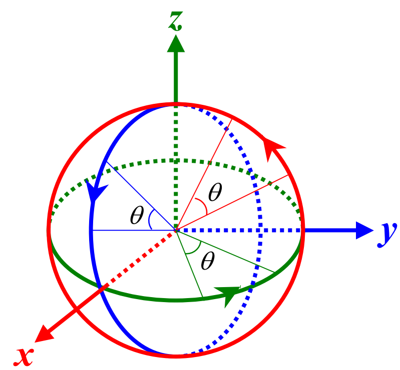
各軸の周りの角度θの回転

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

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

$$R_z(\theta) \equiv \exp(-i\theta\ Z/2) = \begin{bmatrix} \exp(-i\frac{\theta}{2}) & 0 \\ 0 & \exp(i\frac{\theta}{2}) \end{bmatrix}$$

指数演算子



$$e^A \equiv \sum_{n=0}^{\infty} \frac{A^n}{n!} = \mathbf{1} + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots$$

A がエルミート行列のとき $\exp(ixA) = \cos x\ \mathbf{1} + i\sin x\ A$

Hadamardゲート

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

$$-\boxed{H}-$$

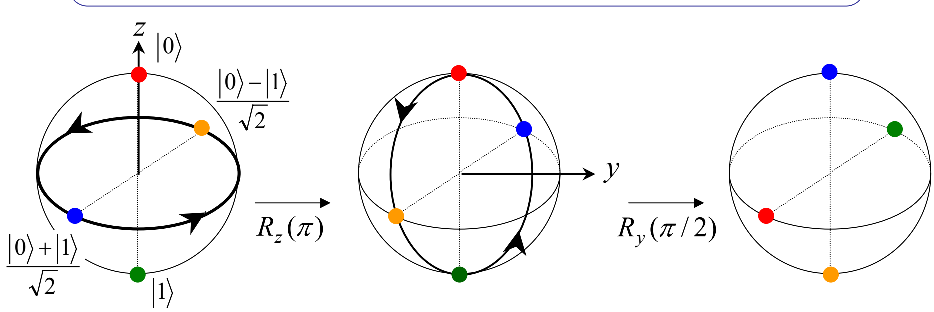
$$HH^\$ = I$$

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

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

$$R_y(\pi/2)R_z(\pi) = -i\ H \qquad R_y(\pi/2) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad R_z(\pi) = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} = -iZ$$

Time



2-qubitの状態

2-qubitの状態は $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ を基底として記述できるはず.

それらと, 1-qubitの状態はどのように結び付けられるか?

1-qubitの基底から2-qubitの基底をつくる演算

↓

テンソル積

計算規則

$$\mathbf{a}\otimes\mathbf{b} = \begin{bmatrix} a_1 \times \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \\ a_2 \times \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{bmatrix}$$

2-qubitの状態の標準基底

$$|00\rangle \equiv |0\rangle_A \otimes |0\rangle_B = \begin{bmatrix} 1\times\begin{bmatrix}1\\0\end{bmatrix} \\ 0\times\begin{bmatrix}1\\0\end{bmatrix} \end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |01\rangle = \begin{bmatrix} 1\times\begin{bmatrix}0\\1\end{bmatrix} \\ 0\times\begin{bmatrix}0\\1\end{bmatrix} \end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |10\rangle = \begin{bmatrix} 0\times\begin{bmatrix}1\\0\end{bmatrix} \\ 1\times\begin{bmatrix}1\\0\end{bmatrix} \end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |11\rangle = \begin{bmatrix} 0\times\begin{bmatrix}0\\1\end{bmatrix} \\ 1\times\begin{bmatrix}0\\1\end{bmatrix} \end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

任意の重ね合わせ状態

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix}\alpha\\\beta\\\gamma\\\delta\end{bmatrix} \qquad |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \quad (\alpha,\beta,\delta,\gamma \in \mathbf{C})$$

2-qubitの量子演算の例

例1. 制御NOTゲート

$$C_{AB} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

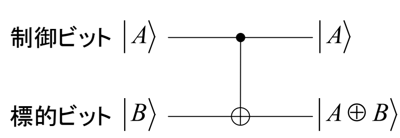
AB

$|00\rangle \to |00\rangle$

$|01\rangle \to |01\rangle$

$|10\rangle \to |11\rangle$

$|11\rangle \to |10\rangle$



mod 2 の足し算

$$C_{BA} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

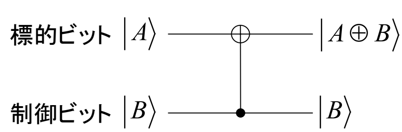
AB

$|00\rangle \to |00\rangle$

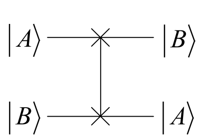
$|01\rangle \to |11\rangle$

$|10\rangle \to |10\rangle$

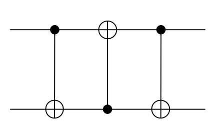
$|11\rangle \to |01\rangle$



例2. SWAPゲート



=

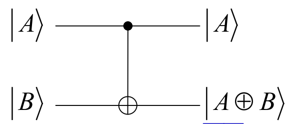


$\because \; x\oplus x = 0, \quad 0\oplus x = x$

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

制御NOT, Entanglement

必ずしも，「上のレールがqubit A，下のレールがqubit Bの情報を運んでいる」わけでは**ない**ことに注意



下のレールにもAの情報が入っている

非局所性，Entanglement

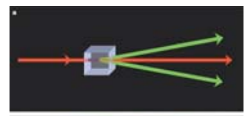
$$|1\rangle_A \otimes \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]_B \xrightarrow{C_{AB}} |1\rangle_A \otimes \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]_B$$

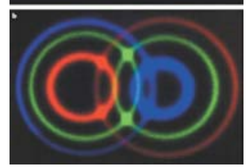
「上のレールが $|1\rangle_A$，下のレールが $(|0\rangle_B + |1\rangle_B)/\sqrt{2}$ の状態」と言ってもよさそう

$$\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]_A \otimes |0\rangle_B \xrightarrow{C_{AB}} \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}}$$

Bell state or EPR state

qubit Aの情報とqubit Bの情報は不可分

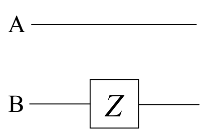




非局所性

2-qubitの量子計算において，1-qubitの演算を行ったとき

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$



$$\alpha|00\rangle \underline{- \beta|01\rangle} + \gamma|10\rangle \underline{- \delta|11\rangle}$$

この演算を表すunitary行列は？ $\cancel{Z_B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}$?

“qubit B”の位相を変えたつもりでも，“qubit-AB”の位相を変えている

→ 4x4行列でないと表現できない

AB

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to -|01\rangle$$
$$|10\rangle \to |11\rangle$$
$$|11\rangle \to -|10\rangle$$

$$Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \mathbf{1} \otimes Z_B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

測定

通常，「測定」は「標準基底による測定」を指す

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

$$\begin{cases} \text{確率 } |\alpha|^2 \text{ で，“0” を得る} \\ \text{確率 } |\beta|^2 \text{ で，“1” を得る} \end{cases}$$

現実の測定では，他の基底でしか測定できないことがありうる

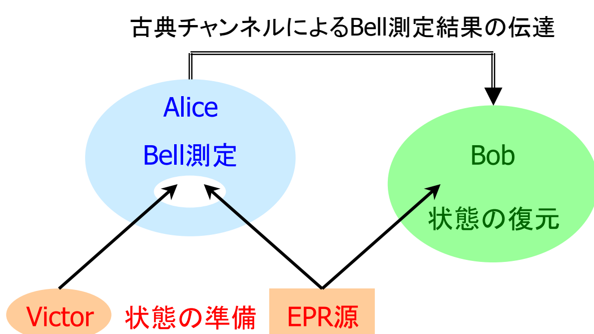
$\begin{cases} |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \\ |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \end{cases}$ の基底で測定すると，$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$ なので，

$$|\psi\rangle \ \pm \quad \begin{cases} \text{確率 } |\alpha+\beta|^2/2 \text{ で，“+” を得る} \\ \text{確率 } |\alpha-\beta|^2/2 \text{ で，“−” を得る} \end{cases}$$

基底の変換

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{H} |\psi\rangle = \alpha|+\rangle + \beta|-\rangle \ \pm \quad \begin{cases} \text{確率 } |\alpha|^2 \text{ で，“+”} \\ \text{確率 } |\beta|^2 \text{ で，“−”} \end{cases}$$

量子テレポーテーション



$$|\psi\rangle_V = \alpha|0\rangle_V + \beta|1\rangle_V \qquad |\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$
$$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$
$$XZ|\psi\rangle = \alpha|1\rangle - \beta|0\rangle$$

Bell基底

$$|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$|\beta_{01}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$$
$$|\beta_{10}\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$$
$$|\beta_{11}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$$

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

確認

$$\left|\psi\right\rangle_V\left|\beta_{00}\right\rangle_{AB}=\frac{1}{2}\left|\beta_{00}\right\rangle_{VA}\left|\psi\right\rangle_B+\frac{1}{2}\left|\beta_{10}\right\rangle_{VA}Z\left|\psi\right\rangle_B+\frac{1}{2}\left|\beta_{01}\right\rangle_{VA}X\left|\psi\right\rangle_B+\frac{1}{2}\left|\beta_{11}\right\rangle_{VA}XZ\left|\psi\right\rangle_B$$

左辺を展開

$$\begin{aligned}\left|\psi\right\rangle_V\left|\beta_{00}\right\rangle_{AB}&=(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\otimes\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)\\&=\boxed{\frac{\alpha}{\sqrt{2}}\left|000\right\rangle+\frac{\alpha}{\sqrt{2}}\left|011\right\rangle+\frac{\beta}{\sqrt{2}}\left|100\right\rangle+\frac{\beta}{\sqrt{2}}\left|111\right\rangle}\end{aligned}$$

右辺を各項ごとに展開

$$\left|\beta_{00}\right\rangle_{VA}\left|\psi\right\rangle_B=\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)\otimes(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)=\boxed{\frac{\alpha}{\sqrt{2}}\left|000\right\rangle}+\cancel{\frac{\beta}{\sqrt{2}}\left|001\right\rangle}+\cancel{\frac{\alpha}{\sqrt{2}}\left|110\right\rangle}+\boxed{\frac{\beta}{\sqrt{2}}\left|111\right\rangle}$$

$$\left|\beta_{10}\right\rangle_{VA}Z\left|\psi\right\rangle_B=\frac{1}{\sqrt{2}}(\left|00\right\rangle-\left|11\right\rangle)\otimes(\alpha\left|0\right\rangle-\beta\left|1\right\rangle)=\boxed{\frac{\alpha}{\sqrt{2}}\left|000\right\rangle}-\cancel{\frac{\beta}{\sqrt{2}}\left|001\right\rangle}-\cancel{\frac{\alpha}{\sqrt{2}}\left|110\right\rangle}+\boxed{\frac{\beta}{\sqrt{2}}\left|111\right\rangle}$$

$$\left|\beta_{01}\right\rangle_{VA}X\left|\psi\right\rangle_B=\frac{1}{\sqrt{2}}(\left|01\right\rangle+\left|10\right\rangle)\otimes(\alpha\left|1\right\rangle+\beta\left|0\right\rangle)=\boxed{\frac{\alpha}{\sqrt{2}}\left|011\right\rangle}+\cancel{\frac{\beta}{\sqrt{2}}\left|010\right\rangle}+\cancel{\frac{\alpha}{\sqrt{2}}\left|101\right\rangle}+\boxed{\frac{\beta}{\sqrt{2}}\left|100\right\rangle}$$

$$\left|\beta_{11}\right\rangle_{VA}XZ\left|\psi\right\rangle_B=\frac{1}{\sqrt{2}}(\left|01\right\rangle-\left|10\right\rangle)\otimes(\alpha\left|1\right\rangle-\beta\left|0\right\rangle)=\boxed{\frac{\alpha}{\sqrt{2}}\left|011\right\rangle}-\cancel{\frac{\beta}{\sqrt{2}}\left|010\right\rangle}-\cancel{\frac{\alpha}{\sqrt{2}}\left|101\right\rangle}+\boxed{\frac{\beta}{\sqrt{2}}\left|100\right\rangle}$$

QTの実行

Step.1 状態の準備

$$\left|\psi\right\rangle_V\left|\beta_{00}\right\rangle_{AB}=\frac{1}{2}\left|\beta_{00}\right\rangle_{VA}\left|\psi\right\rangle_B+\frac{1}{2}\left|\beta_{10}\right\rangle_{VA}Z\left|\psi\right\rangle_B+\boxed{\frac{1}{2}\left|\beta_{01}\right\rangle_{VA}X\left|\psi\right\rangle_B}+\frac{1}{2}\left|\beta_{11}\right\rangle_{VA}XZ\left|\psi\right\rangle_B$$

Step.2 AliceによるBell測定(Bell基底による測定)

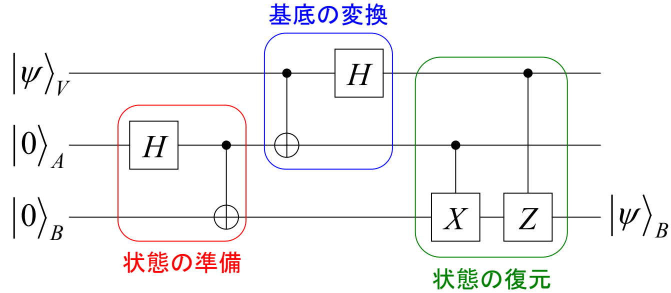
例えば，$\left|\beta_{01}\right\rangle$ を得たとする．この時点でBobの状態は $X\left|\psi\right\rangle_B$ に確定．
しかし，まだBobはそのことを知らないし，測定もしていないので，
Bobの状態は壊れていない．

Step.3 古典チャンネルによるBell測定結果の伝達

Step.4 Bobによる状態の復元

BobはAliceから得た情報を元に，自分の状態にPauli-X ゲートを施す．
Bobの状態は $X(X\left|\psi\right\rangle_B)=\left|\psi\right\rangle_B$ となり，テレポーテーション完了．

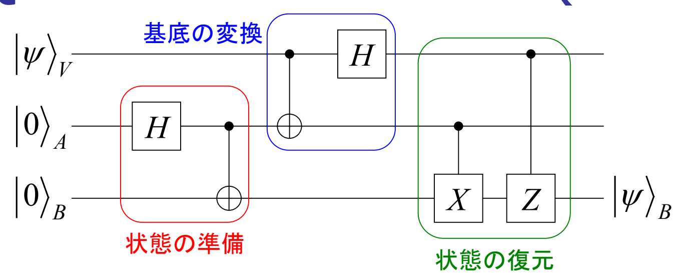
QTを量子回路で考える



$$|\psi\rangle|0\rangle|0\rangle \xrightarrow{H_A} |\psi\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle \xrightarrow{C_{AB}} |\psi\rangle\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

$$\begin{aligned}&=(|00\rangle+|11\rangle)/\sqrt{2}\otimes|\psi\rangle\\ &+(|00\rangle-|11\rangle)/\sqrt{2}\otimes Z|\psi\rangle\\ &+(|01\rangle+|10\rangle)/\sqrt{2}\otimes X|\psi\rangle\\ &+(|01\rangle-|10\rangle)/\sqrt{2}\otimes XZ|\psi\rangle\end{aligned}$$

QTを量子回路で考える(続き)



$$\begin{aligned}&(|00\rangle+|11\rangle)/\sqrt{2}\otimes|\psi\rangle+\\ &(|00\rangle-|11\rangle)/\sqrt{2}\otimes Z|\psi\rangle+\\ &(|01\rangle+|10\rangle)/\sqrt{2}\otimes X|\psi\rangle+\\ &(|01\rangle-|10\rangle)/\sqrt{2}\otimes XZ|\psi\rangle\end{aligned}
\xrightarrow{C_{VA}}
\begin{aligned}&(|00\rangle+|10\rangle)/\sqrt{2}\otimes|\psi\rangle+\\ &(|00\rangle-|10\rangle)/\sqrt{2}\otimes Z|\psi\rangle+\\ &(|01\rangle+|11\rangle)/\sqrt{2}\otimes X|\psi\rangle+\\ &(|01\rangle-|11\rangle)/\sqrt{2}\otimes XZ|\psi\rangle\end{aligned}
\xrightarrow{H_V}
\begin{aligned}&|00\rangle\otimes|\psi\rangle+\\ &|10\rangle\otimes Z|\psi\rangle+\\ &|01\rangle\otimes X|\psi\rangle+\\ &|11\rangle\otimes XZ|\psi\rangle\end{aligned}$$

$$\xrightarrow{CX_{AB}}
\begin{aligned}&|00\rangle\otimes|\psi\rangle+\\ &|10\rangle\otimes Z|\psi\rangle+\\ &|01\rangle\otimes|\psi\rangle+\\ &|11\rangle\otimes Z|\psi\rangle\end{aligned}
\xrightarrow{CZ_{AB}} (|00\rangle+|10\rangle+|01\rangle+|11\rangle)\otimes|\psi\rangle$$

測定と古典チャンネル

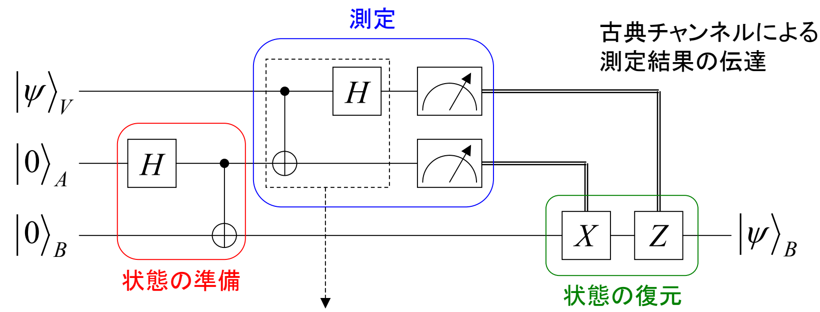
先に測定をしてしまって，必要なゲート操作だけを行っても問題ない

測定

$$\boxed{|00\rangle}\otimes|\psi\rangle+\boxed{|10\rangle}\otimes Z|\psi\rangle+\boxed{|01\rangle}\otimes X|\psi\rangle+\boxed{|11\rangle}\otimes XZ|\psi\rangle$$

復元

$$\xrightarrow{I}|\psi\rangle \qquad \xrightarrow{Z}|\psi\rangle \qquad \xrightarrow{X}|\psi\rangle \qquad \xrightarrow{ZX}|\psi\rangle$$



Bell測定が許される場合は不要．

$|\beta_{xy}\rangle \leftrightarrow |xy\rangle$ と対応させればよい

量子計算の特徴

- 状態の重ね合わせによる量子並列性
- 振幅と位相の非局所性
- Entanglement
- Unitary変換による多様な演算
- 測定による状態の収縮

古典計算機をしのぐ高速計算の可能性?

量子アルゴリズムの発明

量子アルゴリズム

- Deutsch-Jozsa(D-J)のアルゴリズム
  - Proc. R. Soc. London A, 439, 553 (1992)
- Groverの検索アルゴリズム
  - Phys. Rev. Lett., 79, 325 (1997)
- Shorの素因数分解アルゴリズム
  - SIAM J. Comp., 26, 1484 (1997)

D. Deutsch

R. Jozsa

L. K. Grover

P. W. Shor

量子並列性

n-qubitに対するHadamardゲート

$$|0\rangle^{\otimes n} \;\text{—}\; \boxed{H^{\otimes n}} \;\text{—}$$

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

$$\begin{aligned} H^{\otimes n}|0\rangle|0\rangle\cdots|0\rangle &= \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\cdots\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2^{n/2}}\left(|0\cdots00\rangle+|0\cdots01\rangle+\cdots+|1\cdots11\rangle\right) \\ &= \frac{1}{2^{n/2}}\left(|0\rangle+|1\rangle+|2\rangle+\cdots+|N-1\rangle\right) = \frac{1}{2^{n/2}}\sum_{x}^{N-1}|x\rangle \end{aligned}$$

$2^n = N$ 個の状態の等しい重みの重ね合わせ

例えば，$x=0,1,\ldots,N\text{-}1$ に対して0か1の値をとる2値関数 $f(x)$ が与えられたとする
さらに，量子並列性によって $f(x)$ に関する全ての情報の重ね合わせをつくれたとする

$$\frac{1}{2^{n/2}}\left(|f(0)\rangle+|f(1)\rangle+|f(2)\rangle+\cdots+|f(N-1)\rangle\right)$$

$f(x)$ を決定できるか?

NO! 測定したら $f(x)$ の値のどれか1つを得るだけ

Deutschの問題

x=0,1,…,2^n-1 に対して定義された2値関数 $f(x)$ が
“constant”であるか“balanced”であるか判定せよ

constant: 全ての x に対して $f(x)$ の値が同じ (全て0 *or* 全て1)

n=2の例 $f(x)=(0,0,0,0)$ *or* $f(x)=(1,1,1,1)$

balanced: $f(x)$ の値の半分は0, 半分は1

n=2の例 $f(x)=(0,0,1,1)$ とその並べ替え

classical

1回の問い合わせでの判定は不可能. 最悪 $2^{n-1}+1$ 回の問い合わせが必要

$f(0)=?$

$f(1)=?$

$f(2)=?$

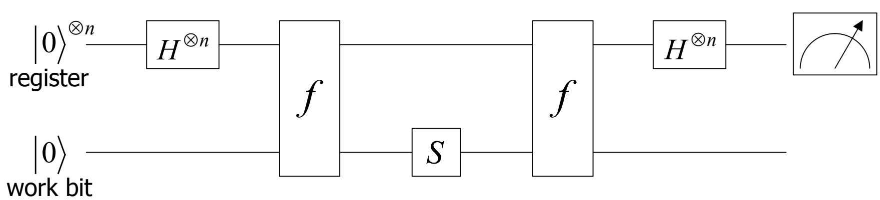
⋮

$f(x)$

quantum

常に1回の問い合わせで判定できる

D-Jを実行する量子回路



Hadamardゲート

$$H|x\rangle=\frac{1}{\sqrt{2}}\sum_z(-1)^{xz}|z\rangle$$

$$\because\quad H|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}\quad H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$H^{\otimes n}|x\rangle=\frac{1}{2^{n/2}}\sum_z(-1)^{x\cdot z}|z\rangle$$

where, $x=x_1x_2\cdots x_n\quad z=z_1z_2\cdots z_n$

$$x\cdot z=x_1z_1+x_2z_2+\cdots+x_nz_n$$

f ゲート

$$f|x\rangle|y\rangle=|x\rangle|y\oplus f(x)\rangle$$

実行例

$$f|x\rangle|0\rangle=|x\rangle|0\oplus f(x)\rangle=|x\rangle|f(x)\rangle$$

$$f|x\rangle|f(x)\rangle=|x\rangle|f(x)\oplus f(x)\rangle=|x\rangle|0\rangle$$

S ゲート

$$S|x\rangle|y\rangle=(-1)^y|x\rangle|y\rangle$$

D-Jの実行過程

$$|0\rangle^{\otimes n}|0\rangle \xrightarrow{H^{\otimes n}} \boxed{\frac{1}{2^{n/2}}\sum_x |x\rangle|0\rangle} \xrightarrow{f} \frac{1}{2^{n/2}}\sum_x|x\rangle\boxed{|f(x)\rangle}$$

重ね合わせ状態をつくる

$f(x)$ の情報をwork bitに
乗せる (entanglement)

$$\xrightarrow{S} \frac{1}{2^{n/2}}\sum_x \boxed{(-1)^{f(x)}}|x\rangle|f(x)\rangle \xrightarrow{f} \frac{1}{2^{n/2}}\sum_x(-1)^{f(x)}|x\rangle\boxed{|0\rangle}$$

$f(x)$ の情報を乗せた
非局所的な位相シフト

work bitから $f(x)$ の情報
を消去 (quantum erasure)

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^n}\sum_{x,z}(-1)^{f(x)+x\cdot z}|z\rangle|0\rangle$$

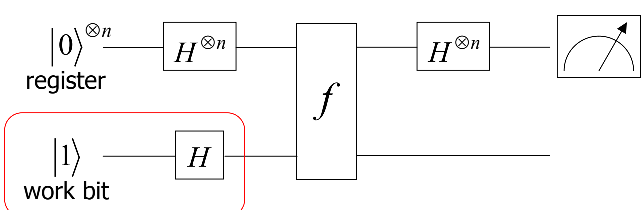
量子並列性と量子干渉を
利用したアルゴリズム

registerを観測

$$|z\rangle=|00\cdots0\rangle \text{ の確率振幅} = \frac{1}{2^n}\sum_x(-1)^{f(x)} = \boxed{\begin{cases}\pm1 & \text{constant}\\ 0 & \text{balanced}\end{cases}}$$

干渉効果

D-J (改良版)



$$\because\ |0\oplus f(x)\rangle-|1\oplus f(x)\rangle=(-1)^{f(x)}\left(|0\rangle-|1\rangle\right)$$

$$|0\rangle^{\otimes n}|1\rangle \xrightarrow{H^{\otimes n+1}} \frac{1}{2^{n/2}}\sum_x|x\rangle\boxed{\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]} \xrightarrow{f} \frac{1}{2^{n/2}}\sum_x(-1)^{f(x)}|x\rangle\boxed{\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]}$$

位相シフトとquantum erasureの
両方の役割を果たしている

↓

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^n}\sum_{x,z}(-1)^{f(x)+x\cdot z}|z\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

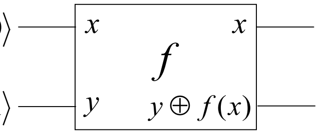
S ゲートと2回目の f ゲート不要!!

f ゲートの例, 2 bit

x	constant		balanced	
	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0

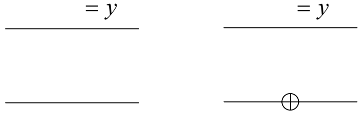
register $H|0\rangle$

work bit $H|1\rangle$



constant

$y \oplus f_1(x) = y \oplus 0 = y$ $\qquad$ $y \oplus f_2(x) = y \oplus 1 = \bar{y}$

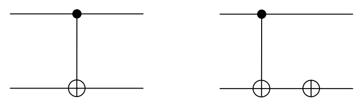


registerの変化 $\quad H|0\rangle \xrightarrow{f_1} H|0\rangle \xrightarrow{H} |0\rangle$

何もしないので元通り. work bitにNOTが入っても全体の位相が変わるだけ

balanced

$y \oplus f_3(x) = y \oplus x$ $\qquad$ $y \oplus f_4(x) = y \oplus \bar{x}$



registerの変化

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{f_3} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{H} |1\rangle$$

$$\because \quad C_{rw}|1\rangle_r \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]_w = -|1\rangle_r \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]_w$$

制御NOTの掛かったregisterは1になる

f ゲートの例, 4 bit

x	constant		balanced					
	f_{c1}	f_{c2}	f_{b1}	f_{b2}	f_{b3}	f_{b4}	f_{b5}	f_{b6}
0	0	1	0	1	0	1	0	1
1	0	1	0	1	1	0	1	0
2	0	1	1	0	0	1	1	0
3	0	1	1	0	1	0	0	1

$f_{b2} = \bar{f}_{b1}$ $\qquad$ $f_{b4} = \bar{f}_{b3}$

$f_{b5} = f_{b1} \oplus f_{b3}$ $\qquad$ $f_{b6} = \overline{f_{b1} \oplus f_{b3}}$

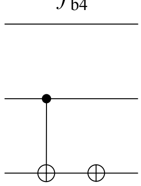
balancedの f ゲートはwork bitが標的のCNOTとwork bitに対するNOTの組み合わせ

⇒元の状態(0)には戻れない

registerの変化

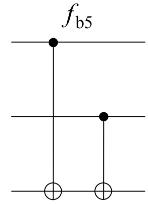
$$\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \xrightarrow{f_{b4}} -\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \xrightarrow{H} -|01\rangle = -|1\rangle$$

f_{b4}



$$\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \xrightarrow{f_{b5}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \xrightarrow{H} |11\rangle = |3\rangle$$

f_{b5}

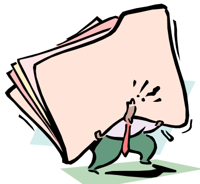


registerの変化

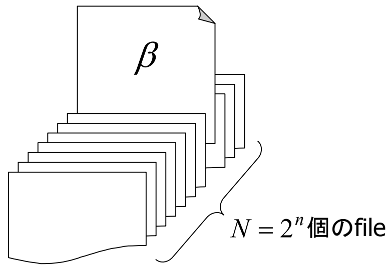
Groverの検索アルゴリズム

$N = 2^n$ 個のfileの中から，所望のfile “β” を検索する

古典的には，順番にfileを調べて，
平均$N/2$回程度の操作が必要



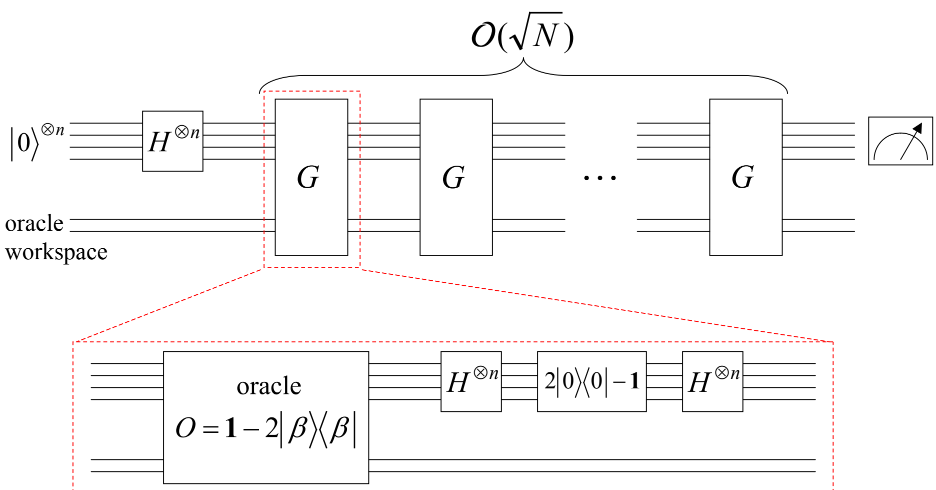
Hard task!!



Groverのアルゴリズムでは，N 個のfile(状態)の重ね合わせから，出発して $\sqrt{N}$ 回程度のunitary演算G を実行することで，ほぼ所望のfileに到達

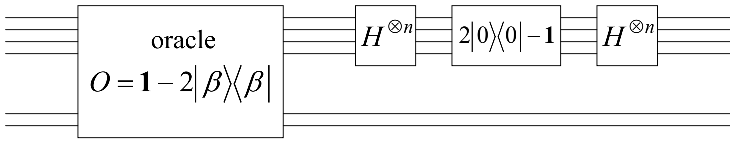
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \longrightarrow \approx |\beta\rangle$$

Groverを実行する量子回路



oracle: 神託．論理ゲートを実行するblack box

Gゲートの解析(1)

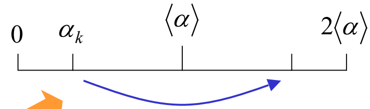


$$\begin{cases} O|\beta\rangle = |\beta\rangle - 2|\beta\rangle\langle\beta|\beta\rangle = -|\beta\rangle \\ O|x\rangle = |x\rangle - 2|\beta\rangle\langle\beta|x\rangle = |x\rangle \quad (x\neq\beta)\end{cases}$$

所望のfileに対してのみ，符号反転

$$H^{\otimes n}(2|0\rangle\langle 0|-\mathbf{1})H^{\otimes n} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n}-\mathbf{1}$$
$$= 2|\psi\rangle\langle\psi|-\mathbf{1}$$

“inversion about average”



$$(2|\psi\rangle\langle\psi|-\mathbf{1})\sum_k \underline{\alpha_k}|k\rangle = \frac{2}{N}\sum_{k,k',k''}\alpha_k|k''\rangle\langle k'|k\rangle - \sum_k\alpha_k|k\rangle$$
$$= \sum_k[\underline{2\langle\alpha\rangle-\alpha_k}]|k\rangle \qquad \because\ \langle\alpha\rangle\equiv\sum_k\frac{\alpha_k}{N}$$

Gゲートの解析(2)

所望のfile(β)以外のN-1個のfileの重ね合わせ

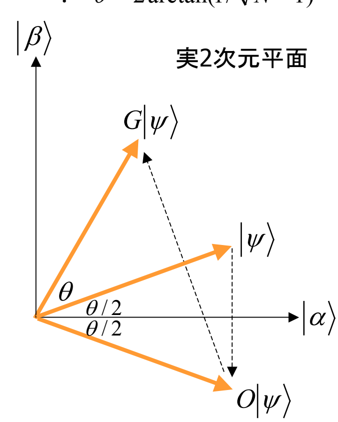
$$|\alpha\rangle = \frac{1}{\sqrt{N-1}}\sum_x{}' |x\rangle = \begin{bmatrix}1\\0\end{bmatrix}$$
$$|\beta\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

$$|\psi\rangle = \sqrt{\frac{N-1}{N}}\,|\alpha\rangle + \frac{1}{\sqrt{N}}|\beta\rangle = \begin{bmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{bmatrix}$$
$$\because\ \theta = 2\arctan(1/\sqrt{N-1})$$

$$O=\mathbf{1}-2|\beta\rangle\langle\beta|$$
$$=\begin{bmatrix}1&0\\0&1\end{bmatrix}-2\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0&1\end{bmatrix}=\boxed{\begin{bmatrix}1&0\\0&-1\end{bmatrix}\ |\alpha\rangle\text{ に関する折り返し}}$$

$$2|\psi\rangle\langle\psi|-\mathbf{1} = 2\begin{bmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{bmatrix}\begin{bmatrix}\cos(\theta/2) & \sin(\theta/2)\end{bmatrix}-\begin{bmatrix}1&0\\0&1\end{bmatrix}$$
$$=\boxed{\begin{bmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{bmatrix}\ |\psi\rangle\text{ に関する折り返し}}$$

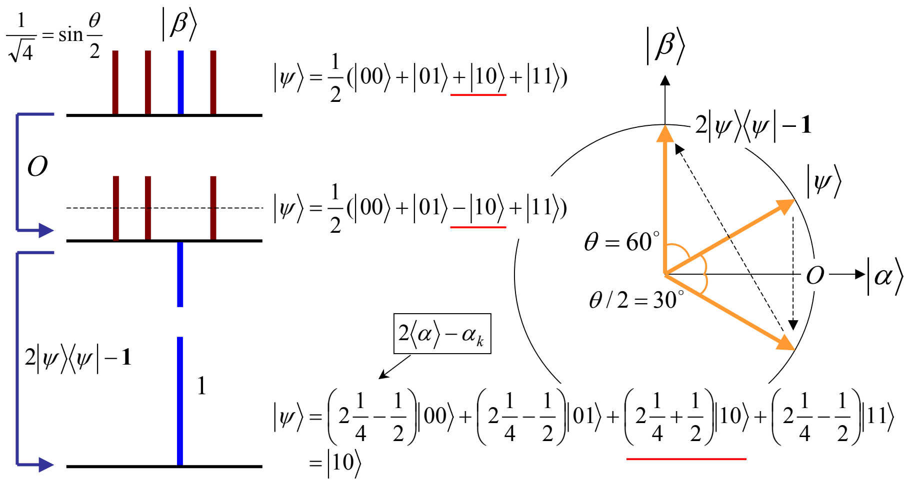
$$G=(2|\psi\rangle\langle\psi|-\mathbf{1})O=\boxed{\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}\ \theta\text{ 回転}}$$



実行例, N=4

各fileの確率振幅の変化

$|\alpha\rangle|\beta\rangle$ 平面での$|\psi\rangle$の変化

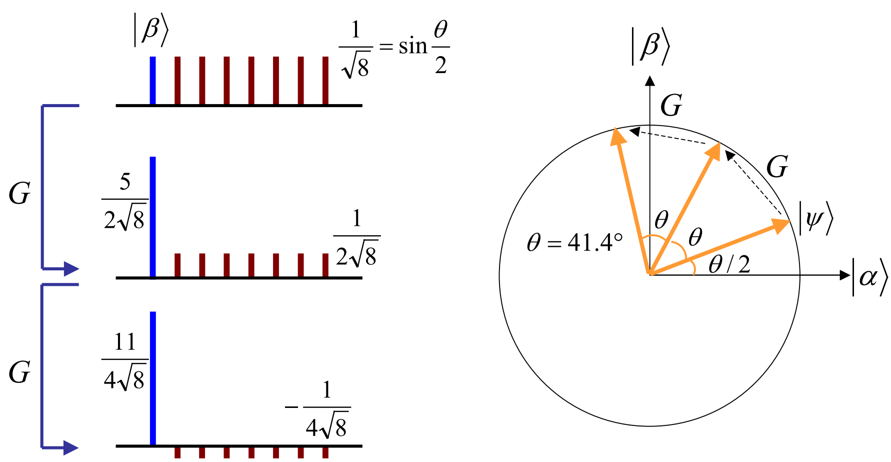


1回のG で100%の確率で所望のfileを得る (rare case)

実行例, N=8

各fileの確率振幅の変化

$|\alpha\rangle|\beta\rangle$ 平面での$|\psi\rangle$の変化



2回のG でほぼ所望のfileに到達. これ以上やると遠ざかる

Groverのアルゴリズムの効率

所望のfileに到達するまで，何回のG ゲートが必要か?

始状態が $|\psi\rangle = \begin{bmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{bmatrix}$ で，1回 G を実行するごとにθ回転するので，

k 回実行した後の状態は

$$G^k|\psi\rangle = \begin{bmatrix}\cos\frac{2k+1}{2}\theta\\ \sin\frac{2k+1}{2}\theta\end{bmatrix}$$

アルゴリズムを終了するのは，$\frac{2n+1}{2}\theta \approx \frac{\pi}{2}$ となるとき.

$\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \approx \frac{\theta}{2}$ とすると，

$n \approx \frac{\pi}{4}\sqrt{N}$ 回程度繰り返せばよい.

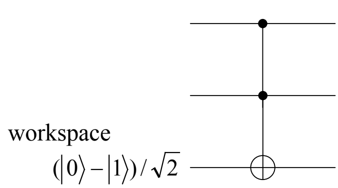
Oracle

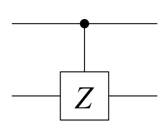
所望のfileの中身を“知らない”のに，oracleを構成できるのか?

例えば，「37で割り切れる番号のfileが欲しい」ときには，「file番号を37で割る回路」をつくって，「割り切れたときのみ符号反転」させればよい.
つまり， oracle は「検索条件」だけで構成できる

応用範囲が広い!! (e.g. quantum simulation, quantum counting)

例　「file番号3のfileが欲しい」ときのoracle (N=4)





$$CZ = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$$

Shorの素因数分解アルゴリズム

$$66554087 = 6703 \times 9929$$

古典的な方法では，指数オーダーの時間を要する
素因数分解アルゴリズムしか知られていない

Shorのアルゴリズムは，古典アルゴリズムと量子アルゴリズムの併用

本講義では，古典アルゴリズムの部分の詳細については省略し，量子アルゴリズムの部分に焦点を絞ることにする

解説の流れ

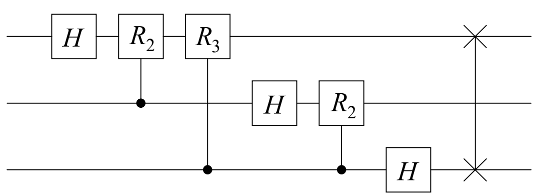
1. 量子Fourier変換
2. Order-findingアルゴリズム
3. Shorのアルゴリズム

量子Fourier変換

FFTの量子計算版 $\left|j\right\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi ijk/N)\left|k\right\rangle$

例　QFT_8を実行する量子回路

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^k) \end{bmatrix}$$



QFT_8の行列表示

$$QFT_8 = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

$$\omega = \exp(2\pi i/8) = \sqrt{i}$$
$$\omega^i + \omega^{i+4} = 0$$

QFTの実行例, N=8

$$\sum_{j=0}^{7}\alpha_j|j\rangle \xrightarrow{QFT_8} \sum_{k=0}^{7}\beta_k|k\rangle$$

r	input string $\{\alpha_j\}$		output string $\{\beta_k\}$	N/r
8	1 0 0 0 0 0 0 0	→	1 1 1 1 1 1 1 1	1
4	1 0 0 0 1 0 0 0	→	1 0 1 0 1 0 1 0	2
2	1 0 1 0 1 0 1 0	→	1 0 0 0 1 0 0 0	4
1	1 1 1 1 1 1 1 1	→	1 0 0 0 0 0 0 0	8

$$\frac{1}{\sqrt{2}}(|0\rangle+|4\rangle) \xrightarrow{QFT_8} \frac{1}{2}(|0\rangle+|2\rangle+|4\rangle+|6\rangle)$$

input string $\{\alpha_j\}$		output string $\{\beta_k\}$
1 0 0 0 1 0 0 0	→	1 0 1 0 1 0 1 0
0 1 0 0 0 1 0 0	→	1 0 i 0 -1 0 $-i$ 0
0 0 1 0 0 0 1 0	→	1 0 -1 0 1 0 -1 0
0 0 0 1 0 0 0 1	→	1 0 $-i$ 0 -1 0 i 0

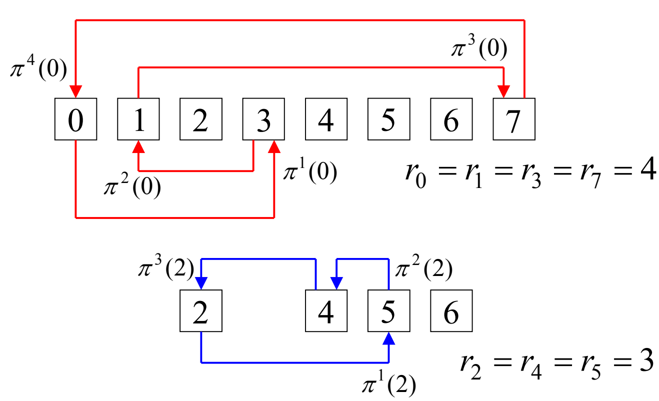
$$\frac{1}{\sqrt{2}}(|3\rangle+|7\rangle) \xrightarrow{QFT_8} \frac{1}{2}(|0\rangle-i|2\rangle-|4\rangle+i|6\rangle)$$

置換の位数(order)

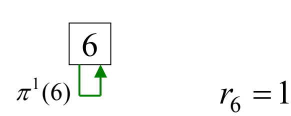
y から置換 π を繰り返して，元のy に戻る最小の回数を置換 $\pi(y)$の位数 r_y と呼ぶ

置換 $\pi(y)$の例

y	$\pi(y)$
0	3
1	7
2	5
3	1
4	2
5	4
6	6
7	0

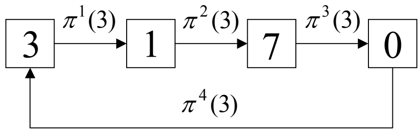


一般に，置換の位数の決定(order-finding)には，指数オーダーの時間を要する

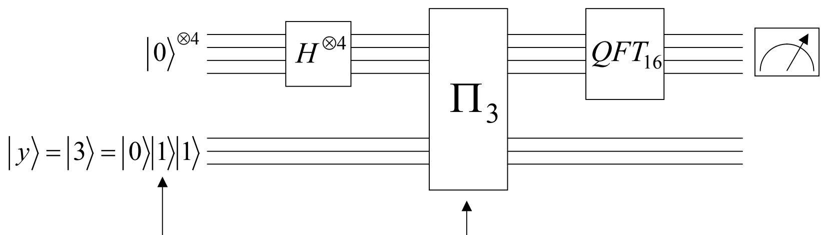


Order-finding

例として，$y=3$の場合を考える



$$\pi^0(3)=\pi^4(3)=\pi^8(3)=\pi^{12}(3)=\cdots=3$$
$$\pi^1(3)=\pi^5(3)=\pi^9(3)=\pi^{13}(3)=\cdots=1$$
$$\pi^2(3)=\pi^6(3)=\pi^{10}(3)=\pi^{14}(3)=\cdots=7$$
$$\pi^3(3)=\pi^7(3)=\pi^{11}(3)=\pi^{15}(3)=\cdots=0$$



$y=0,1,\ldots,7$ なので3-qubitをwork bitに用意

$$\Pi_y|x\rangle|y\rangle=|x\rangle|\pi^x(y)\rangle$$

Order-findingの実行過程

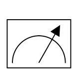
$$|0\rangle^{\otimes 4}|3\rangle \xrightarrow{H^{\otimes 4}} \frac{1}{4}\sum_{x=0}^{15}|x\rangle|3\rangle$$

$$QFT_{16}=\frac{1}{\sqrt{16}}\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \lambda^1 & \lambda^2 & \cdots & \lambda^{15}\\ 1 & \lambda^2 & \lambda^4 & \cdots & \lambda^{14}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \lambda^{15} & \lambda^{14} & \cdots & \lambda^1\end{bmatrix}$$

$$\lambda=\exp(2\pi i/16)$$
$$\lambda^i+\lambda^{i+8}=0$$

$$\xrightarrow{\Pi_3} \frac{1}{4}\sum_{x=0}^{15}|x\rangle|\pi^x(3)\rangle$$
$$=\frac{1}{4}(|0\rangle+|4\rangle+|8\rangle+|12\rangle)|3\rangle$$
$$+\frac{1}{4}(|1\rangle+|5\rangle+|9\rangle+|13\rangle)|1\rangle$$
$$+\frac{1}{4}(|2\rangle+|6\rangle+|10\rangle+|14\rangle)|7\rangle$$
$$+\frac{1}{4}(|3\rangle+|7\rangle+|11\rangle+|15\rangle)|0\rangle$$

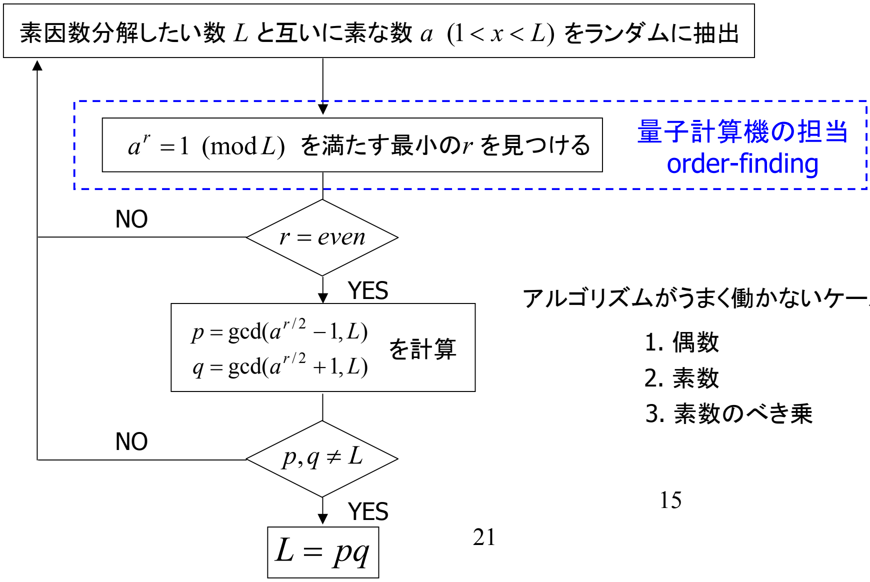
$$\xrightarrow{QFT_{16}} \frac{1}{4}(|0\rangle+|4\rangle+|8\rangle+|12\rangle)|3\rangle+$$
$$\frac{1}{4}(|0\rangle+i|4\rangle-|8\rangle-i|12\rangle)|1\rangle+$$
$$\frac{1}{4}(|0\rangle-|4\rangle+|8\rangle-|12\rangle)|7\rangle+$$
$$\frac{1}{4}(|0\rangle-i|4\rangle-|8\rangle+i|12\rangle)|0\rangle$$



→ 0, 4, 8, 12
(N/r =16/r の整数倍)
のいずれかを得る

→ 古典コンピュータを用いた連分数展開により r を決定

Shorのアルゴリズムの流れ



アルゴリズムがうまく働かないケース

1. 偶数
2. 素数
3. 素数のべき乗

15

21

乗法群の位数

$a^r = 1 \pmod{L}$ を満たす最小のr を「乗法群の位数」と呼ぶ

➡ 「置換の位数」との関係は?

➡ $\pi(y) \equiv ay \pmod{L}$ とすると, $\pi(y)$ は「置換」になっている

$L=15$以下のL と互いに素な数　$a = \{2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14\}$

$a = 7$ のとき

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8

$a = 11$ のとき

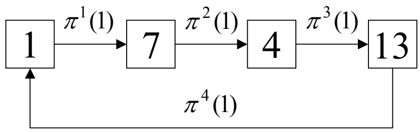
y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4

$a^x \pmod{L}$ $\Leftrightarrow$ $\pi^x(1)$ だから, 「乗法群の位数」は「置換 $\pi(y)$ の位数」と同じ

素因数分解, L=15の例

L =15以下のL と互いに素な数　$a = \{2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14\}$

$a = 7$

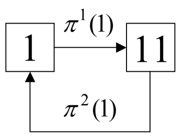


$r_2 = r_7 = r_8 = r_{13} = 4$

$a^{r/2} - 1 = 48 \quad \to \quad \gcd(48,\ 15) = 3$

$a^{r/2} + 1 = 50 \quad \to \quad \gcd(50,\ 15) = 5$

$a = 11$

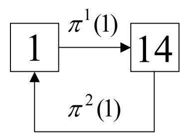


$r_4 = r_{11} = r_{14} = 2$

$a^{r/2} - 1 = 10 \quad \to \quad \gcd(10,\ 15) = 5$

$a^{r/2} + 1 = 12 \quad \to \quad \gcd(12,\ 15) = 3$

$a = 14$



失敗!!

$a^{r/2} - 1 = 13 \quad \to \quad \cancel{\gcd(13,\ 15) = 1}$

$a^{r/2} + 1 = 15 \quad \to \quad \cancel{\gcd(15,\ 15) = 15}$

Euclidの互除法

最大公約数を求める
アルゴリズム

例　$\gcd(494,\ 133)$

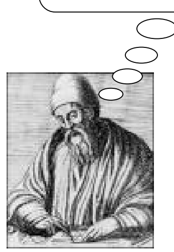
$494 = 133 \times 3 + 95$

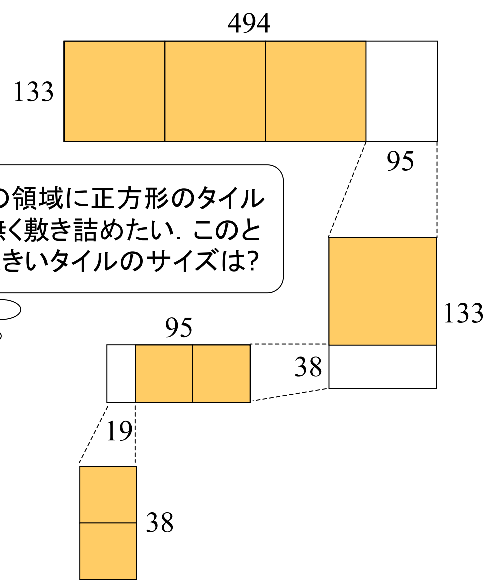
$133 = 95 \times 1 + 38$

$95 = 38 \times 2 + 19$

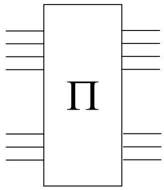
$38 = \underline{19} \times 2$

長方形の領域に正方形のタイルを隙間無く敷き詰めたい. このとき最も大きいタイルのサイズは?





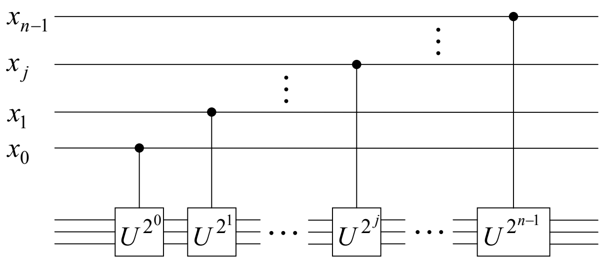
Πゲート



$$\Pi|x\rangle|y\rangle = |x\rangle|a^x y (\mathrm{mod}\, L)\rangle$$

$x = 2^{n-1}x_{n-1} + 2^{n-2}x_{n-2} + \cdots + 2x_1 + x_0$ だから，

$$a^x (\mathrm{mod}\, L) = a^{2^{n-1}x_{n-1}} a^{2^{n-2}x_{n-2}} \cdots a^{2x_1} a^{x_0} (\mathrm{mod}\, L)$$
$$= (a^{2^{n-1}x_{n-1}} (\mathrm{mod}\, L))(a^{2^{n-2}x_{n-2}} (\mathrm{mod}\, L)) \cdots (a^{x_0} (\mathrm{mod}\, L))$$



$$U^{2^j}|y\rangle = |a^{2^j} y (\mathrm{mod}\, L)\rangle$$

$a^{2^j} (\mathrm{mod}\, L)$ の値は，古典計算機ですぐに計算できるので，ゲートを構成できる

「x_j が1のときにゲートを実行」を繰り返す

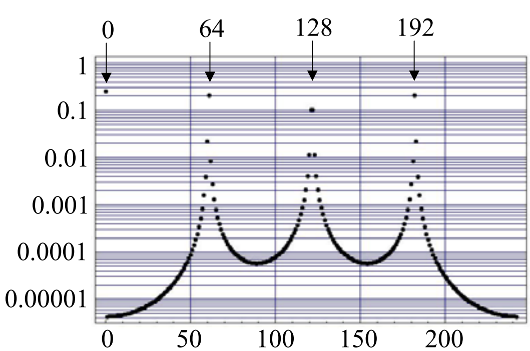
15の素因数分解

Step.1 ランダムに a を選ぶ

$$a = 7$$

Step.2 Order-finding

QFTの結果の例 (N=2^8=256)



© Colin P. Williams (1997)

Step.3 観測し，連分数展開で r を決定

$$r = 4$$

Step.4 $p = \gcd(a^{r/2} - 1, L)$, $q = \gcd(a^{r/2} + 1, L)$ を計算

$$a^{r/2} - 1 = 48 \quad \rightarrow \quad \gcd(48,\ 15) = 3$$
$$a^{r/2} + 1 = 50 \quad \rightarrow \quad \gcd(50,\ 15) = 5$$

$$15 = 3 \times 5$$

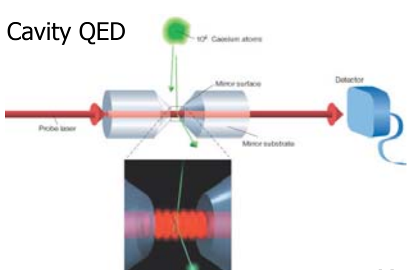
アルゴリズム終了

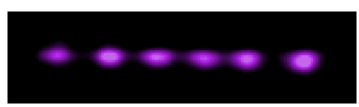
量子アルゴリズムのまとめ

- Deutsch-Jozsaのアルゴリズム
  - 量子並列性と量子干渉を利用
  - 決定性アルゴリズム
- Groverの検索アルゴリズム
  - Oracleの利用した汎用性の高いアルゴリズム
- Shorの素因数分解アルゴリズム
  - QFTによる周期性の発見
  - 確率的アルゴリズム

Physical Realization

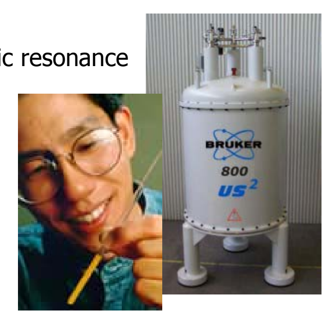
Cavity QED

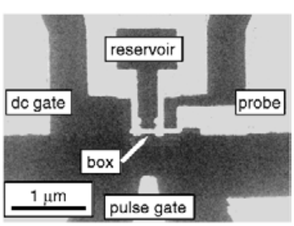




Ion trap

Magnetic resonance

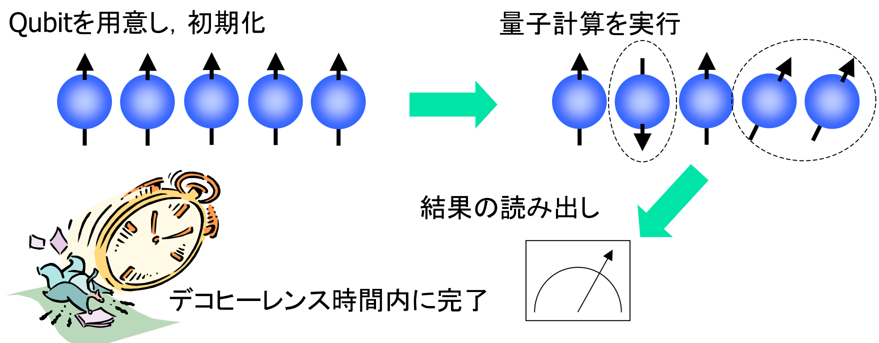




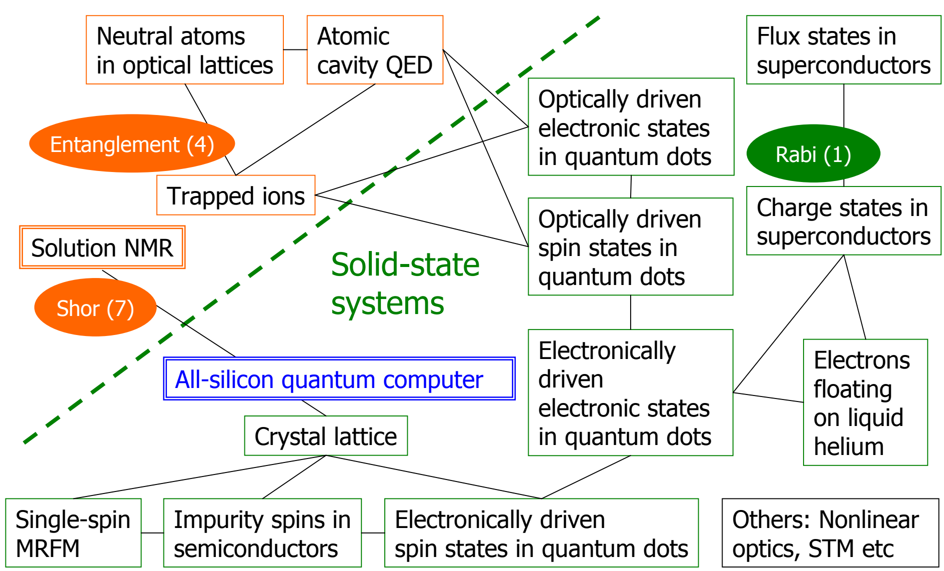
Superconductor

DiVincenzo's Criteria

1. Well defined extensible qubit array
2. Preparable in the “000…” state
3. Long decoherence time
4. Universal set of gate operations
5. Single quantum measurements



量子コンピュータの提案



補遺:量子Fourier変換

$$|j\rangle \ \rightarrow \ \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp(2\pi ijk/N)|k\rangle$$

2進数による表現

$$|j_1 j_2\cdots j_n\rangle \ \rightarrow \ \frac{1}{2^{n/2}}\left[|0\rangle+\exp(2\pi i0.j_n)|1\rangle\right]\left[|0\rangle+\exp(2\pi i0.j_{n-1}j_n)|1\rangle\right]\cdots\left[|0\rangle+\exp(2\pi i0.j_1 j_2\cdots j_n)|1\rangle\right]$$

$$\text{where,} \quad j = j_1 j_2\cdots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0 \quad 0.j_1 j_2\cdots j_n = \frac{j_1}{2}+\frac{j_2}{2^2}+\cdots+\frac{j_n}{2^n}$$

$$|j\rangle \rightarrow \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1}\exp(2\pi ijk/2^n)|k\rangle$$
k の2進数表示

$$=\frac{1}{2^{n/2}}\boxed{\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}}\exp\boxed{(2\pi ij\sum_{l=1}^{n}k_l 2^{-l})|k_1\cdots k_n\rangle}$$
状態のテンソル積＆指数法則

$$=\frac{1}{2^{n/2}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\boxed{\bigotimes_{l=1}^{n}}\exp(2\pi ijk_l 2^{-l})\boxed{|k_l\rangle}$$
状態ごとにばらばらに計算可能

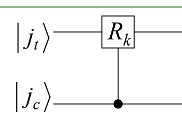
$$=\frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\left[\boxed{\sum_{k_l=0}^{1}}\exp(2\pi ij\boxed{k_l}2^{-l})\boxed{|k_l\rangle}\right]$$
k_l=0,1 を代入

$$=\frac{1}{2^{n/2}}\bigotimes_{l=1}^{n}\boxed{\left[|0\rangle+\exp(2\pi ij2^{-l})|1\rangle\right]}$$
j の2進数表示＆指数関数の周期性

$$=\frac{1}{2^{n/2}}\left[|0\rangle+\exp(2\pi i\boxed{0.j_n})|1\rangle\right]\left[|0\rangle+\exp(2\pi i\boxed{0.j_{n-1}j_n})|1\rangle\right]\cdots\left[|0\rangle+\exp(2\pi i\boxed{0.j_1 j_2\cdots j_n})|1\rangle\right]$$

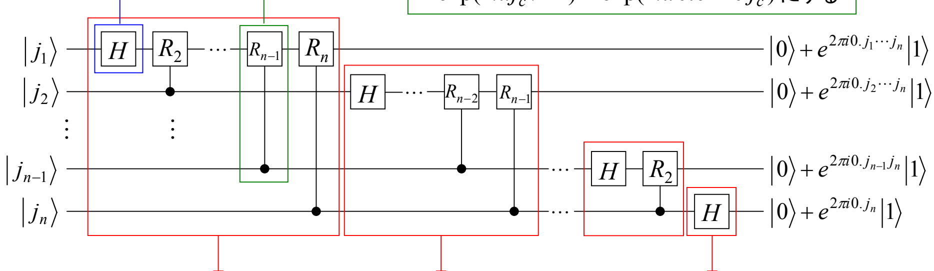
補遺:QFTを実行する量子回路

$$\left.\begin{array}{ll}|0\rangle+|1\rangle & (j_k=0)\\ |0\rangle-|1\rangle & (j_k=1)\end{array}\right\} = |0\rangle+\exp(\pi ij_k)|1\rangle$$
$$= |0\rangle+\exp(2\pi i0.j_k)|1\rangle$$



$$R_k = \begin{bmatrix}1 & 0\\ 0 & \exp(2\pi i/2^k)\end{bmatrix}$$

$|j_c\rangle=|0\rangle$ のときも含めて, $|j_t\rangle=|1\rangle$ の位相を $\exp(2\pi ij_c/2^k)=\exp(2\pi i0.0\cdots0j_c)$ にする



$$\frac{1}{2^{n/2}}\left[|0\rangle+\exp(2\pi i0.j_1 j_2\cdots j_n)|1\rangle\right]\left[|0\rangle+\exp(2\pi i0.j_2\cdots j_n)|1\rangle\right]\cdots\left[|0\rangle+\exp(2\pi i0.j_n)|1\rangle\right]$$

SWAP

$$\frac{1}{2^{n/2}}\left[|0\rangle+\exp(2\pi i0.j_n)|1\rangle\right]\left[|0\rangle+\exp(2\pi i0.j_{n-1}j_n)|1\rangle\right]\cdots\left[|0\rangle+\exp(2\pi i0.j_1 j_2\cdots j_n)|1\rangle\right]$$