# 量子信息与量子密码

*Quantum Information & Quantum Cryptology*

# [第5次课] 量子逻辑线路模型

授课教师：杨理

授课时间：2022年4月2日

# 内容概要

一、Deutsch定理

二、单量子比特酉变换

三、受控运算

四、量子线路的测量问题

五、通用运算的有效离散集合

六、两极酉门

# 一、Deutsch定理

Deutsch定理（ 量子网络的可分解定理）

任意 $d$ 维酉变换总可以被分解为 $2d^2-d$ 个二维酉变换的乘积，并且任何作用在一组量子位上的酉变换均可以用一系列单量子位门（ $U(\alpha,\phi)$ 门）和双量子位门（ CNOT 门）依次作用来实现。

证明：可证用 $d-1$ 个酉变换可实现 $\begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

# Deutsch定理（2）

为此，取 $A_2 = \dfrac{1}{\sqrt{|a_1|^2 + |a_2|^2}} \begin{bmatrix} a_1^* & a_2^* \\ a_2 & -a_1 \end{bmatrix}$，

有 $A_2 \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} \sqrt{|a_1|^2 + |a_2|^2} \\ 0 \end{bmatrix}$。

# Deutsch定理（3）

再取：

$$A_3 = \frac{1}{\sqrt{|a_1|^2 + |a_2|^2 + |a_3|^2}} \begin{bmatrix} \sqrt{|a_1|^2 + |a_2|^2} & a_3^* \\ a_3 & -\sqrt{|a_1|^2 + |a_2|^2} \end{bmatrix}$$

$$A_3 \begin{bmatrix} \sqrt{|a_1|^2 + |a_2|^2} \\ a_3 \end{bmatrix} = \begin{bmatrix} \sqrt{|a_1|^2 + |a_2|^2 + |a_3|^2} \\ 0 \end{bmatrix}$$

# Deutsch定理（4）

如此继续下去，可得

$$\tilde{A}_d \cdots \tilde{A}_3 \tilde{A}_2 \begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix} = \sqrt{|a_1|^2 + \cdots + |a_d|^2} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$A$ 是酉阵，必有 $\sqrt{|a_1|^2 + \cdots + |a_d|^2}$

这里 $\tilde{A}_i$ 是 $2 \times 2$ 矩阵 $A_i$ 所对应的 $d \times d$ 矩阵。

# Deutsch定理（5）

①证明任意酉变换 $U$ 可表为 $d(2d-1)$ 个二级酉变换的乘积。

②任何二级酉变换均可用 $U(\alpha,\phi)$ 和量子 CNOT 门来实现。

# 关于①和②的证明

①的原始证明：直接构造方法。

①的改进证明（教材）：降低了复杂度。

②的证明（教材4.5.2）：单量子位门和受控非门构成通用门组

# 二、单量子比特酉变换

1、Pauli矩阵：在以 $\sigma_z$ 的本征态为基的表示中，

$$X \equiv \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y \equiv \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z \equiv \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$X, Y, Z$ : 量子信息中常用的记号.

注意：$\vec{\sigma}$是以矩阵为分量的三维向量.

# 单量子比特酉变换（2）

2、定义：$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}, T=\begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{bmatrix},$

相位门　　　$\frac{\pi}{8}$门

易见：$T^2=S, S^2=Z, Z^2=Y^2=X^2=1.$

# 单量子比特变换（3）

## 3、Bloch球面：

$\alpha|0\rangle+\beta|1\rangle \leftrightarrow$ 单位球面上的点$(\theta,\ \varphi)$，

$\alpha=\cos\frac{\theta}{2}, \beta=e^{i\varphi}\sin\frac{\theta}{2},$

$\frac{\theta}{2}$的取法是使$\theta$对应于自旋在三维空间中的取向.

## Bloch矢量：

$\vec{\lambda}=(\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta),$

与Poincare球(面)的区别：Poincare球(面)针对经典光学偏振态，与态向量对应。

Bloch球(面)是关于任意量子二态系统，与密度矩阵对应。

# 单量子比特酉变换（4）

4、旋转算子：

$$R_x(\theta) \equiv e^{-i\theta X/2}, R_y(\theta) \equiv e^{-i\theta Y/2}, R_z(\theta) \equiv e^{-i\theta Z/2},$$

一个有用的公式：

对$\forall A$ 满足$A^2 = I$, 有 $\exp(i\,A\,x) = \cos x\, I + i \sin x\, A$ ,

# 单量子比特酉变换（5）

$$\Rightarrow\begin{cases}R_x(\theta)=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}X=\begin{bmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix},\\ R_y(\theta)=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Y=\begin{bmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix},\\ R_z(\theta)=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Z=\begin{bmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{bmatrix}.\end{cases}$$

(图像：$\vec{\lambda}$ 绕 $x, y, z$ 轴旋转 $\theta$)

# 单量子比特酉变换（6）

易见 $T=R_z\left(\dfrac{\pi}{4}\right)$,

$$R_{\vec{n}}(\theta)\equiv e^{-i\theta\vec{n}\cdot\vec{\sigma}/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}\left(n_xX+n_yY+n_zZ\right),$$

$\left(\vec{\lambda}\text{绕}\vec{n}\text{轴旋转}\,\theta\right)$

因子 $\dfrac{1}{2}$: 旋转 $4\pi$ 才回到原来的值.

原因是 $SU(2)$ 对称性 ,这是 $\dfrac{1}{2}$ 旋量的特点. 旋转 $\theta=2\pi$ , $R_{\vec{n}}(2\pi)=-I$.

# 单量子比特酉变换（7）

在经典力学中，刚体的一般转动可用欧拉角 $(\psi,\theta,\phi)$ 描述：

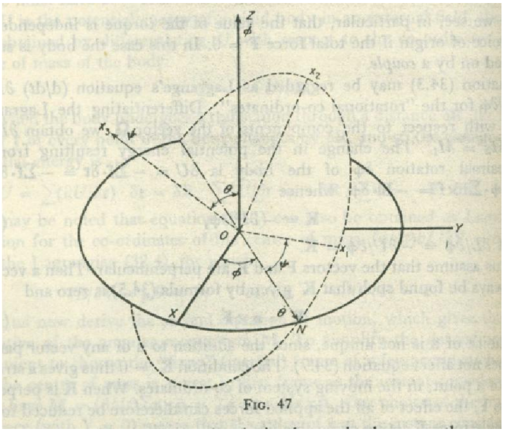


Fig. 47

$\phi$: 进动角（轴转动）

$\psi$: 自转角

$\theta$: 章动角（z轴上下颤动）

欧拉运动学方程：

$$\begin{cases} \omega_x = \dot{\varphi}\sin\theta\sin\psi + \dot{\theta}\cos\psi \\ \omega_y = \dot{\varphi}\sin\theta\cos\psi - \dot{\theta}\sin\psi \\ \omega_z = \dot{\varphi}\cos\theta + \dot{\psi} \end{cases}$$

# 单量子比特酉变换（8）

在量子力学中，球坐标下有（ $\vec{J}$ 为角动量算符）

$$e^{-iJ_y\theta}\hat{J}_z e^{iJ_y\theta} = J_z\cos\theta + J_x\sin\theta,$$

$$e^{-iJ_z\varphi}J_x e^{iJ_z\varphi} = \hat{J}_x\cos\varphi + J_y\sin\varphi.$$

若 $\Psi_m^{(0)}$ 是 $J_z$ 的本征函数，即$J_z\Psi_m^{(0)} = m\Psi_m^{(0)}$，

则 $\Psi_m = e^{-iJ_z\varphi}e^{-iJ_y\theta}\Psi_m^{(0)}$ 是算符

$$J_\xi = J_x\sin\theta\cos\varphi + J_y\sin\theta\sin\varphi + J_z\cos\theta$$

的本征函数，即：

$$\hat{J}_\xi\Psi_m = m\Psi_m.$$

# 单量子比特酉变换（9）

考虑欧拉角描述。当转动欧拉角$(\theta,\psi,\varphi)$时，自旋函数分量的变换矩阵为：

$$\begin{pmatrix} e^{\frac{i}{2}(\varphi+\psi)}\cos\frac{\theta}{2} & ie^{\frac{i}{2}(\varphi-\psi)}\sin\frac{\theta}{2} \\ ie^{-\frac{i}{2}(\varphi-\psi)}\sin\frac{\theta}{2} & e^{-\frac{i}{2}(\varphi+\psi)}\cos\frac{\theta}{2} \end{pmatrix}\left(=R_z\left(-2\varphi\right)R_x\left(-2\theta\right)R_z\left(-2\psi\right)\right).$$

故有自旋函数分量的变换算符为：

$$\hat{T}\left(\psi,\theta,\varphi\right)=e^{i\varphi s_z}e^{i\theta s_x}e^{i\psi \hat{s}_z},$$

# 单量子比特酉变换（10）

对于绕 $\vec{n}$ 轴转 $\phi$ 角，转动算符为

$$\hat{R}(\vec{n},\theta)=e^{i\phi\vec{n}\cdot\vec{s}}=e^{i\phi\vec{n}\cdot\left(\frac{1}{2}\vec{\sigma}\right)}$$

$$=\cos\frac{\phi}{2}+i\vec{n}\cdot\vec{\sigma}\sin\frac{\phi}{2}.$$

# 单量子比特酉变换（11）

欧拉角 $(\theta,\psi,\varphi)$ 与 $(\bar{n},\phi)$ 的关系：

$$\cos\frac{\phi}{2}=\cos\frac{\theta}{2}\cos\frac{1}{2}(\varphi+\psi),$$

$$n_x\sin\frac{\phi}{2}=\sin\frac{\theta}{2}\cos\frac{1}{2}(\varphi-\psi),$$

$$n_y\sin\frac{\phi}{2}=\sin\frac{\theta}{2}\sin\frac{1}{2}(\varphi-\psi),$$

$$n_z\sin\frac{\phi}{2}=\cos\frac{\theta}{2}\sin\frac{1}{2}(\varphi+\psi).$$

注意： $e^{i\phi\bar{n}\cdot\bar{s}}\neq e^{i\phi n_x\cdot s_x}e^{i\phi n_y\cdot s_y}e^{i\phi n_z\cdot s_z}$.

# 单量子比特酉变换（12）

5、单量子比特的y-z和x-z分解：

（1）任一单量子比特酉算子可以写成 $U = \exp(i\alpha) R_{\vec{n}}(\theta)$ 形式。

（2）定理：对任意单量子比特的 $U$ 变换，存在实参数 $\alpha, \beta, \gamma, \delta$，使得 $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$,

# 单量子比特酉变换（13）

可以从酉矩阵的定义出发，得到

$$U=\begin{bmatrix} e^{i\left(\alpha-\frac{\beta}{2}-\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} & -e^{i\left(\alpha-\frac{\beta}{2}+\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} \\ e^{i\left(\alpha+\frac{\beta}{2}-\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} & e^{i\left(\alpha+\frac{\beta}{2}+\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} \end{bmatrix},$$

从而证实定理所述分解的存在。

但分解定理的来源是 $\hat{T}$ 的欧拉角表示。

# 单量子比特酉变换（14）

（3）推论：存在酉算子 $A, B, C$,满足$ABC = I$,

使：$U = e^{i\alpha} AXBXC.$

证明：取

$$A = R_z(\beta) R_y\left(\frac{\gamma}{2}\right),$$

$$B = R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right),$$

$$C = R_z\left(\frac{\delta-\beta}{2}\right),$$

则：

$$ABC = R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right) R_z\left(\frac{\delta-\beta}{2}\right)$$

$$= R_z(\beta) R_z(-\beta) = I\ .$$

# 单量子比特酉变换（15）

$$XYX=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&-i\\i&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&i\\-i&0\end{pmatrix}=-Y,$$

$$\begin{aligned}XR_y(\theta)X&=X\left(\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Y\right)X=\cos\frac{\theta}{2}I+i\sin\frac{\theta}{2}Y\\&=\cos\left(-\frac{\theta}{2}\right)I-i\sin\left(-\frac{\theta}{2}\right)Y=R_y(-\theta),\end{aligned}$$

$$XBX=XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)X=R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right),$$

# 单量子比特酉变换（16）

$$\Rightarrow AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right)$$

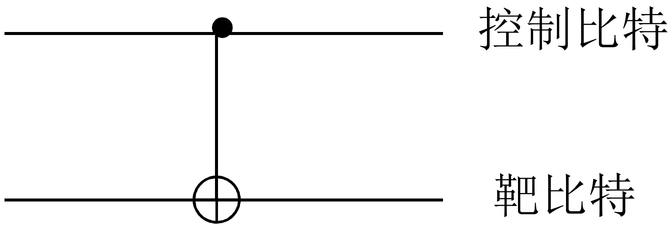
$$= R_z(\beta)R_y(\gamma)R_z(\delta),$$

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

练习：$z-x$ 分解.

# 三、受控运算

（1）CNOT门

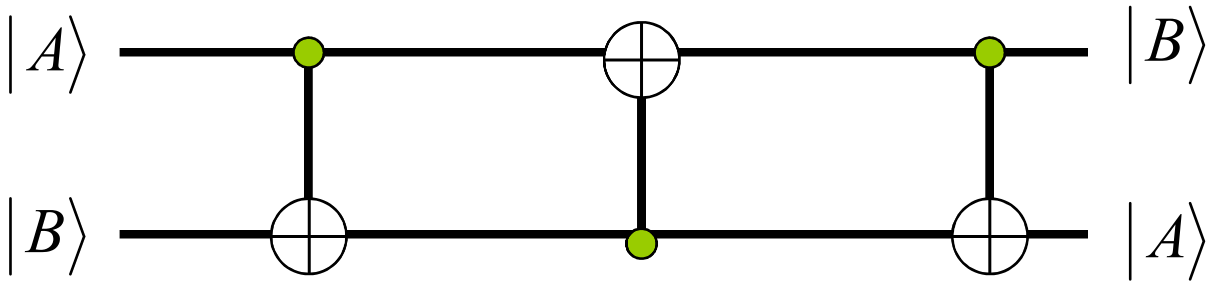



$$|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle.$$

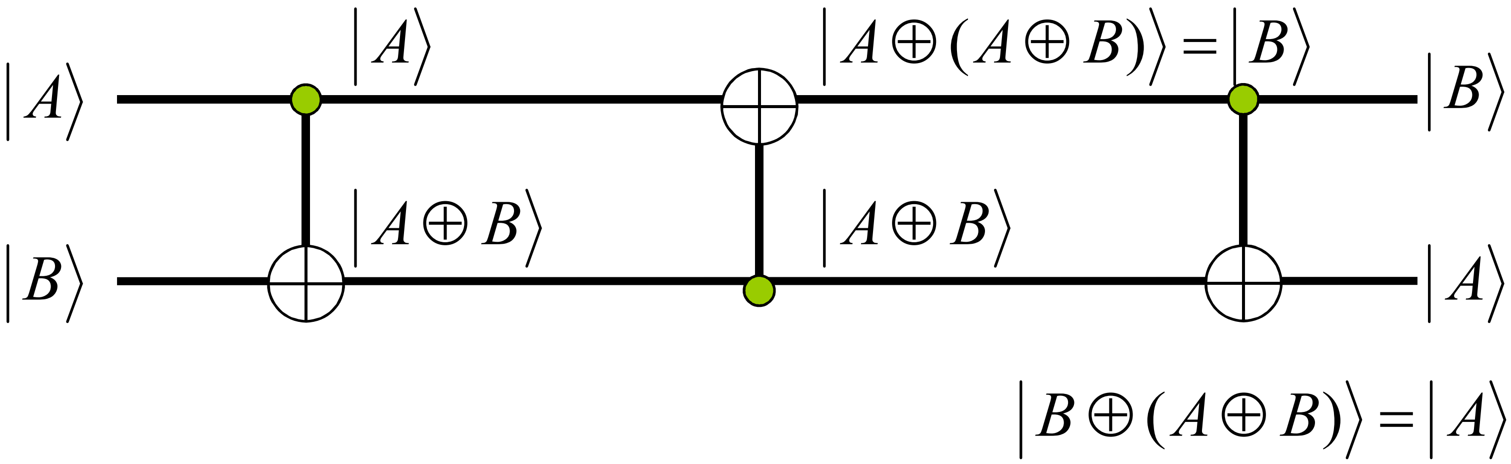
矩阵表示：
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

# Qubit Swap Circuit

- Using the conventions for control and target qubits, we can build interesting circuits
- Example: **A Qubit Swap Circuit**



# Qubit Swap Circuit

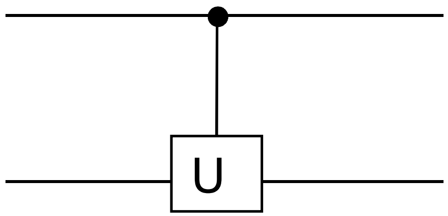



**思考题：**基于此给出Toffoli门到Fridkin门的构造。

# 受控U变换

（2）一般的受控变换：

$C(U)$ 门：



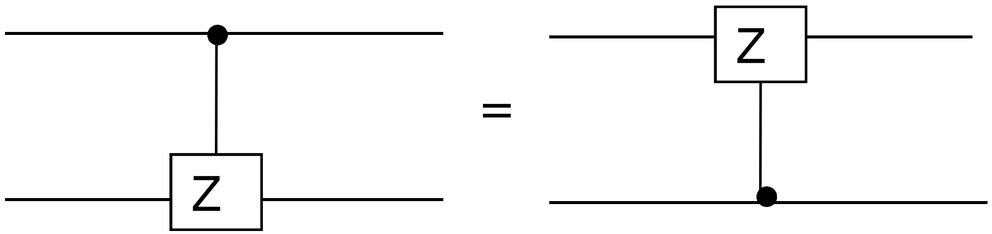

$$|c\rangle|t\rangle \to |c\rangle U^{c}|t\rangle.$$

如：$\frac{1}{\sqrt{2}}\left(|0\rangle|t_0\rangle+|1\rangle|t_1\rangle \to \frac{1}{\sqrt{2}}|0\rangle|t_0\rangle+|1\rangle U|t_1\rangle\right).$

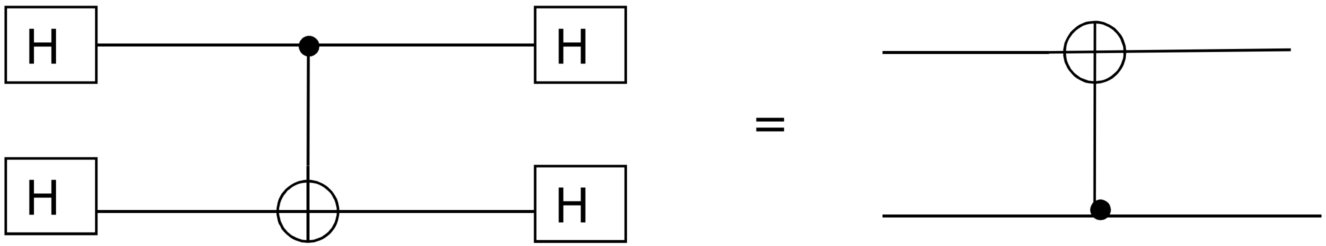
# 两个练习

证明:

①



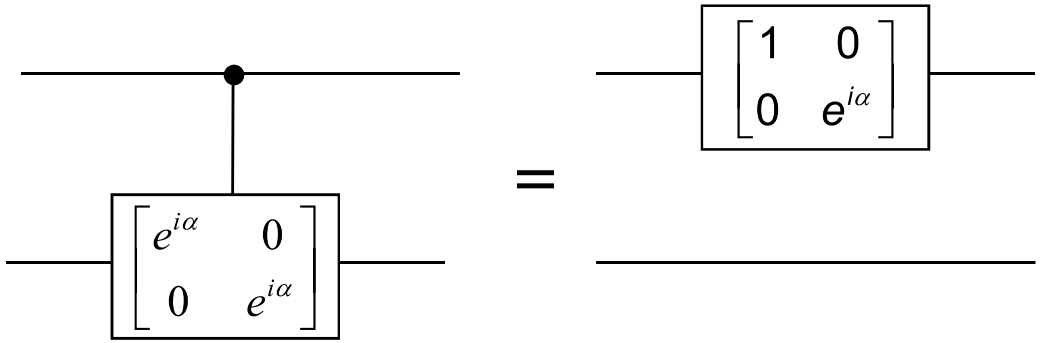

②



# 如何实现 $C(U)$运算？

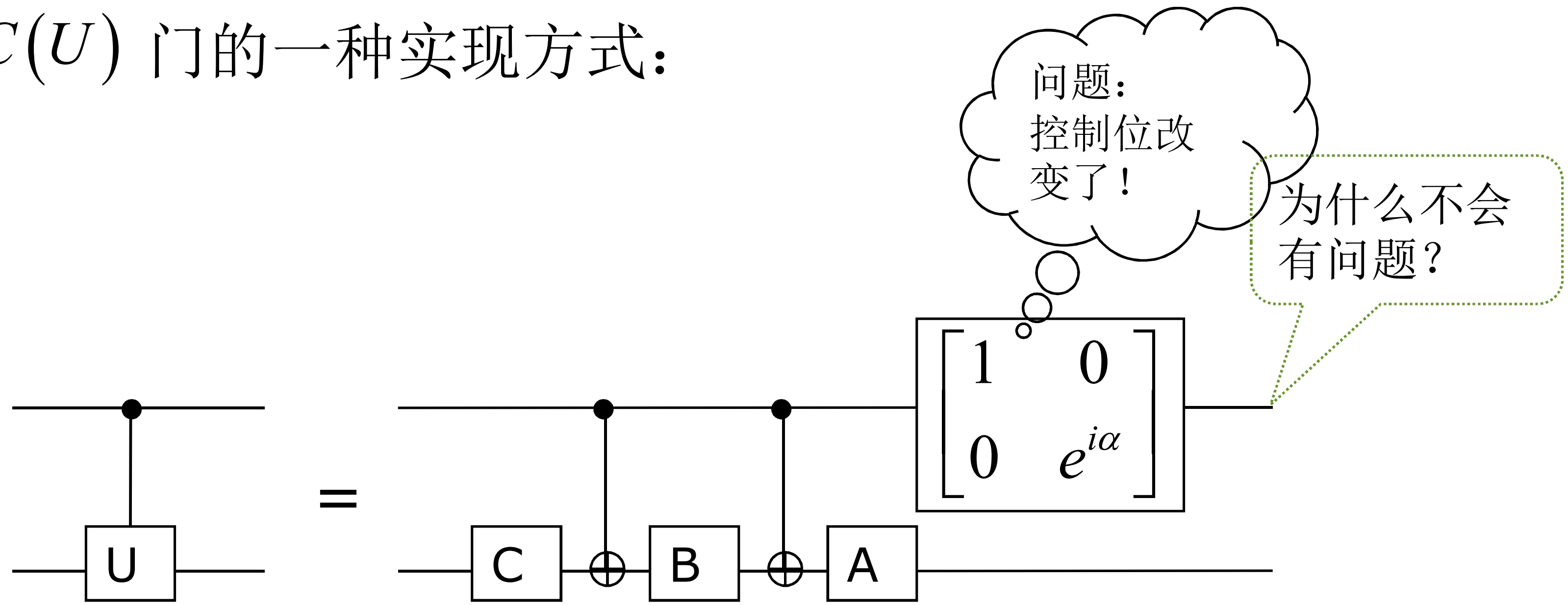
① 受控相移 $\left(e^{i\alpha}\right)$:
$$\begin{cases} |00\rangle \to |00\rangle, \\ |01\rangle \to |01\rangle, \\ |10\rangle \to e^{i\alpha}|10\rangle, \\ |11\rangle \to e^{i\alpha}|11\rangle. \end{cases}$$

$\Rightarrow$



# 如何实现 $C(U)$运算？

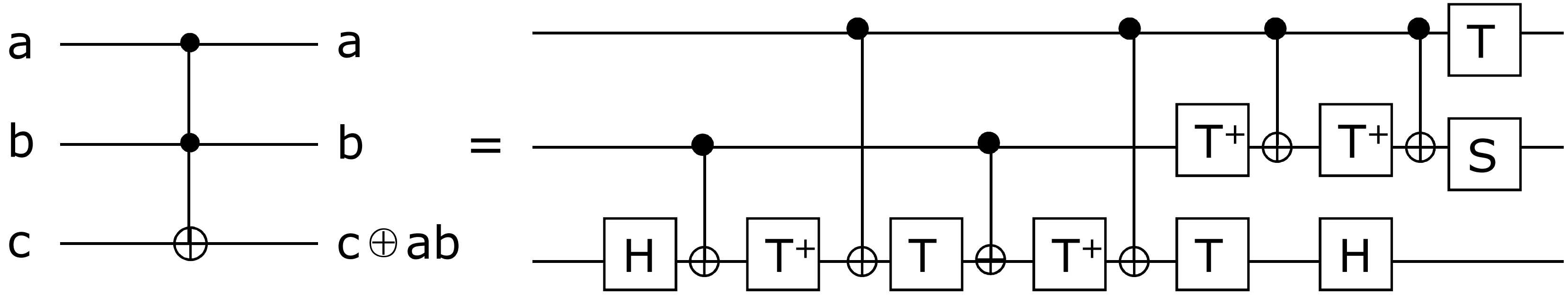
② $C(U)$ 门的一种实现方式：



# 受控运算（5）

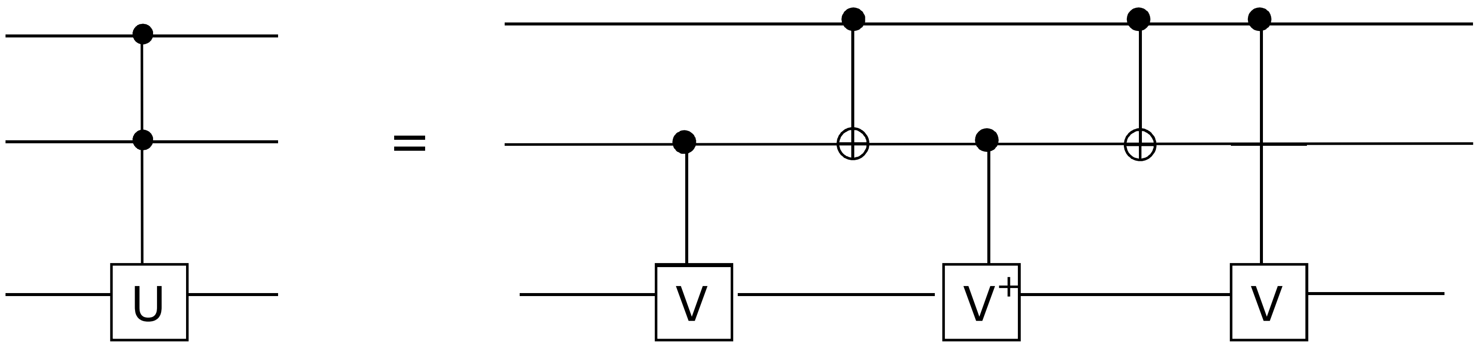
（3）Toffoli门：可逆计算的通用门

（经典计算时，CNOT+单比特门不是通用门）



# 受控运算（6）

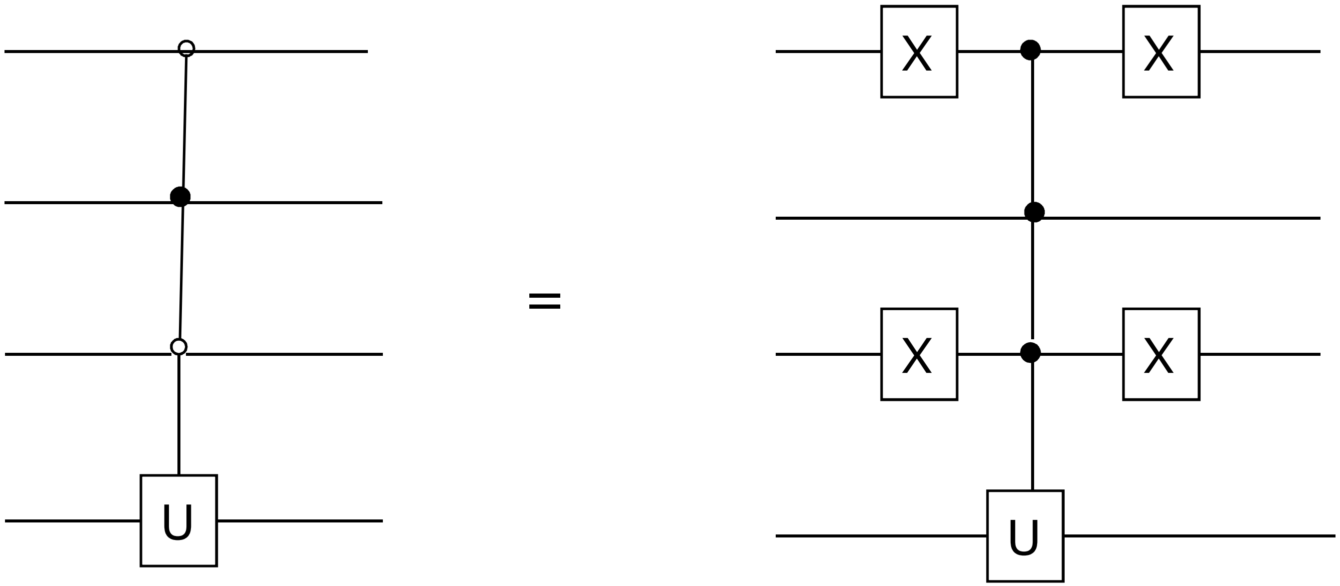
（4）$C^2(U)$ 门：设 $V^2=U$ 则有：




思考题：取U=X，利用受控U变换的ABC分解，得到Toffoli门到CNOT门+单量子位门的分解。

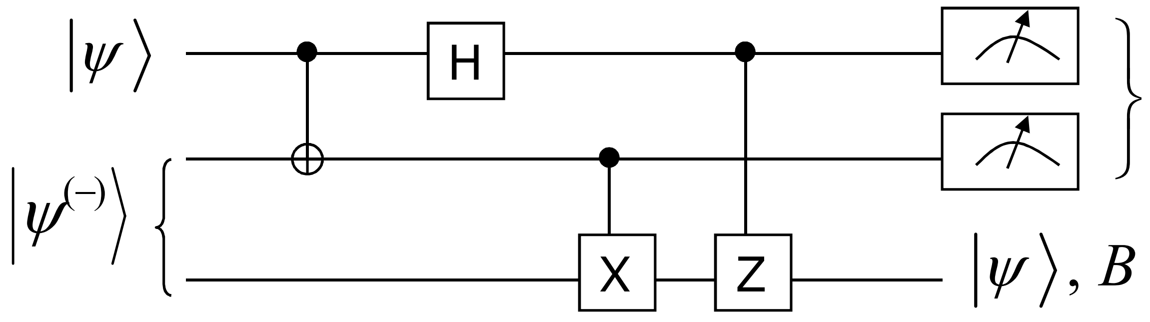
# 受控运算（7）

（5）




作业：练习4.31

# 四、量子线路的测量问题




（教材图4.15）

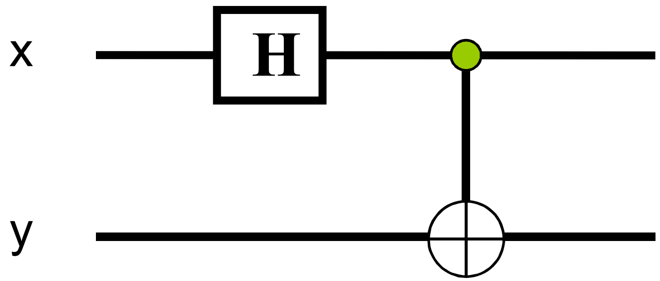
（1）“deferred measurement”，纠缠态问题

（2）“implicit measurement”，超光速信号传递问题

（可将纠缠输出的线路分送远离的A和B）

作业：练习4.35

# The Bell State Circuit




| x | y | Output |
|---|---|---|
| $\|0\rangle$ | $\|0\rangle$ | $\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$ |
| $\|0\rangle$ | $\|1\rangle$ | $\frac{1}{\sqrt{2}}(\|01\rangle+\|10\rangle)$ |
| $\|1\rangle$ | $\|0\rangle$ | $\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)$ |
| $\|1\rangle$ | $\|1\rangle$ | $\frac{1}{\sqrt{2}}(\|01\rangle-\|10\rangle)$ |

# 量子Teleportation

- If Alice and Bob each have a single particle from an entangled pair, then:
  - **It is possible for Alice to teleport a qubit to Bob, using only a classical channel**
  - The state of the original qubit will be destroyed
- How?
  - Using the properties of entangled particles

# 量子Teleportation（2）

- Alice wants to teleport particle 1 to Bob

$$\left|\psi\right\rangle_1 = \alpha\left|0\right\rangle_1 + \beta\left|1\right\rangle_1$$

- Two particles, 2 and 3, are prepared in an entangled state

$$\left|\Phi^+\right\rangle_{23} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2\left|0\right\rangle_3 + \left|1\right\rangle_2\left|1\right\rangle_3\right)$$

- Particle 2 is given to Alice, particle 3 is given to Bob

# 量子Teleportation（3）

- In order to teleport particle 1, **Alice** now entangles it with her particle using the CNot and Hadamard gates:

$$\mathrm{CNOT}\left(\left|\psi\right\rangle_1, \left|\psi\right\rangle_2\right); \quad \mathrm{H}\left(\left|\psi\right\rangle_1\right)$$

- Thus, particle 1 is “disassembled” and combined with the entangled pair
- **Alice** measures particles 1 and 2, producing a classical outcome: **00, 01, 10 or 11**.

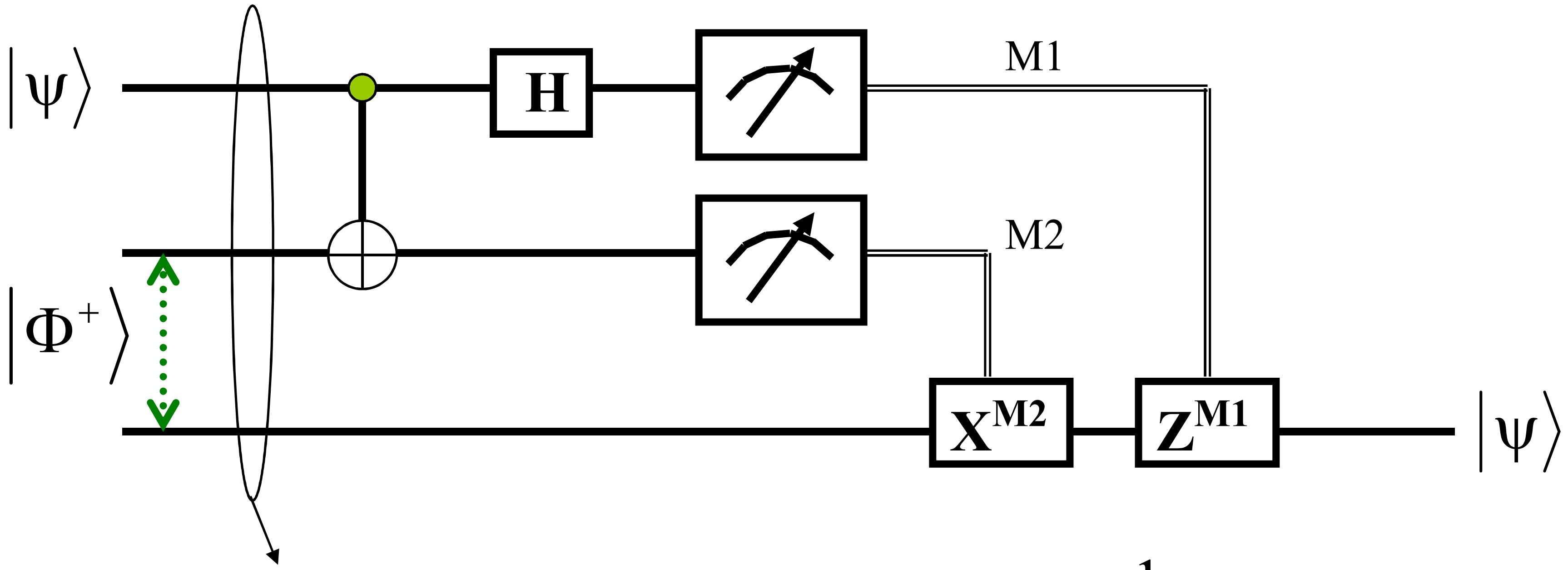
# 量子Teleportation（4）

- Depending on the outcome of **Alice's** measurement, **Bob** applies a Pauli operator to particle 3, "reincarnating" the original qubit
- If outcome=**00**, Bob uses operator **I**
- If outcome=**01**, Bob uses operator $\boldsymbol{\sigma_x}$ (=X)
- If outcome=**11**, Bob uses operator $\boldsymbol{\sigma_y}$ (=Y)
- If outcome=**10**, Bob uses operator $\boldsymbol{\sigma_z}$ (=Z)
- **Bob's** measurement produces the original state of particle 1.

# Summary of Teleportation

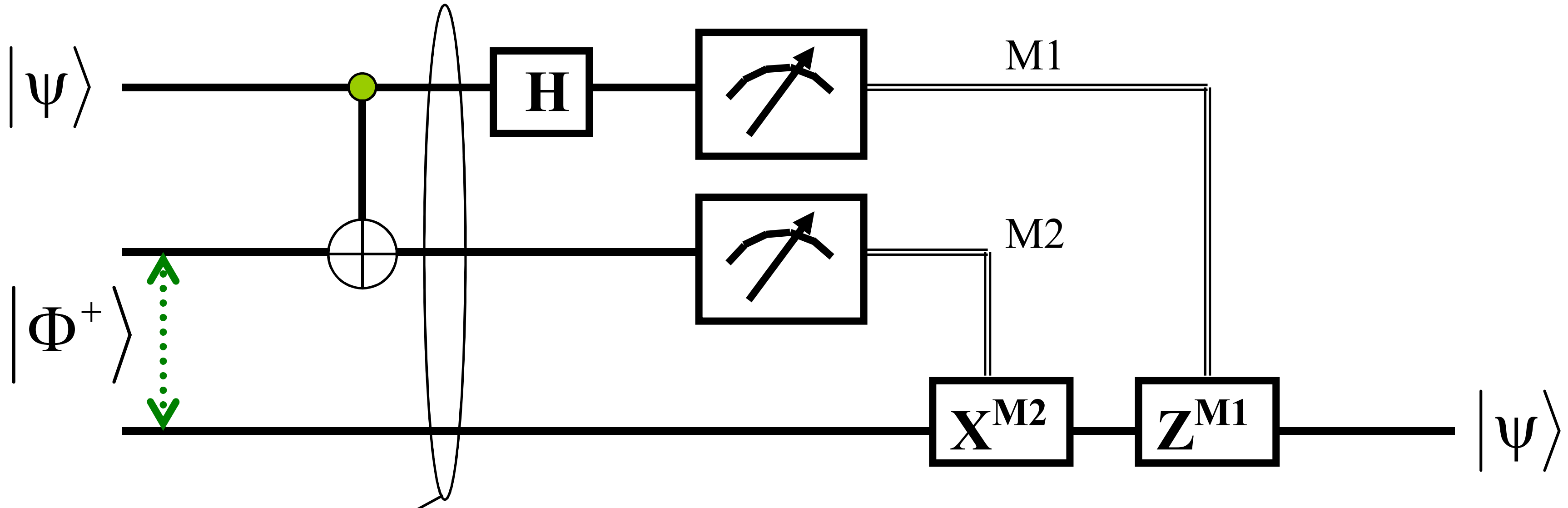
- The basic idea is that Alice and Bob can perform a sequence of operations on their qubits to "move" the quantum state of a particle from one location to another
- The actual operations are more involved than we have presented here; see the standard texts on quantum computing for details

# 量子Teleportation线路



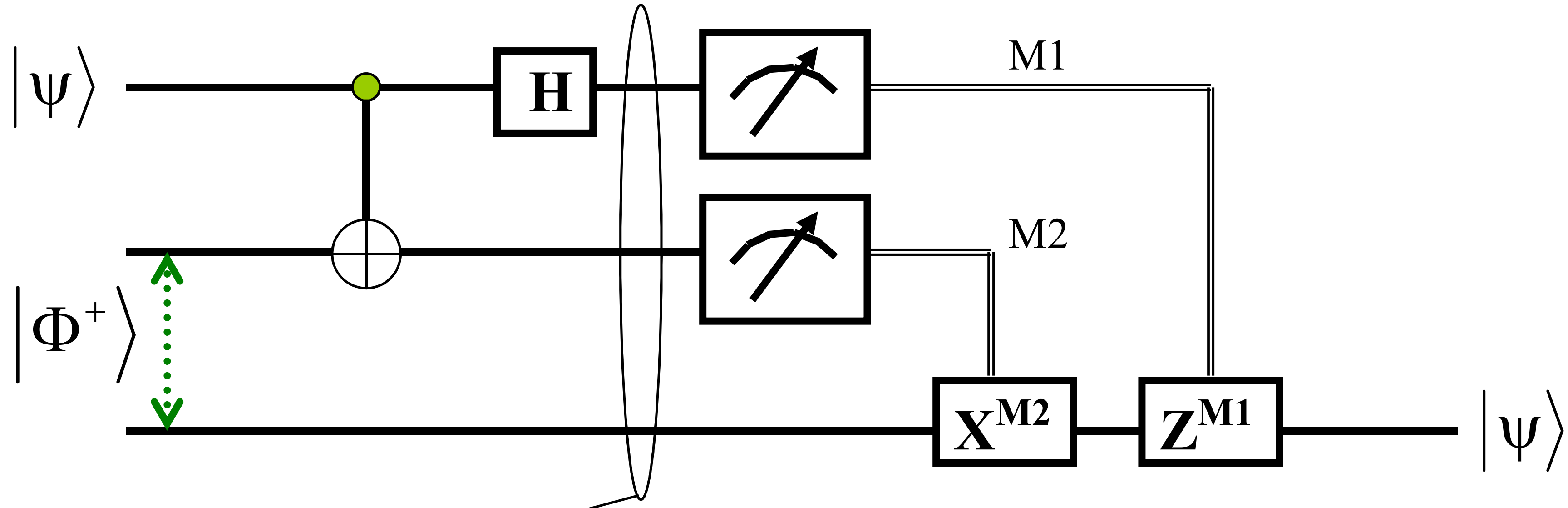

$$|\psi_0\rangle = |\psi\rangle \cdot |\Phi^+\rangle = \left(\alpha|0\rangle + \beta|1\rangle\right) \cdot \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

# 量子Teleportation线路（2）



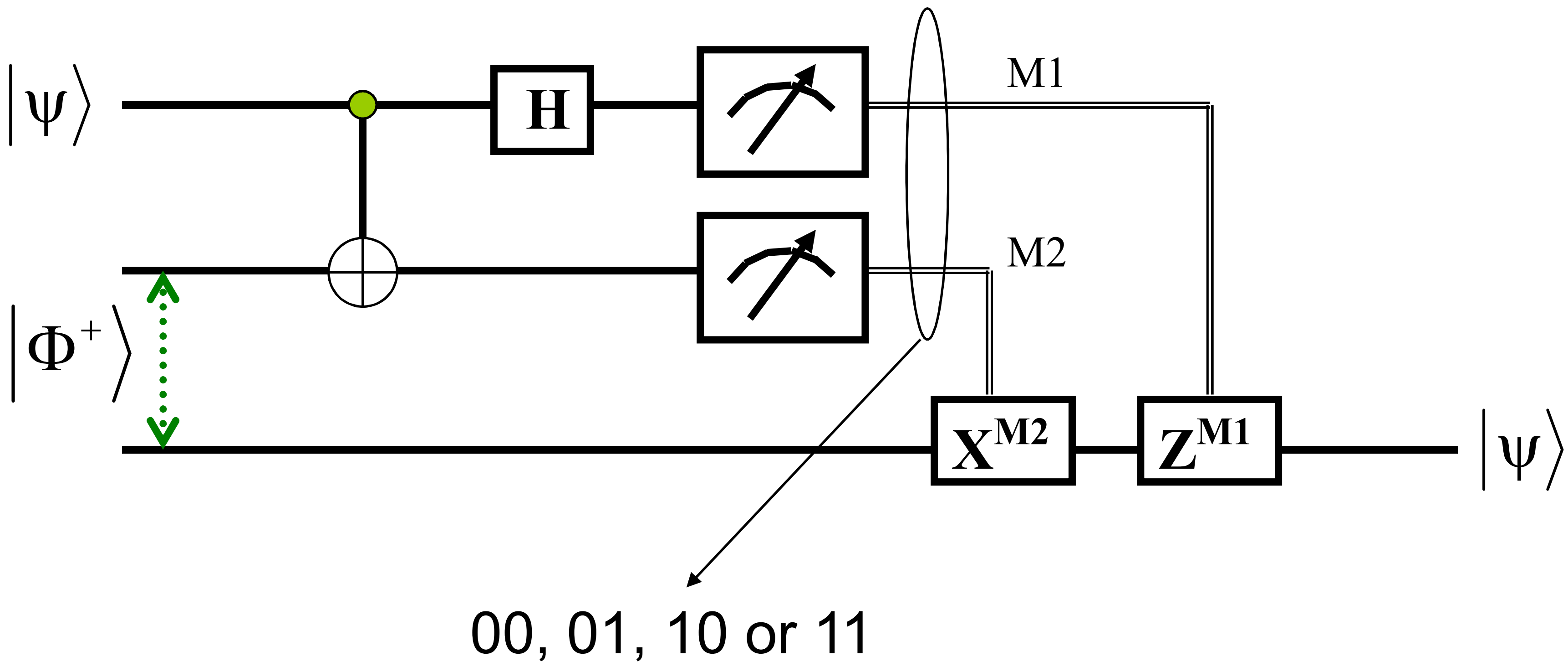

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(\alpha|0\rangle\cdot\big(|00\rangle+|11\rangle\big)+\beta|1\rangle\cdot\big(|01\rangle+|10\rangle\big)\Big)$$

# 量子Teleportation线路（3）




$$|\psi_2\rangle = \frac{1}{2}\begin{bmatrix} |00\rangle\cdot(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\cdot(\alpha|1\rangle+\beta|0\rangle)+ \\ |10\rangle\cdot(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\cdot(\alpha|1\rangle-\beta|0\rangle) \end{bmatrix}$$

# 量子Teleportation线路（4）



# 量子Teleportation的四种情形

| If Alice obtains | Then Bob's qubit is in state | So Bob applies gate | obtaining |
|---|---|---|---|
| **00** | $\alpha\|0\rangle+\beta\|1\rangle$ | **I** | $\alpha\|0\rangle+\beta\|1\rangle$ |
| **01** | $\alpha\|1\rangle+\beta\|0\rangle$ | **X** | |
| **10** | $\alpha\|0\rangle-\beta\|1\rangle$ | **Z** | |
| **11** | $\alpha\|1\rangle-\beta\|0\rangle$ | **ZX** | |

# 五、通用运算的有效离散集合

通用运算的一个有效离散集合：

POVM： 半正定算符取值测度。

$M$ : 任意 POVM 元，$U, V$ 任意两酉演化，定义：

$$E(U,V) \equiv \max_{|\psi\rangle} \left\| (U - V)|\psi\rangle \right\|,$$

对于初态 $|\psi\rangle$，定义

$$P_U \equiv \langle\psi|U^{+}MU|\psi\rangle \quad \text{和} \quad P_V \equiv \langle\psi|V^{+}MV|\psi\rangle,$$

则可证：$|P_U - P_V| \le 2E(U,V).$

# 通用运算的有效离散集合（2）

对应于量子计算中的门运算，用 $V_1,\cdots,V_m$ 来近似 $U_1,\cdots,U_m$，

可证：$E\left(U_m U_{m-1}\cdots U_1, V_m V_{m-1}\cdots V_1\right)\le\sum_{j=1}^{m}E\left(U_j,V_j\right).$

有效离散集合的选取：

$\left\{\overline{H},\overline{P},\overline{CNOT},\overline{Toff}\right\}$， 或 $\left\{\overline{H},\overline{P},\overline{CNOT},\overline{T}\right\}$

其中 $T$ 为 $\frac{\pi}{8}$ 门：$T=\begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{bmatrix}$， $\begin{cases}T^2=P=\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\\ \overline{T}^2=\overline{P}\end{cases}$

# 通用运算的有效离散集合（3）

教材上证明：$H$ 加 $T$ 可以以任意精度近似单量子比特酉运算。（$T$ 和 $HTH$ 可有效逼近任意单比特酉门）

中译本一个打字错误：转动轴的方向应为

$$\vec{n}=\left(n_x,n_y,n_z\right)=\frac{\sin\frac{\pi}{8}}{\sin\frac{\theta}{2}}\left(\cos\frac{\pi}{8},\sin\frac{\pi}{8},\cos\frac{\pi}{8}\right).$$

# 通用运算的有效离散集合（4）

① 近似效率：以 $\varepsilon$ 精度近似包含 $m$ 个 CNOT 门和单比特门的线路，需 $O\left(m\log^c\left(m/\varepsilon\right)\right)$ 个门。

② 近似一般酉门是困难的：

存在 $n$ 量子比特的一组状态，需要 $\Omega\left(2^n\log\left(\frac{1}{\varepsilon}\right)\Big/\log n\right)$ 次运算近似到距离 $\varepsilon$ 以内。

——除去不重要的因子，$2^n$ 是运算次数的下界。

# 关于教材的更正和解释

$$\left(ZX=\sigma_z\sigma_x=i\sigma_y=iY\right)$$

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

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

$$R_z(\theta)\equiv e^{-i\frac{\theta}{2}Z}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Z\,,$$

$$R_{\vec{n}}(\theta)\equiv e^{-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}\left(n_xX+n_yY+n_zZ\right),$$

(绕 $\vec{n}$ 旋转$\theta$)

(因子$\frac{1}{2}$：旋转$4\pi$为恒等算子）

# 关于教材的更正和解释（2）

$$T \equiv \exp\left(-i\frac{\pi}{8}Z\right), \quad HTH \equiv \exp\left(-i\frac{\pi}{8}X\right)$$

故有：

$$T \cdot HTH = \left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right]$$

$$= \cos^2\frac{\pi}{8}I - i\left[\sin\frac{\pi}{8}\cos\frac{\pi}{8}Z + \sin\frac{\pi}{8}\cos\frac{\pi}{8}X\right] - \sin^2\frac{\pi}{8}ZX$$

$$= \cos^2\frac{\pi}{8}I - i\left[\sin\frac{\pi}{8}\cos\frac{\pi}{8}X + \sin^2\frac{\pi}{8}Y + \sin\frac{\pi}{8}\cos\frac{\pi}{8}Z\right]$$

# 关于教材的更正和解释（3）

$$\Rightarrow \begin{cases} \cos\dfrac{\theta}{2} = \cos^2\dfrac{\pi}{8} & (1) \\ n_x \sin\dfrac{\theta}{2} = \sin\dfrac{\pi}{8}\cos\dfrac{\pi}{8} & (2) \\ n_y \sin\dfrac{\theta}{2} = \sin^2\dfrac{\pi}{8} & (3) \\ n_z \sin\dfrac{\theta}{2} = \sin\dfrac{\pi}{8}\cos\dfrac{\pi}{8} & (4) \end{cases}$$

从 $(2),(3),(4)$ 可直接得到

$$\vec{n} = \left(n_x, n_y, n_z\right) = \frac{\sin\dfrac{\pi}{8}}{\sin\dfrac{\theta}{2}}\left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right).$$

# 六、两级酉门

两级酉门：改变两个叠加分量上的几率幅的酉门。

两级（two-level)酉门是通用的。

两级酉阵：有效作用于两个分量上的酉矩阵，仍然是 $2^n$ 阶酉阵。

以 $d=3$ 为例，$U=\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$

如果能找到两级酉阵 $U_1, U_2, U_3$ 使 $U_3U_2U_1U=I$ ，

则有 $U=U_1^{+}U_2^{+}U_3^{+}$

# 两级酉门（2）

其中：$U_1^+, U_2^+, U_3^+$ 也是两级酉阵，则知 $U$ 可分解三个两级酉矩阵之积。

具体变换：记 $r_{ab}=\sqrt{|a|^2+|b|^2}$ , $r_{ac}=\sqrt{|a'|^2+|c'|^2}$

$$U_1=\begin{bmatrix} \frac{a^*}{r_{ab}} & \frac{b^*}{r_{ab}} & 0 \\ \frac{b}{r_{ab}} & \frac{-a}{r_{ab}} & 0 \\ 0 & 0 & 1 \end{bmatrix}, U=\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$$

# 两级酉门（3）

即：$U_1 = \begin{bmatrix} V_{2\times2} & 0 \\ 0 & 1 \end{bmatrix}$， $V_{2\times2}$ 是酉阵，由：

$$\begin{bmatrix} \frac{a^*}{r_{ab}} & \frac{b^*}{r_{ab}} & 0 \\ \frac{b}{r_{ab}} & \frac{-a}{r_{ab}} & 0 \\ 0 & 0 & 1 \end{bmatrix}^+ = \begin{bmatrix} \frac{a}{r_{ab}} & \frac{b^*}{r_{ab}} & 0 \\ \frac{b}{r_{ab}} & -\frac{a^*}{r_{ab}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

# 两级酉门（4）

可得：

$$\begin{bmatrix} \frac{a^*}{r_{ab}} & \frac{b^*}{r_{ab}} & 0 \\ \frac{b}{r_{ab}} & \frac{-a}{r_{ab}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{a}{r_{ab}} & \frac{b^*}{r_{ab}} & 0 \\ \frac{b}{r_{ab}} & -\frac{a^*}{r_{ab}} & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{|a|^2+|b|^2}{\left(\sqrt{|a|^2+|b|^2}\right)^2} & \frac{a^*b^*-b^*a^*}{\left(\sqrt{|a|^2+|b|^2}\right)^2} & 0 \\ \frac{ba-ab}{\left(\sqrt{|a|^2+|b|^2}\right)^2} & \frac{|b|^2+|a|^2}{\left(\sqrt{|a|^2+|b|^2}\right)^2} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

# 两级酉门（5）

$$U_1U=\begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix},\qquad U_2=\begin{bmatrix} \frac{a'^*}{r_{ac}} & 0 & \frac{c'^*}{r_{ac}} \\ 0 & 1 & 0 \\ \frac{c'}{r_{ac}} & 0 & \frac{-a'}{r_{ac}} \end{bmatrix},$$

$$U_2U_1U=\begin{bmatrix} a'' & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}\Rightarrow\begin{cases} |a''|=1, \\ d''=g''=0 \\ \text{(酉阵的行和列向量模为1）} \end{cases}$$

# 两级酉门（6）

即：$U_2U_1U=\begin{bmatrix}1 & 0 & 0\\ 0 & e'' & h''\\ 0 & f'' & j''\end{bmatrix}$， 取 $U_3=\begin{bmatrix}1 & 0 & 0\\ 0 & e''^* & f''^*\\ 0 & h''^* & j''^*\end{bmatrix}\left(=(U_2U_1U)^\dagger\right)$

必有 $U_3U_2U_1U=I.$

即 $U=U_1^+U_2^+U_3^+$ 是 $U$ 的两级酉阵分解。

一般情形：$d$ 维 $H$ 空间上酉变换矩阵的二级酉阵分解可通过类似构造得到。

# 第四章 量子逻辑线路模型

Q&A