量子計算基礎

東京工業大学
河内　亮周

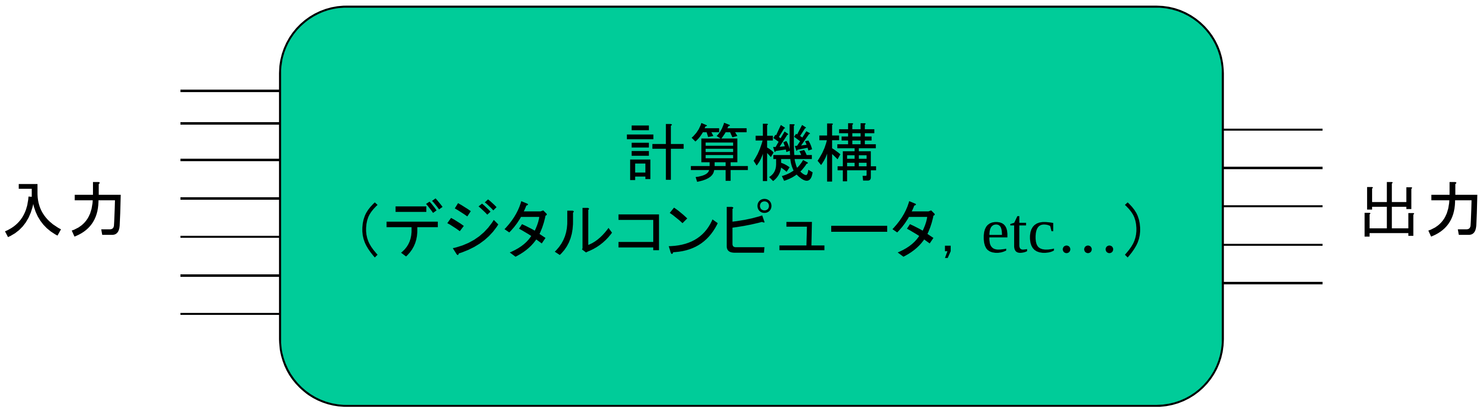
概要

- 計算って何？
  - 数理科学的に「計算」を扱うには･･･
- 量子力学を計算に使おう！
  - 量子情報とは？
  - 量子情報に対する演算＝量子計算
- 一般的な量子回路の構成方法

計算って何？

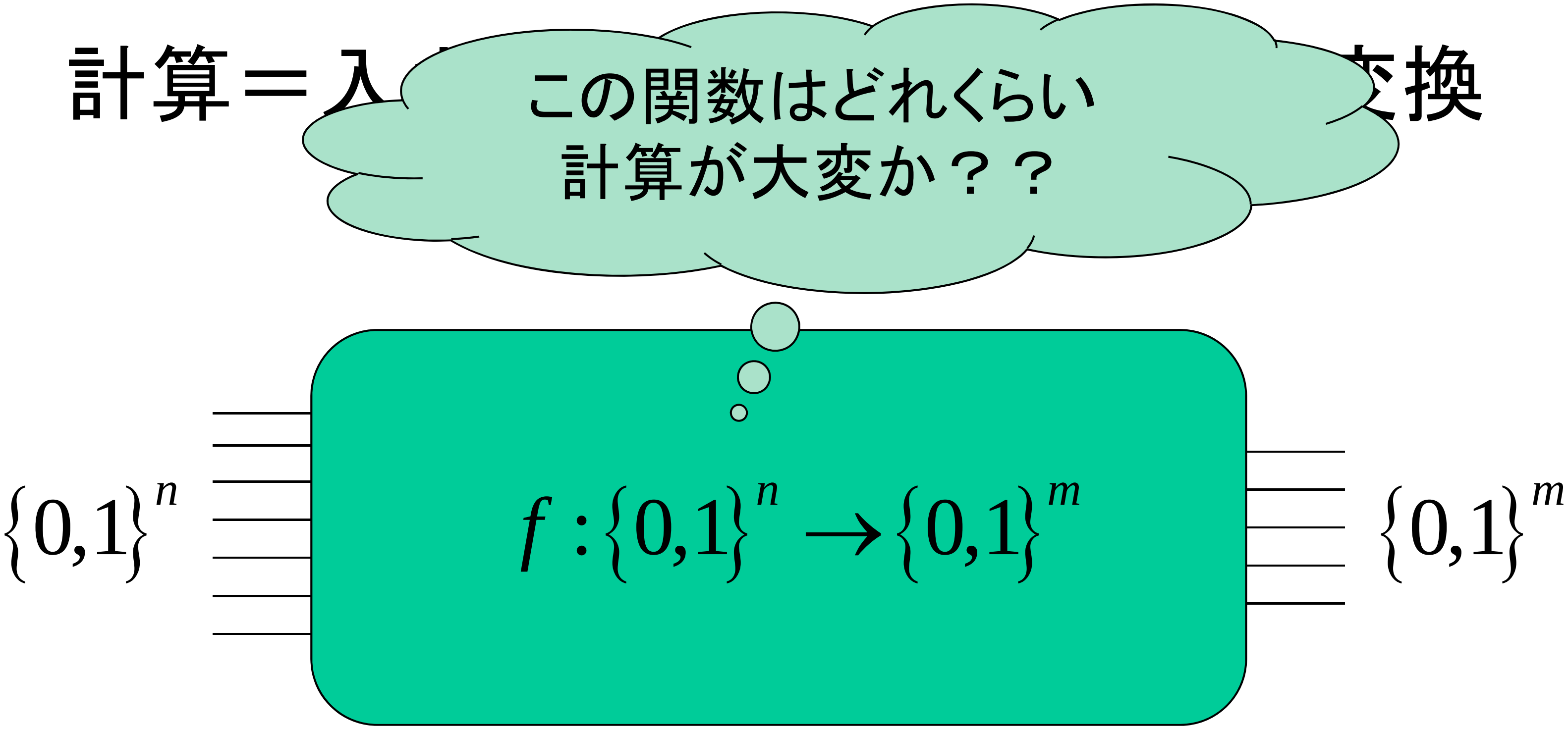
計算とは？

計算＝入力情報から出力情報への変換



計算とは？

計算＝入　変換



計算モデル

- 「計算の複雑さ」を定量的に扱いたい！
  - 計算したい関数は難しい？易しい？
  - **入力の大きさ**に応じてどれぐらい難しくなる？

- まず「基準」となる計算モデルを決めよう！
  - Turing機械
  - 論理回路（族）
  - Branching Program
  - etc…

論理関数を使った計算

- 論理関数　$f:\{0,1\}^n \to \{0,1\}^m$（今回はｍ＝１）

e.g.: ４入力１出力論理関数

$$f(x_1, x_2, x_3, x_4) = (x_1 \vee x_2 \vee \neg x_4) \wedge (\neg x_3 \vee x_1 \vee \neg x_2)$$

- 計算したい関数を「基本素子」で構成しよう！
  - 基本素子 : AND, OR, NOT

- 計算＝「関数」を「基本構成要素」の組合せで実現
- 計算の複雑さ＝「基本構成要素」がどれくらいいるか？

AND:

$$\{0,1\}^2 \to \{0,1\}$$

x	y	$x \wedge y$
0	0	0
1	0	0
0	1	0
1	1	1

OR:

$$\{0,1\}^2 \to \{0,1\}$$

x	y	$x \vee y$
0	0	0
1	0	1
0	1	1
1	1	1

NOT:

$$\{0,1\} \to \{0,1\}$$

x	$\neg x$
0	1
1	0

任意の論理関数が表現可能

例：偶奇判定

- 入力：n ビット列　$x_1, \cdots, x_n \in \{0,1\}$
- 出力：“1”の数が偶数ならば 0，奇数ならば 1

例：4ビットの偶奇判定を行う論理関数

$$f(0000) = 0$$
$$f(0001) = 1$$
$$f(0010) = 1$$
$$\vdots$$
$$f(1111) = 0$$

偶奇判定関数

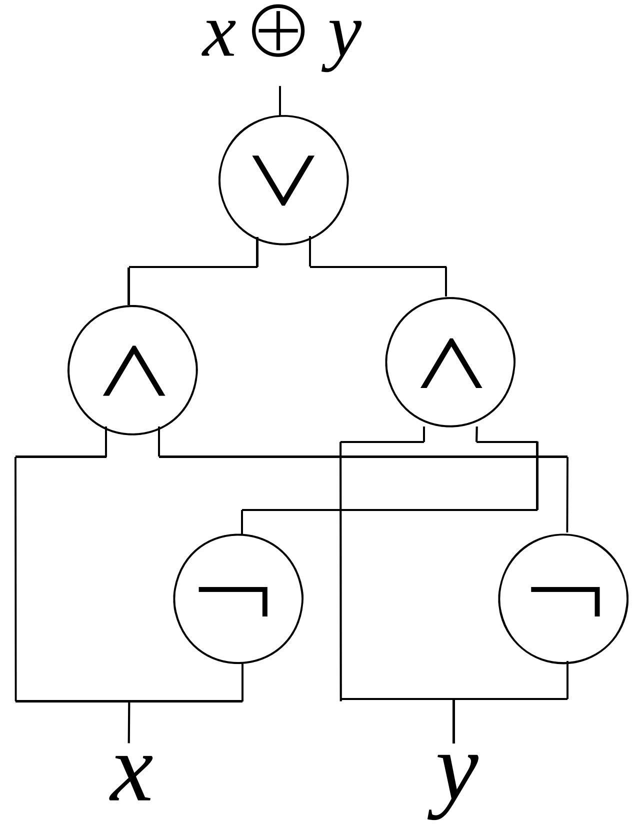
$$f\left(x_1,\cdots,x_n\right)=x_1\oplus\cdots\oplus x_n$$

$\oplus$: 排他的論理和（XOR）

（＝mod 2の足し算）

x	y	$x\oplus y$
0	0	0
1	0	1
0	1	1
1	1	0

$$x \oplus y = (\neg x \wedge y) \vee (x \wedge \neg y)$$



$$f\left(x_1,\cdots,x_n\right)=x_1\oplus\cdots\oplus x_n$$
$$=\left(x_1\oplus x_2\oplus\cdots\right)\oplus\left(\cdots\oplus x_{n-1}\oplus x_n\right)$$

e.g., ４変数の場合

$$\left(x_1\oplus x_2\right)\oplus\left(x_3\oplus x_4\right)$$
$$=\left(\left(x_1\oplus x_2\right)\wedge\neg\left(x_3\oplus x_4\right)\right)\vee\left(\neg\left(x_1\oplus x_2\right)\wedge\left(x_3\oplus x_4\right)\right)$$

再帰的に{AND,OR,NOT}に展開可能！

➔偶奇判定関数は基本素子で実現可能

計算の複雑さの指標：e.g., 使用する素子数 $\left(O(n)\right)$

オーダー記法について

- 計算複雑さの評価＝入力サイズnの関数
  - nが大きくなるにつれて「大体」どうなるか？
  - 支配的なところだけを抜き出したい

ある論理回路のサイズ $s(n)$ がオーダー $t(n)$

$$s(n) = O(t(n)) \Leftrightarrow \exists C > 0 : \overline{\lim_{n\to\infty}} \left| \frac{s(n)}{t(n)} \right| < C$$

例:

$$s(n) = 4n^2 + 200n + 84241 \quad \Rightarrow \quad s(n) = O(n^2)$$

$$s(n) = 5n\log n + 3n\log\log n \quad \Rightarrow \quad s(n) = O(n\log\log n)$$

$$s(n) = 50n^{10}2^{0.08n} \quad \Rightarrow \quad s(n) = O(n^{10}2^{0.08n})$$

一般の論理関数では？

- Shannon 展開を使うと $O\left(2^n\right)$個の素子で実現可能！

$\boxed{\text{Shannon展開}}$

$$f\left(x_1, x_2, ..., x_n\right)$$

$$= \left(x_1 \wedge f\left(1, x_2, ..., x_n\right)\right) \vee \left(\neg x_1 \wedge f\left(0, x_2, ..., x_n\right)\right)$$

$s\left(n\right)$ ＝n変数論理関数を実現するのに十分な素子数

$$s\left(n\right) \leq 2s\left(n-1\right) + 4, \quad s\left(1\right) = 1$$

$$s\left(n\right) = O\left(2^n\right)$$

量子力学を計算に使おう！

～古典情報処理から量子情報処理へ～

古典情報と量子情報の違い

- 古典的な1ビットの内容は

  0 or 1

- 量子情報における1ビットの内容は

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

“0である状態と1である状態の(量子力学的)重ね合わせ”

α :状態 $\left|0\right\rangle$ の振幅　β :状態 $\left|1\right\rangle$ の振幅

量子ビット(q-bit)

- 量子ビットを「観測」すると

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

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

確率 $\left|\alpha\right|^2$で $\left|0\right\rangle$

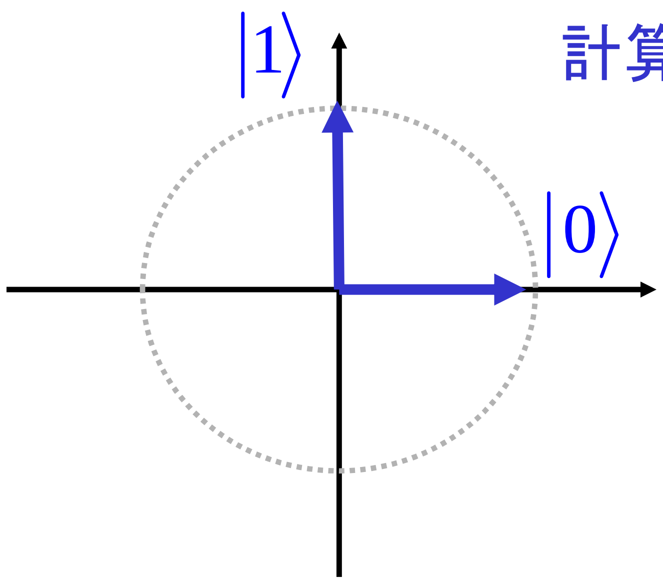
確率 $\left|\beta\right|^2$で $\left|1\right\rangle$

量子ビットは観測により確率的に振舞う

量子ビットの表現

１量子ビット＝2次元複素ベクトル（長さ1）

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



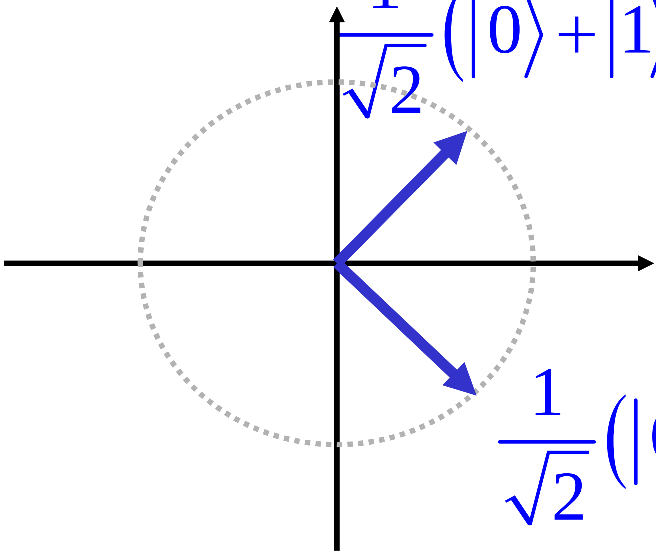
計算基底 $|0\rangle, |1\rangle$

量子ビットの表現

１量子ビット＝2次元複素ベクトル（長さ1）

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

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



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

量子ビットの測定

$$\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$$ を射影測定 $$M = \left\{M_0, M_1\right\}$$ で測定

$$M_0 = \left|0\right\rangle\left\langle 0\right| = \begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$M_1 = \left|1\right\rangle\left\langle 1\right| = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

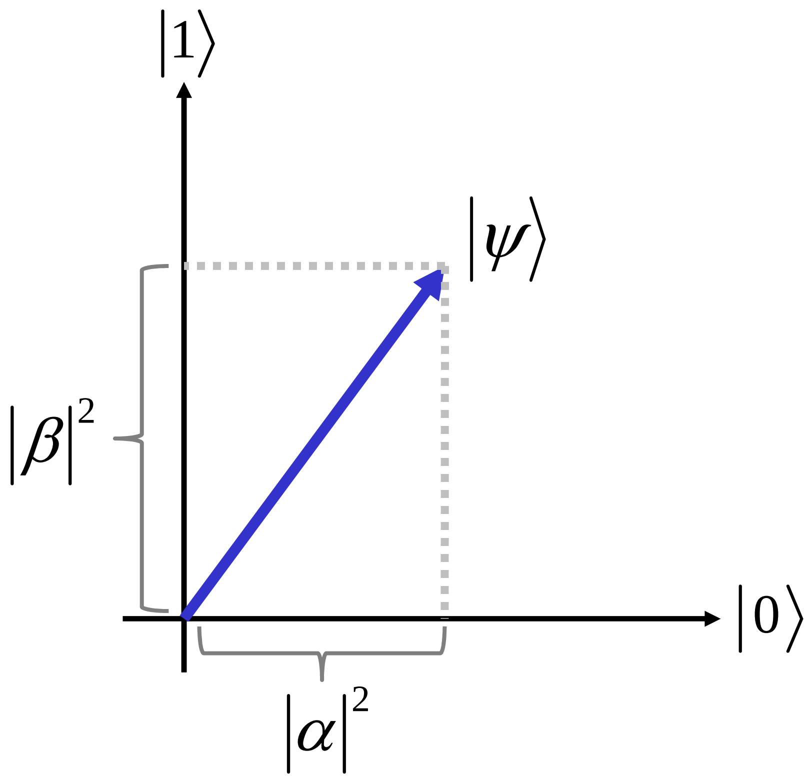
$$\Pr\left[\text{"0"㈴牋幘}\right] = \left\langle\psi\right|M_0^\dagger M_0\left|\psi\right\rangle = \left\langle\psi\right|\left|0\right\rangle\left\langle 0\right|\left|\psi\right\rangle = \left|\alpha\right|^2$$

$$\Pr\left[\text{"1"㈴牋幘}\right] = \left\langle\psi\right|M_1^\dagger M_1\left|\psi\right\rangle = \left\langle\psi\right|\left|1\right\rangle\left\langle 1\right|\left|\psi\right\rangle = \left|\beta\right|^2$$

量子ビットの測定

$$\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$$ を射影測定 $M = \{M_0, M_1\}$ で測定

$$M_0 = |0\rangle\langle 0|,\ M_1 = |1\rangle\langle 1|$$



複数の量子ビット＝各ビットのテンソル積

$$\left|\psi,\varphi\right\rangle=\left|\psi\right\rangle\otimes\left|\varphi\right\rangle=\left|\psi\right\rangle\left|\varphi\right\rangle$$

e.g.,

$$\left|00\right\rangle=\left|0\right\rangle\left|0\right\rangle=\left|0\right\rangle\otimes\left|0\right\rangle=\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

n 量子ビット＝ 2^n 次元複素ベクトル（長さ1）

$$\overset{0}{|00\rangle} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}\begin{matrix}<0\\ \\ \\ \end{matrix}$$

$$\overset{1}{|01\rangle} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\begin{matrix}\\ <1\\ \\ \end{matrix}$$

$$\overset{2}{|10\rangle} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}\begin{matrix}\\ \\ <2\\ \end{matrix}$$

$$\overset{3}{|11\rangle} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\begin{matrix}\\ \\ \\ <3\end{matrix}$$

おやくそく

- 量子状態は純粋状態のみ

- 測定は計算基底の射影測定のみ
  - 1ビット分の測定: $M = \left\{ |0\rangle\langle 0|, |1\rangle\langle 1| \right\}$
  - nビット分の測定:

$$M = \left\{ \underbrace{\overbrace{|0\cdots 00\rangle}^{n\text{㊯㊟㊤}}\overbrace{\langle 0\cdots 00|}^{n\text{㊯㊟㊤}}, |0\cdots 01\rangle\langle 0\cdots 01|, \cdots, |1\cdots 11\rangle\langle 1\cdots 11|}_{2^n\text{函}} \right\}$$

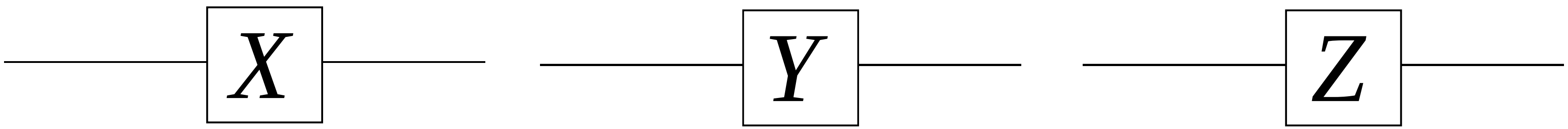
量子情報をどう処理する？

- 古典計算
  - 入出力: 古典ビット列
  - 演算: 論理回路
    - 基本論理素子の組み合わせにより実現
- 量子計算
  - 入出力: 量子状態
  - 演算: ユニタリ変換（と測定）
    - 基本量子素子と測定の組み合わせで実現
    - ユニタリ変換には可逆性が必要！➔ 入力長＝出力長

基本的なユニタリ変換

Pauli行列（１量子ビット入出力）

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



基本的なユニタリ変換

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = NOT$$

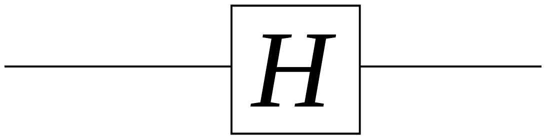
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \;\text{———}\; \boxed{X} \;\text{———}\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

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

基本的なユニタリ変換

Hadamard変換（１量子ビット入出力）

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



基本的なユニタリ変換

Hadamard変換（１量子ビット入出力素子）

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)$$

$$\left|0\right\rangle \;\text{———}\; \boxed{H} \;\text{———}\; \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)$$

基本的なユニタリ変換

Hadamard変換（１量子ビット入出力素子）

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

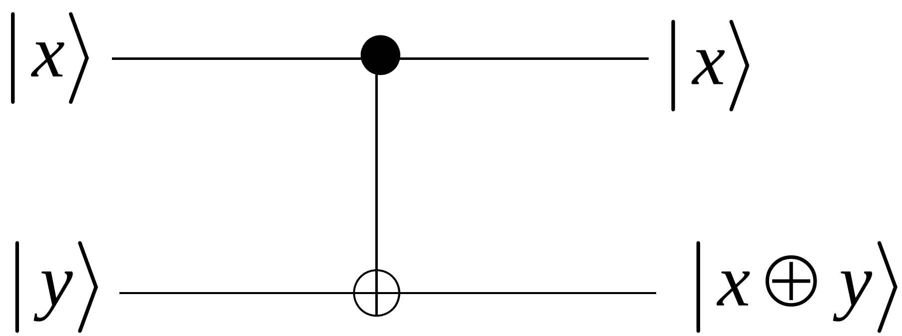
$$|1\rangle \;\text{———}\boxed{H}\text{———}\; \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

基本的なユニタリ変換

制御NOT（２量子ビット入出力素子）

$$CNOT = \begin{pmatrix} 1 & & 0 & \\ & 1 & & \\ & & 0 & 1 \\ 0 & & 1 & 0 \end{pmatrix}$$

$x, y \in \{0,1\}$

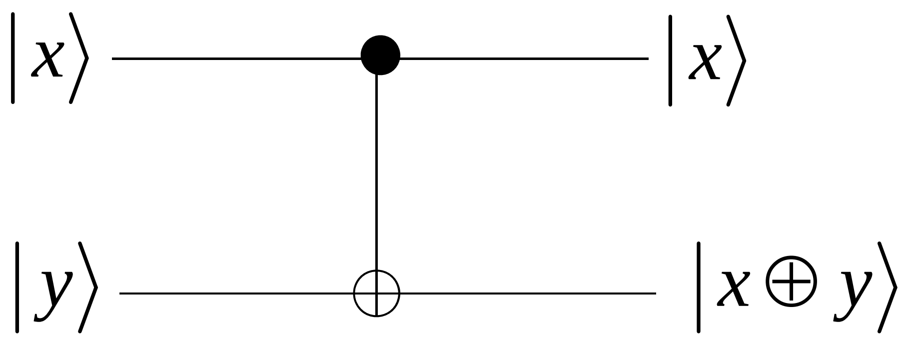


基本的なユニタリ変換

制御NOT（２量子ビット入出力素子）

$$CNOT \begin{cases} x=0 \longrightarrow y \text{ を素通し} \\ x=1 \longrightarrow y \text{ を反転} \end{cases}$$

$x, y \in \{0,1\}$

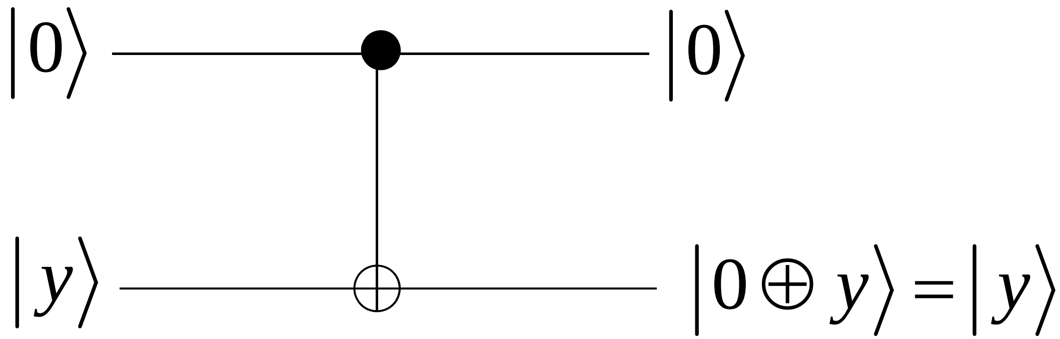


基本的なユニタリ変換

制御NOT（２量子ビット入出力素子）

$$CNOT \begin{cases} x=0 \longrightarrow y \text{ を素通し} \\ x=1 \longrightarrow y \text{ を反転} \end{cases}$$

$y \in \{0,1\}$

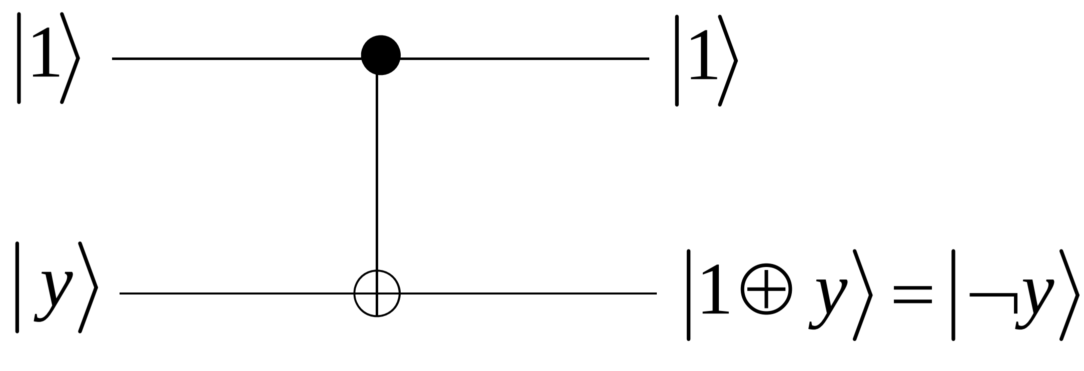


基本的なユニタリ変換

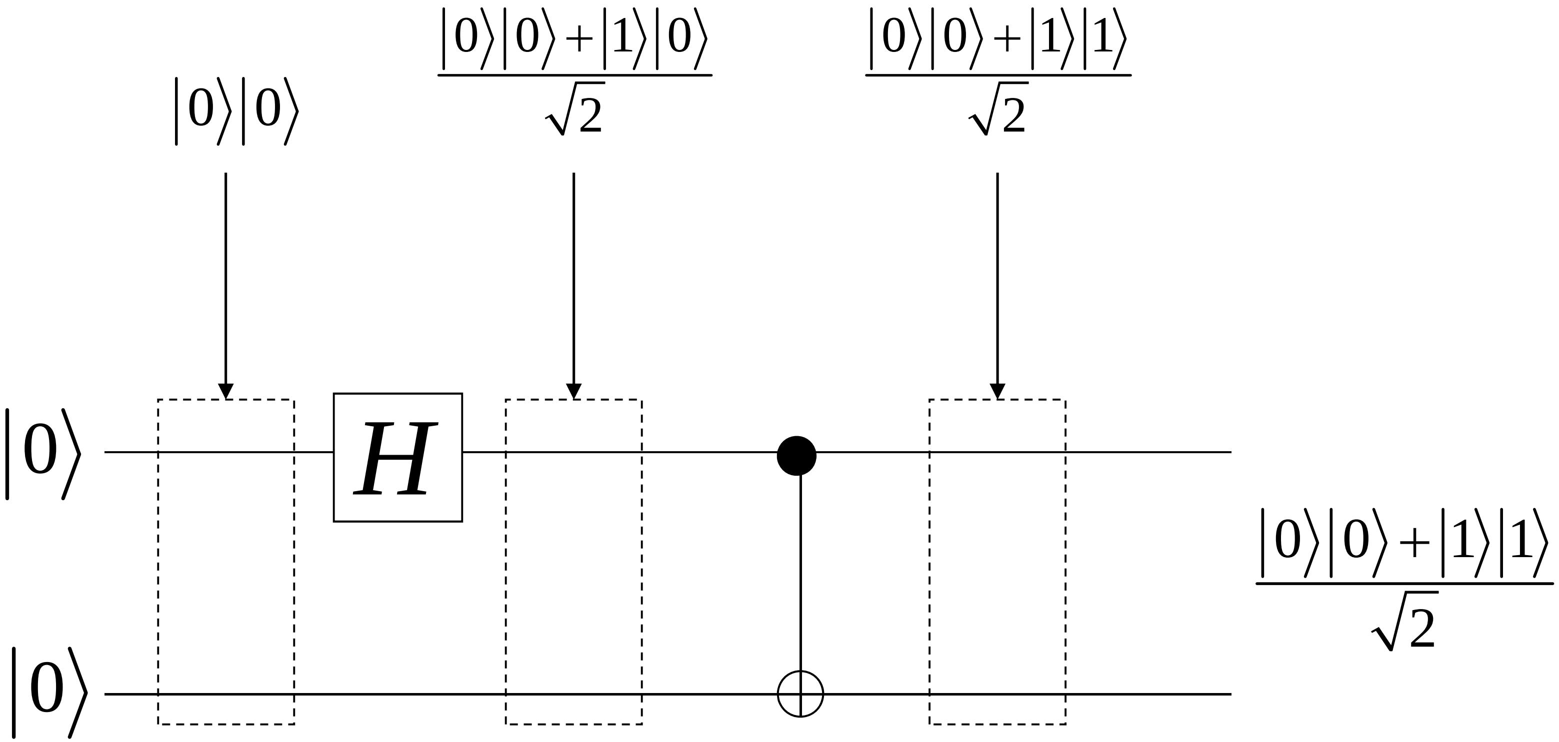
制御NOT（２量子ビット入出力素子）

$$CNOT \begin{cases} x=0 \longrightarrow y \text{ を素通し} \\ x=1 \longrightarrow y \text{ を反転} \end{cases}$$

$y \in \{0,1\}$



量子回路の例



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

基本量子素子から大きな量子回路へ

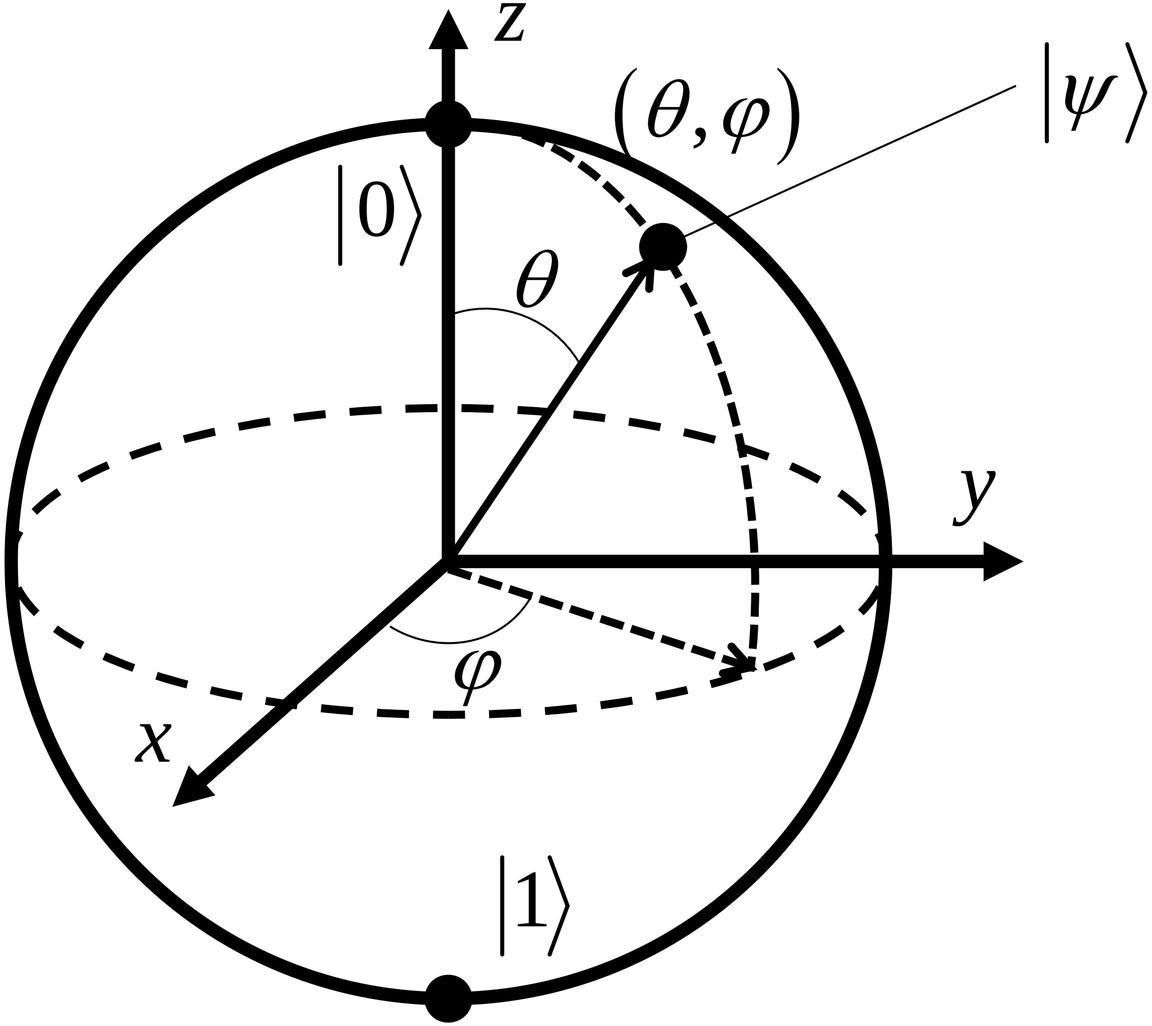
- 古典計算の場合，AND,OR,NOTを組み合わせて任意の論理関数を実現できた.
  - 素子数＝$O\left(2^n\right)$ 個（nビット入力）
- 量子計算の場合では？

  ➔１量子ビット素子とCNOTで可能！
  - 素子数＝$O\left(n^2 4^n\right)$ 個（n量子ビット入力）

１量子ビット素子の構成

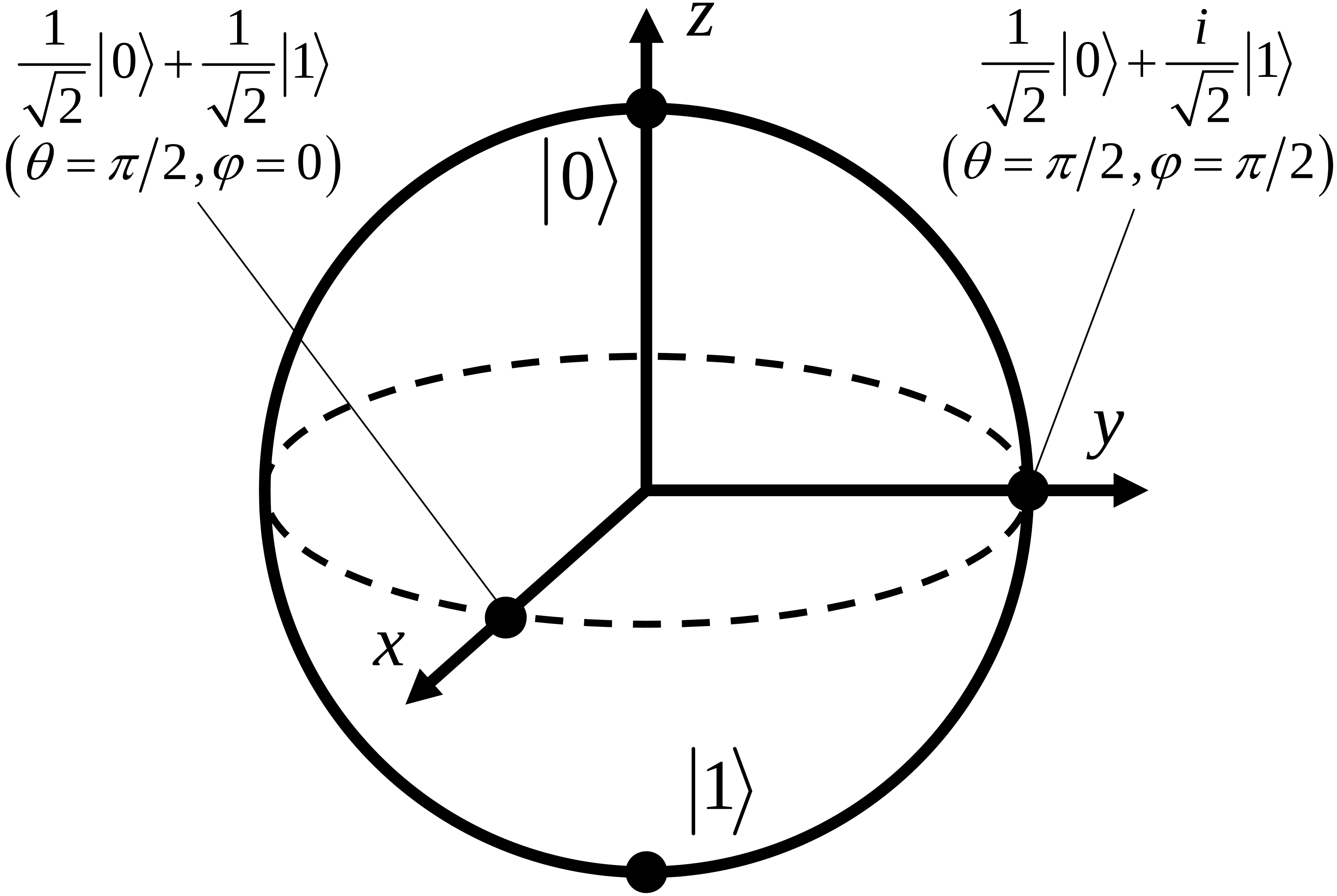
- Bloch球上の「回転素子」を使う
  - Bloch球＝１量子ビットの幾何的表現方法

Bloch球



$$\left|\psi\right\rangle = \cos\left(\theta/2\right)\left|0\right\rangle + e^{i\varphi}\sin\left(\theta/2\right)\left|1\right\rangle$$

Bloch球



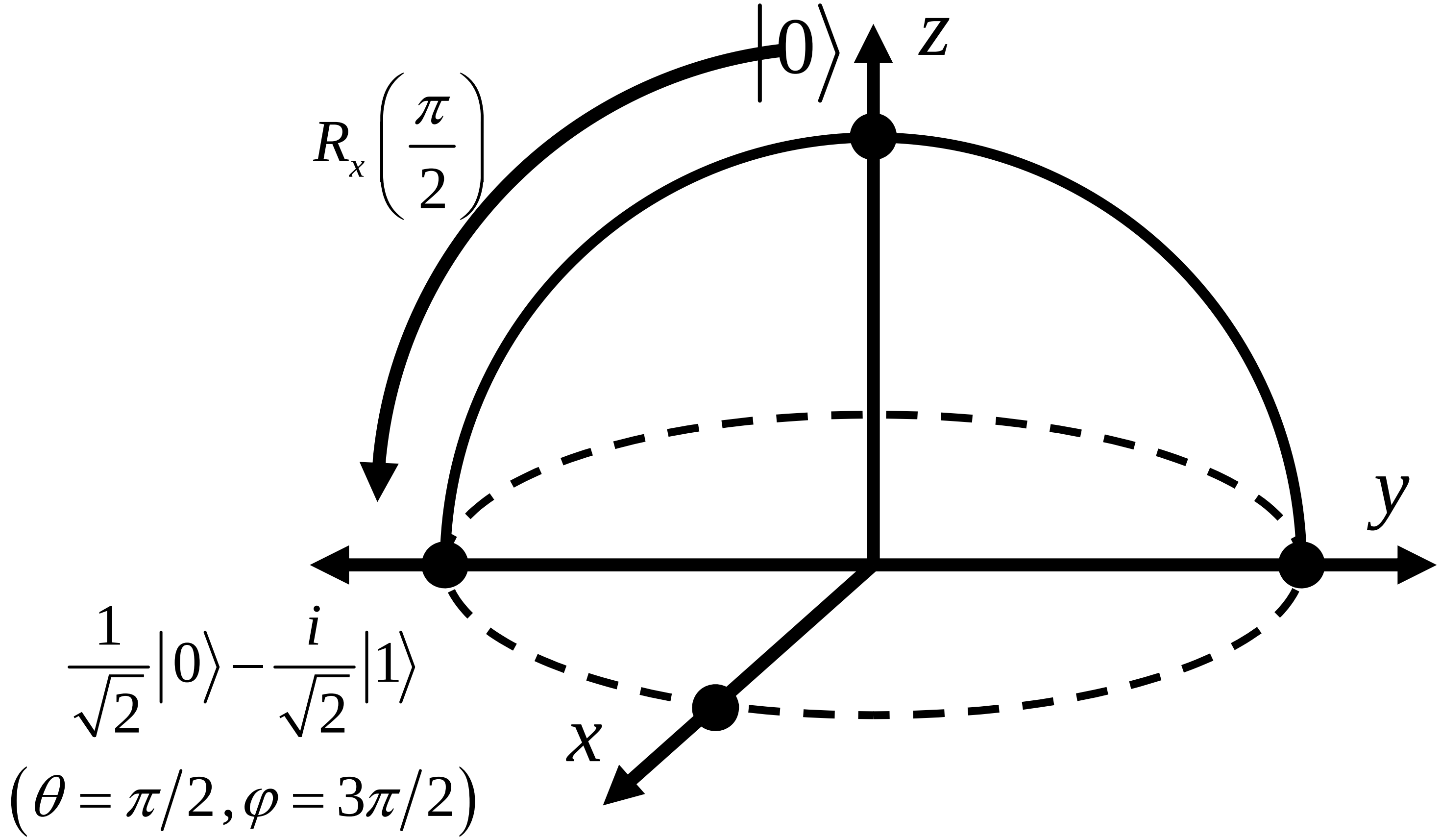
$$|\psi\rangle=\cos(\theta/2)|0\rangle+e^{i\varphi}\sin(\theta/2)|1\rangle$$

回転行列

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

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

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



$$R_x\left(\frac{\pi}{2}\right)|0\rangle = \begin{pmatrix} \cos\frac{\pi}{4} & -i\sin\frac{\pi}{4} \\ -i\sin\frac{\pi}{4} & \cos\frac{\pi}{4} \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$$

回転行列による表現

$$R_{\hat{n}}\left(\theta\right) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}\left(\hat{n}_x X + \hat{n}_y Y + \hat{n}_z Z\right)$$

$\hat{n} = \left(\hat{n}_x, \hat{n}_y, \hat{n}_z\right) \in \mathbb{R}^3$ ：回転軸

定理

$\forall U$ ：２次元ユニタリ変換（１量子ビット素子）

$\exists\alpha, \exists\hat{n}, \exists\theta$ ｓ．ｔ． $U = e^{i\alpha} R_{\hat{n}}\left(\theta\right)$

Z-Y回転分解

定理

$\forall U$：２次元ユニタリ変換（１量子ビット素子）

$\exists\alpha, \exists\beta, \exists\gamma, \exists\delta$　s．t.

$$U = e^{i\alpha} R_z\left(\beta\right) R_y\left(\gamma\right) R_z\left(\delta\right)$$

大域的位相 $e^{i\alpha}$ を無視すれば
１量子ビット素子は回転素子 $R_y\left(\theta\right), R_z\left(\theta\right)$ で実現できる

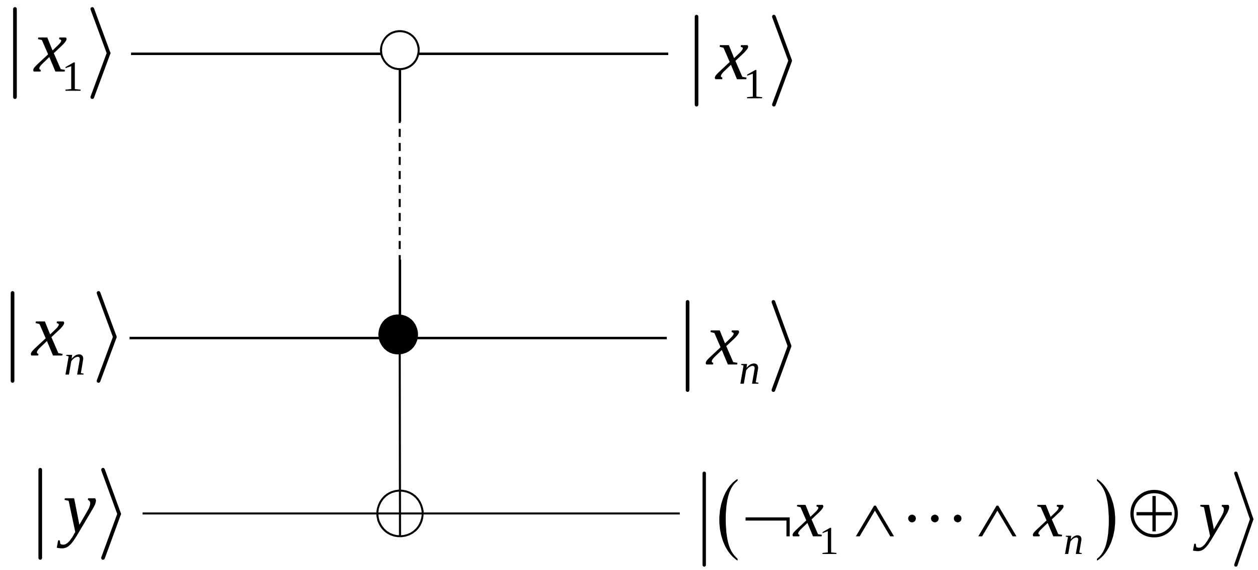
(R_z と R_x を入れ替えたX-Y回転分解も可能)

n量子ビット上ユニタリ行列

- 方針
  1. n-qbit U ➔ 一般化CNOT+制御1qbit素子
  2. 一般化CNOT ➔ 1-qbit素子+CNOT
  3. 制御1-qbit素子 ➔ 1-qbit素子+CNOT

最終的には 1-qbit素子＋CNOT で構成可能！

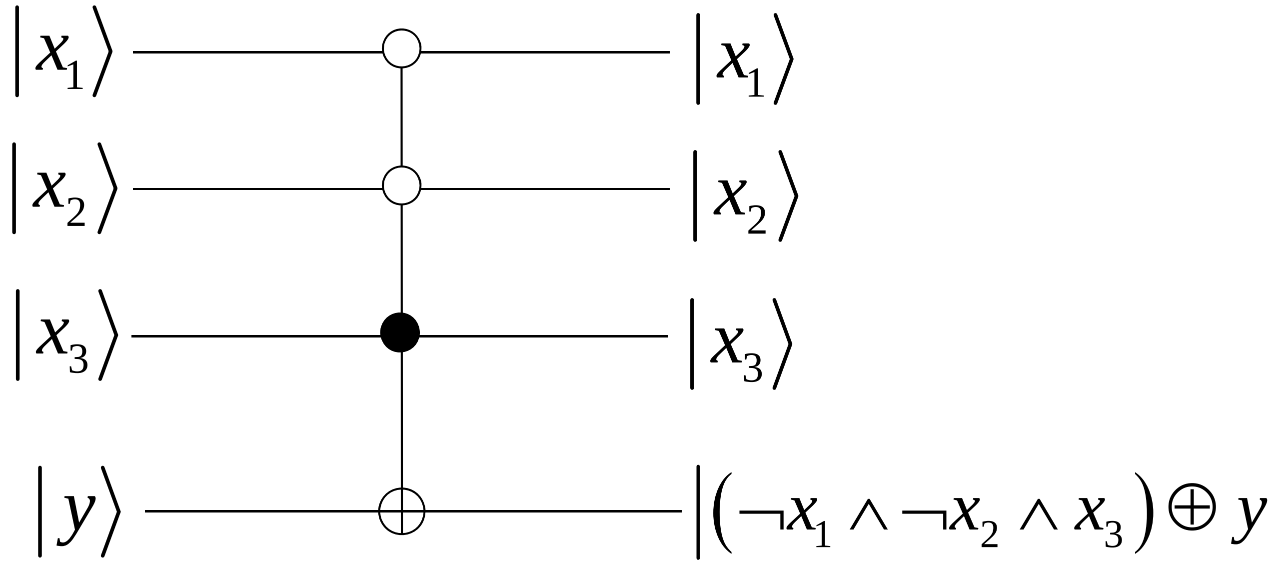
一般化CNOT素子



黒丸 ● ： 1が入力されるとスイッチオン

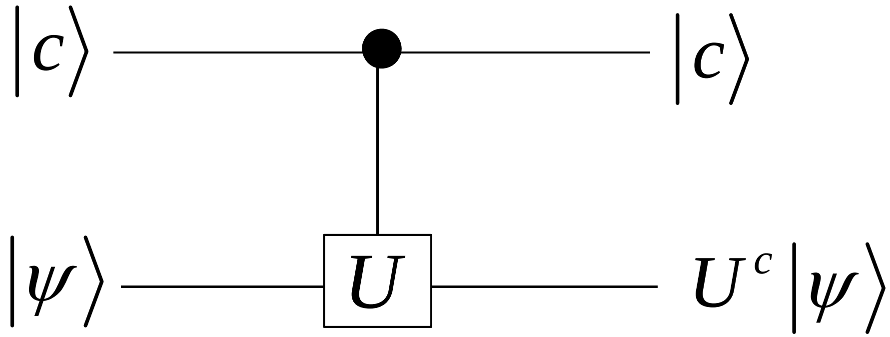
白丸 ○ ： 0が入力されるとスイッチオン

一般化CNOT素子（例）



$(x_1, x_2, x_3) = (0,0,1)$ のときのみ y を反転

制御1-qbit素子



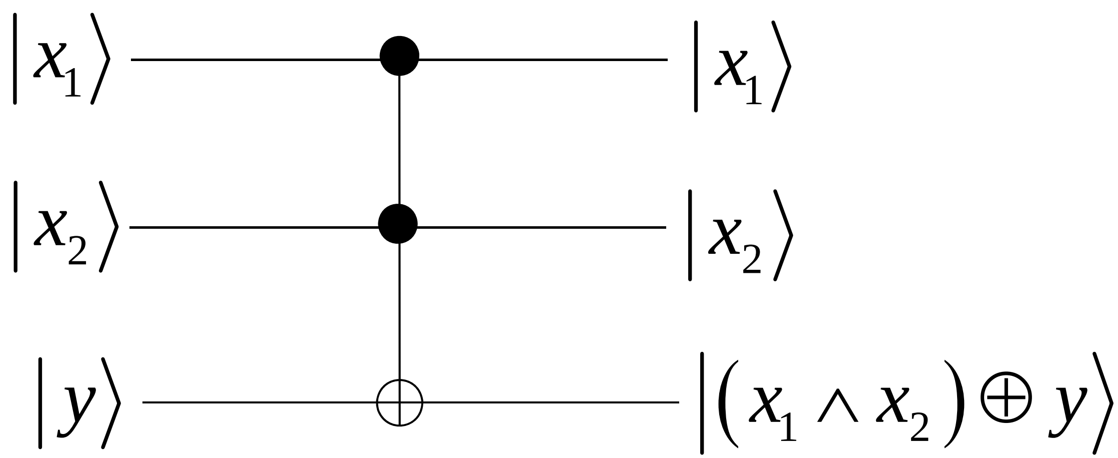
$$C(U) = \begin{pmatrix} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} & \mathbf{0} \\ \mathbf{0} & U \end{pmatrix}$$

詳細は板書にて

Toffoli素子（CCNOT素子）

$$CCNOT = \overbrace{\begin{pmatrix} 1 & & 0 & & \\ & \ddots & & & 0 \\ 0 & & 1 & & \\ & & & 0 & 1 \\ & 0 & & 1 & 0 \end{pmatrix}}^{8}$$

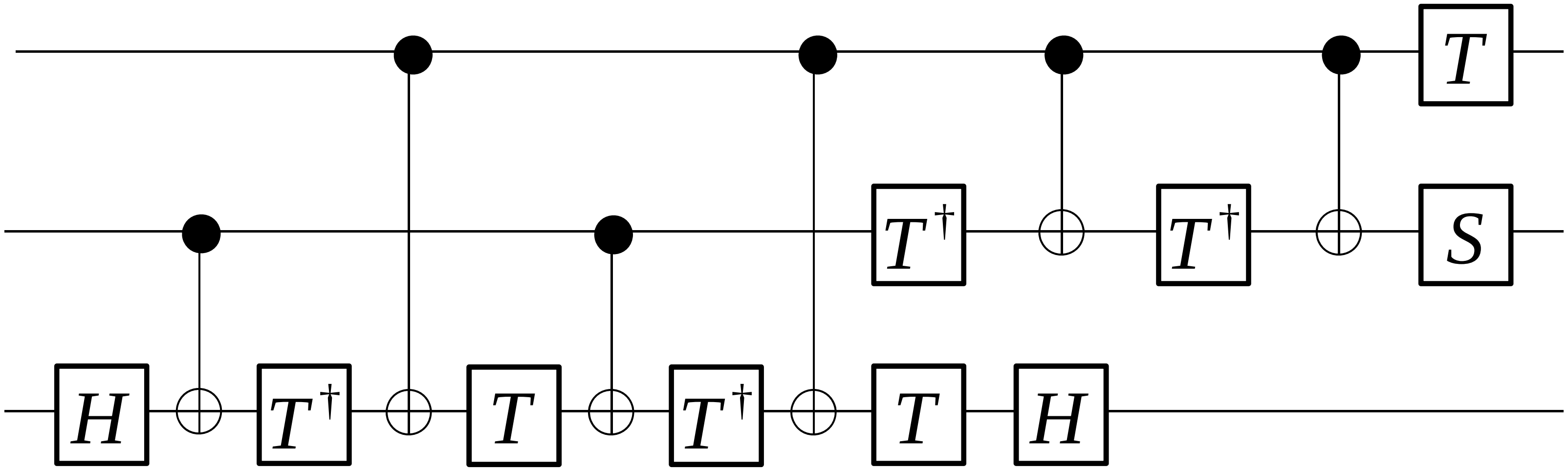
$$x_1, x_2, y \in \{0,1\}$$



x_1, x_2 ともに1が入力されたときのみ y を反転

Toffoli素子（CCNOT素子）

$CCNOT =$



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

指数関数 vs. 多項式関数

- 量子回路の一般的構成は入力サイズnに対して指数関数的！➔効率が悪すぎる
- 計算量理論では「多項式関数的」である方が現実的だと考えられている.
- 特定の問題に対して良い回路設計（＝アルゴリズム設計）は？

量子計算の主な結果

- 高速素因数分解アルゴリズム(Shor, 1994)
  - 素因数分解問題を高速に解くことができる.
  - RSA公開鍵暗号の解読

- 高速検索アルゴリズム(Grover, 1996)
  - 構造の全くない検索問題に対して高速検索
  - 次の講義で解説

古典 vs 量子

- 合成数 N（二進 $\log_2 N$ 桁）の素因数分解

古典：一般数体篩法

– 計算量：準指数関数

$$O\left(\exp\left(\left(C+o(1)\right)\left(\ln N\right)^{1/3}\left(\ln\ln N\right)^{2/3}\right)\right),\quad C=\left(64/9\right)^{1/3}$$

量子：Shorのアルゴリズム（1994）

– 計算量：多項式関数

$$O\left(\left(\log_2 N\right)^2\right)$$

$n = \log_2 N$ （二進表現の桁数＝入力サイズ）

$$C(N) = \exp\left((64/9)^{1/3} (\ln N)^{1/3} (\ln \ln N)^{2/3}\right)$$

$$Q(N) = (\log_2 N)^2$$

$$N \approx 2^{9.9} (\approx 960) \Rightarrow C(N) \approx 2 \times 10^{25}, Q(N) \approx 2 \times 10^{9}$$

参考:京速計算機（10PFLOPS, 1秒間に10^{16}回浮動小数点演算）で

2×10^{25}回の浮動小数点演算に対して必要な時間

６３．４年

参考:RSA公開鍵暗号の主流のパラメータn = 1024（推奨 n = 2048）

量子計算の主な結果

- 高速素因数分解アルゴリズム(Shor, 1994)
  - 素因数分解問題を高速に解くことができる.
  - RSA公開鍵暗号の解読

- 高速検索アルゴリズム(Grover, 1996)
  - 構造の全くない検索問題に対して高速検索
  - 次の講義で解説