1.1.1 量子コンピュータの歴史

- 量子力学
- 計算機科学
- 情報理論
- 暗号理論

量子力学の歴史

1920年代初頭: 量子力学誕生

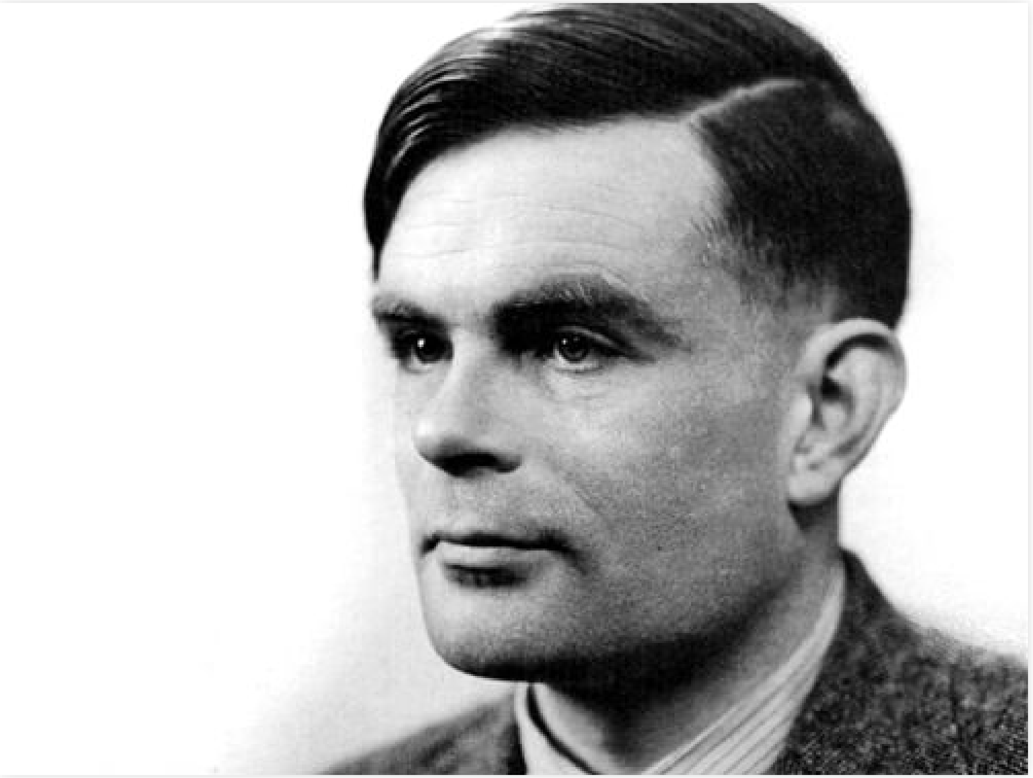
1970年代: 単一量子を制御するシステムの発展

1980年代初頭: 量子複製不可能性定理

- 複製可能なら光より早く信号を送れる。

計算機科学の歴史

チューリングマシン(1936)



アラン・チューリング (Alan Turing)

チューリングマシン(1936)

計算機を数学的に議論するための単純化・理想化された仮想機械 数学的定義

ハード

- 無限長のテープ
- ヘッド
- ヘッドによる読み書きと、テープの左右へのシークを制御する機能を持つ、有限オートマトン

ソフト

- テープに読み書きされる有限個の種類の記号
- 最初から（初期状態において）テープにあらかじめ書かれている記号列
- 有限オートマトンの状態遷移規則群

チューリングマシン(1936)

有限オートマトンの状態遷移規則群

- テープの「現在の場所」に新しい記号を書き込む（あるいは、現在の記号をそのままにしてもよい）
- ヘッドを右か左に一つシークする（あるいは、移動しなくてもよい）
- 有限オートマトンを次の状態に状態遷移させる（同じ状態に遷移してもよい）

万能チューリング・マシン

- あらゆるチューリングマシンをシミュレートできるチューリングマシンが可能

トランジスタの発明(1947)

ムーアの法則

- 2年ごとに計算能力は2倍に
- 2020年ごろには終焉か
- => 新しいパラダイムの必要

チャーチ・チューリングのテーゼ(1960年代後期-)

物理的装置で実行できるアルゴリズムという概念と万能チューリングマシンの数学的概念は等価

強いチャーチ・チューリングのテーゼ(1960年代後期-)

「いかなるアルゴリズムもチューリングマシンで効率的にシュミレートできる」

↓しかし

ソロベイ・シュトラッセン素数判定法(1977)

=> ランダム性を取り入れたアルゴリズムの可能性

↓

修正された強いチャーチ・チューリングのテーゼ

「いかなるアルゴリズムも確率的チューリングマシンで効率的にシュミレートできる」

デイヴィッド・ドイッチュ David Deutch (1985)

確率的チューリングマシンでも効率的に解けないが量子コンピュータなら解ける問題が存在することを示す。

量子コンピュータで高速に解けるアルゴリズム

ピーター・ショア Peter Shor (1995)

1. 素因数分解
2. 離散対数問題

Lov Grover (1995)

未整序DBの探索問題の高速化

Richard Feynman(1982)

古典的コンピュータで量子力学系をシミュレートするのは難しい。

量子コンピュータはそれを解決する。

=> 量子力学系のシミュレーションが量子コンピュータの主要なアプリの1つとなる。

量子コンピュータのアルゴリズムを見つけるのは難しい

- 人間の直感に反する
- 量子力学を使うだけでなく、古典的コンピュータより速いものでなければならない。

情報理論の歴史

クロード・シャノン Claude Shannon 1948

- "通信の数学的理論" (The Mathmatical Theory of Communication)
- シャノンの情報源符号化定理(シャノンの第一基本定理)
  - データ圧縮の可能な限界と情報量（シャノンエントロピー）の操作上の意味を確立する定理
  - => 情報を保存するには物理的リソースが必要
- シャノンの通信路符号化定理(シャノンの第二基本定理)
  - ノイズを含む通信経路でどれだけエラーのないデータを送れるかを示す

ベン・シューマチャー Ben Schumacher (1995)

- 量子ビット(quantum bit, qubit)を定義

CSS codes (Rovert Calderbank, Peter Shor, Andrew steane) 1996

- 量子誤り訂正符号
- 古典的誤り訂正は使えない(<= 複製不可能定理)

量子テレポテーション (quantum telepotation)

- 容量0の量子チャネルを往復させると、情報を伝えることができる。

暗号理論理論の歴史

共通鍵暗号

鍵配送問題

- 第三者によって盗聴される可能性

量子暗号(量子鍵配送)

- 観測されると盗聴者の存在が明らかになる
- 1960年代後半 Stephen Wiesnerが提案
- 1984 Charles Bennet, Gilles Brassardがプロトコルを提唱

公開鍵暗号

RSA暗号、離散対数問題はショアのアルゴリズムで破られる。

1.2 量子ビット (Qubit, Quantum bits)

≡

1量子ビットの状態

$$|\psi\rangle = \alpha|0\rangle + \beta|0\rangle \qquad (\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1)$$

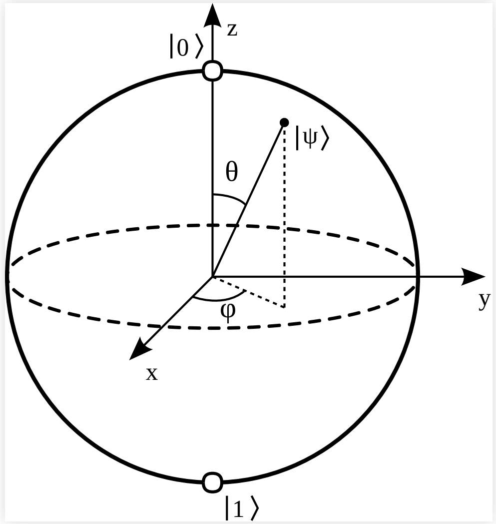
- 古典ビットの0,1 => $|0\rangle, |1\rangle$
- $|\rangle$: ディラック(Dirac)の記法、ブラケット記法
- 2次元複素ベクトル空間のベクトル
  - $|0\rangle, |1\rangle$ は正規直交基底
  - $|0\rangle, |1\rangle$ はcomputational basis state(計算基礎状態)
- 量子状態は観測できない $\Leftrightarrow \alpha, \beta$ は観測できない。
- 観測されるまでは、$|0\rangle$ と $|1\rangle$ の間の連続的状態をとる。
- 観測されると確率的に0または1と観測される。

ブロッホ球 Bloch sphere

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1)$$
$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle) \qquad (\theta, \varphi \in \mathbb{R})$$

$e^{i\gamma}$は観察可能な影響を与えない

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



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

- 50%の確率で0,50%の確率で1の状態

様々な物理システムが量子ビットを実現

- 2つの異なる偏光の光子
- 平等磁界(uniform magnetic field)に置ける核スピンアラインメント
- 単一原子を旋回する電子の状態
  - ground 基底状態
  - excited 励起状態

1.2.1 複数量子ビット Multiple qubits

2量子状態

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

1つ目の量子ビットが0と観測されると

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

ベル状態 (Bell state, EPR pair)

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

- 量子テレポテーションで重要
- 一方を測定すれば他方もわかる
- Einstein, Podolskey, Rosenが指摘

n 量子ビット

2^n 個の状態

量子ゲート

単一量子ゲート

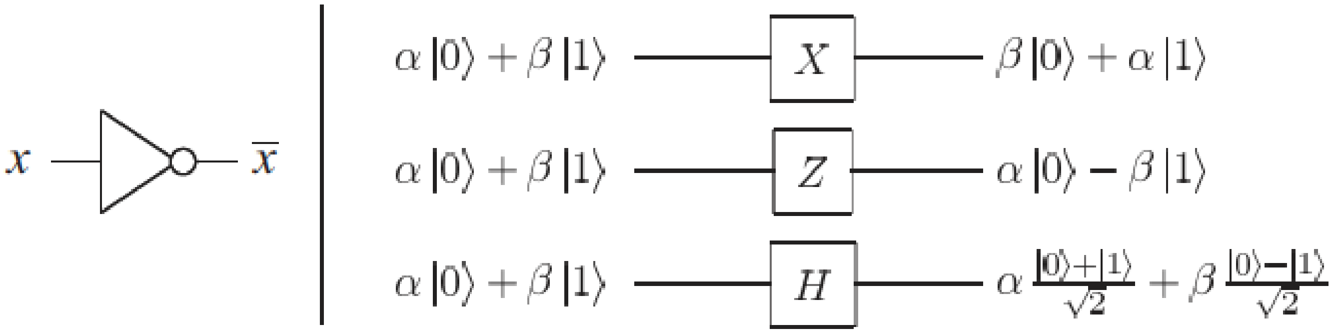


Figure 1.5. Single bit (left) and qubit (right) logic gates.

1) NOTゲート

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

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

2) Z ゲート

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

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

3) Hadamardゲート (アダマールゲート)

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

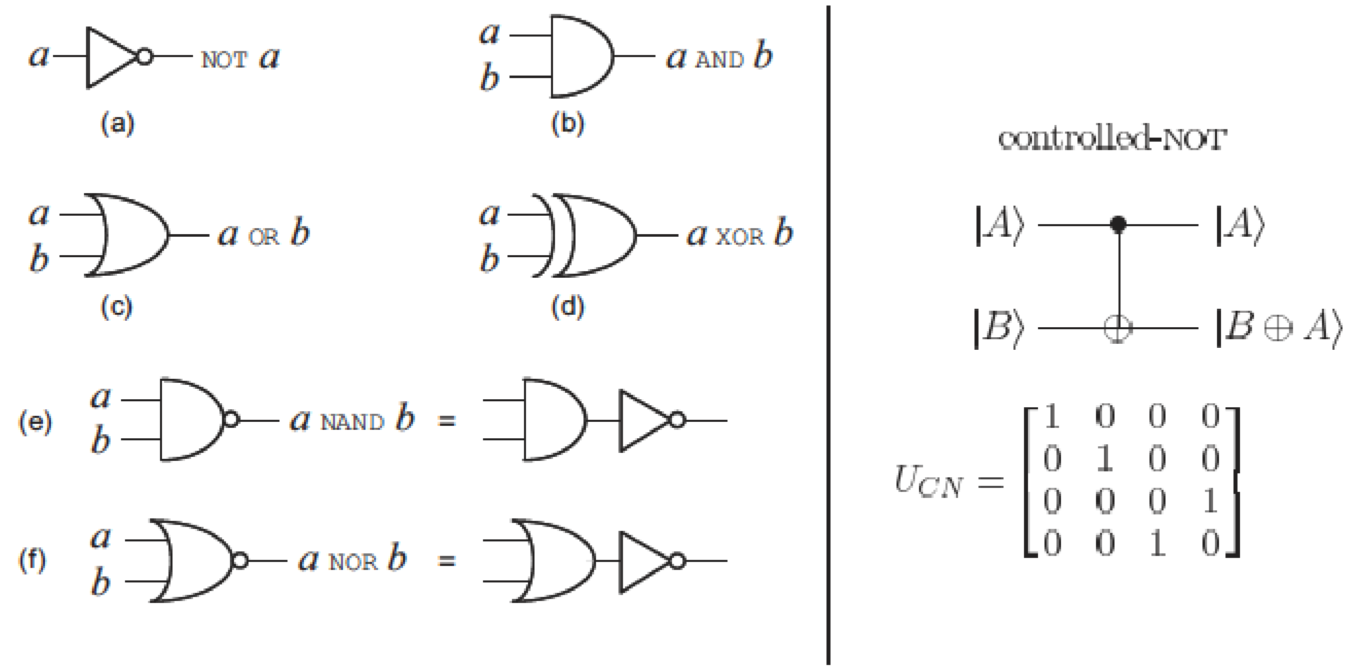
- NOTゲートの平方根と言われることもある。
- ブロッホ球でy軸を中心に90°、x軸を中心に180°回転する処理

- 単一量子ゲートは2x2のユニタリ行列となる。
- 任意のユニタリ行列は量子ゲートとなる。
- 2x2のユニタリ行列は下記のように合成できる。(詳細は4.2)

$$
U = e^{i\alpha} \begin{bmatrix} e^{-\frac{i\beta}{2}} & 0 \\ 0 & e^{\frac{i\beta}{2}} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}, \begin{bmatrix} e^{-\frac{i\delta}{2}} & 0 \\ 0 & e^{\frac{i\delta}{2}} \end{bmatrix}
$$

$$
\alpha, \beta, \gamma, \delta \in \mathbb{R}
$$

複数量子ゲート



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

古典ゲート

AND, OR, XOR, NAND, NOR

NANDゲートのみで全てのゲートを構成可能

=> ユニバーサルゲート

CNOTゲート (controlled-NOTゲート, 制御NOTゲート)

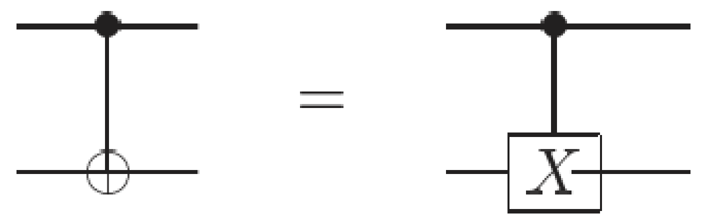


Figure 1.9. Two different representations for the controlled-NOT.

- 入力
  - コントロール量子ビット
  - ターゲット量子ビット

$$
\begin{aligned}
|00\rangle &\longrightarrow |00\rangle \\
|01\rangle &\longrightarrow |01\rangle \\
|10\rangle &\longrightarrow |11\rangle \\
|11\rangle &\longrightarrow |10\rangle
\end{aligned}
$$

XORを用いると次のように表現できる

$$|A, B\rangle \longrightarrow |A, B \oplus A\rangle$$

行列を用いると、

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

U_{CN}もユニタリ行列

$$ U^{\dagger}{CN}U{CN}=I $$

任意の複数論理量子ゲートはCNOTゲートと単一量子ゲートの組み合わせで構成できる。

量子回路

ルール

- 右から左に読む
- 回路の入力は基本的には全て$|0\rangle$

特徴

- 非周期的(acyclic) - ループできない
- FANINできない
  - 出力数以上の入力量子ビットを扱うゲートは作れない
- FANOUTできない
  - 出力を複製できない(量子複製不可能性定理)

スワッピング回路

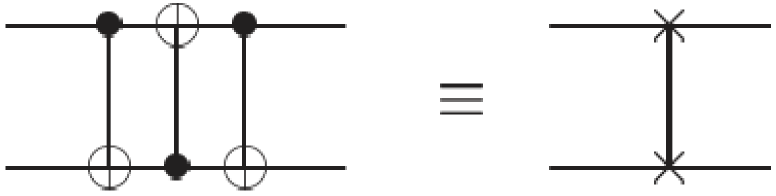


Figure 1.7. Circuit swapping two qubits, and an equivalent schematic symbol notation for this common and useful circuit.

$$
\begin{aligned}
&|a, b\rangle \\
&\longrightarrow |a, a \oplus b\rangle \\
&\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\
&\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle
\end{aligned}
$$

controlled-Uゲート

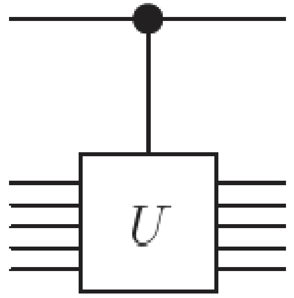


Figure 1.8. Controlled-U gate.

- 入力
  - 1コントロール量子ビット
  - nターゲット量子ビット

コントロール量子ビットが0の時、ターゲット量子ビットは変化しない

コントロール量子ビットが1の時、n個の量子ビットに対してユニタリ行列Uを作用させる

測定

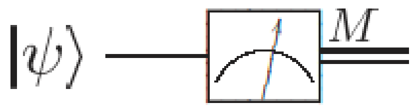


Figure 1.10. Quantum circuit symbol for measurement.

量子ビット$|\psi\rangle$を測定して古典ビットMに変換

二重線は古典ビットを示す

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

のとき、α^2の確率で0にβ^2の確率で1に変換される。

量子ビットをコピーする回路は可能か?

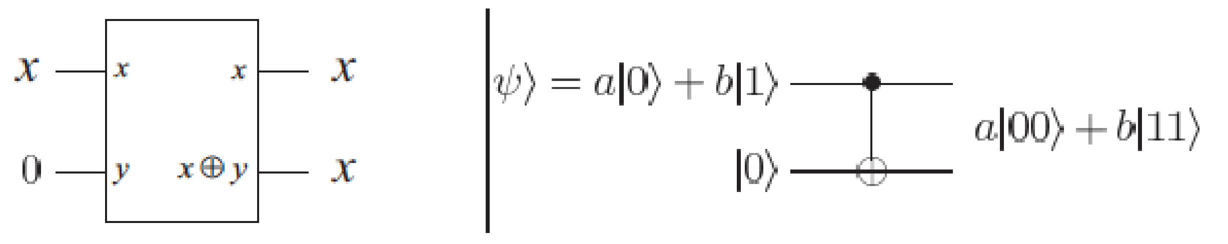


Figure 1.11. Classical and quantum circuits to 'copy' an unknown bit or qubit.

不可能

$$a|00\rangle + b|11\rangle$$

- 1つの量子ビットが確定するともう1つも確定する。
- aとbに関する追加の情報は得られない。
- コピーできれば、$a|0\rangle + b|1\rangle$ を複数回観測できるので、aとbに関する追加の情報を得れる。

Bell状態 (EPR状態, EPRペア)

- Bell, Einstein, Podolsky, Rosen

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

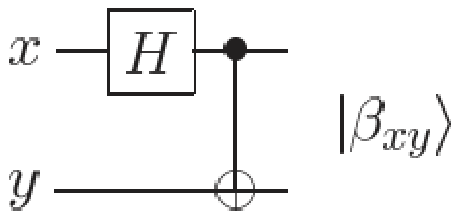


Figure 1.12. Quantum circuit to create Bell states, and its input–ouput quantum 'truth table'.

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

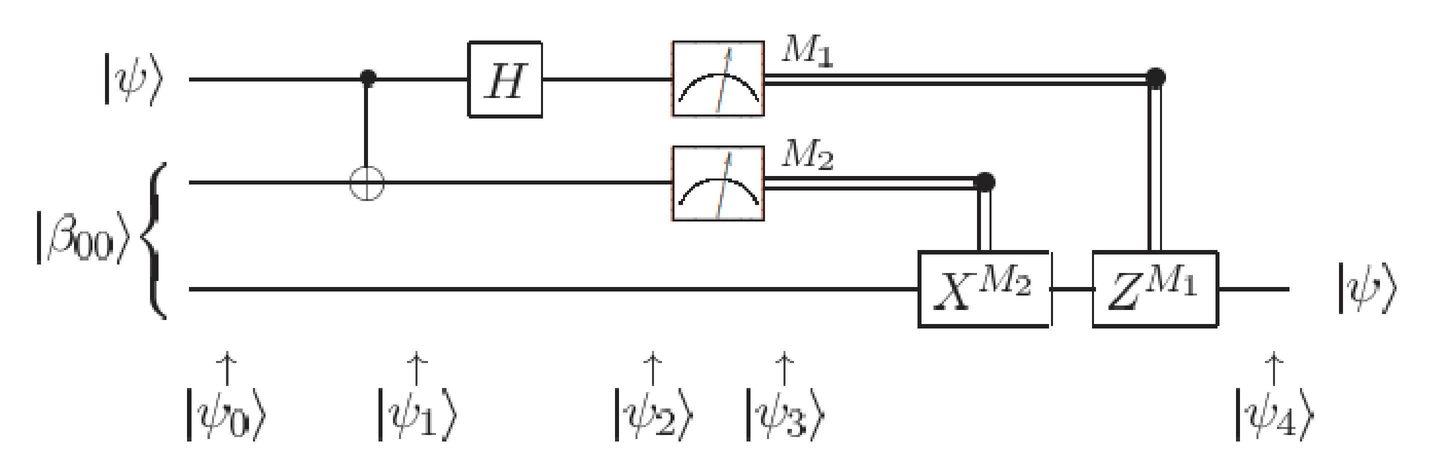
$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$\implies |\beta_{xy}\rangle = \frac{|0, y\rangle + (-1^{x})\,|1, \overline{y}\rangle}{\sqrt{2}}$$

量子テレポーテーション



上の2量子ビットをアリスが所有し、下の1量子ビットをボブが所有する。

アリスは2つの量子ビットを測定し、その結果をボブに伝えることにより、ボブに一番上の量子ビットを伝えることができる。

$\longrightarrow$ EPRペアをシェアして、2つの古典ビットを伝えることで量子ビットを伝えることができる

$\longrightarrow$ 異なる量子系のリソースの可換性を示す。

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

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

$$|\psi_0\rangle$$

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

$$= \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|00\rangle + |11\rangle\right)\right]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|10\rangle + |01\rangle\right)]$$

$$\because CNOT : |00\rangle \longrightarrow |00\rangle, |01\rangle \longrightarrow |01\rangle, |10\rangle \longrightarrow |11\rangle, |11\rangle \longrightarrow |10\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[\alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}\left(|10\rangle + |01\rangle\right)\right]$$

$$\because H : \alpha'|0\rangle + \beta'|1\rangle \longrightarrow \alpha'\,\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta'\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= \frac{1}{2}[\alpha\left(|0\rangle + |1\rangle\right)\left(|00\rangle + |11\rangle\right) + \beta\left(|0\rangle - |1\rangle\right)\left(|10\rangle + |01\rangle\right)]$$

$$= \frac{1}{2}[|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) + |10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)]$$

前方2量子ビット観測

$$|\psi_3\left(00\right)\rangle \equiv \left[\alpha|0\rangle + \beta|1\rangle\right]$$

$$|\psi_3\left(01\right)\rangle \equiv \left[\alpha|1\rangle + \beta|0\rangle\right]$$

$$|\psi_3\left(10\right)\rangle \equiv \left[\alpha|0\rangle - \beta|1\rangle\right]$$

$$|\psi_3\left(11\right)\rangle \equiv \left[\alpha|1\rangle - \beta|0\rangle\right]$$

古典ビット伝達

$$|\psi_4(00)\rangle$$

$$= Z^0 X^0 |\psi_3(00)\rangle = [\alpha|0\rangle + \beta|1\rangle] = |\psi\rangle$$

$$|\psi_4(01)\rangle$$

$$= Z^0 X^1 |\psi_3(01)\rangle = X[\alpha|1\rangle + \beta|0\rangle] = [\alpha|0\rangle + \beta|1\rangle] = |\psi\rangle$$

$$|\psi_4(10)\rangle$$

$$= Z^1 X^0 |\psi_3(10)\rangle = Z[\alpha|0\rangle - \beta|1\rangle] = [\alpha|0\rangle + \beta|1\rangle] = |\psi\rangle$$

$$|\psi_4(11)\rangle$$

$$= Z^1 X^1 |\psi_3(11)\rangle = ZX[\alpha|1\rangle - \beta|0\rangle] = [\alpha|0\rangle + \beta|1\rangle] = |\psi\rangle$$

- 光より早く情報は伝えられない
  - 古典的コミュニケーションで古典ビットを伝える必要があるため
- 量子ビットのコピーは作れない
  - アリスの$|\psi\rangle$は失われてしまう