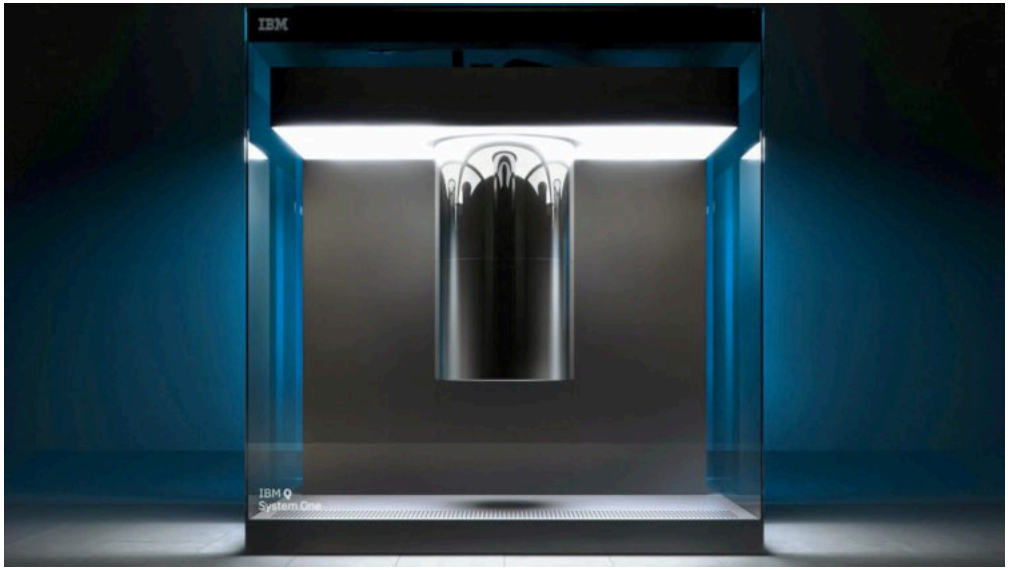
量子通信
-- 量子コンピュータとコンピュータとのハイブリッドの世界

コンピュータ

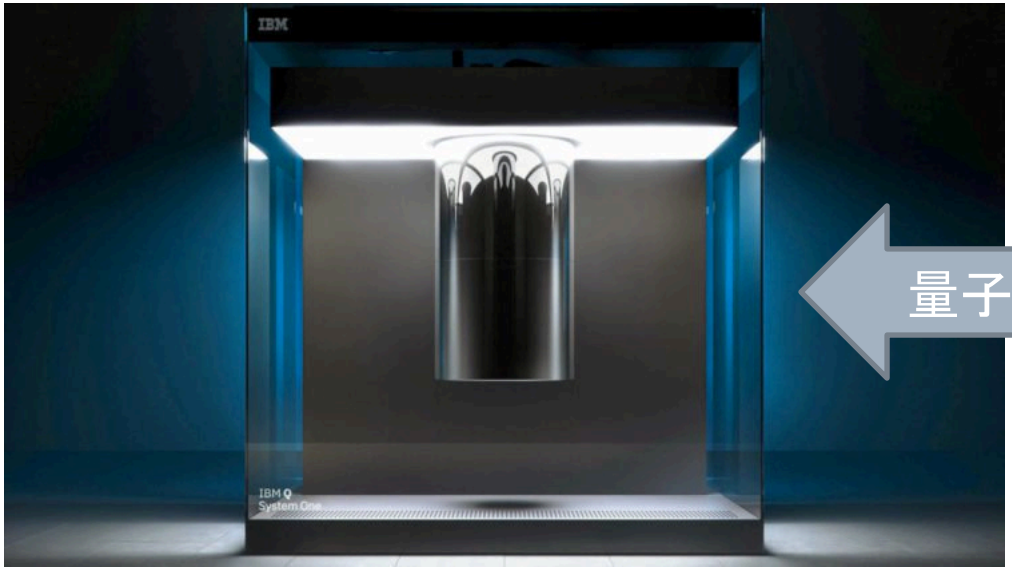
コンピュータ



量子コンピュータ

コンピュータ

ネットワーク



量子通信

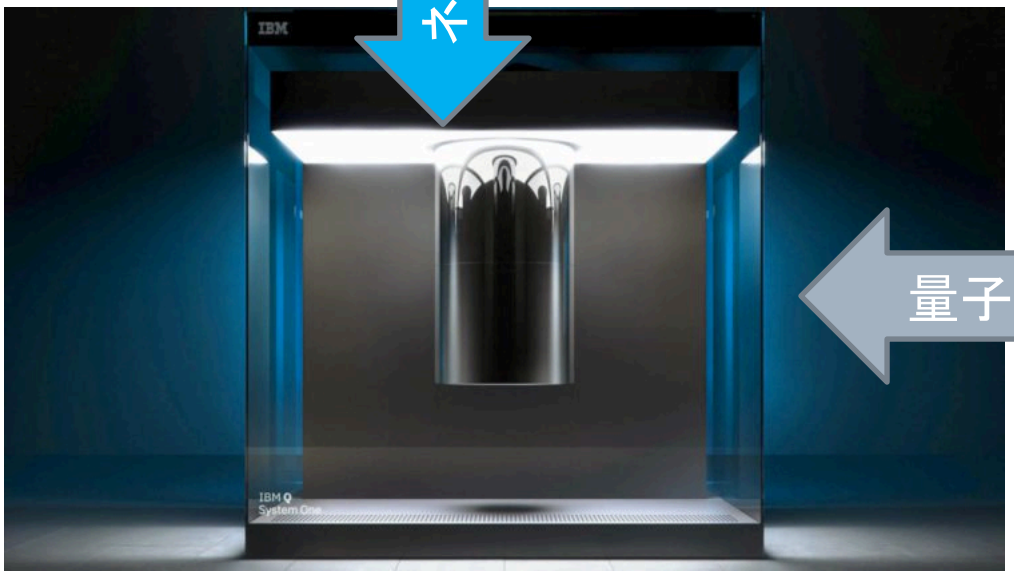
量子コンピュータ

コンピュータ

ネットワーク

量子通信

ネットワーク



量子通信

量子コンピュータ

古典コンピュータと量子コンピュータ

古典bitと量子bit(qubit)

一次元の点としての古典bit
二次元のベクトルとしての量子bit

- 古典bitは、0 または 1 の値しかとらない二つの離散的な点として表現される。
- 量子bit qubitは、|0>と|1>という二つのベクトルによって張られ、aとbという二つの数によって決定される二次元のベクトルとして表現される。この状態を「重ね合わせ」という。

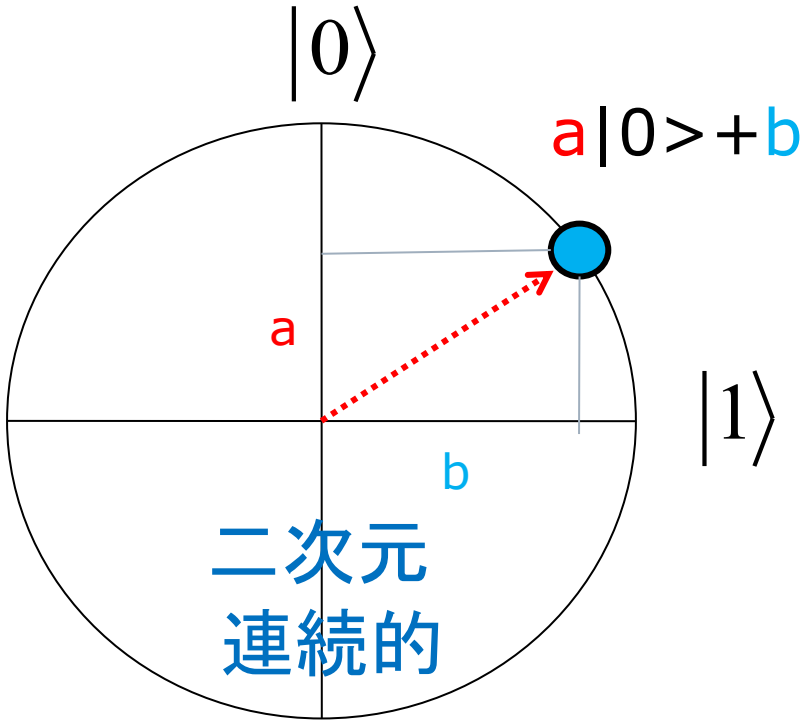
$$|Qubit> = a|0> + b|1>$$

この時、$|a|^2+|b|^2=1$ という条件がつく。
a, b は、複素数の値を取る。

- qubitは、二次元の複素ベクトルとして表現される。

二つのビットは、異なる性質を持つ

qubit



qubitは、|0>と|1>の「重ね合わせ」で、aとbの二つの数で決まる

$$\begin{pmatrix} a \\ b \end{pmatrix}$$

|0>の成分

|1>の成分

という二次元ベクトルである。

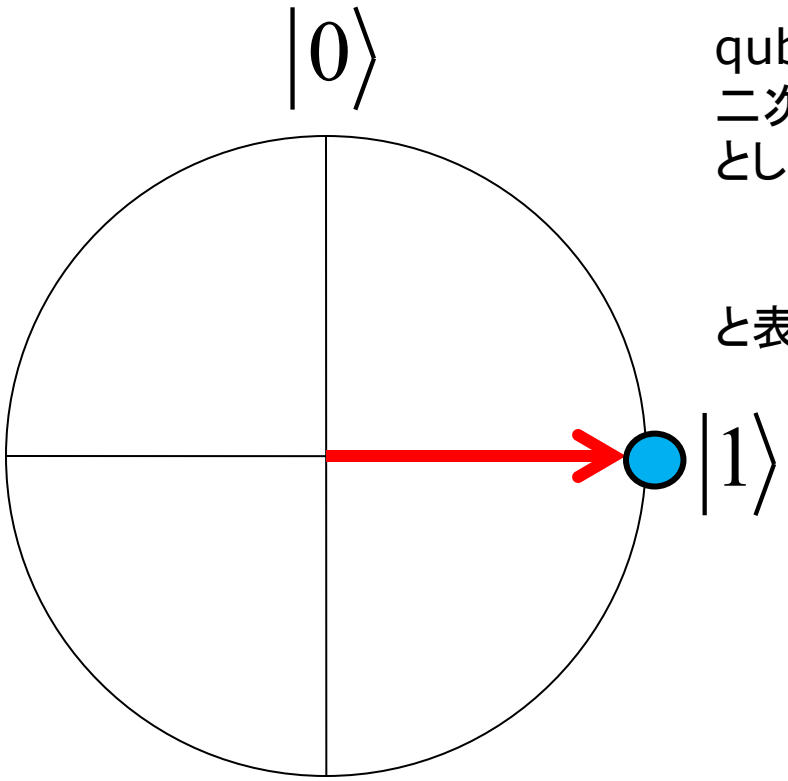
$|a|^2+|b|^2=1$

である。

bit

一次元
離散的

|Qubit> = a|0>+b|1>
で、a=0, b=1の時の状態

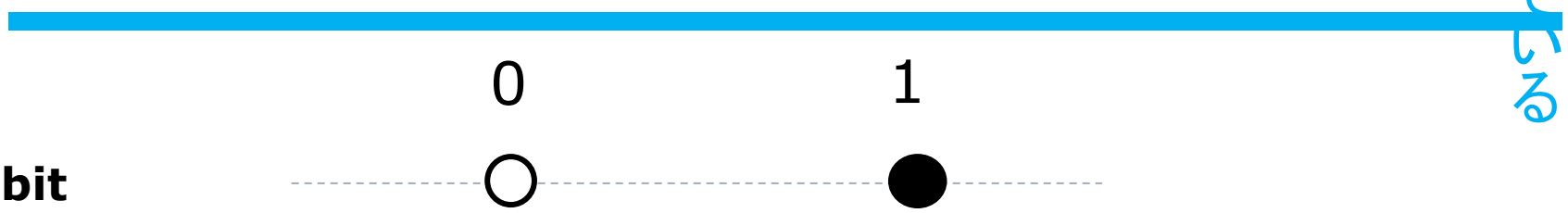


qubit |1>は、
二次元のベクトル
として、

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

と表される

qubit



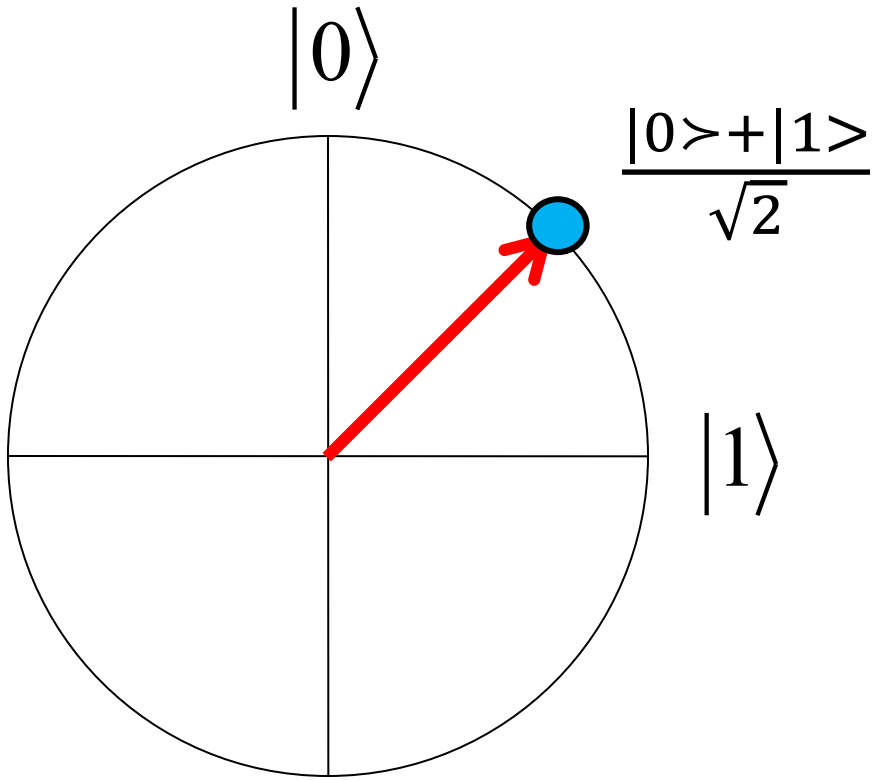
qubit $|1\rangle$ と bit 1 は、対応している

|Qubit> = a|0>+b|1>

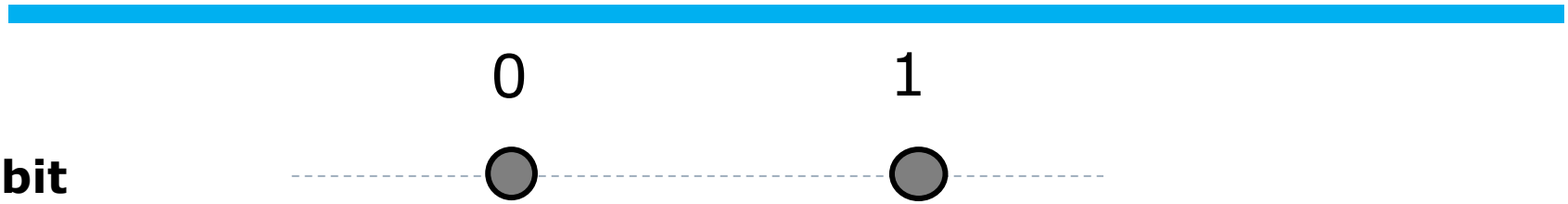
で、a=$\frac{1}{\sqrt{2}}$, b= $\frac{1}{\sqrt{2}}$ の時の状態

qubit と bit は、対応しない

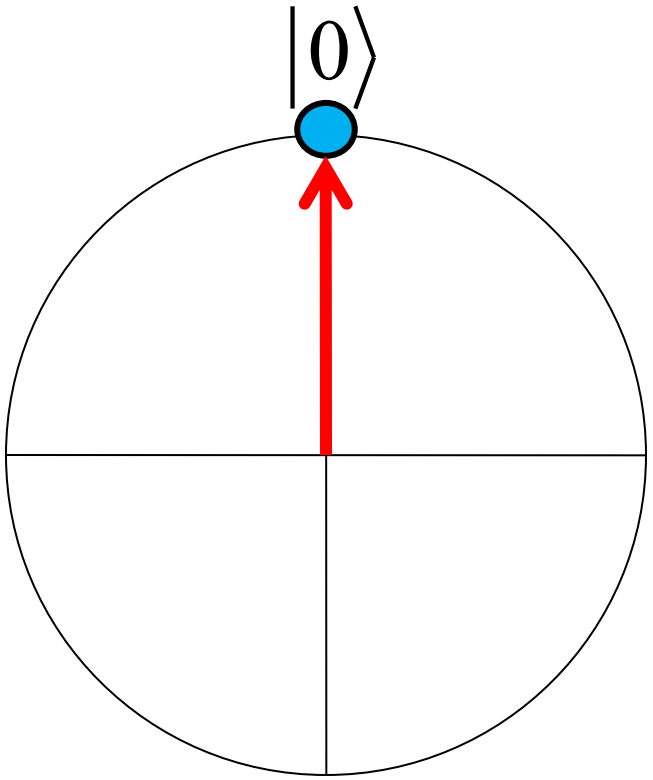
qubit



bit



|Qubit> = a|0>+b|1>
で、a=1, b= 0の時の状態



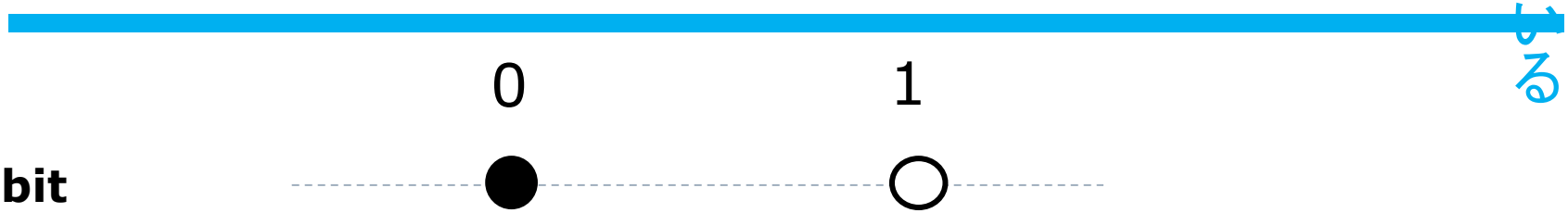
qubit |0>は、
二次元のベクトル
として、

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

と表される

qubit $|0\rangle$ と bit 0は、対応している

qubit



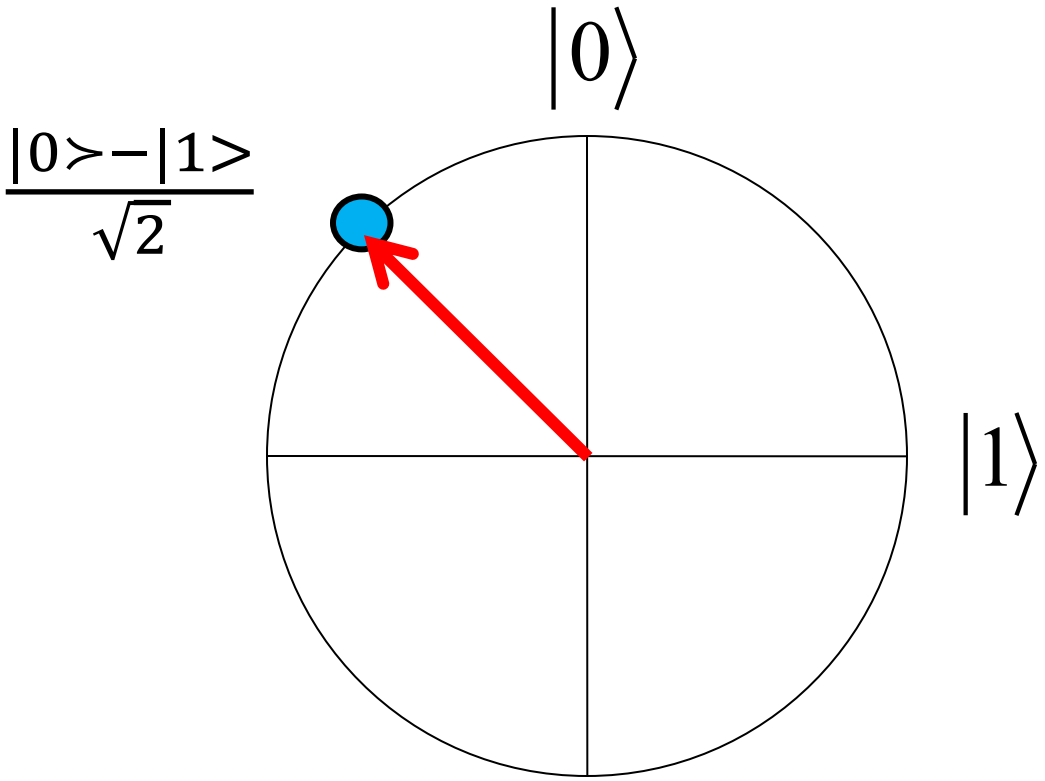
bit

|Qubit> = a|0>+b|1>

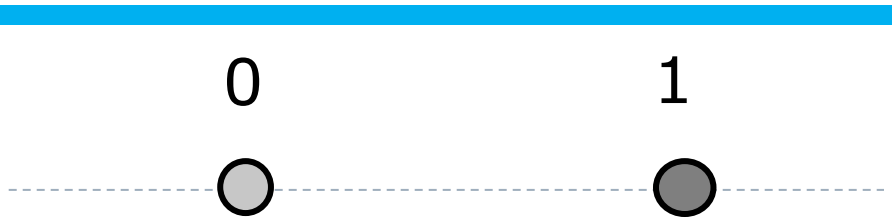
で、$a=\frac{1}{\sqrt{2}}$, $b=-\frac{1}{\sqrt{2}}$ の時の状態

qubit と bit は、対応しない

qubit



bit



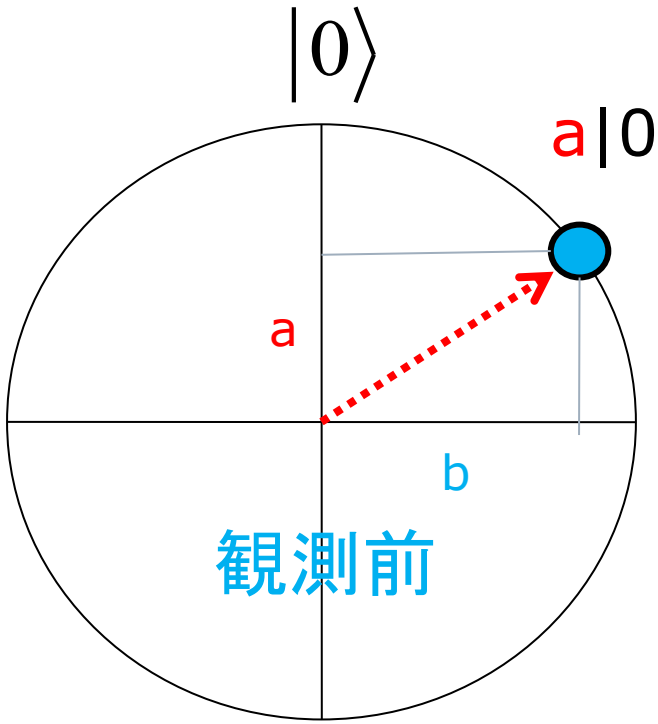
qubitの観測

- **|Qubit> = a|0>+b|1> を観測すると、重ね合わせの状態は破れて失われ、|0>または|1>のいずれかの状態になる。**

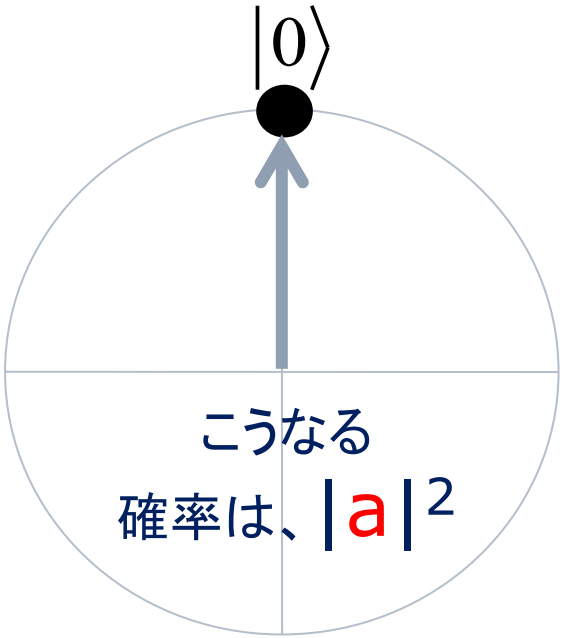
- **この時、**
  |0>を観測する確率は、$|a|^2$で与えられ、
  |1>を観測する確率は、$|b|^2$で与えられる。

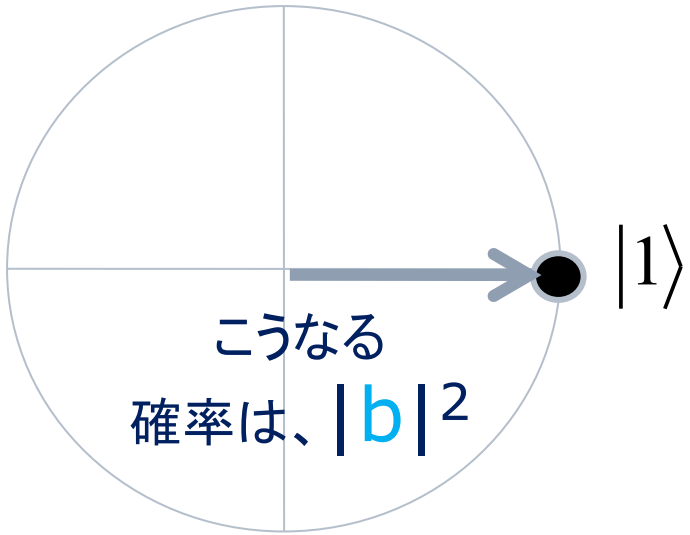
qubitの観測

観測によって、
「重ね合わせの状態」は
失われる



観測後





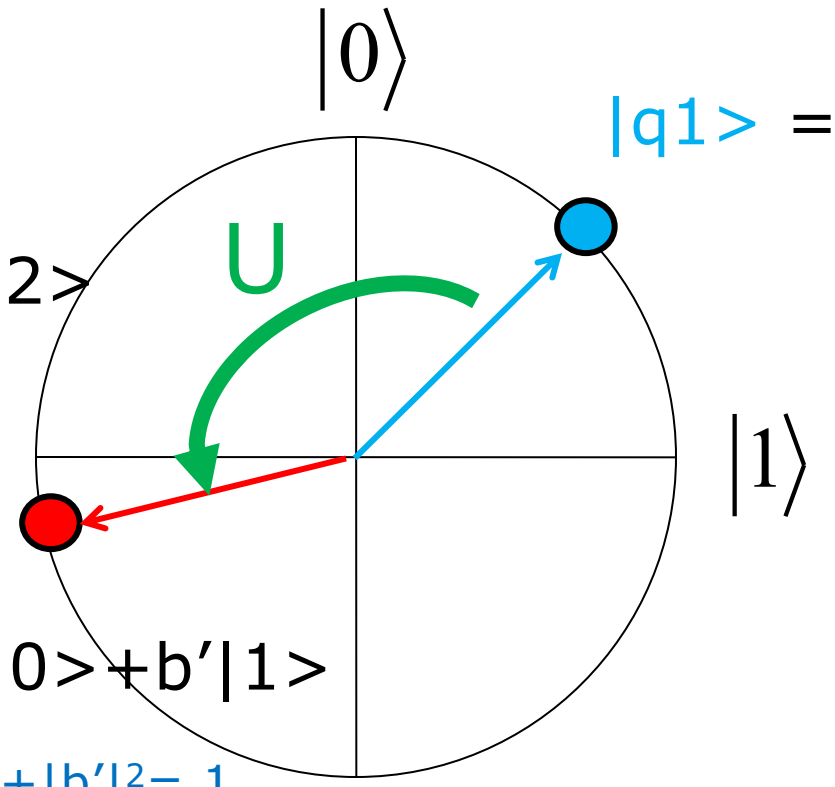
qubitの状態変化　ユニタリ変換

- qubitの状態 |q1> = a|0>+b|1>が、
  別の状態 |q2> = a′|0>+b′|1> に変化したとしよう
- それぞれのqubitの成分 a, b, a′, b′は、次の条件を満たす
  $|a|^2+|b|^2 = 1$
  $|a'|^2+|b'|^2 = 1$
- これは、すべてのqubitが、先の図では、原点から長さ 1の円周上の一点として表現できることを表している。（いくつか簡略化しているのだが）
- ベクトルの長さを変えない回転の変換を「ユニタリ変換」という。
  qubit |q1>から qubit |q2>への状態変化は、ユニタリ演算子 Uを用いて **$U|q1> = |q2>$** と表すことができる。
- Uの同じ角度での逆方向への回転を$U^{\dagger}$とすれば、
  $UU^{\dagger} = I$ (単位行列) となる。
  （回転して、今度は逆方向に回転すれば、元の位置に戻る）

|q1> = a|0>+b|1> から
|q2> = a’|0>+b’|1> への
状態変化

ユニタリ変換

ユニタリ変換Uは、
長さを変えない
回転である



|q1> = a|0>+b|1>

$|a|^2+|b|^2 = 1$

U|q1> = |q2>

|q2> = a’|0>+b’|1>

$|a'|^2+|b'|^2 = 1$

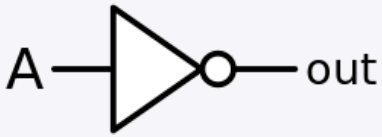
古典回路と量子回路

古典ゲートと量子ゲートの比較

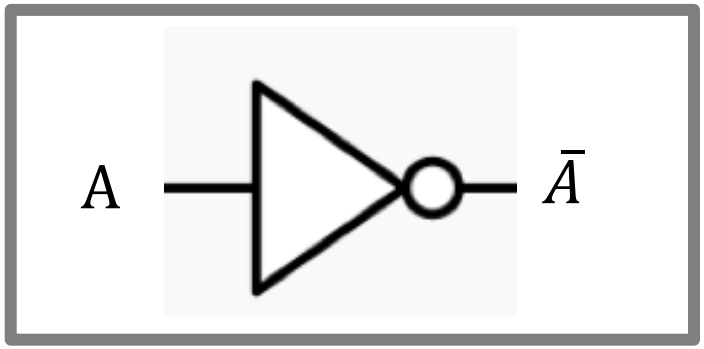
- ここでは、まず、古典的ゲートと量子ゲートの共通点を持て見よう。もちろん、入力があって出力があるのは同じである。
- qubitの|0>,|1> をそれぞれ古典ビットの 0, 1 に等しいとみなすと、入力と出力の値の対応を見れば、よく似た働きをするゲートを見つけることはできる。例えば、
  - 1bitのNOTゲートと1qubitのXゲート
  - 2bitのXORゲートと2qubitのCNOTゲート

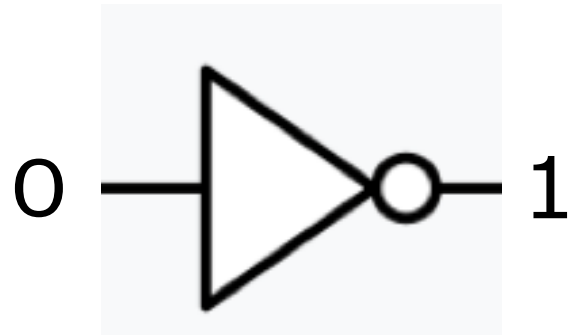
- ただ、この例でも、XORゲートの出力は一つだが、CNOTの出力は二つである。実は、量子ゲートでは、入力の数と出力の数は、つねに同じでなければならない。これについては後で述べる。

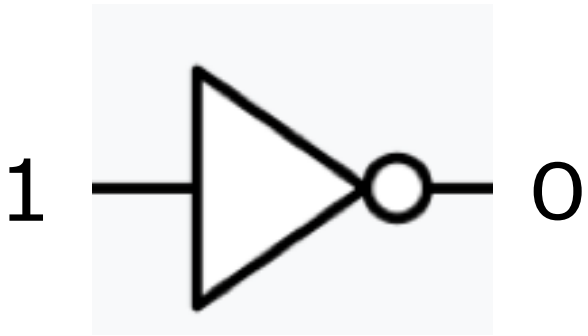
古典論理ゲートの例

論理	論理式	回路記号（MIL記号）
NOT	$\overline{A}$	
OR	$A + B$	
AND	$A \cdot B$	
XOR	$A \oplus B$	

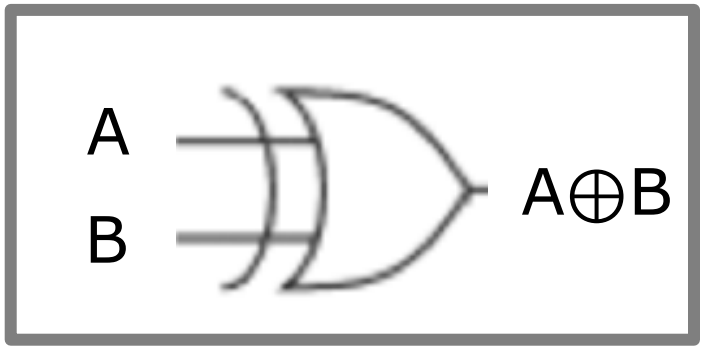
否定の論理ゲート（bit)



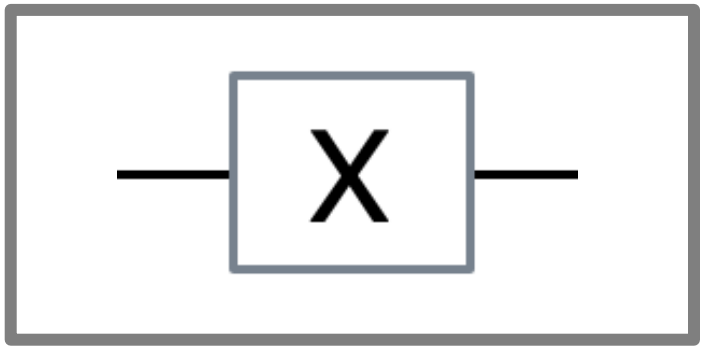




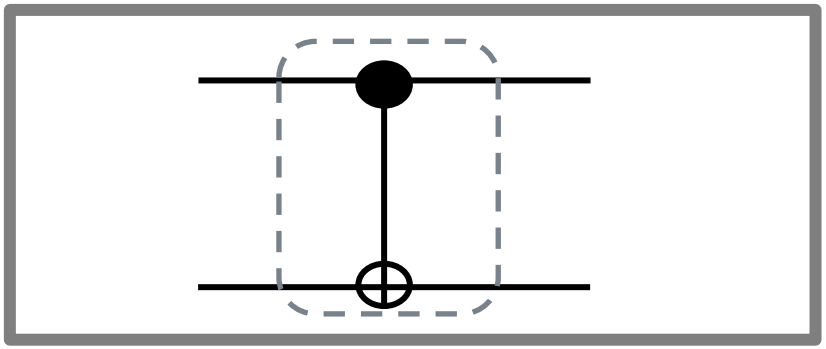
排他的論理和の論理ゲート（bit）

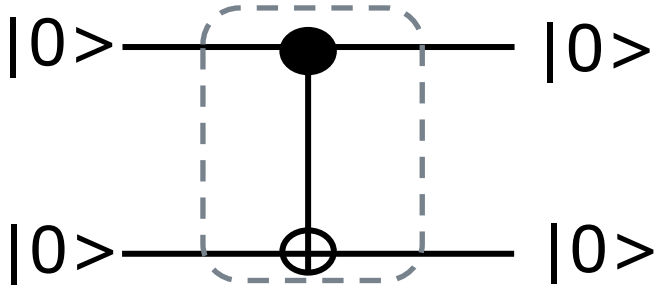


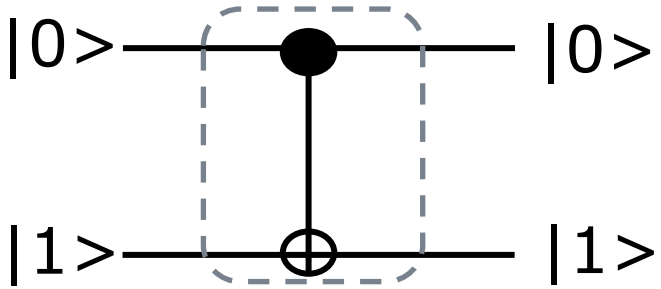
量子ゲート X（qubit)

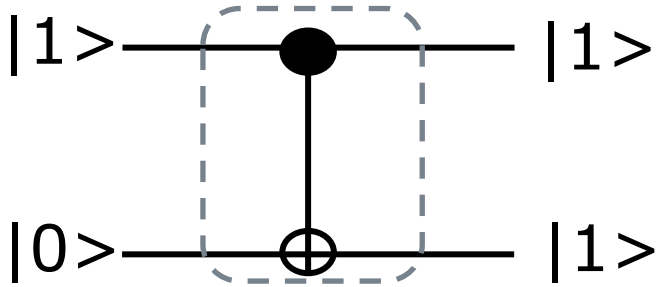


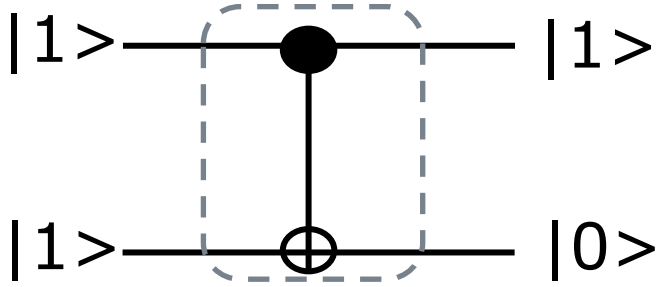
CNOT量子ゲート (qubit)



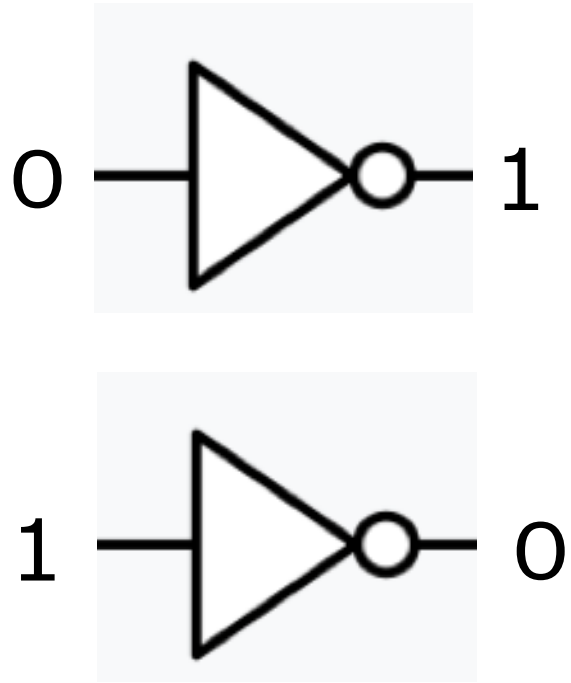






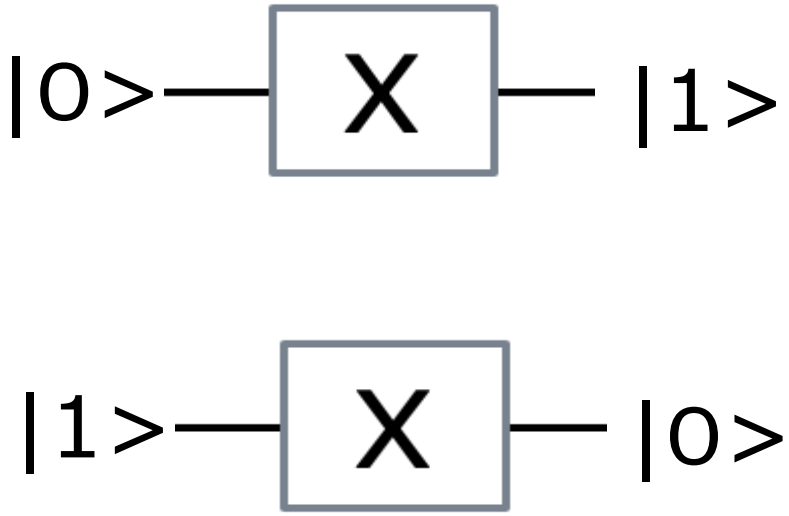


bit

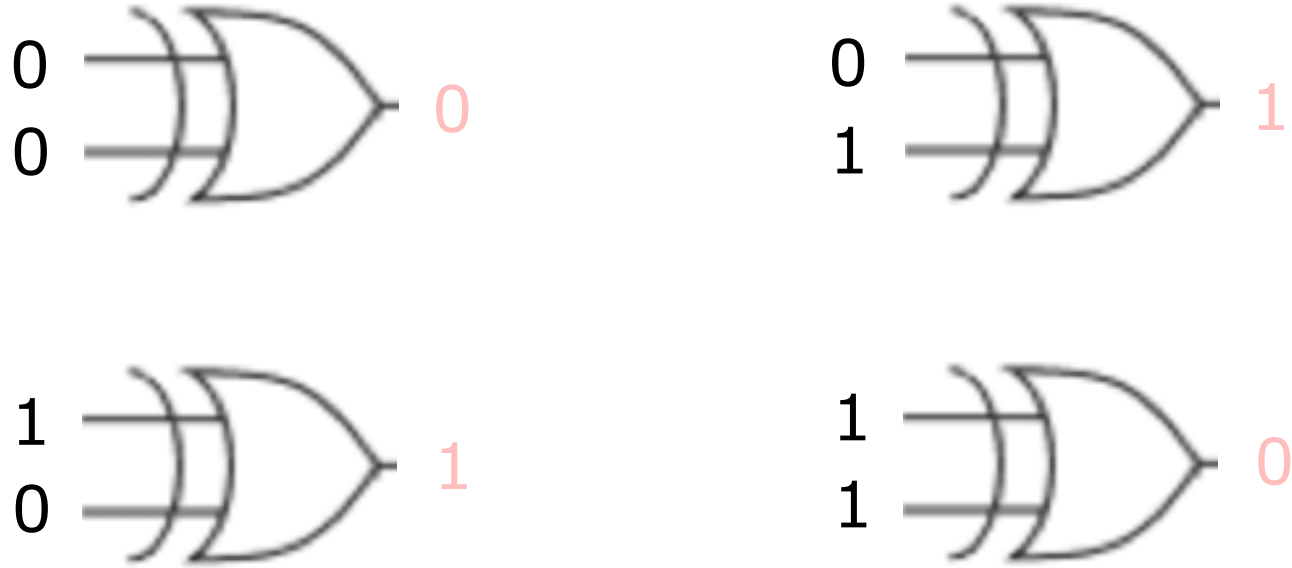


二つのゲートは、1対応している

qubit

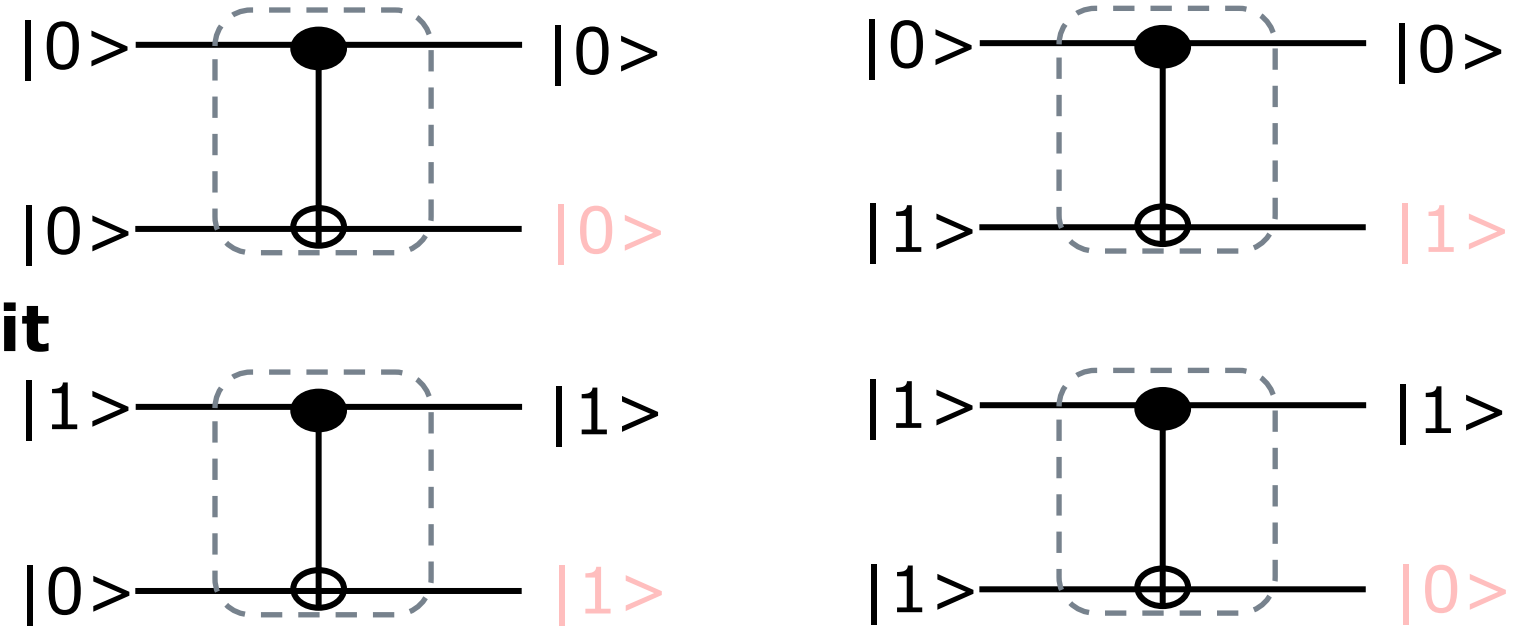


bit



二つのゲートは、対応している

qubit

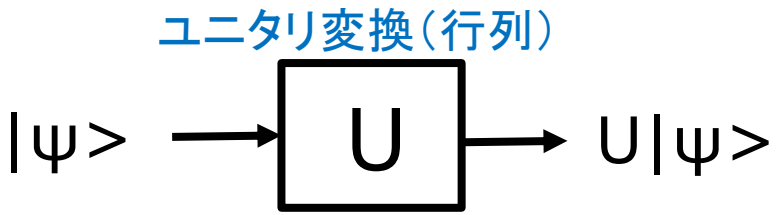


量子ゲートはどのような働きをするのか？

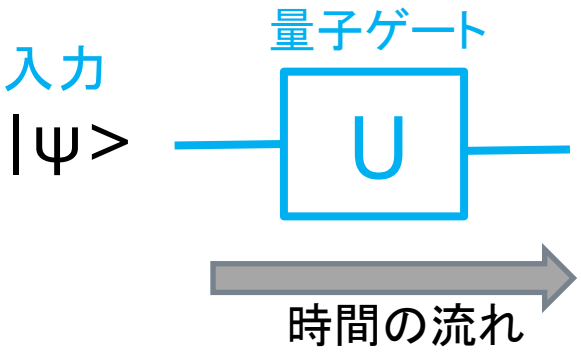
- 量子ゲートは、入力のqubitたちを出力のqubitたちに変換する。それは、古典的なゲートが、古典ビットの入力を古典ビットの出力に変換するのと同じである。
- 古典的なゲートは、基本的には、AND, OR, NOTといった「論理的」な演算で定義されるが、量子的なゲートは数学的には、「ユニタリ変換」として定義される。「ユニタリ変換」は、「ユニタリ行列」で定義される。
- 「ユニタリ行列」は、入力のqubitの「入力ベクトル」を出力のqubitの「出力ベクトル」に変換する。
- 一つの量子ゲートには、一つの「ユニタリ行列」が対応する。
- 古典的なゲートとは異なって、量子ゲートでは入力のqubitの数と出力のqubitの数は等しい。

量子ゲートとユニタリ行列

- 量子の状態 $|\psi\rangle$は、ユニタリ変換U（ユニタリ行列）の作用を受けて、状態 $U|\psi\rangle$ に変化する。
- この変化 $|\psi\rangle \rightarrow U|\psi\rangle$を、次のように表そう。

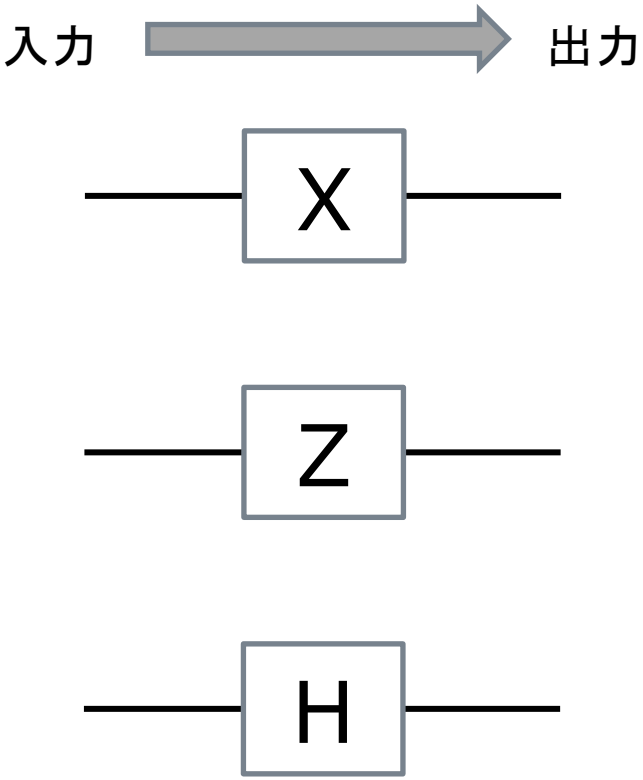


- この時、Uを、$|\psi\rangle$ を入力、$U|\psi\rangle$ を出力とする回路と考えることができる。これを、「量子ゲート」と呼ぶ。



量子ゲートは
ユニタリ行列と
一対一に対応する

代表的な1-qubitのゲート X, Z, H



Bit Flipper

$a|0\rangle+b|1\rangle \rightarrow b|0\rangle+a|1\rangle$

Phase Flipper

$a|0\rangle+b|1\rangle \rightarrow a|0\rangle-b|1\rangle$

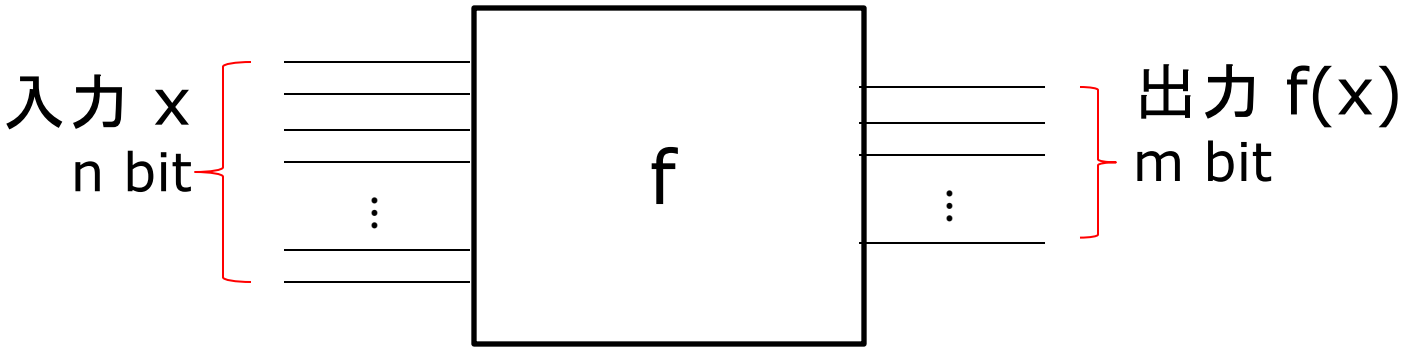
Hadamard

$a|0\rangle+b|1\rangle \rightarrow$

$\frac{1}{\sqrt{2}}(a+b)|0\rangle+\frac{1}{\sqrt{2}}(a-b)|1\rangle$

古典回路を量子回路でシミュレーションすることは可能か？

- 関数 f を計算する古典的な回路を考えよう。入力 x のビット数 n と、出力 f(x)のビット数 m とは一般に独立である。



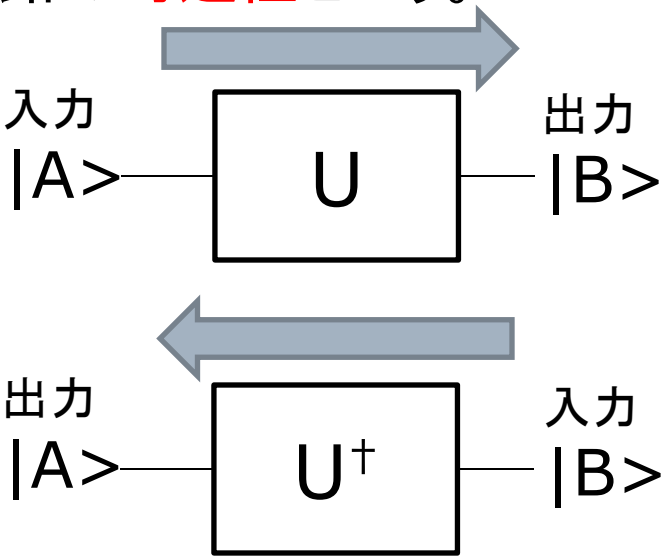
- 例えば、XORゲートでは、入力のビット数 nは2で、出力のビット数 mは1である。

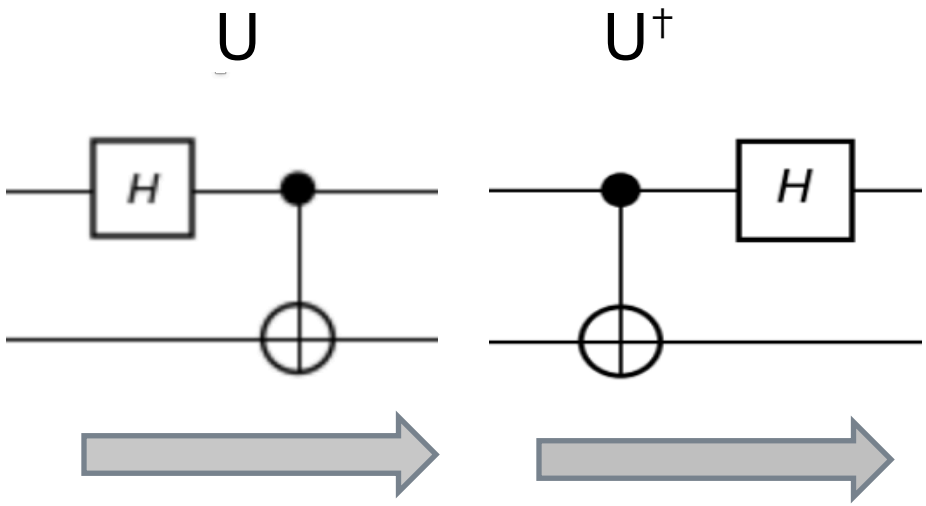
量子回路のユニタリ性

- 関数 f を計算する量子的なアルゴリズでも、入力 x のqubit数 n と、出力 f(x)のqubit数 m とは一般に独立である。
- それでは、関数 f を計算する量子回路は、先の古典回路と同じような形を取るのだろうか？　そうはならない。
- 量子ゲートはユニタリ変換を行うゲートなのだが、量子ゲートから構成される量子回路も、それ自体がユニタリ性を持たねばならない。量子回路全体に対応するユニタリ行列は、巨大なものになる。
- 例えば、2-qubitの入力を受け取り、2-qubitを出力する量子ゲート（CNOTがそうである）は、4次元のベクトルを受け取り、4次元のベクトルに変換する 4x4の行列で表現される。
- n-qubitの入力を受け取り、n-qubitを出力する量子回路は、$2^n \times 2^n$ のユニタリ行列で表現される。

量子回路の可逆性（reversibility）

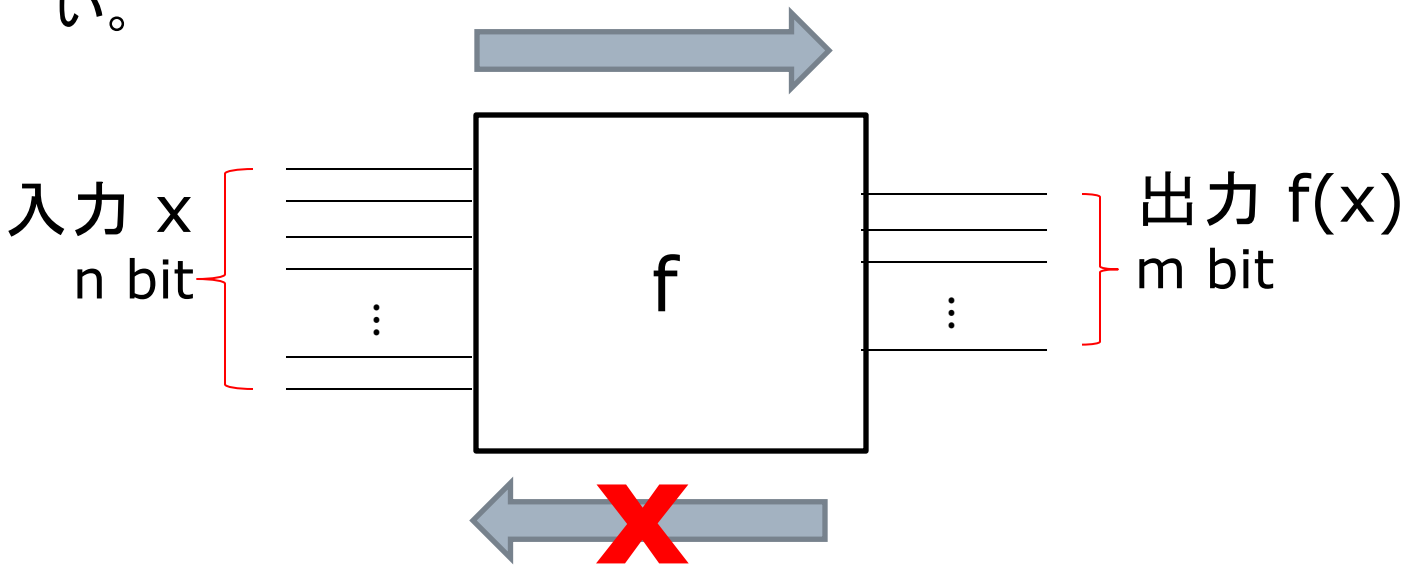
- 回路全体を表現するユニタリ行列Uを書き下ろすことができないにしても、Uの性質 $UU^{\dagger}=U^{\dagger}U=I$ から次のことがわかる。
- 回路U（行列Uに対応する）の入力と出力を入れ替えても、すなわち、Uに対するある入力|A>の結果であるUの出力|B>を、Uの出力側に与えても、Uは|A>を出力する。これを、量子回路の可逆性という。



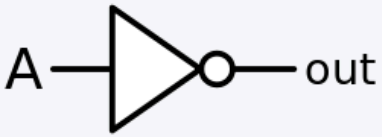


古典回路は非可逆である
任意の関数は、ユニタリでは表現できない

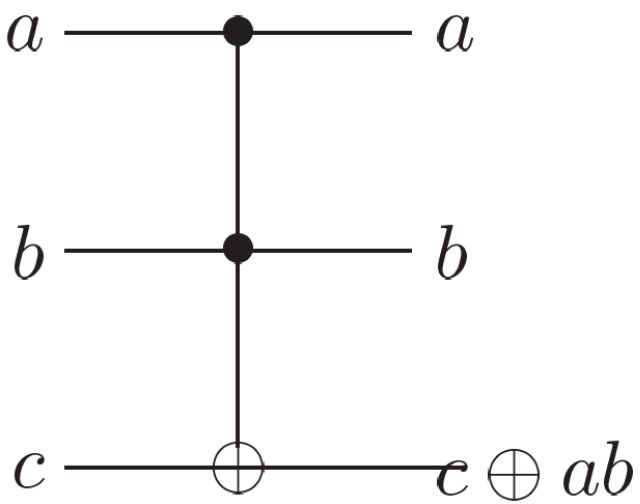
- 古典回路は、非可逆である。
- また、任意の関数 f をユニタリ行列で表現できるわけではない。
  - 例えば、f(x)=z, f(y)=z という関数 f がユニタリ行列で表現できたとする。これは、U|x>=|z>, U|y>=|z>を意味するのだが、両式を引くと $U(|x\rangle-|y\rangle)=\vec{0}$ となるのだが、こうしたUはユニタリではない。



古典論理ゲートは可逆か？

論理	論理式	回路記号（MIL記号）	
NOT	$\overline{A}$		○
OR	$A + B$		×
AND	$A \cdot B$		×
XOR	$A \oplus B$		×

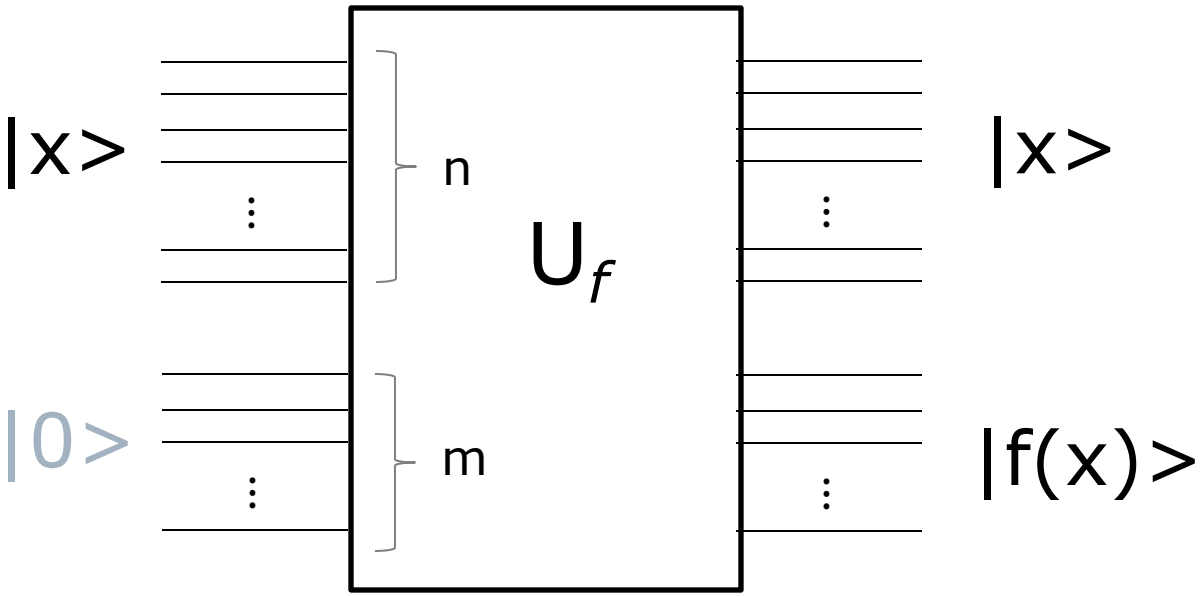
実は、次のような
ゲートを使えば、
古典回路も可逆に
できる



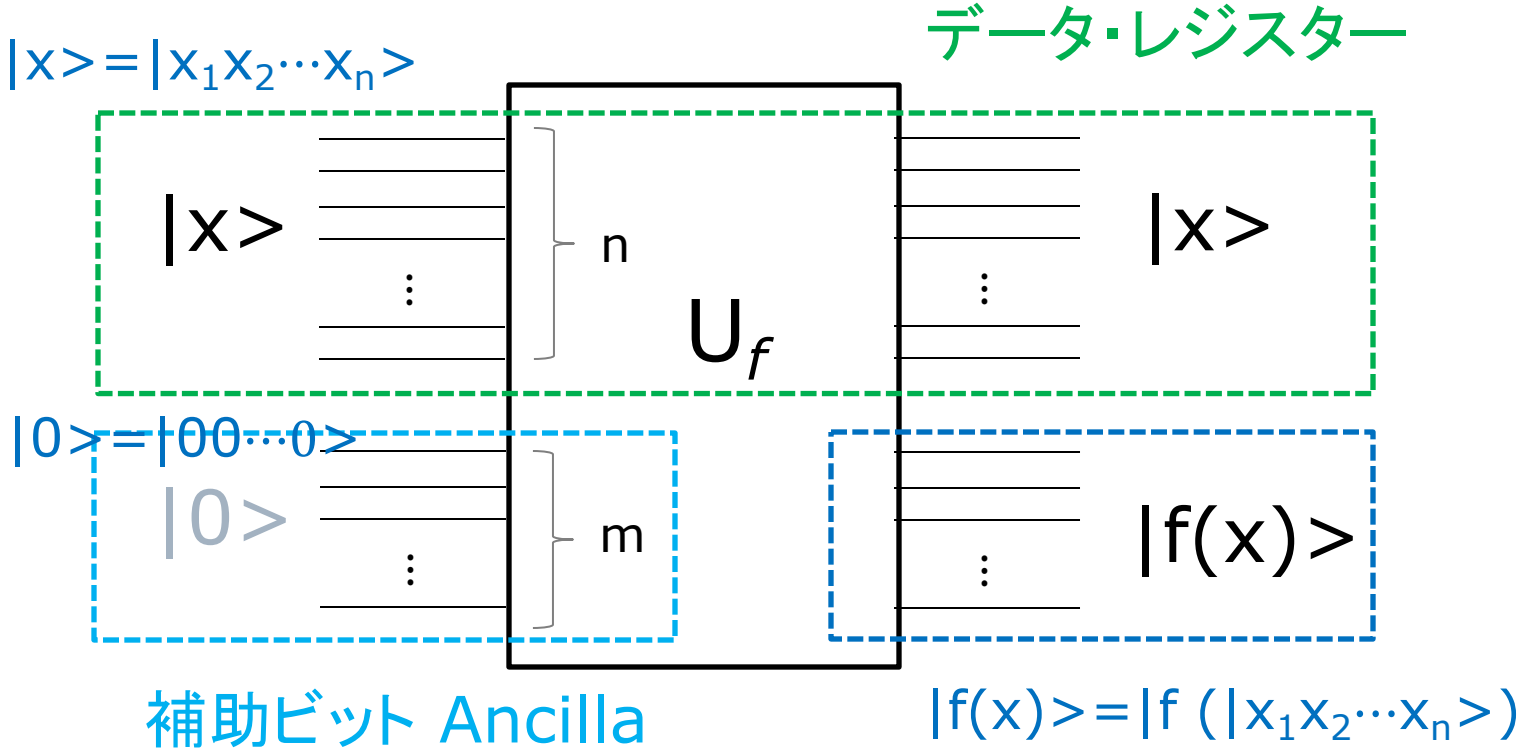
Toffoli ゲート

任意のf(x)を計算し、かつユニタリな量子回路U_fの一般的な形

f(x)の具体的な実装を与えているわけではない。



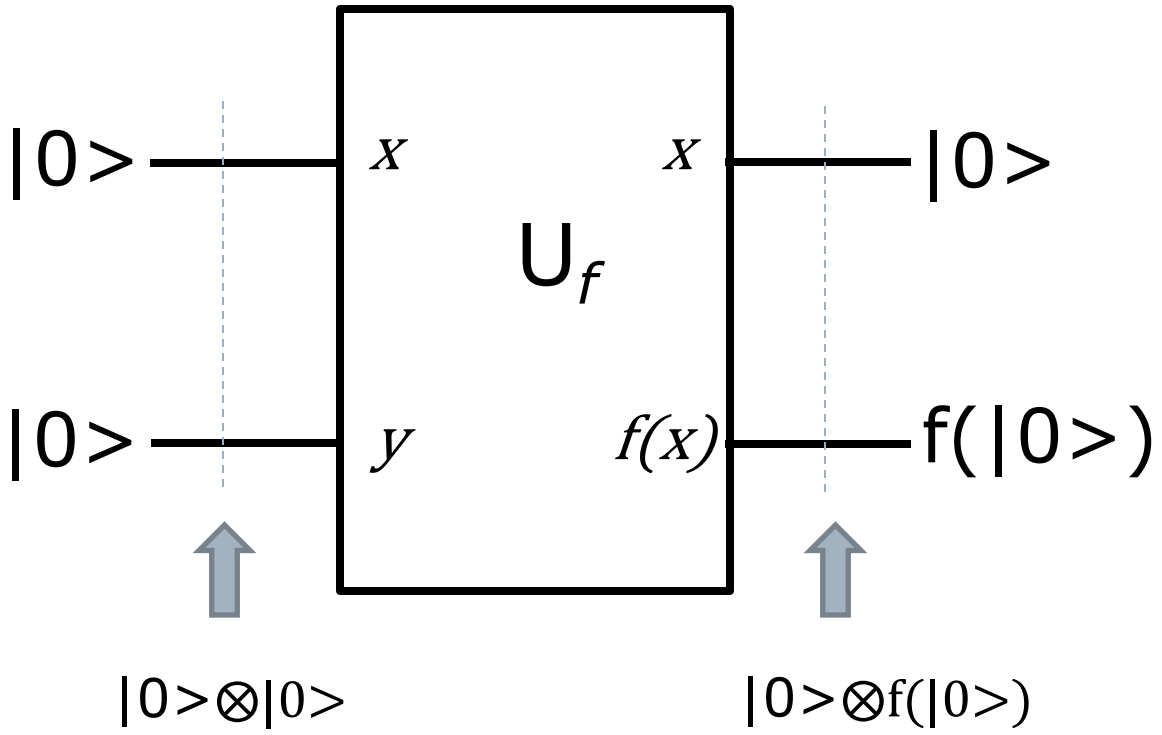
任意のf(x)を計算し、かつユニタリな量子回路U_fの一般的な形



量子回路で古典的な関数を計算する

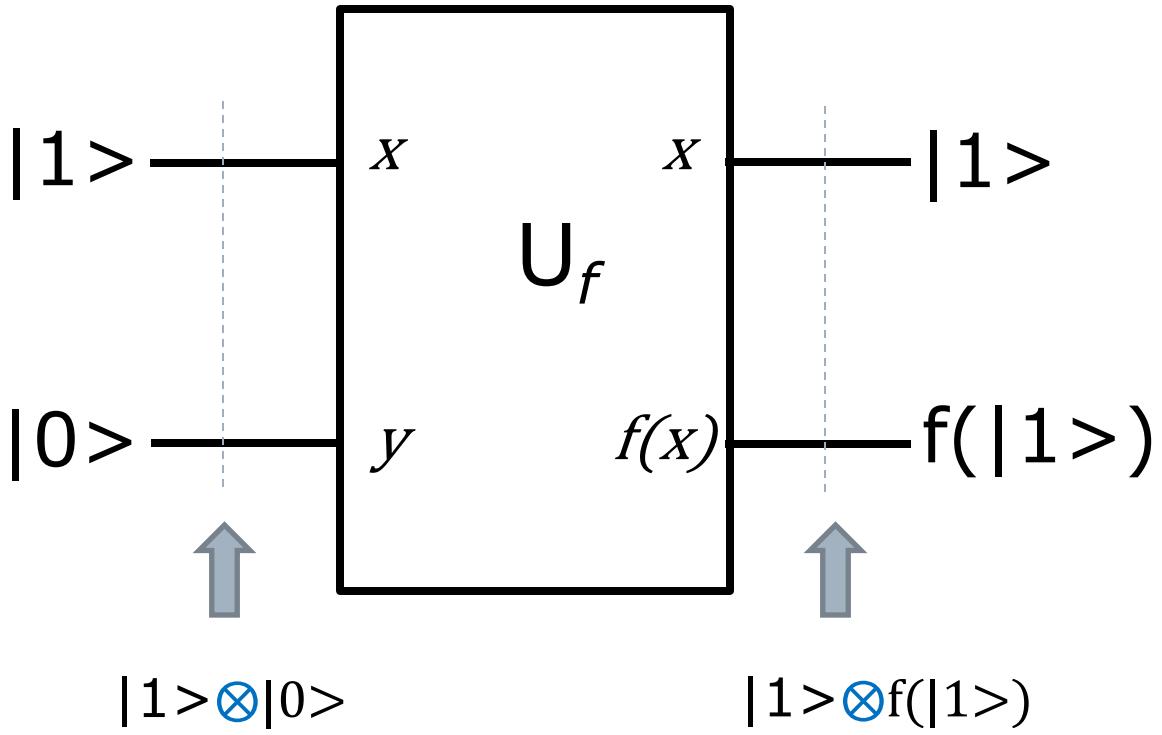
2-qubit(入力　1-qubit, 出力 1-qubit)の単純な回路U_fを考える

入力 x = |0> の時



2-qubit(fの入力 1-qubit, fの出力 1-qubit)の単純な回路U_fを考える

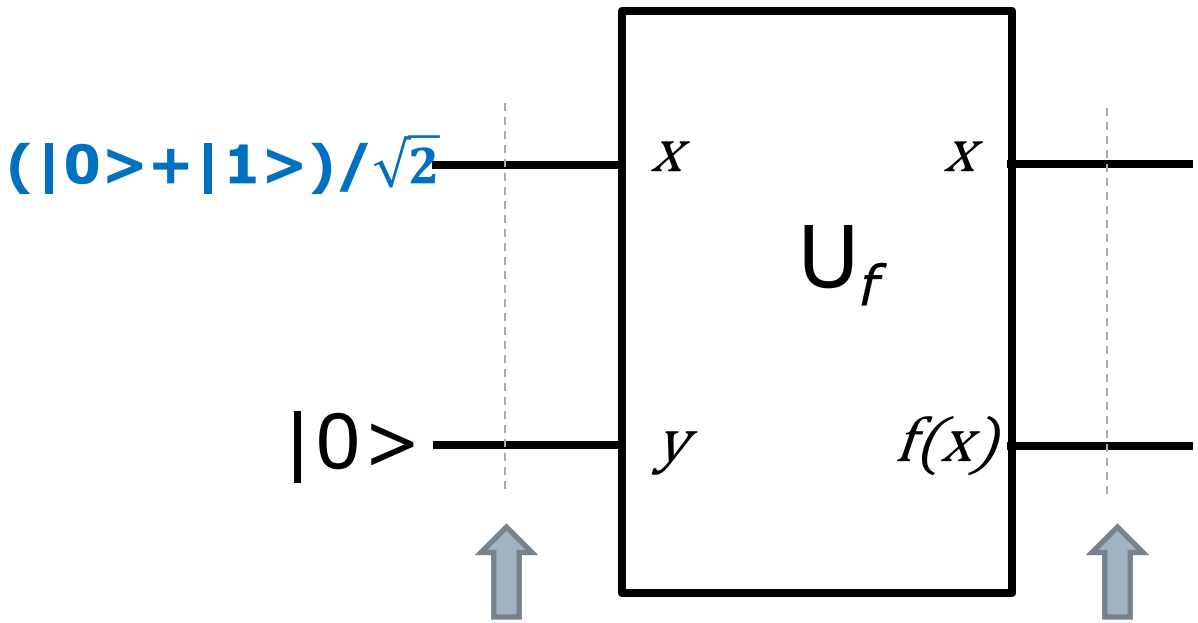
入力 x = |1> の時



意味が明確ならテンソル記号を省略してもいい

2-qubit(fの入力 1-qubit, fの出力 1-qubit)の単純な回路U_fを考える

入力 $x = (|0>+|1>)/\sqrt{2}$ の時



$|(|0>+|1>)/\sqrt{2} \otimes |0>$

$|0>f(|0>)/\sqrt{2} + |1>f(|1>)/\sqrt{2}$

テンソル記号を省略した

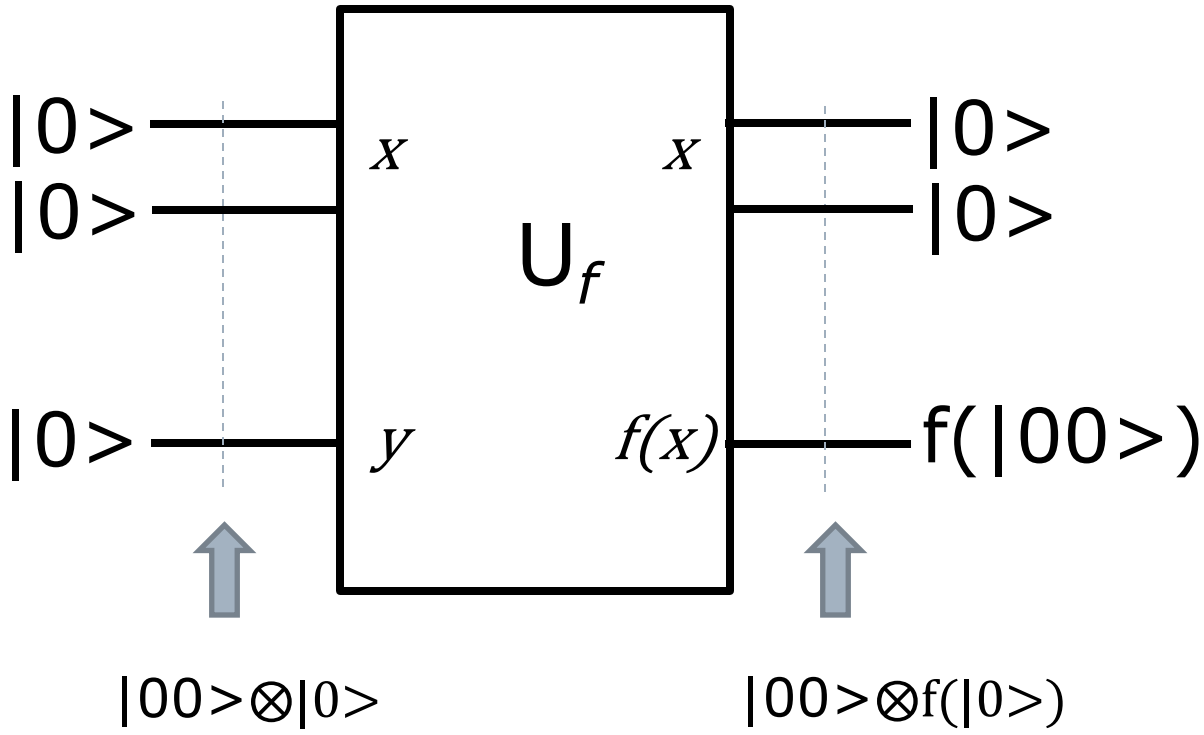
なぜ？

$|0\rangle f(|0\rangle)/\sqrt{2} + |1\rangle f(|1\rangle)/\sqrt{2}$

- 関数 f は線形であるとは限らないが、Ufはユニタリであり線形である。Mが線形であるとは、
  $M(a|A\rangle+b|B\rangle)=aM|A\rangle+bM|B\rangle$が成り立つことをいう。
- $x = |0\rangle$ の時と $x = |1\rangle$ の時の例から、Ufは次の式を満たすことがわかる。
  $Uf(|0\rangle\otimes|0\rangle)= |0\rangle\otimes f(|0\rangle)$
  $Uf(|1\rangle\otimes|0\rangle)= |1\rangle\otimes f(|1\rangle)$
- この時、Ufは線形であるので、
  $Uf((|0\rangle+|1\rangle)/\sqrt{2}\otimes|0\rangle)$
  $= Uf((|0\rangle/\sqrt{2}\otimes|0\rangle+|1\rangle/\sqrt{2}\otimes|0\rangle)$
  $= Uf(|0\rangle\otimes|0\rangle)/\sqrt{2} + Uf(|1\rangle\otimes|0\rangle)/\sqrt{2}$
  $= |0\rangle\otimes f(|0\rangle)/\sqrt{2} + |1\rangle\otimes f(|1\rangle)/\sqrt{2}$
  $= |0\rangle f(|0\rangle)/\sqrt{2} + |1\rangle f(|1\rangle)/\sqrt{2}$

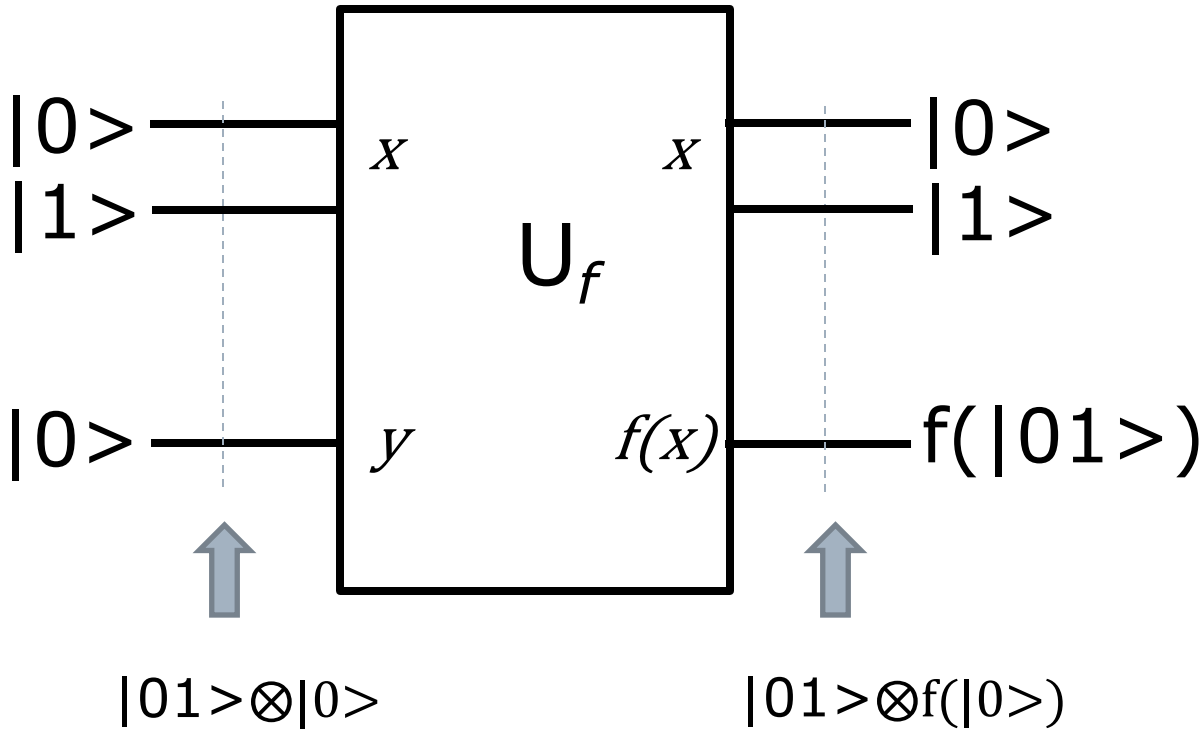
3-qubit(fの入力 2-qubit, fの出力 1-qubit)の単純な回路U_fを考える

入力 x = |0>⊗|0> = |00> の時



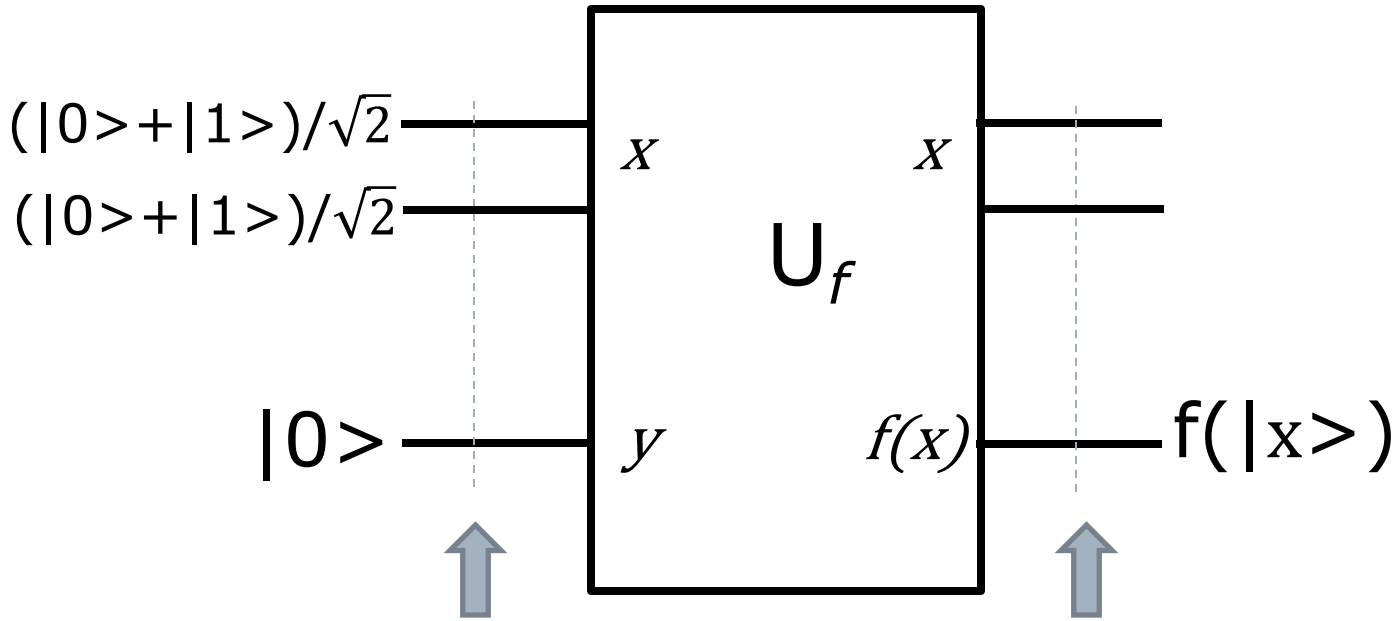
3-qubit(fの入力 2-qubit, fの出力 1-qubit)の単純な回路U_fを考える

入力 x = |0>⊗|1> = |01> の時



3-qubit(fの入力 2-qubit, fの出力 1-qubit)の単純な回路U_fを考える

入力 x = (|0>+|1>)/√2)⊗(|0>+|1>)/√2 の時



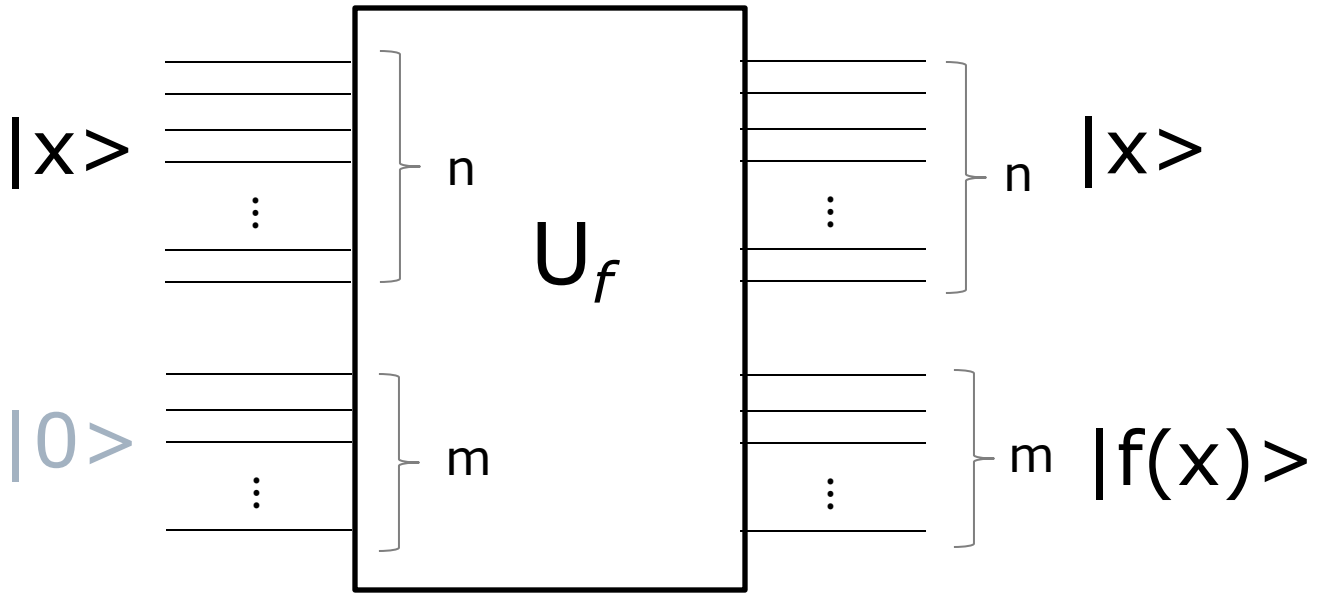
|x>⊗|0>

(|00>f(|00>) + |01>f(|01>) +
|10>f(|10>) + |11>f(|11>))/2

なぜなら

- $x = (|0\rangle+|1\rangle)/\sqrt{2})\otimes(|0\rangle+|1\rangle)/\sqrt{2}$ とする。
  $x = (|00\rangle+|01\rangle+|10\rangle+|11\rangle)/2$ である。
- この時、
  $Uf(|x\rangle\otimes|0\rangle)$
  $= Uf((|00\rangle+|01\rangle+|10\rangle+|11\rangle)\otimes|0\rangle)/2$
  $= (Uf(|00\rangle\otimes|0\rangle)+Uf(|01\rangle\otimes|0\rangle)+$
  $Uf(|10\rangle\otimes|0\rangle)+Uf(|11\rangle\otimes|0\rangle))/2$
  $= (|00\rangle\otimes f(|00\rangle)+|01\rangle\otimes f(|01\rangle)+$
  $|10\rangle\otimes f(|10\rangle)+|00\rangle\otimes f(|11\rangle)/2$
  $=(|00\rangle f(|00\rangle) + |01\rangle f(|01\rangle) +$
  $|10\rangle f(|10\rangle) + |11\rangle f(|11\rangle))/2$

ここまでは、f(x)が1-qubitで表現される例をみてきた。このことは、関数 f(x)が、0または1の値をとることを意味する。
もし、関数f(x)が m-qubitで表現されるのなら、そのことは関数 fが、0～2^{m-1}の範囲の値を取ることを意味する。それは、古典ビットでも同様である。



$\{0,1\}^n \ni x$ で、

Uf($\Sigma|x>|0>$) = Σ Uf ($|x>|0>$) = Σ $|x>|f(x)>$

量子コンピュータでは
なぜ高速な計算ができるのか？

古典コンピュータと量子コンピュータの違い

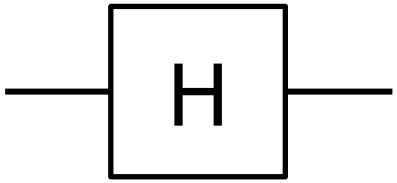
アダマール・ゲート

アダマール行列とアダマール・ゲート

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

という行列を、アダマール（Hadamard）行列という。

この行列に対応するゲートを、アダマール・ゲートといい、次のように表す。



アダマール行列の性質

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$,

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ とすると

1. $H|0\rangle = |+\rangle$
2. $H|1\rangle = |-\rangle$
3. $H|+\rangle = |0\rangle$
4. $H|-\rangle = |1\rangle$
5. $HH = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 単位行列

|+>と|−>の観測　量子コイン

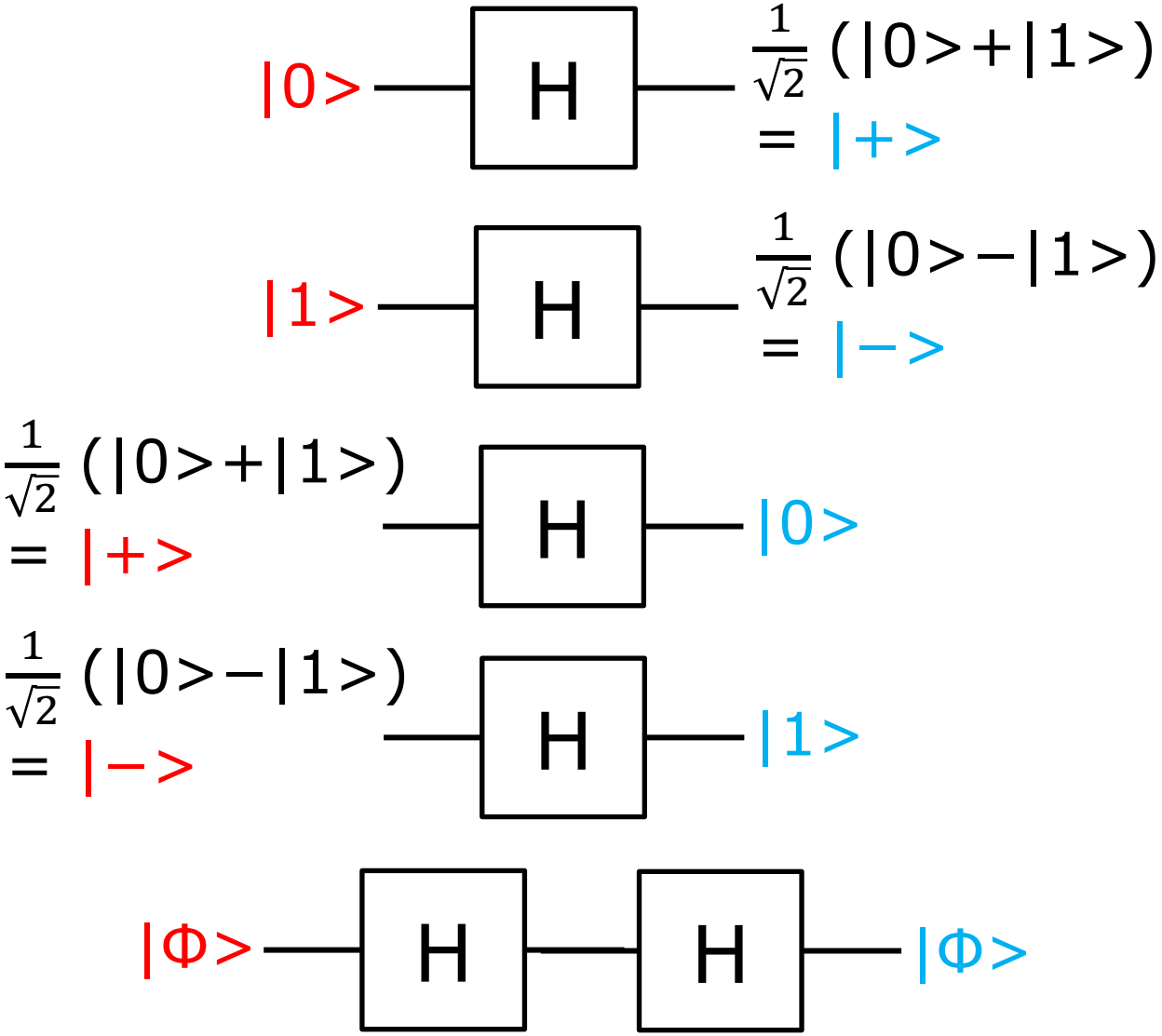
- |+>= $\frac{1}{\sqrt{2}}$ |0>+$\frac{1}{\sqrt{2}}$|1> を観測したとする。この時、
  |0>を観測する確率は、|$\frac{1}{\sqrt{2}}$ |^2=1/2
  |1>を観測する確率は、|$\frac{1}{\sqrt{2}}$ |^2=1/2
- |−>= $\frac{1}{\sqrt{2}}$ |0>−$\frac{1}{\sqrt{2}}$|1> を観測したとする。この時、
  |0>を観測する確率は、|$\frac{1}{\sqrt{2}}$ |^2=1/2
  |1>を観測する確率は、|−$\frac{1}{\sqrt{2}}$|^2=1/2
- |+>と|−>は、等しい確率 1/2で|0>と|1>を観測する。
  これは、コインを投げて裏・表が出る確率と等しい。
  |+>と|−>を、「量子コイン」と呼ぶことがある。
- |+>と|−>は、明らかに異なる状態だが、観測によっては区別することができない。

アダマール行列の性質(先の式の計算)

1. $H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$
2. $H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
3. $H|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2\\ 0\end{pmatrix} = |0\rangle$
4. $H|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}0\\ 2\end{pmatrix} = |1\rangle$
5. $HH = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

単位行列

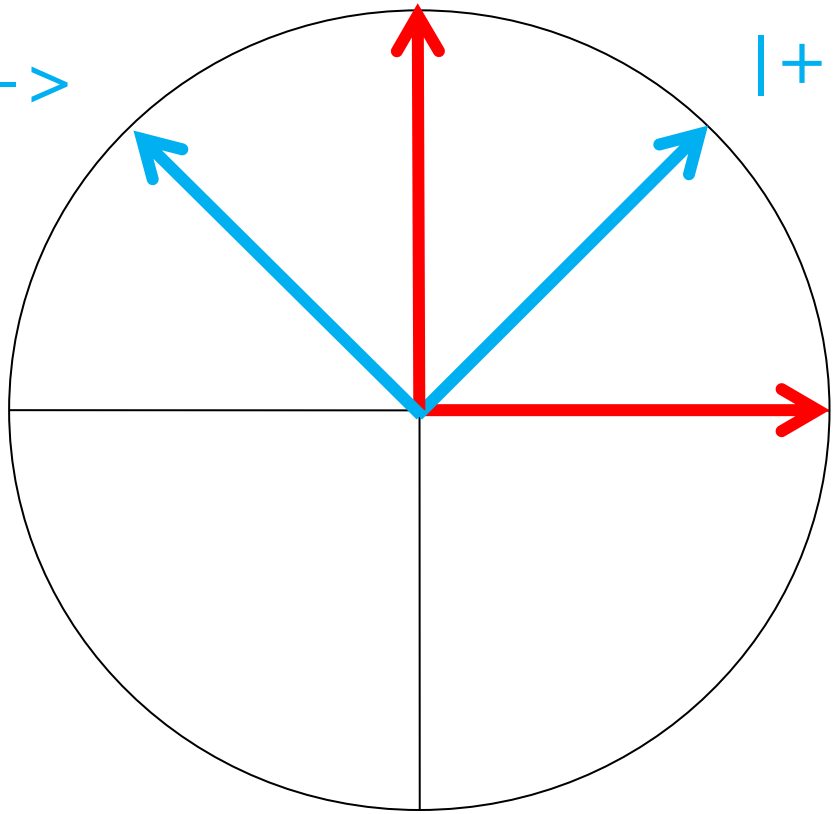
アダマール・ゲートの性質



標準基底とアダマール基底

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

$|->$ $|+>$



$|1\rangle$

アダマール変換は、
基底 |0>, |1> で
張られた座標系を
基底 |+>, |−> で
張られた座標系に
変換する、

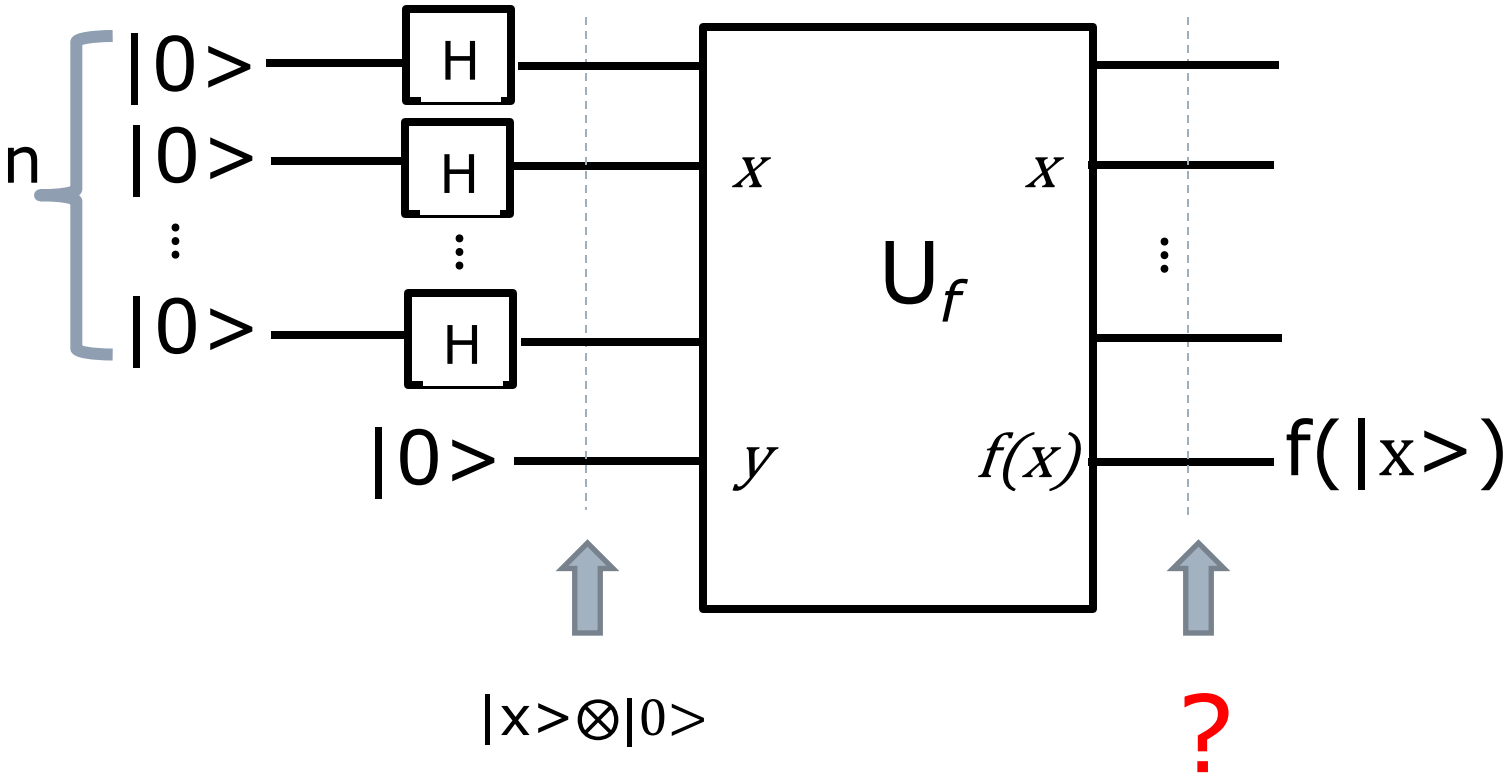
基底 |0>, |1> を
標準基底（計算基底）
基底 |+>, |−> を
アダマール基底
と呼ぶ

Quantum Parallelism

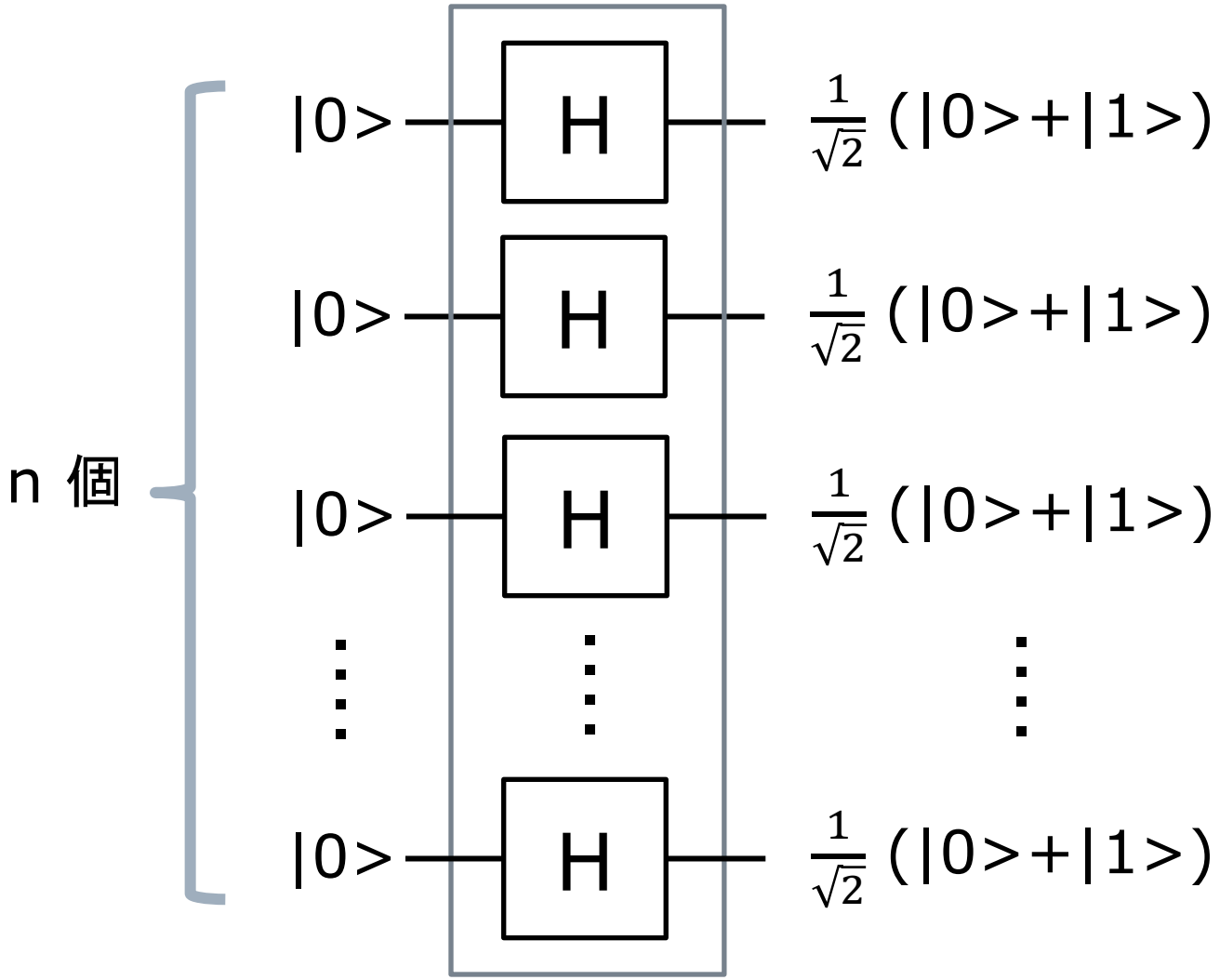
量子コンピュータでは、n個の入力に対して、その全ての状態の2^n個の「重ね合わせ」について同時並行的に計算ができる。普通のコンピュータと比較して「指数関数的」な高速化が可能となる。

(n+1)-qubit(fの入力　n-qubit, fの出力 1-qubit)の回路U_fを考える

Ufの入力に、パラレルに置かれたアダマール・ゲート n個の出力（それぞれの入力は|0>）をつなげてみよう



パラレルに置いたアダマール・ゲート n 個の出力



アダマール･ゲート n 個の場合

n個の出力のテンソル積

$$\Rightarrow \frac{1}{\sqrt{2}}(|0>+|1>)\otimes\frac{1}{\sqrt{2}}(|0>+|1>)\otimes\cdots\otimes\frac{1}{\sqrt{2}}(|0>+|1>)$$

（n個）

$$= \left(\frac{1}{\sqrt{2}}\right)^n \sum |Xi>$$

$|Xi>$は、次のようなすべての基底である

（n桁）

$$|X_0> = |000\cdots\cdots000>$$
$$|X_1> = |000\cdots\cdots001>$$
$$|X_2> = |000\cdots\cdots010>$$
$$|X_3> = |000\cdots\cdots011>$$
$$\vdots \qquad\qquad \vdots$$
$$|X_k> = |111\cdots\cdots111>$$

2^n個

先の回路U_fの出力を考える

- Ufへの入力xは、$H^{\otimes n}|0\rangle^{\otimes n}$ で、これは$\left(\frac{1}{\sqrt{2}}\right)^n \sum |Xi\rangle$ に等しい。ただし、$Xi \in \{0,1\}^n$であるすべてについて和をとる。
- $Uf(|x\rangle \otimes |0\rangle) = Uf\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum |Xi\rangle \otimes |0\rangle\right)$

  $= \left(\frac{1}{\sqrt{2}}\right)^n \sum Uf(|Xi\rangle \otimes |0\rangle)$

  $= \left(\frac{1}{\sqrt{2}}\right)^n \sum (|Xi\rangle \otimes f(|Xi\rangle))$

Quantum Parallelism

- 例えば、n=3の時、Ufの出力は次のようになる。

$$\left(\frac{1}{\sqrt{2}}\right)^3 (\\ |000>\mathrm{f}(|000>)+|001>\mathrm{f}(|001>) \\ +\ |010>\mathrm{f}(|010>)+|011>\mathrm{f}(|011>) \\ +\ |100>\mathrm{f}(|100>)+|101>\mathrm{f}(|101>) \\ +\ |110>\mathrm{f}(|110>)+|111>\mathrm{f}(|111>) \\ )$$

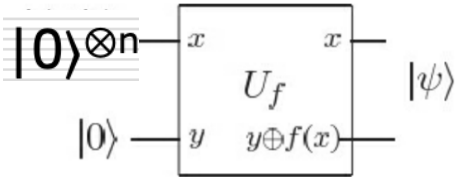
ただし、|x> ⊗ f(|x>)のテンソル記号を省略している。
三つのqubitに対する一回のUfの呼び出しが、f(|000>)から
f(|111>)までの8つのfの値を計算していることがわかる。

一般に、n個のqubitに対するUfの呼び出しは、2^n個の f の値を計算することになる。

Quantum Parallelism

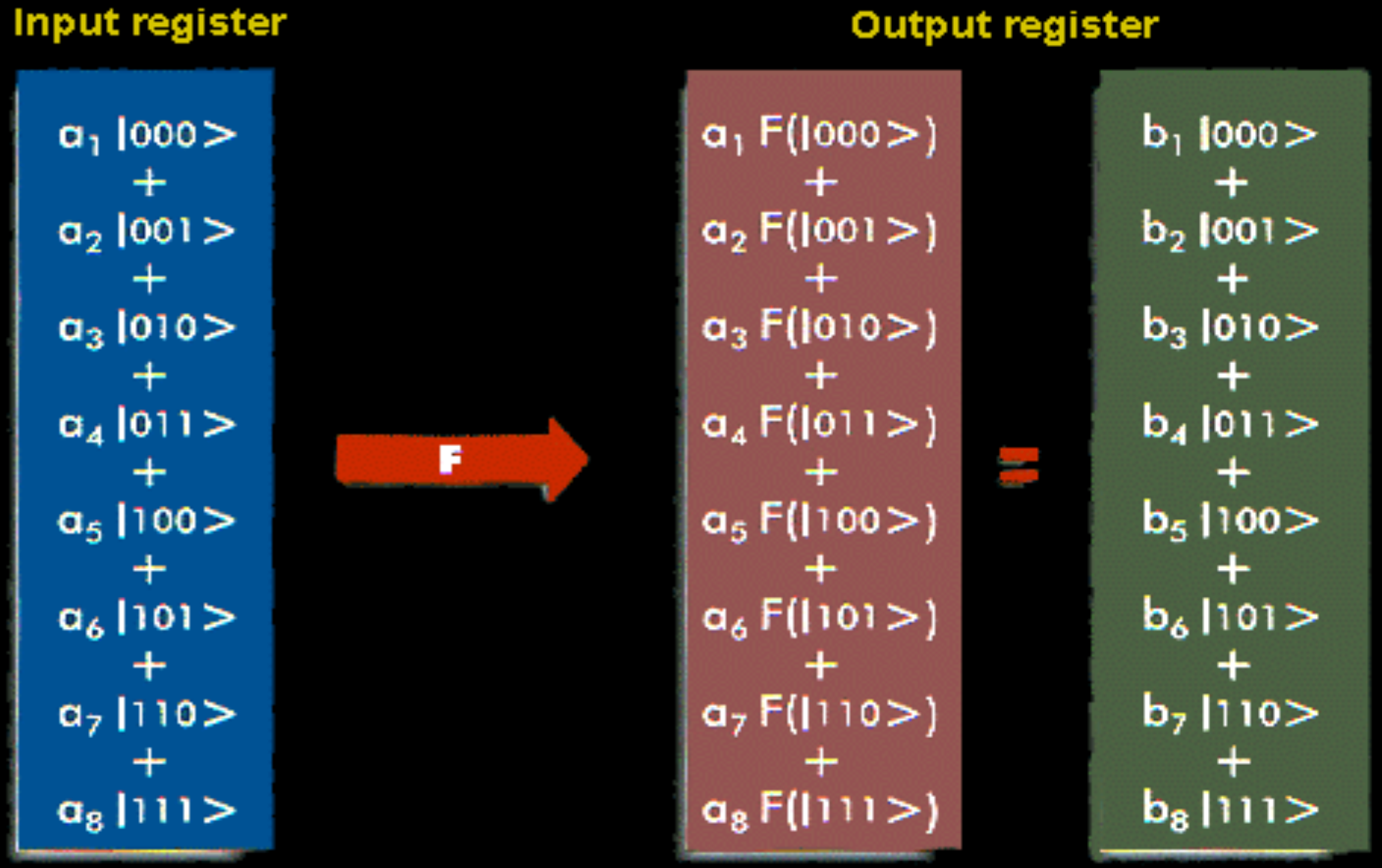
- nビットの入力xと1ビットの出力 f(x)を持つ関数の量子並列評価は、次のように実行される。
- n+1 qubitの状態 $|0\rangle^{\otimes n}|0\rangle$を用意する。次に、最初のn qubitに、アダマール変換を適用する。その出力をU_fの量子回路の入力に接続すると、次の状態が生み出される。

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



- ある意味では、量子並列処理は、関数fの全ての可能な2^n個の値を同時に評価する。たとえ、我々は明らかにfを一回だけ評価するのであるが。

n個のqubitで、2^n個の並行計算が可能



量子コンピュータの出力は、どう取り出せるのか？

出力を取り出す＝出力を観測する

- 先のような回路を組めば、一回のUfの適用で出力側に $\{0,1\}^n \ni x$ なるすべてのxについて、$\Sigma|x> f(|x>)$ が現れるので、2^n 回の f の計算ができるように見える。
- ところが、話はそう簡単ではない。出力結果を取り出すということは、結果を観測することである。
- 観測について復習しておこう。

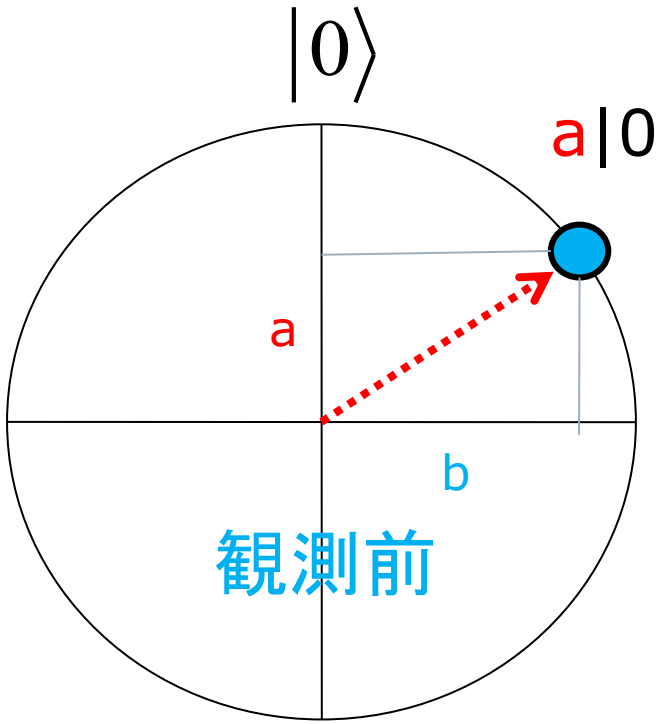
qubitの観測

- |Qubit> = a|0>+b|1> を観測すると、重ね合わせの状態は破れて失われ、|0>または|1>のいずれかの状態になる。

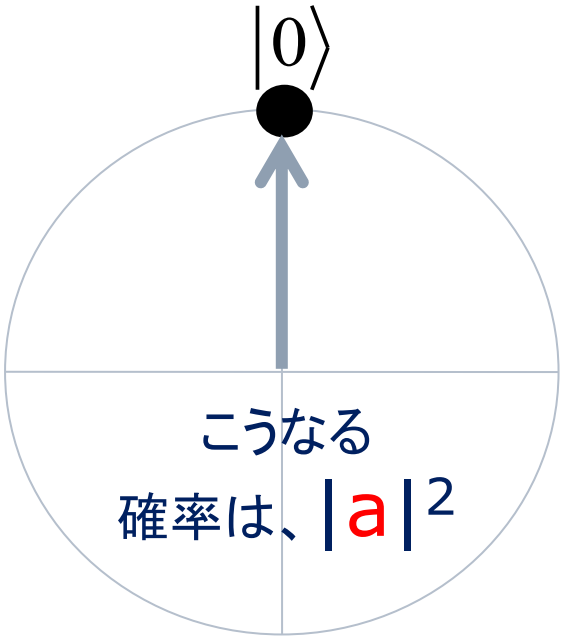
- この時、
  |0>を観測する確率は、$|a|^2$で与えられ、
  |1>を観測する確率は、$|b|^2$で与えられる。

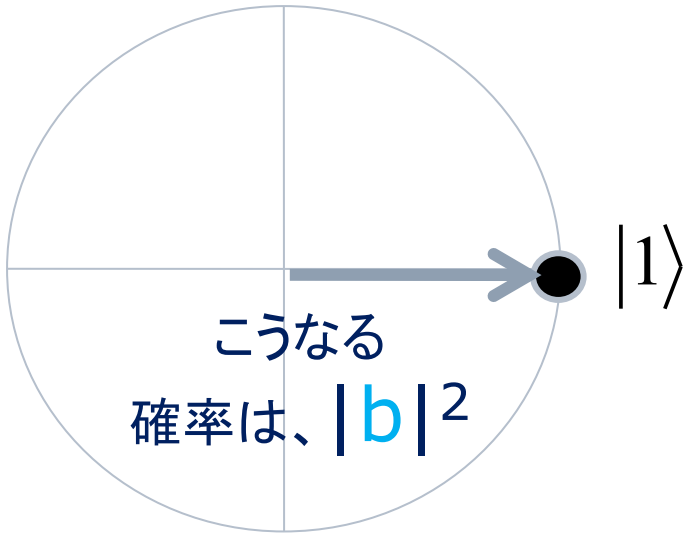
qubitの観測

観測によって、
「重ね合わせの状態」は
失われる



観測後





$\sum|x> f(|x>)$の観測

- 重ね合わせの状態の$\sum|x> f(|x>)$ を観測したとたんに、重ね合わせの状態は失われ、我々が観測するのは 個別の $|x> f(|x>)$のみである。
- 例えば、n=3の時、Ufの出力が次のようになっていても、

$$\left(\frac{1}{\sqrt{2}}\right)^3 (\\ |000> \mathrm{f}(|000>) + |001> \mathrm{f}(|001>) \\ + |010> \mathrm{f}(|010>) + |011> \mathrm{f}(|011>) \\ + |100> \mathrm{f}(|100>) + |101> \mathrm{f}(|101>) \\ + |110> \mathrm{f}(|110>) + |111> \mathrm{f}(|111>) \\ )$$

我々が観測できるのは、xの一つの値についての $|000> \mathrm{f}(|000>)$ または $|001> \mathrm{f}(|001>)$ または・・・ $|111> \mathrm{f}(|111>)$ のみである。

一般の量子状態の観測

一般の量子状態 $|\psi\rangle = \sum_{k=0}^{n-1} c_k|k\rangle$ が与えられた時、

状態 $|0\rangle$ が観測される確率は、$|c_0|^2$ で与えられる。
観測前の状態 $|\psi\rangle$は、新しい状態 $|0\rangle$に変わる。

状態 $|1\rangle$ が観測される確率は、$|c_1|^2$ で与えられる。
観測前の状態$|\psi\rangle$は、新しい状態 $|1\rangle$に変わる。

…

状態 $|k\rangle$ が観測される確率は、$|c_k|^2$ で与えられる。
観測前の状態$|\psi\rangle$は、新しい状態 $|k\rangle$に変わる。

何かが必要である

- しかし、この並列計算は、直ちに有用なわけではない。
  最初の単一qubitのサンプルで $\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$ 、

  この状態の測定は、|0> f(0) 〉か |1> f(1)〉の値のどれかを返すだけだ。もっと一般的に、状態 Σ_x |x> f(x) 〉の測定は、一つの値xについてのf(x)の値を返すだけだ。もちろん、古典的なコンピュータは、そうしたことを簡単にやってのける。
- 量子計算が役に立つためには、単なる量子並行計算以上の何かが必要になる。すなわち、Σ_x |x> f(x) 〉のような重ね合わせの状態から、f(x)の一つの値より多くの値の情報を引き出せるような能力が必要になる。

古典通信と量子通信のハイブリッド

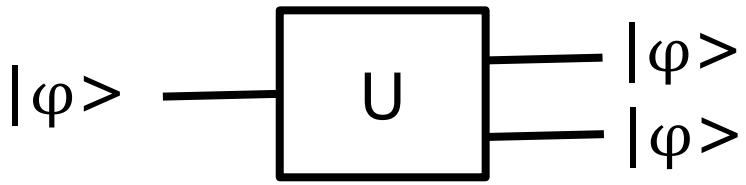
No Cloning Theorem
Super Dense Coding
Quantum Teleportation

No Cloning 定理

未知の量子の状態を複数コピーすることはできない

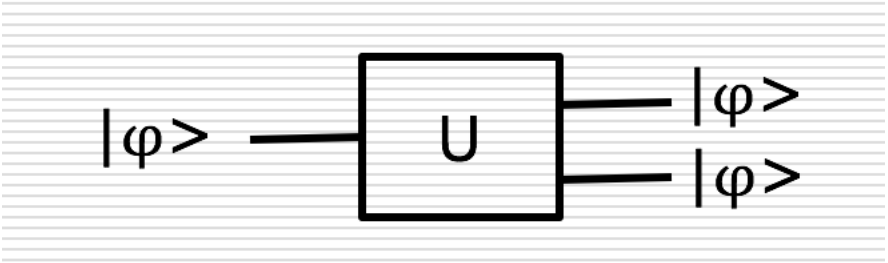
No Cloning 定理

- ある状態 $|\varphi\rangle=\alpha_0|0\rangle+\alpha_1|1\rangle$に対して、$|\varphi\rangle\otimes|\varphi\rangle$ すなわち自己のコピーをもう一つ生成する回路を考えよう。実は、量子ゲートの世界では、こうした基本的な操作ができないのだ。これを、No Cloning 定理と呼ぶ。以下、それを説明しよう。



こうした回路は存在しない！

No Cloning 定理の証明



- 先のような回路（ユニタリ変換U）が存在したとする。
  その回路は、一般のφだけでなく、|0>, |1> に対しても働くので、

$$U|0\rangle = |00\rangle$$
$$U|1\rangle = |11\rangle$$

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ とすれば、

$$U|\psi\rangle = \alpha U|0\rangle + \beta U|1\rangle = \alpha|00\rangle + \beta|11\rangle$$

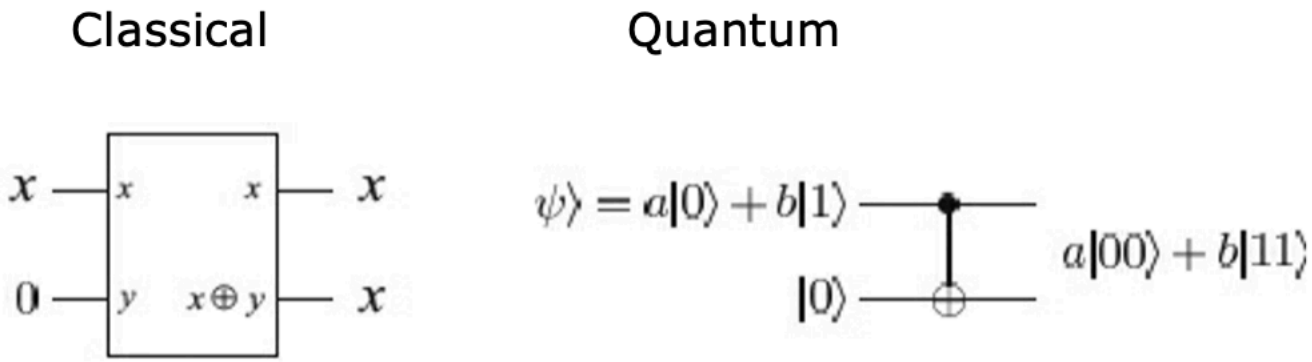
- Uは、|ψ>もコピーできるはずなので、

$$U(|\psi\rangle) = |\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

- しかし、この二つの条件を満たすα, βは、存在しない。

CNOTとコピー回路

CNOTに相当する古典回路は、古典情報をコピーする。



未知の状態 |Ψ⟩ = a|0⟩ + b|1⟩ のあるqubitを、CNOTゲートを使ってコピーしようとしたとしよう。二つのqubitの入力の状態は、次のようにかける。

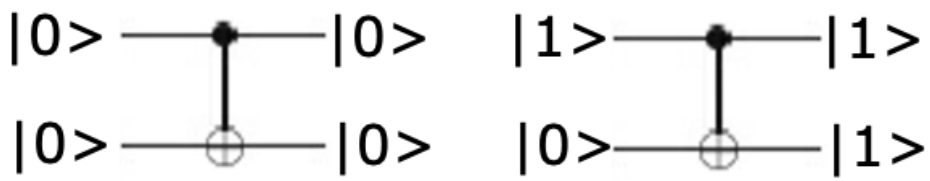
$[a|0> + b|1>] \otimes |0> = a|00> + b|10>$

CNOTの機能は、第一qubitが1の時、第二のqubitを否定することだから、この出力は、単純で、a|00⟩ + b|11⟩となる。

CNOT(a|00>+b|10>) =a|00>+b|11>

CNOTとコピー回路

この時、首尾よく |Ψ⟩をコピーできたであろうか？ すなわち、状態 |Ψ⟩|Ψ⟩を生み出すことができたであろうか？
確かに、 |Ψ⟩ ＝ |0⟩ あるいは |Ψ⟩ ＝ |1⟩ の時には、この回路は、まさにそれをしている。CNOT回路を、|0> あるいは|1>にエンコードされた古典情報をコピーするのに利用することは可能なのだ。



CNOTとコピー回路

しかし、もっと一般的な状態 |Ψ⟩ については、 |Ψ⟩|Ψ⟩は次のようになる。

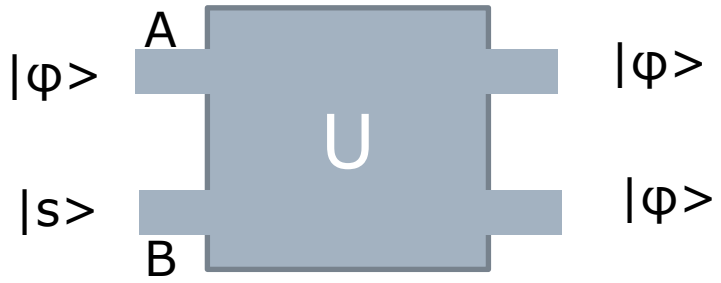
$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle.$$

a|00 ⟩ + b|11⟩ と比較すると、ab=0でなければ、CNOT回路は、入力の量子状態をコピーしていないことがわかる。

実際、未知の量子状態をコピーすることは、不可能だということがわかる。qubitはコピーされないというこの性質は、No-cloning定理として知られている、量子情報と古典情報の主要な違いの一つである。

もう少し、きちんとした証明

二つのスロットA, Bを持つ量子回路を考えよう。スロットAはデータスロットで、最初の状態では、未知のピュアな状態|φ> が与えられている。それが、ターゲットスロットのBにコピーされるとしよう。



もう少し、きちんとした証明

この時、次の式が成り立つ。

$U(|\psi>\otimes|s>)=|\psi>\otimes|\psi>$

$U(|\varphi>\otimes|s>)=|\varphi>\otimes|\varphi>$

両辺の内積を取る。

左辺は、$(\ U(|\psi>\otimes|s>), U(|\varphi>\otimes|s>)\ ) =$ Uは内積を保存するから

$=(\ |\psi>\otimes|s>, |\varphi>\otimes|s>)=<\psi|\varphi><s|s>=<\psi|\varphi>$

右辺は、$(\ |\psi>\otimes|\psi>, |\varphi>\otimes|\varphi>)=<\psi|\varphi>\ <\psi|\varphi>=$

$=(<\psi|\varphi>)^2$

よって、 $<\psi|\varphi>==(<\psi|\varphi>)^2$

テンソル積の内積の定義

$$\left(\sum_i a_i|v_i\rangle\otimes|w_i\rangle, \sum_j b_j|v'_j\rangle\otimes|w'_j\rangle\right) \equiv \sum_{ij} a_i^* b_j \langle v_i|v'_j\rangle\langle w_i|w'_j\rangle.$$

もう少し、きちんとした証明

ただ、$\langle\psi|\varphi\rangle=(\langle\psi|\varphi\rangle)^2$ ということだが、$x = x^2$ には、二つの解しかない。$x = 0$ と $x = 1$である。だから、$\langle\psi|\varphi\rangle=0$ であるか、$\langle\psi|\varphi\rangle=1$のいずれかということになる。

$|\psi\rangle = |\varphi\rangle$ であるか、 $|\psi\rangle$ と $|\varphi\rangle$ が直交するかのどちらかである。こうして、クローニング回路は、もし存在するとしても、お互いに直交する状態しかコピーできない。

よって、一般的な量子状態をコピーするマシンは、不可能である。

同時にこのことは、なぜ、0と1の古典ビットからなる古典情報がコピー可能なのかの説明にもなっている。

At first sight the no-cloning theorem appears rather peculiar. After all, isn't classical physics a special case of quantum mechanics? How is it possible that we can copy classical information if we can't copy quantum states? The answer is that the no-cloning theorem does not prevent all quantum states from being copied, it simply says that nonorthogonal quantum states cannot be copied. More precisely, suppose and are two non-orthogonal quantum states. Then the no-cloning theorem implies that it is not possible to build a quantum device that, when input with $|\psi\rangle$ or $|\varphi\rangle$ will output two copies of the input state, $|\psi\psi\rangle$ or $|\varphi\varphi\rangle$.

On the other hand, if $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal, then the no-cloning theorem doesn't prohibit their cloning. Indeed, it is rather easy to design quantum circuits which copy such states!

This observation resolves the apparent contradiction between the no-cloning theorem and the ability to copy classical information, for the different states of classical information can be thought of merely as orthogonal quantum states.

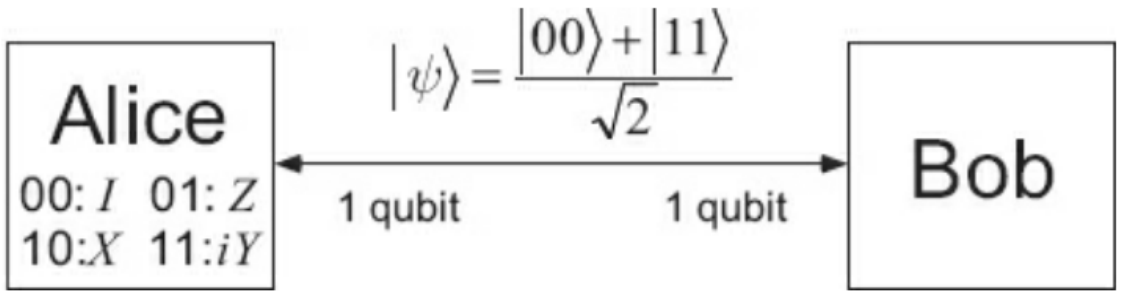
Nielsen, Michael A..
Quantum Computation and Quantum Information (p.531).
Cambridge University Press.

Super Dense Coding

一つのqubitで、二つの古典ビットをコードして送ることができる

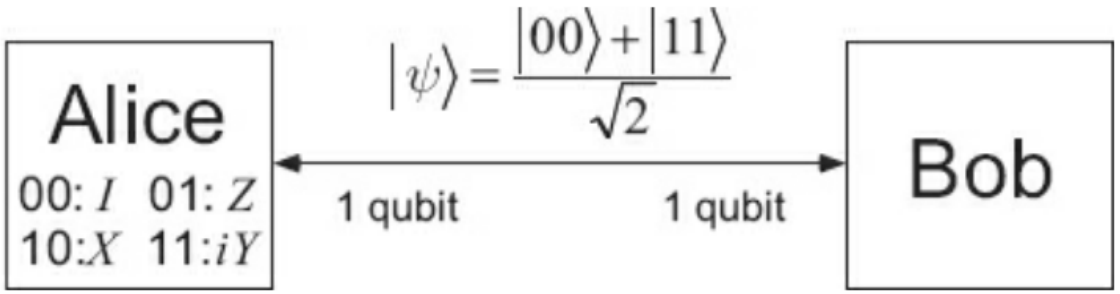
Superdense coding

- Superdense codingというのは、あらかじめ用意されたエンタングルメントを利用して、AliceからBobに、一つのqubitを送るだけで、二つの古典ビットを送ることができることをいう。



- AliceとBobは、次のようなエンタングルした状態を共有しているとする。第一ビットがAliceのqubit, 第二qubitがBobのqubitとしよう。

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$



- もし、ビット列'00'を送りたいのなら何もしない。もし、'01'を送りたいのなら、自分のqubitにフェーズ・フリップのZを適用する。'10'だったら、量子NOTゲートのXを、'11'だったら、iYを適用する。結果は次のようになる。

I $\quad 00 : |\psi\rangle \rightarrow \dfrac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \Phi^{+}$

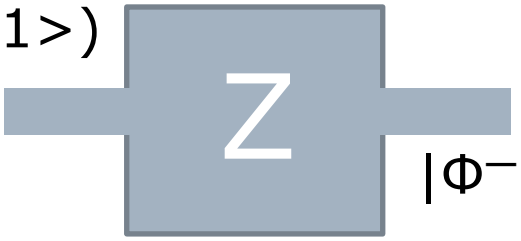
Z $\quad 01 : |\psi\rangle \rightarrow \dfrac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad \Phi^{-}$

X $\quad 10 : |\psi\rangle \rightarrow \dfrac{|10\rangle + |01\rangle}{\sqrt{2}} \qquad \Psi^{+}$

iY $\quad 11 : |\psi\rangle \rightarrow \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}. \qquad \Psi^{-}$

$Z|\Phi^+> \rightarrow \Phi^-$

$|\Phi^+> = 1/\sqrt{2}\ (|00> + |11>)$

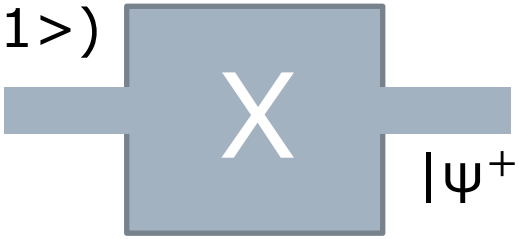


$|\Phi^-> = 1/\sqrt{2}\ (|00> - |11>)$

Phase Flip

$X|\Phi^+> \rightarrow \psi^+$

$|\Phi^+> = 1/\sqrt{2}\ (|00> + |11>)$

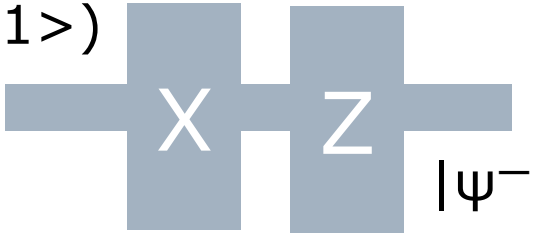


$|\psi^+> = 1/\sqrt{2}\ (|10> + |01>)$

Bit Flip

$ZX|\Phi^+> \rightarrow \psi^-$

$|\Phi^+> = 1/\sqrt{2}\ (|00> + |11>)$



$|\psi^-> = 1/\sqrt{2}\ (|10> - |01>)$

- この四つの状態は、Bell基底として知られているものである。AliceがBobにこの手順でqubitを送ったとすれば、Bobは、Bell基底で測定すれば、Aliceが送った四つの可能なビット列を決定できる。

- まとめれば、Aliceは、ただ一つのqubitと相互作用するだけで、Bobに2ビットの情報を送ることができる。もちろん、このプロトコルでは、二つのqubitが利用されているのだが、Aliceは、二番目のqubitとは、相互作用する必要はない。

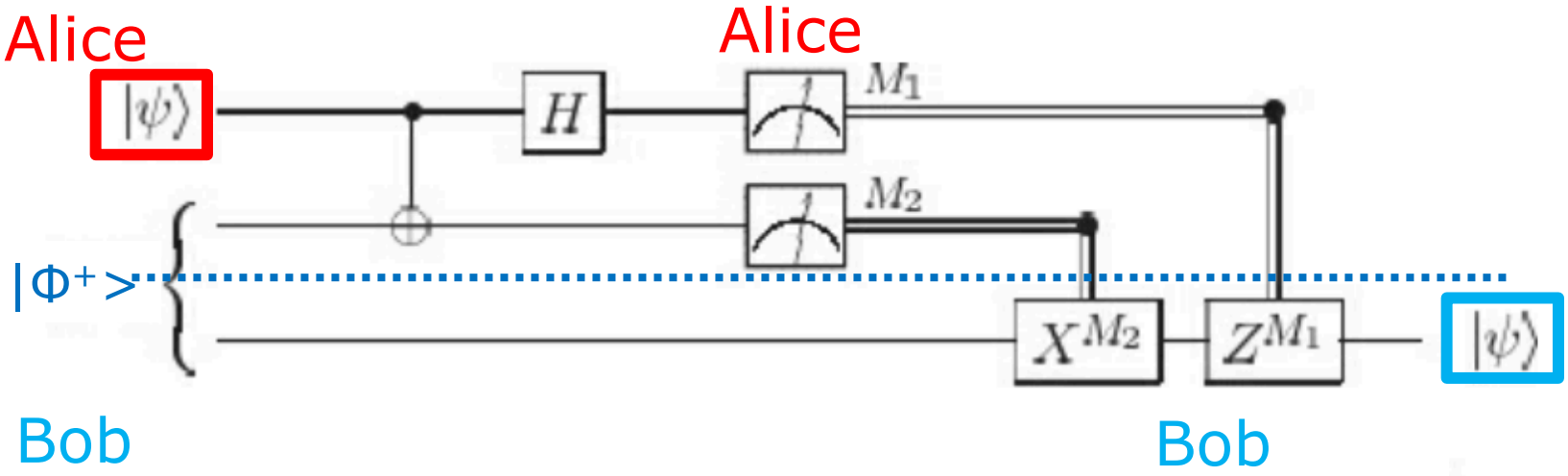
- Even more interesting are the results in distributed quantum computation. Imagine you have two computers networked, trying to solve a particular problem. How much communication is required to solve the problem? Recently it has been shown that quantum computers can require exponentially less communication to solve certain problems than would be required if the networked computers were classical!

- Unfortunately, as yet these problems are not especially important in a practical setting, and suffer from some undesirable technical restrictions. A major challenge for the future of quantum computation and quantum information is to find problems of real-world importance for which distributed quantum computation offers a substantial advantage over distributed classical computation.

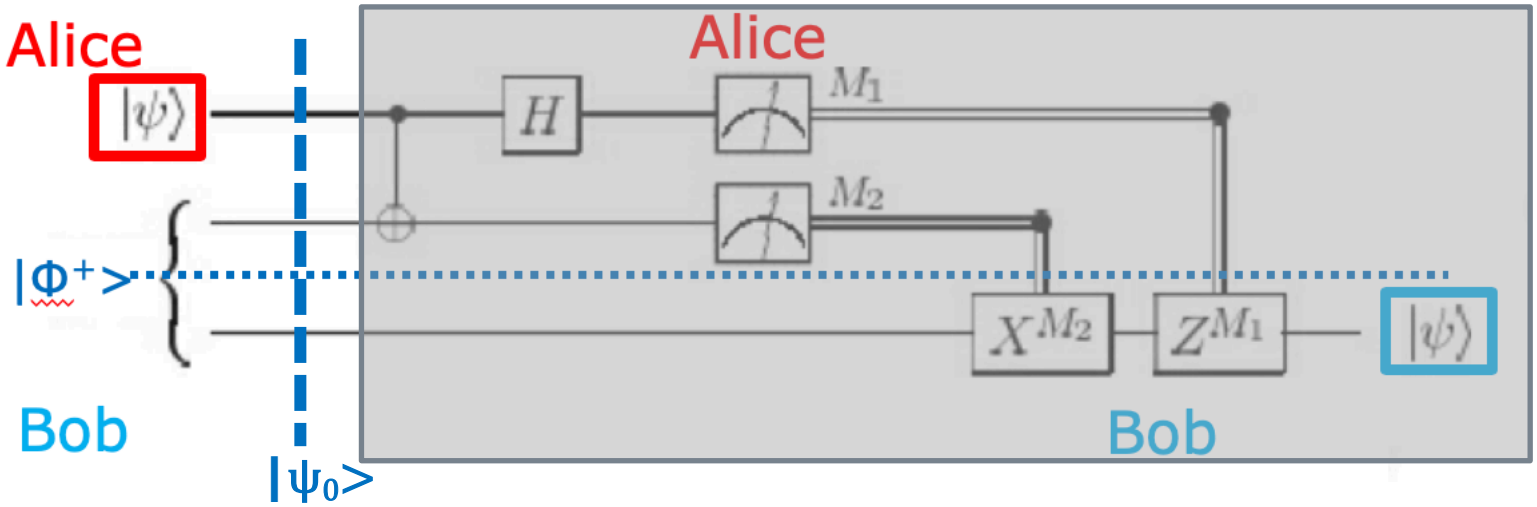
Nielsen, Michael A..
Quantum Computation and Quantum Information (p.9).
Cambridge University Press.

量子テレポーテーション

量子テレポーテーションを実現する回路



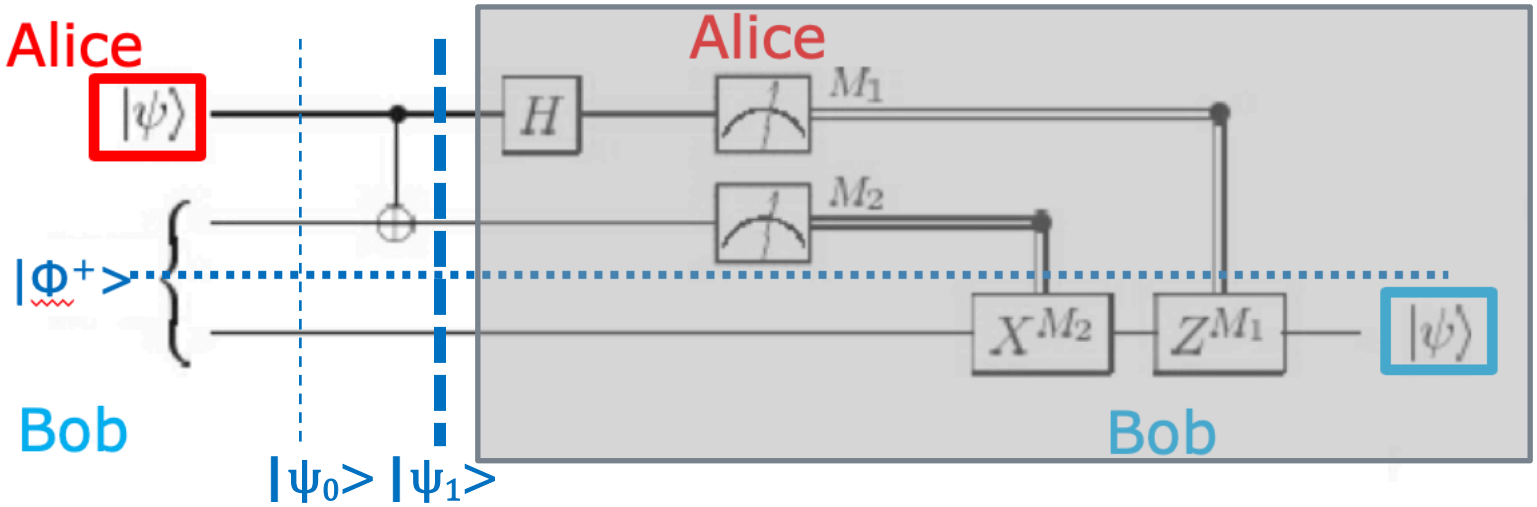
この回路図は、横長に書かれているが、通信が行われるのは、AliceからBobへ、縦方向に行われることに注意。また、すでにAliceとBobは、エンタングル状態にあることが前提されている。（図の$|\Phi^+\rangle$がそれを表している。）



$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$, $|\Phi^+\rangle = 1/\sqrt{2}\,(|00\rangle + |11\rangle)$ とすると。

$$|\psi_0\rangle = |\psi\rangle \otimes |\Phi^+\rangle$$
$$= (\alpha|0\rangle+\beta|1\rangle) \otimes 1/\sqrt{2}\,(|00\rangle + |11\rangle)$$
$$= 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle +|11\rangle)+\beta|1\rangle\otimes(|00\rangle + |11\rangle))$$

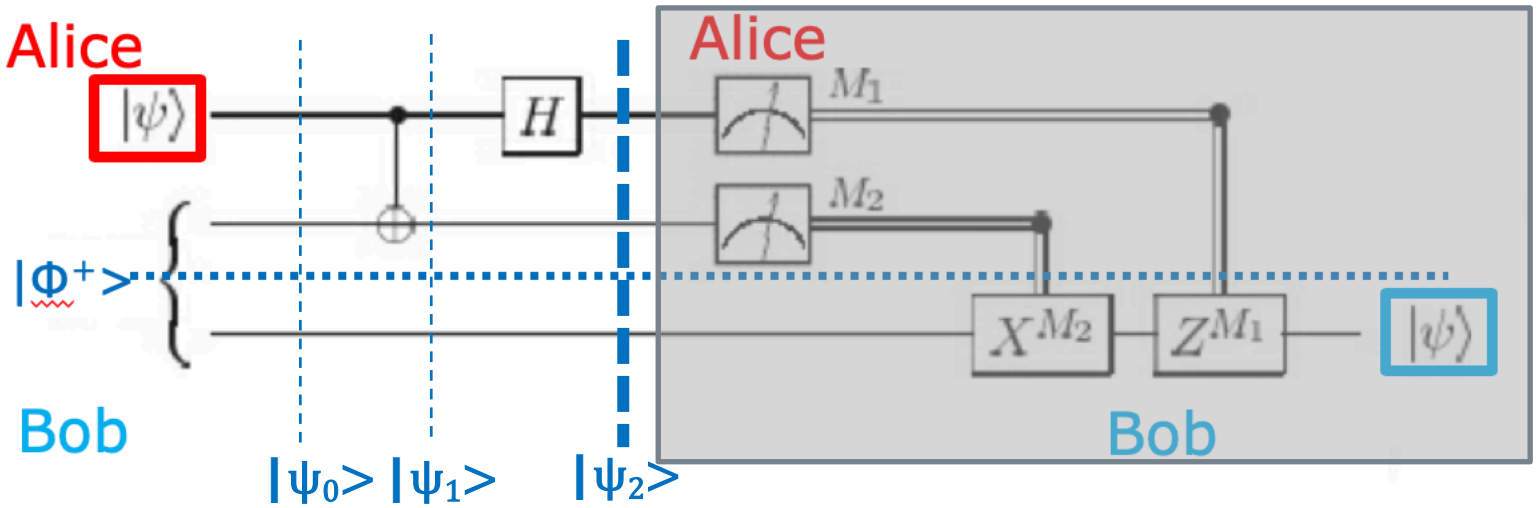
回路に入る直前の $|\psi_0\rangle$段階でのシステムの状態



$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|10\rangle + |01\rangle))$$

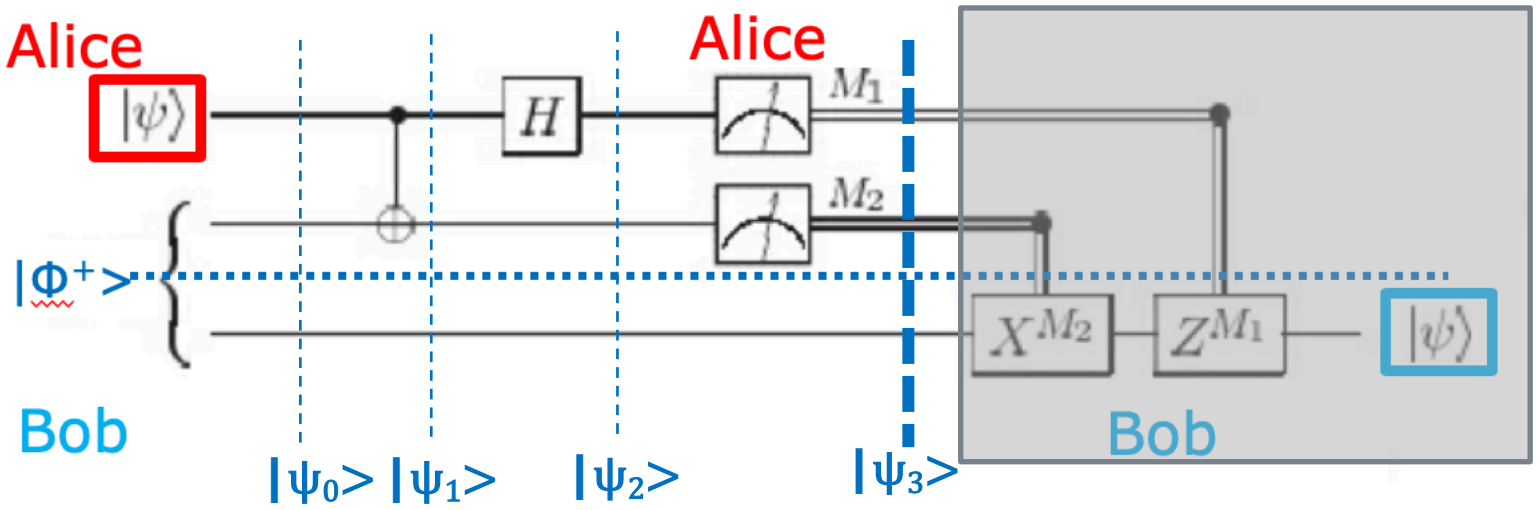
回路上のCNOTを実行した直後の $|\psi_1\rangle$段階でのシステムの状態



$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|10\rangle + |01\rangle))$$

$$\begin{aligned}|\psi_2\rangle &= 1/\sqrt{2}\,(\alpha(|0\rangle+|1\rangle)\otimes(|00\rangle + |11\rangle) + \\ &\qquad \beta(|0\rangle-|1\rangle)\otimes(|10\rangle + |01\rangle)\,) \\ &= 1/\sqrt{2}\,(\alpha(|000\rangle+|011\rangle+|100\rangle+|111\rangle) + \\ &\qquad \beta(|010\rangle+|001\rangle-|110\rangle-|101)\,) \\ &= 1/\sqrt{2}\,(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle) + \\ &\qquad |10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\,(\alpha|1\rangle-\beta|0\rangle)\,)\end{aligned}$$

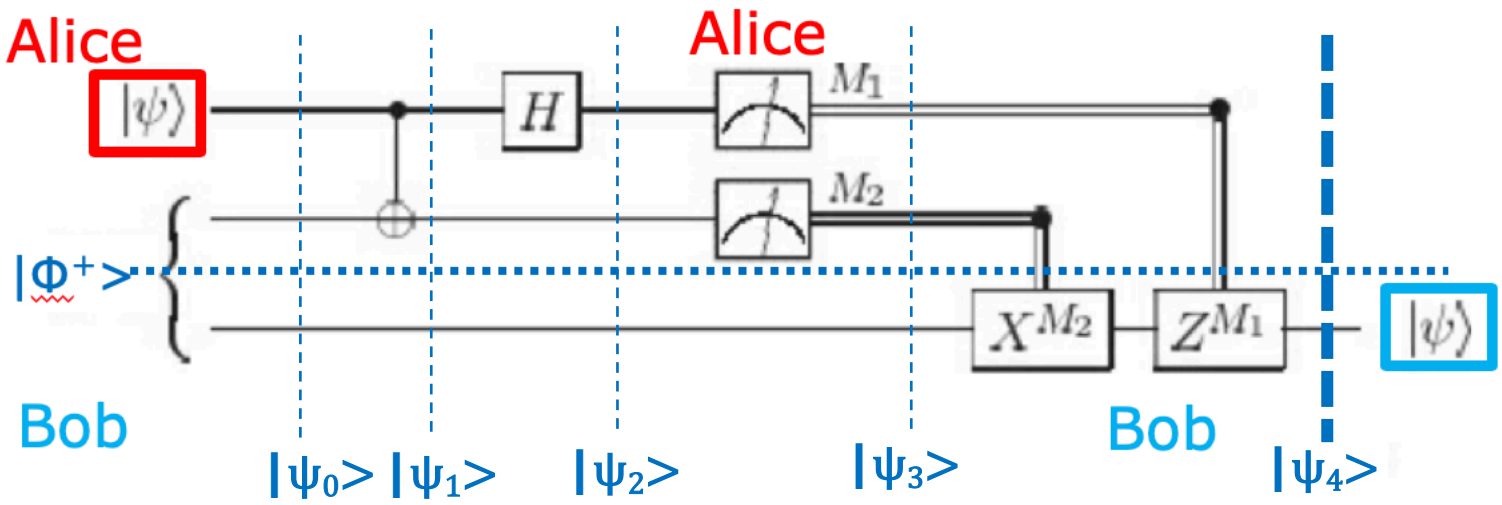


$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|10\rangle + |01\rangle))$$

$$|\psi_2\rangle = 1/\sqrt{2}\,(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle\,(\alpha|1\rangle - \beta|0\rangle)\,)$$

$$|\psi_3(00)\rangle = (\alpha|0\rangle + \beta|1\rangle)$$
$$|\psi_3(01)\rangle = (\alpha|1\rangle + \beta|0\rangle)$$
$$|\psi_3(10)\rangle = (\alpha|0\rangle - \beta|1\rangle)$$
$$|\psi_3(11)\rangle = (\alpha|1\rangle - \beta|0\rangle)$$



$|\psi_3(00)\rangle = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_3(01)\rangle = (\alpha|1\rangle+\beta|0\rangle)$
$|\psi_3(10)\rangle = (\alpha|0\rangle-\beta|1\rangle)$
$|\psi_3(11)\rangle = (\alpha|1\rangle-\beta|0\rangle)$

$|\psi_4(00)\rangle = \psi_3(00)\rangle = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(01)\rangle = X\,|\psi_3(01)\rangle = X(\alpha|1\rangle+\beta|0\rangle) = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(10)\rangle = Z|\psi_3(10)\rangle = Z(\alpha|0\rangle-\beta|1\rangle) = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(11)\rangle = ZX|\psi_3(11)\rangle = ZX\,(\alpha|1\rangle-\beta|0\rangle) = (\alpha|0\rangle+\beta|1\rangle)$

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

いくつかの疑問

- 第一。量子テレポーテーションは、光より早く量子状態を送ることができるのだろうか？
  これに対する答えは、明確にノーだ。テレポーテーションを実行するためには、Aliceは観測結果を、古典的な通信路で、Bobに送らなければならないのだから。

- 第二。量子テレポーテーションは、未知の量子状態のコピーを禁じたNo Cloning定理を破ることにならないか？
  これについても、答えはノーだ。Bobのもとで、量子状態は再現されるのだが、Aliceのもとにあったオリジナルの量子状態は、Aliceの観測によって、|0>か|1>かの状態に変わって、失われている。