量子信息导论
PHYS5251P

中国科学技术大学
物理学院/合肥微尺度物质科学国家研究中心

陈凯

2026.1

联系方式

- 主讲教师1：陈凯，
  E-mail: kaichen@ustc.edu.cn
  Tel. 63607083；Office: 物质B楼1013-1室
  主页: http://staff.ustc.edu.cn/~kaichen

- 主讲教师2：徐飞虎教授 feihuxu@ustc.edu.cn

- 助教　　杨挪亚, nyyang@mail.ustc.edu.cn

参考书目

教材

- Quantum computation and quantum information by M.A. Nielsen and I.L. Chuang, Cambridge University Press, 2010

其他参考书

- 量子信息

马雄峰、张行健、黄溢智，《量子信息简明教程》，清华大学出版社，2023.

- 量子力学

王向斌、沈艺鑫、于云龙、秦季茜、徐海，《量子力学基础教程》，清华大学出版社，2023.

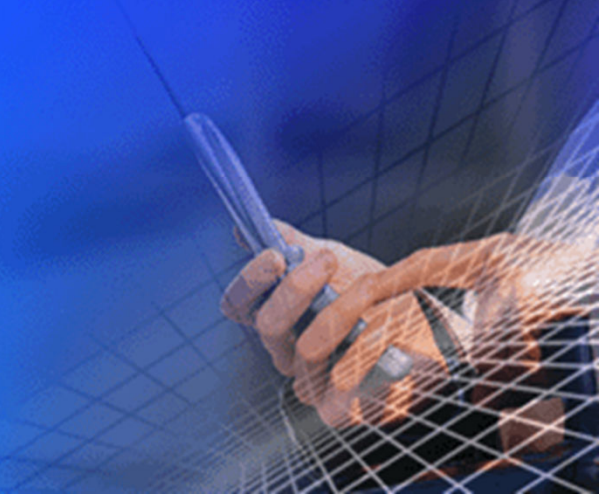
Course Description

This course is open to all graduate students and undergraduates. The final grades are based on:

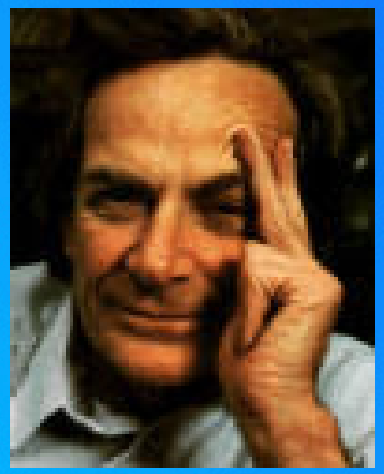
- final exam (60%),
- homework and attendance of the class (20%),
- a report about quantum information (20%, the subject can be arbitrary, which is preferably related to your current research project, recent progress or your own ideas along one specific area on theoretical or experimental quantum information)

量子信息处理

It's a "mystery". THE mystery. We don't understand it, but we can tell you how it works. *(Feynman)*



量子信息发展史



(Richard Feynman)

"There's plenty of room at the bottom"

Quantum Turing machine

(Paul Benioff)

(C. Bennett)

(G. Brassard)

Quantum key distribution BB84

Universal QC

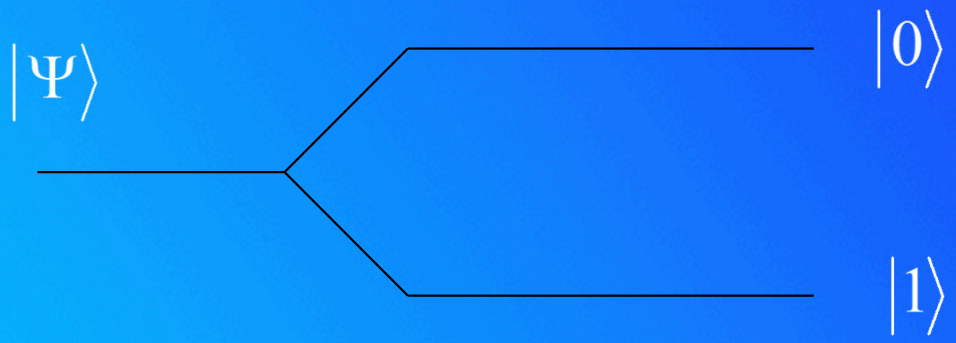
(David Deutsch)

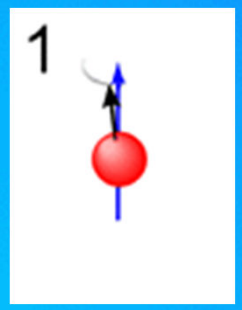
量子信息能做什么？


量子隐形传态
量子中继
高保密通信
量子模拟
量子信息处理
因数分解、搜索等快速实现
量子力学基本检验
量子定位
高精度测量

量子比特(qubit)

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$





$$|spin\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

最简单的量子系统

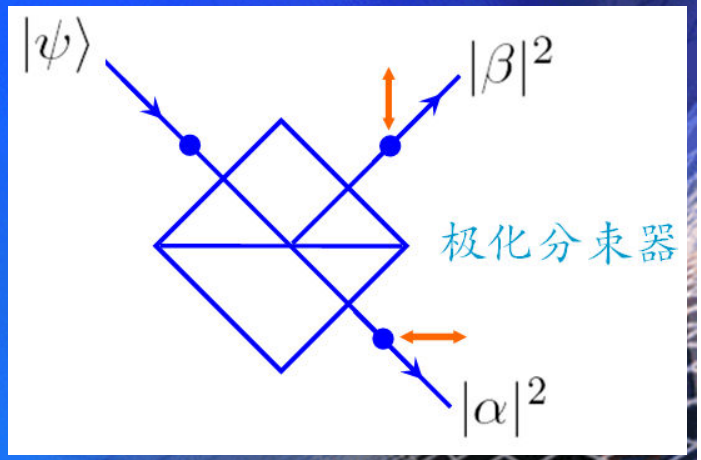
量子比特 是一个两维量子系统、即由一个两维Hilbert空间表示的量子系统

该Hilbert空间的一组正交归一基可以表示为 $|0\rangle,\ |1\rangle$

- 两能级原子（上能级、下能级）
- 光子极化（水平极化、竖直极化）
- 光子数（真空态、单光子态）
- 电子自旋（自旋向上、自旋向下）
- 单个粒子穿过两路干涉仪时所走的路径（路径1、路径2）

量子叠加 量子比特可以处在任意叠加态

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$



量子比特的表示和性质

- 一个量子比特有两个可能的状态: $|0\rangle$ & $|1\rangle$
- 不像经典比特，量子比特可以处于任意相干叠加

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

- 一个量子比特可以表征为2维Hilbert空间的单位矢量
- $|0\rangle$ & $|1\rangle$ 称作 orthonormal computational basis

- 量子比特的可能的状态可以表示为

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

量子比特的表示和性质

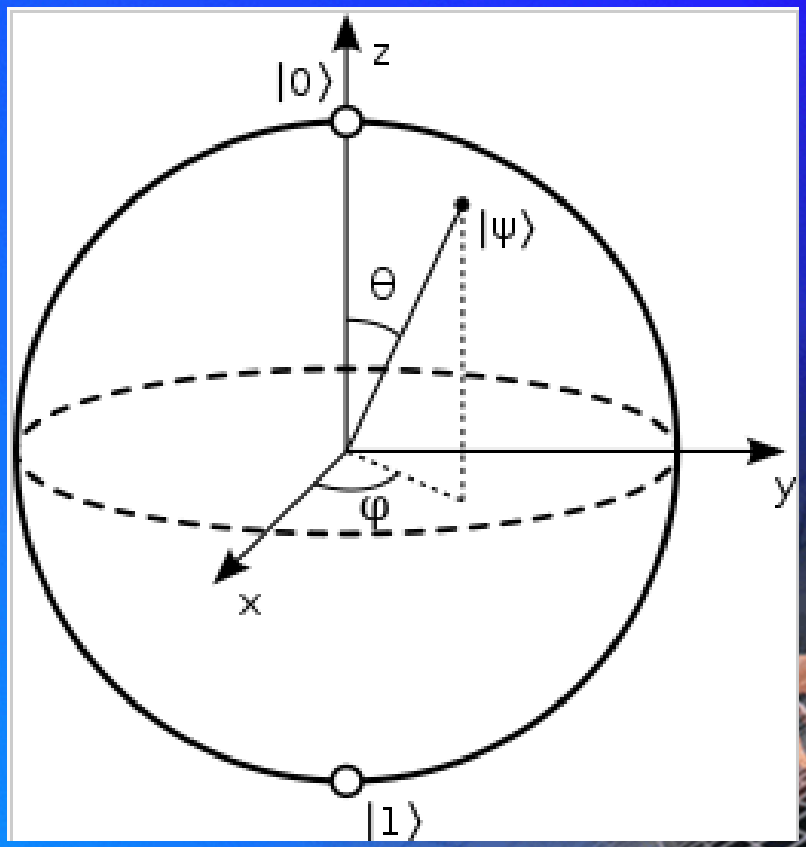
- 对于量子比特的测量得到0的概率为 $|\alpha|^2$ ， 得到1的概率为 $|\beta|^2$
- 量子比特测量之后不再能被恢复
- 量子比特可以与其它量子比特之间有关联和纠缠关系
- 量子比特可以有指数级增长的量子信息

量子比特的表示和性质

- 量子比特总可以表示为

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

称作Bloch Sphere表示



Pauli矩阵

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

性质

$$\sigma_k^\dagger = \sigma_k^{-1}, \quad \mathrm{Tr}(\sigma_k) = 0, \qquad \sigma_k^\dagger = \sigma_k, \quad k = x, y, z$$

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathrm{Id}$$

$$\sigma_i \sigma_j + \sigma_j \sigma_i = 2\delta_{ij}\,\mathrm{Id}$$

$$[\sigma_x, \sigma_y]_+ = [\sigma_y, \sigma_z]_+ = [\sigma_z, \sigma_x]_+ = 0$$

$$\sigma_i \sigma_j - \sigma_j \sigma_i = 2i\varepsilon_{ijk}\sigma_k$$

Pauli矩阵

$$\mathrm{Tr}(\sigma_i \sigma_j) = 2\delta_{ij}$$

从而对于任意2维线性算子有

$$A = \frac{1}{2}\mathrm{Tr}(A)\,\mathrm{Id} + \frac{1}{2}\sum_{k=1}^{3}\mathrm{Tr}(A\sigma_k)\sigma_k$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i\left(|0\rangle\langle 1| - |1\rangle\langle 0|\right)$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|\,.$$

Pauli矩阵

作用在量子比特上

$$\sigma_x|0\rangle = |1\rangle \qquad \sigma_x \text{ exchanges } (\textit{bit flip})$$
$$\sigma_x|1\rangle = |0\rangle$$

$$\sigma_y|0\rangle = i|1\rangle \qquad \sigma_y \text{ exchanges and introduces the phase } \pm i$$
$$\sigma_y|1\rangle = -i|0\rangle$$

$$\sigma_z|0\rangle = +|0\rangle \qquad \sigma_z \text{ introduces the phase } \pm 1 \ (\textit{phase flip}).$$
$$\sigma_z|1\rangle = -|1\rangle.$$

密度矩阵 (Density Matrices)

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

注意到 $\alpha = \langle 0|\phi\rangle$ 以及 $\beta = \langle 1|\phi\rangle$.

因此对于量子态|ϕ⟩测得0的概率为

$$p(0) = |\alpha|^2 = |\langle 0|\phi\rangle|^2$$

$$= \langle 0|\phi\rangle(\langle 0|\phi\rangle)^* = \langle 0|\phi\rangle\langle\phi|0\rangle$$

$$= \langle 0\|\phi\rangle\langle\phi\|0\rangle = Tr(\langle 0\|\phi\rangle\langle\phi\|0\rangle)$$

$$= Tr(|0\rangle\langle 0\|\phi\rangle\langle\phi|) = Tr(|0\rangle\langle 0|\rho)$$

这里定义ρ =|ϕ⟩⟨ϕ| 为量子态|ϕ⟩ 的

密度矩阵(density matrix)

密度矩阵 (Density Matrices)

(i) ρ is positive: $\langle\varphi|\rho|\varphi\rangle \geq 0$, $\forall\ |\varphi\rangle \in \mathcal{H}_d$ (and thus Hermitian, $\rho^\dagger = \rho$)

(ii) $tr[\rho] = 1$

(iii) $\rho^2 = \rho$.

(iii*) $\mathrm{tr}[\rho^2] = 1$

混合量子态

由态矢量 $|\phi\rangle$ 所描述的量子态称为纯态

考虑情形若一个量子系统处于 $|\phi_1\rangle$ 的几率为 p_1，处于 $|\phi_2\rangle$ 的几率为 p_2?

更一般地，考虑统计混合的情形

$$\phi = \left\{ \left(|\phi_1\rangle, p_1 \right), \left(|\phi_2\rangle, p_2 \right), \cdots \right\}$$

混合态系统综情形

假使我们做一个投影算子的P_0的测量，从而输出为0的几率为

$$p(0)=\sum_i p_i\cdot\left(\text{给定量子态}\left|\phi_i\right\rangle\text{测得0的几率}\right)$$

$$=\sum_i p_i\cdot Tr\left(\left|0\right\rangle\left\langle 0\right|\left|\phi_i\right\rangle\left\langle\phi_i\right|\right)$$

$$=Tr\sum_i p_i\left|0\right\rangle\left\langle 0\right|\left|\phi_i\right\rangle\left\langle\phi_i\right|$$

$$=Tr\left(\left|0\right\rangle\left\langle 0\right|\rho\right)=Tr\left(P_0\rho\right)$$

从而我们表示混合态的密度矩阵为

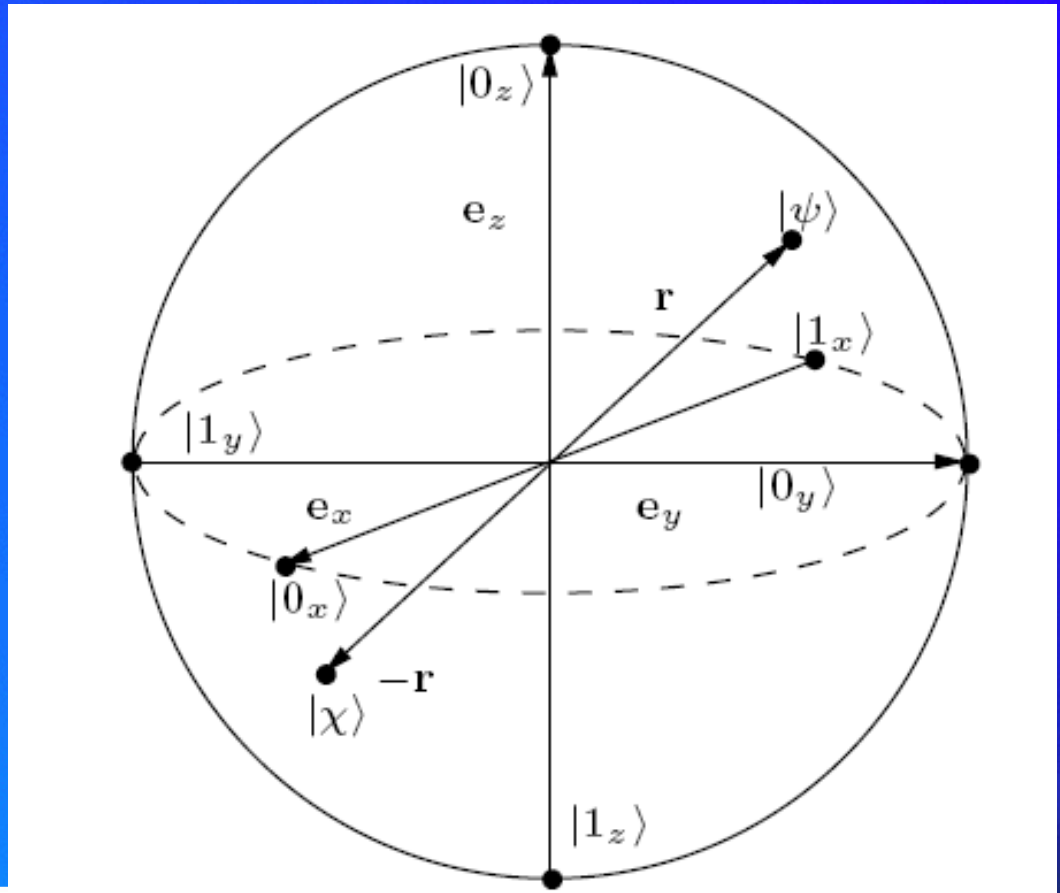
$$\rho=\sum_i p_i\left|\phi_i\right\rangle\left\langle\phi_i\right|$$

该密度矩阵包含了关于此量子态的所有有用和测量统计信息

混合态密度矩阵Bloch球表示

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{r}\boldsymbol{\sigma})$$

$$\mathbf{r} := \mathrm{tr}[\rho\boldsymbol{\sigma}]$$



$$\mathrm{tr}[\rho^2] = \frac{1}{4}\mathrm{tr}[\mathbb{1} + 2\mathbf{r}\boldsymbol{\sigma} + \sum_{i,j} r_i r_j \sigma_i \sigma_j]$$

$$= \frac{1}{2}(1 + |\mathbf{r}|^2) \ .$$

不可克隆定理

No-Cloning

$$|0\rangle|\ \rangle \Rightarrow |0\rangle|0\rangle$$

$$|1\rangle|\ \rangle \Rightarrow |1\rangle|1\rangle$$

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

$$\neq \left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right]\left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right]$$

It is impossible to create identical copies of an arbitrary unknown quantum state!

Wootters and Zurek, Nature 299, 802 (1982)
Dieks, Phys. lett. A 92, 271 (1982)

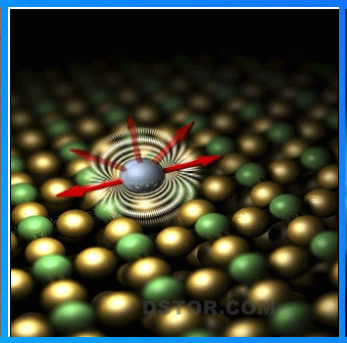
量子比特与量子纠缠

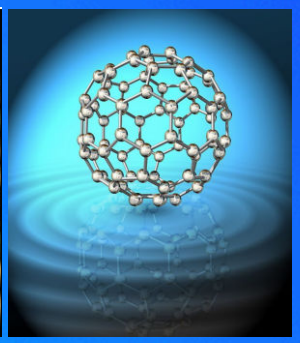
量子　　是构成物质的最基本单元

是能量的最基本携带者

不可分割

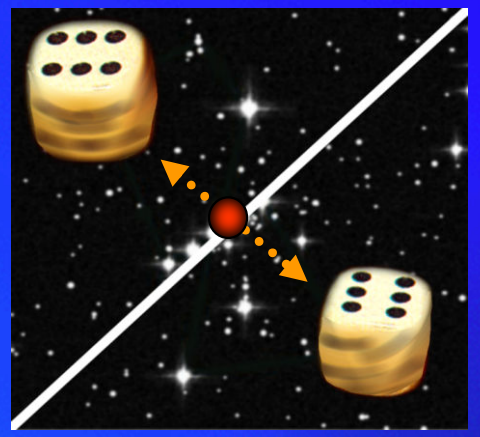

光子


原子


分子

量子纠缠

$$|\text{↑}\rangle|\text{↑}\rangle + |\text{→}\rangle|\text{→}\rangle$$



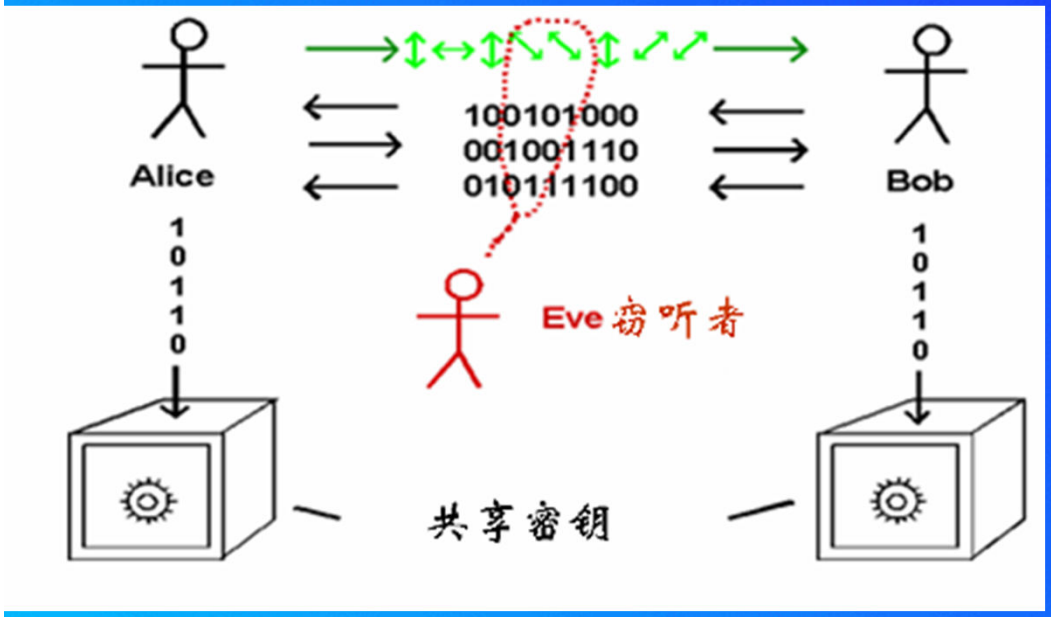
遥远地点之间的惊人关联！

经典比特	0	1
量子比特	$\|0\rangle$	$\|1\rangle$
叠加态	$\|\text{↑}\rangle + \|\text{→}\rangle$	
光子极化	↕	↔


量子叠加

中国科学技术大学 陈凯

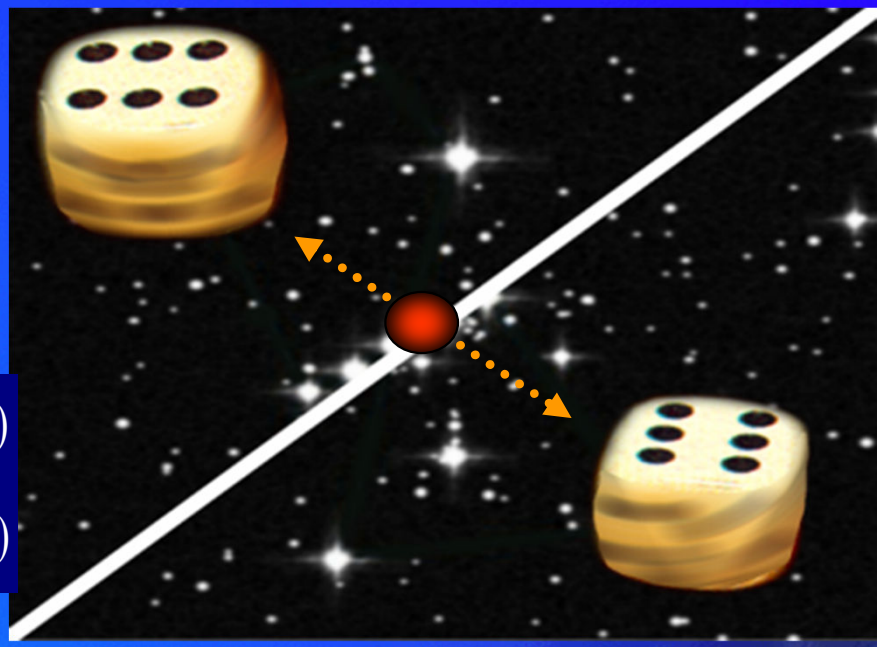
量子通信技术:量子加密术



无条件安全的密钥生成

纠缠态方案

Ekert, PRL 67, 661 (1991)



单粒子方案

Bennett & Brassard (1984)

$$|\Phi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2\pm|\updownarrow\rangle_1|\updownarrow\rangle_2\right)$$

$$|\Psi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_1|\updownarrow\rangle_2\pm|\updownarrow\rangle_1|\leftrightarrow\rangle_2\right)$$

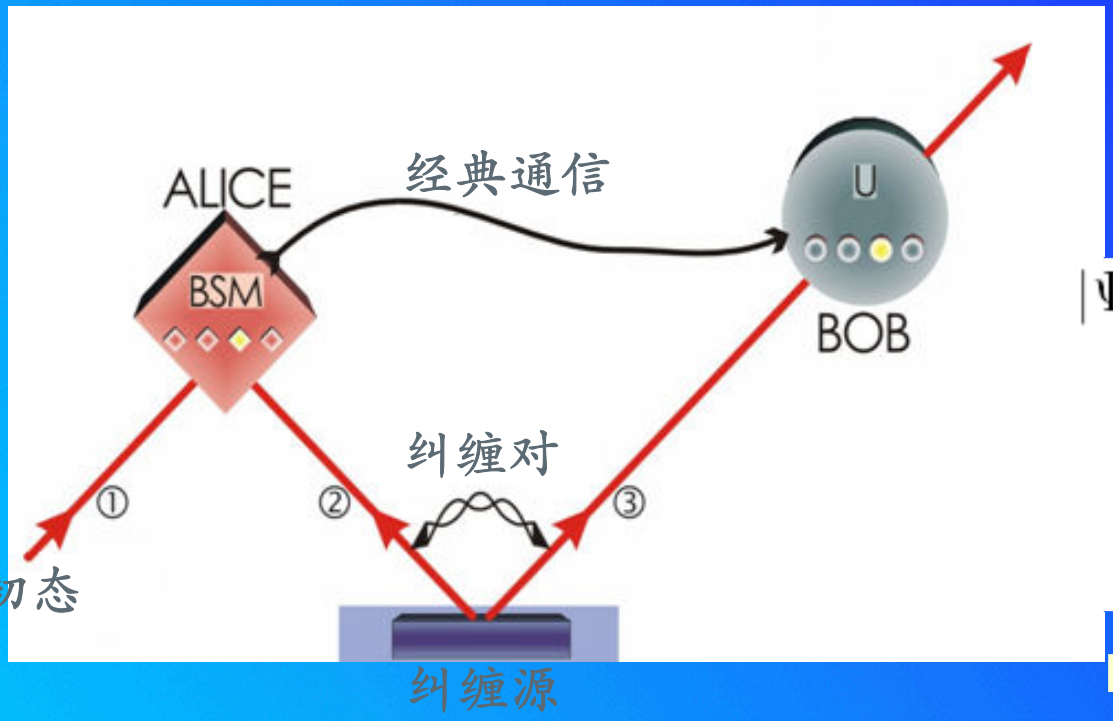
量子不可克隆定理

量子不可分割

一次一密，完全随机

无条件安全

量子通信技术:量子隐形传态



初态 $|\Phi\rangle_1 = \alpha|\leftrightarrow\rangle_1 + \beta|\updownarrow\rangle_1$

纠缠对 $|\Phi^+\rangle_{23}$

$$
\begin{aligned}
|\Psi\rangle_{123} = \; & |\Phi^+\rangle_{12} \otimes (\alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3) + \\
& |\Phi^-\rangle_{12} \otimes (\alpha|\leftrightarrow\rangle_3 - \beta|\updownarrow\rangle_3) + \\
& |\Psi^+\rangle_{12} \otimes (\alpha|\updownarrow\rangle_3 + \beta|\leftrightarrow\rangle_3) + \\
& |\Psi^-\rangle_{12} \otimes (\alpha|\updownarrow\rangle_3 - \beta|\leftrightarrow\rangle_3)
\end{aligned}
$$

Bennett et al., PRL 73, 3801 (1993)

量子计算与量子通信

量子并行性

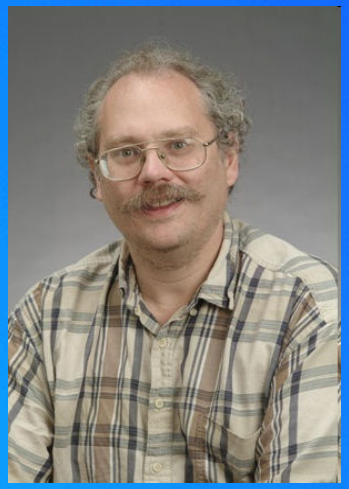
经典比特	量子比特
0 或 1	0 + 1
00，01，10 或 11	00 + 01 + 10 + 11
000，001，010……	000 + 001 + 010 + ……
⋮	⋮

量子并行性使得量子计算机可以同时对 2^N 个数进行数学运算，其效果相当于经典计算机重复实施 2^N 次操作。

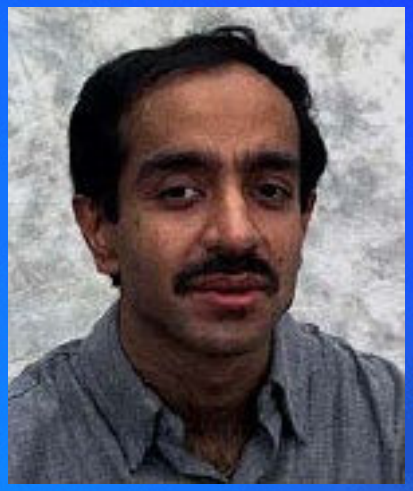
$$U\sum_{i=1}^{2^N} a_i|i\rangle = \sum_{i=1}^{2^N} a_i U|i\rangle, \quad 2^N!$$

Shor算法

- 计算步数 $\sqrt{N} \Rightarrow \log N$
- 利用经典THz计算机分解300位的大数，需10^{24}步，150000年。
- 利用Shor算法THz计算机，只需10^{10}步，1秒！
- RSA将不再安全！



P. W. Shor



L. K. Grover

Grover搜寻算法

- 如何在草堆中找到一根针？
- 经典搜寻：N 步
- 量子搜寻：$N^{1/2}$ 步
- 可破译DES密码：2^{56} 个数中搜寻密钥

1000年 $\Rightarrow$ 4分钟

中国科学技术大学 陈凯

Schmidt decomposition

任意两体纯态

$$|\Phi\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}|i\rangle\otimes|j\rangle$$

假设 n ≤m

存在一组正交态$|\mu_1\rangle, |\mu_2\rangle, \ldots, |\mu_n\rangle$ 以及$|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ 使得

$$|\Phi\rangle = \sum_{c=1}^{n} \sqrt{p_c}|\mu_c\rangle\otimes|\varphi_c\rangle$$

$|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$为 $Tr_1|\Phi\rangle\langle\Phi|$ 的本征态

参考QCQI §2.5, M.A. Nielsen and I.L. Chuang

密度矩阵矩阵元的表示

$$I=\sigma_0=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \sigma_1=\begin{pmatrix}0&1\\1&0\end{pmatrix}\ \sigma_2=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

也即

$$I=|0\rangle\langle 0|+|1\rangle\langle 1|$$

$$\sigma_1=|0\rangle\langle 1|+|1\rangle\langle 0|$$

$$\sigma_3=|0\rangle\langle 0|-|1\rangle\langle 1|$$

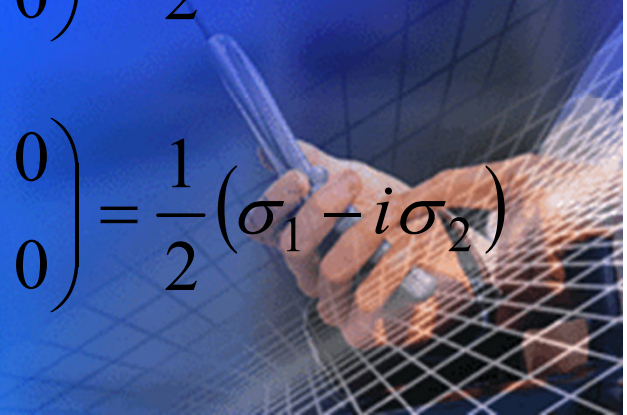
$$\sigma_2=-i|0\rangle\langle 1|+i|1\rangle\langle 0|$$

$$|0\rangle\langle 0|=\begin{pmatrix}1&0\\0&0\end{pmatrix}=\frac{1}{2}(I+\sigma_3)$$

$$|0\rangle\langle 1|=\begin{pmatrix}0&1\\0&0\end{pmatrix}=\frac{1}{2}(\sigma_1+i\sigma_2)$$

$$|1\rangle\langle 1|=\begin{pmatrix}0&0\\0&1\end{pmatrix}=\frac{1}{2}(I-\sigma_3)$$

$$|1\rangle\langle 0|=\begin{pmatrix}0&0\\1&0\end{pmatrix}=\frac{1}{2}(\sigma_1-i\sigma_2)$$



密度矩阵性质

$$
\begin{aligned}
\varrho^2 &= \varrho * \varrho \\
&= \sum_i p_i |\psi_i\rangle\langle\psi_i| \sum_j p_j |\psi_j\rangle\langle\psi_j| \\
&= \sum_i p_i p_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j| \\
&= \sum_i p_i^2 |\psi_i\rangle\langle\psi_i| \ .
\end{aligned}
$$

因此 $Tr\rho^2 = \sum_i p_i^2$ 混合程度，最小值？

纯态 $\sum_i p_i^2 = 1$

混合态 $\mathrm{tr}(\varrho^2) < 1$

$$\rho = \frac{1}{d}\mathbb{1}$$

密度矩阵性质

所有N维Hilbert空间H中的密度矩阵构成一个凸集

$$\rho(\lambda) = \lambda\rho_1 + (1-\lambda)\rho_2$$

(i) ρ is positive: $\langle\varphi|\rho|\varphi\rangle \geq 0$, $\forall\ |\varphi\rangle \in \mathcal{H}_d$ (and thus Hermitian, $\rho^\dagger = \rho$)

(ii) $tr[\rho] = 1$

一般地

$$\rho = \sum_{l=1}^{k} r_l \rho_l$$

仍然为一个密度矩阵

密度矩阵演化

作用一个幺正变换**U**在初态 $|\psi\rangle$ ，我们有

$$U|\psi\rangle$$

密度矩阵变为

$$U|\psi\rangle\left(U|\psi\rangle\right)^{\dagger}=U|\psi\rangle\langle\psi|U^{\dagger}$$

系综分解

任意系综生成和表示

$$\rho=\sum_a p_a|\psi_a\rangle\langle\psi_a|=\sum_a|\tilde{\psi}_a\rangle\langle\tilde{\psi}_a|,\quad |\tilde{\psi}_a\rangle:=\sqrt{p_a}|\psi_a\rangle,$$

正交归一基矢下的系综分解

$$\rho=\sum_{n=1}^{d}\lambda_n|n\rangle\langle n|=\sum_{n=1}^{d}|\tilde{n}\rangle\langle\tilde{n}|$$

可以证明，同一密度矩阵的两组系综之间存在一个幺正变换关系

$$|\tilde{\psi}_i\rangle=\sum_j u_{ij}|\tilde{\varphi}_j\rangle$$

Trace操作

$$\mathrm{tr}(\varrho) = \sum_k \langle k|\varrho|k\rangle$$

对于混合态 $\varrho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$$\begin{aligned}
\mathrm{tr}(\varrho) &= \sum_k \langle k| \sum_i p_i |\psi_i\rangle\langle\psi_i||k\rangle \\
&= \sum_i p_i \ \mathrm{tr}(|\psi_i\rangle\langle\psi_i|) \\
&= \sum_i p_i \\
&= 1 \, .
\end{aligned}$$

意味着对于各种量子态的测量输出总的概率为1

Trace操作性质

矩阵对角元求和

$$Tr\begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix} = a_{00} + a_{11} + a_{22}$$

特性

$$Tr[xA + yB] = xTr[A] + yTr[B]$$

$$Tr[AB] = Tr[BA]$$

$$Tr[ABC] = Tr[CAB]$$

$$Tr[UAU^{\dagger}] = Tr[A]$$

$$Tr[A] = \sum_i \langle \varphi_i | A | \varphi_i \rangle$$

正交基展开 $|\varphi_i\rangle$

Trace操作

$$Tr(|\psi\rangle\langle\varphi|) = \langle\varphi|\psi\rangle$$

可分离态情形

$$\rho_A \otimes \rho_B = \sum_{ij} (p_i |i_A\rangle \otimes \langle i_A|)(q_j |j_B\rangle \otimes \langle j_B|)$$

$$Tr_B(\rho_A \otimes \rho_B) = \rho_A \otimes Tr(\rho_B)$$

Trace操作

纠缠态情形

$$\mathrm{tr}|\psi\rangle\langle\phi| = \langle\psi|\phi\rangle$$

$$|\psi_{AB}\rangle = \sum_i \alpha_i |i_A\rangle|i_B\rangle$$

$$\varrho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}| = \sum_i \alpha_i |i_A\rangle|i_B\rangle \sum_m \alpha_j^* \langle j_A|\langle j_B|$$

我们得到

$$\begin{aligned}
\mathrm{tr}_B \varrho_{AB} &= \sum_{i,j} \alpha_i \alpha_j^* |i_A\rangle\langle j_A|\langle j_B||i_B\rangle \\
&= \sum_{i,j} \alpha_i \alpha_j^* |i_A\rangle\langle j_A|\delta_{ij} \\
&= \sum_i |\alpha_i|^2 |i_A\rangle\langle i_A| \ .
\end{aligned}$$

Trace操作

一个例子

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$$

我们得到

$$Tr_B(|\Phi^+\rangle\langle\Phi^+|) = Tr_B\left(\frac{1}{2}(|0_A 0_B\rangle + |1_A 1_B\rangle)(\langle 0_A 0_B| + \langle 1_A 1_B|)\right)$$

$$= \frac{1}{2}(|0_A\rangle\langle 0_A| \otimes Tr(|0_B\rangle\langle 0_B|) + |1_A\rangle\langle 0_A| \otimes Tr(|1_B\rangle\langle 0_B|) + |0_A\rangle\langle 1_A| \otimes Tr(|0_B\rangle\langle 1_B|) + |1_A\rangle\langle 1_A| \otimes Tr(|1_B\rangle\langle 1_B|))$$

$$= \frac{1}{2}(|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|)$$

量子态纯化**Purification**

$$\varrho = \sum_i p_i |i\rangle\langle i|$$

$$|\psi\rangle = \sum_i \sqrt{p_i}|i_A\rangle \otimes |i_B\rangle$$

Trace操作 作用在矩阵上

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \xrightarrow{Tr_2} \begin{bmatrix} Tr\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} & Tr\begin{bmatrix} a_{02} & a_{03} \\ a_{12} & a_{13} \end{bmatrix} \\ Tr\begin{bmatrix} a_{20} & a_{21} \\ a_{30} & a_{31} \end{bmatrix} & Tr\begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} a_{00} + a_{11} & a_{02} + a_{13} \\ a_{20} + a_{31} & a_{22} + a_{33} \end{bmatrix}$$

量子测量

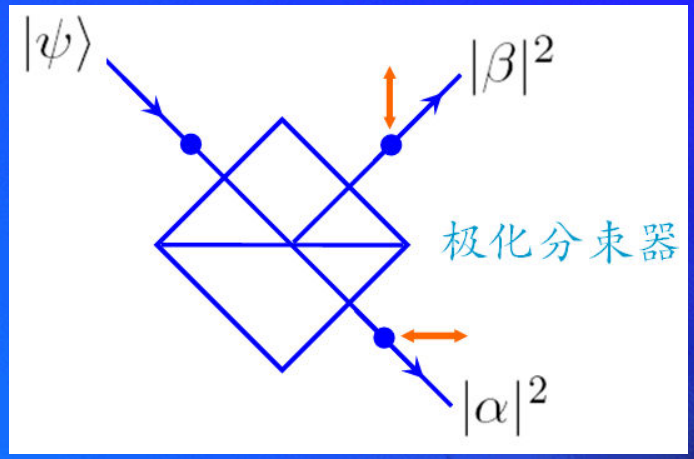
$$|\phi\rangle=\sum_{i=1}^{n}a_i|\beta_i\rangle,\sum_{i=1}^{n}|a_i|^2=1$$

沿基矢 $\{\beta_i\}_{i=1}^{n}$ 进行测量

几率幅 $a_i=\langle\beta_i|\phi\rangle$

几率 $|a_i|^2$

量子测量 如对于任意叠加态



$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle,\quad |\alpha|^2+|\beta|^2=1$$

Von Neumann测量

Von Neumann测量是投影测量的一种类型。给定一组正交基 $\{|\psi_k\rangle\}$，如果我们对于量子态 $|\Phi\rangle=\sum\alpha_k|\psi_k\rangle$ $\{|\psi_k\rangle\}$ 实施沿基矢 $|\psi_k\rangle$ 的Von Neumann测量，则有

$$|\alpha_k|^2=|\langle\psi_k|\Phi\rangle|^2=\langle\psi_k|\Phi\rangle\langle\Phi|\psi_k\rangle$$

$$=Tr\left(\langle\psi_k|\Phi\rangle\langle\Phi|\psi_k\rangle\right)=Tr\left(|\psi_k\rangle\langle\psi_k\|\Phi\rangle\langle\Phi|\right)$$

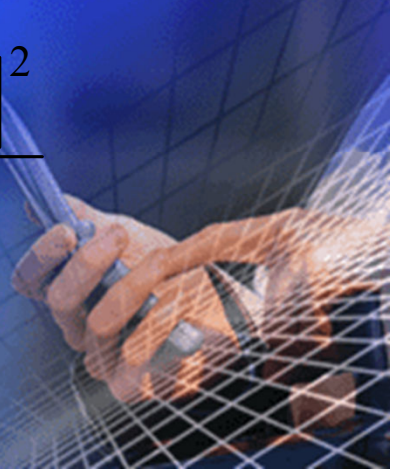
Von Neumann测量

例如考虑对于量子态 $|\Phi\rangle=(\alpha|0\rangle+\beta|1\rangle)$

实施相对于基矢 $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}},\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$ 的Von Neumann测量

注意到 $$|\Phi\rangle=\frac{\alpha+\beta}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)+\frac{\alpha-\beta}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

因此我们有测得 $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$ 的几率为 $\frac{|\alpha+\beta|^2}{2}$



Von Neumann测量

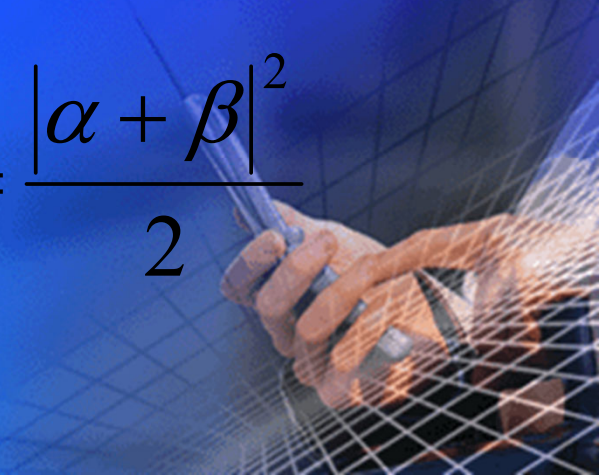
实际上

$$\left(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right)|\Phi\rangle=\frac{\alpha+\beta}{\sqrt{2}}$$

$$\langle\Phi|\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{\alpha^{*}+\beta^{*}}{\sqrt{2}}$$

$$\left(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right)|\Phi\rangle\langle\Phi|\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

$$=Tr\left(\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right)|\Phi\rangle\langle\Phi|\right)=\frac{|\alpha+\beta|^{2}}{2}$$



投影测量(Projective measurements)

可观测量M存在一个谱分解

$$M = \sum_m m P_m$$

满足

$$P_m P_n = P_m \delta_{m,n}$$

$$\sum_m P_m = I$$

获得结果m的几率为

$$p(m) = \mathrm{tr}(P_m \varrho)$$

系统的量子态变为

$$\frac{P_m \varrho P_m}{p(m)}$$

投影测量(Projective measurements)

可观测量M存在一个谱分解

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\sigma_2 = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

$$\sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|$$

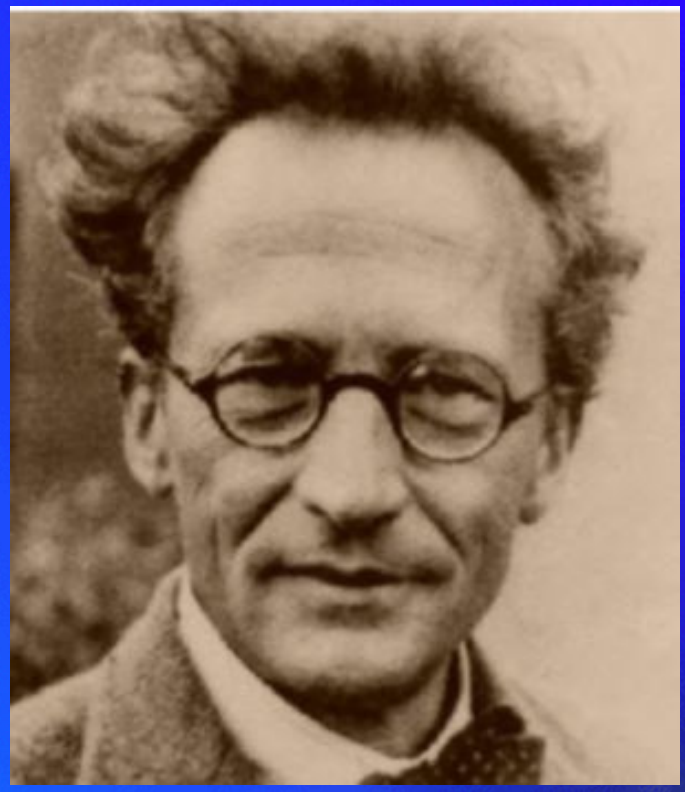
更一般地定义可观测量

$$\vec{v}\cdot\vec{\sigma} \equiv v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3$$

称为自旋沿着 $\vec{v}$ 轴方向的测量

量子纠缠

"Entanglement is *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought".



- Quantum computation
- Quantum teleportation
- Dense coding
- Quantum cryptography
- Quantum error correction

E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935)

量子纠缠

$$\rho^{AB} \neq \rho^{A} \otimes \rho^{B}$$

可分离态

$$\rho^{AB} = \sum_{r=1}^{m} p_r \rho_r^A \otimes \rho_r^B \quad , \quad p_r > 0 \quad , \quad \sum_r p_r = 1$$

LOCC操作
“local operations and classical communication”

局域操作：unitary dynamic actions, measurements, and all other local manipulations

经典通信：exchange information via classical communication

量子纠缠

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

A pure or mixed quantum state which is not separable is called entangled. An entangled quantum state thus contains non-classical correlations, which are also called quantum correlations or EPR correlations.

量子纠缠

Pure state: Tensor Product

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta 1 \\ \alpha_1\beta_0 \\ \alpha_1\beta 1 \end{pmatrix}$$

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

Separable

Entangled

量子纠缠性质

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)$$
$$= \frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}$$

$$\rho^1 = \mathrm{tr}_2(\rho)$$
$$= \frac{\mathrm{tr}_2(|00\rangle\langle 00|) + \mathrm{tr}_2(|11\rangle\langle 00|) + \mathrm{tr}_2(|00\rangle\langle 11|) + \mathrm{tr}_2(|11\rangle\langle 11|)}{2}$$
$$= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2}$$
$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}$$
$$= \frac{I}{2}.$$

This strange property, that the joint state of a system can be completely known, yet a subsystem be in mixed states, is another hallmark of quantum entanglement.

Two or more systems:

a state $|\Psi\rangle$ of the system can be in: $|00\rangle, |01\rangle, |10\rangle, |11\rangle,$

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

where $|00\rangle = |0\rangle \otimes |0\rangle$

The system is entangled if

$$|\Psi\rangle \neq |\Psi\rangle_A \otimes |\Psi\rangle_B$$

Example: Bohm state $|\Psi^-\rangle = 1/\sqrt{2}\,(|01\rangle - |10\rangle)$

i.e. EPR (Einstein, Podolsky and Rosen) pair

量子纠缠应用：superdense coding

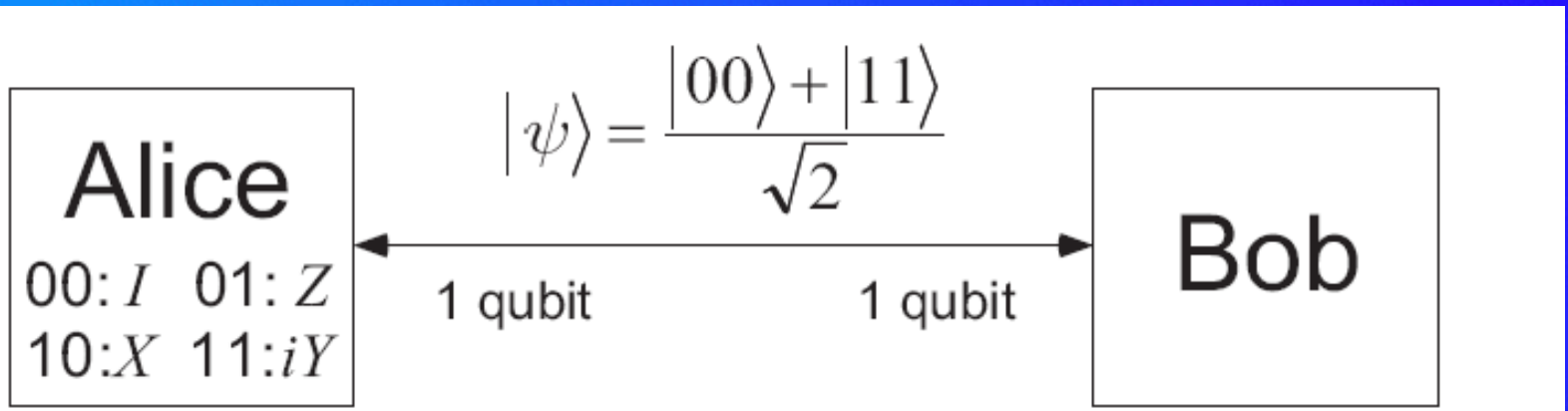


Figure 2.3. The initial setup for superdense coding, with Alice and Bob each in possession of one half of an entangled pair of qubits. Alice can use superdense coding to transmit two classical bits of information to Bob, using only a single qubit of communication and this preshared entanglement.

编码和解码

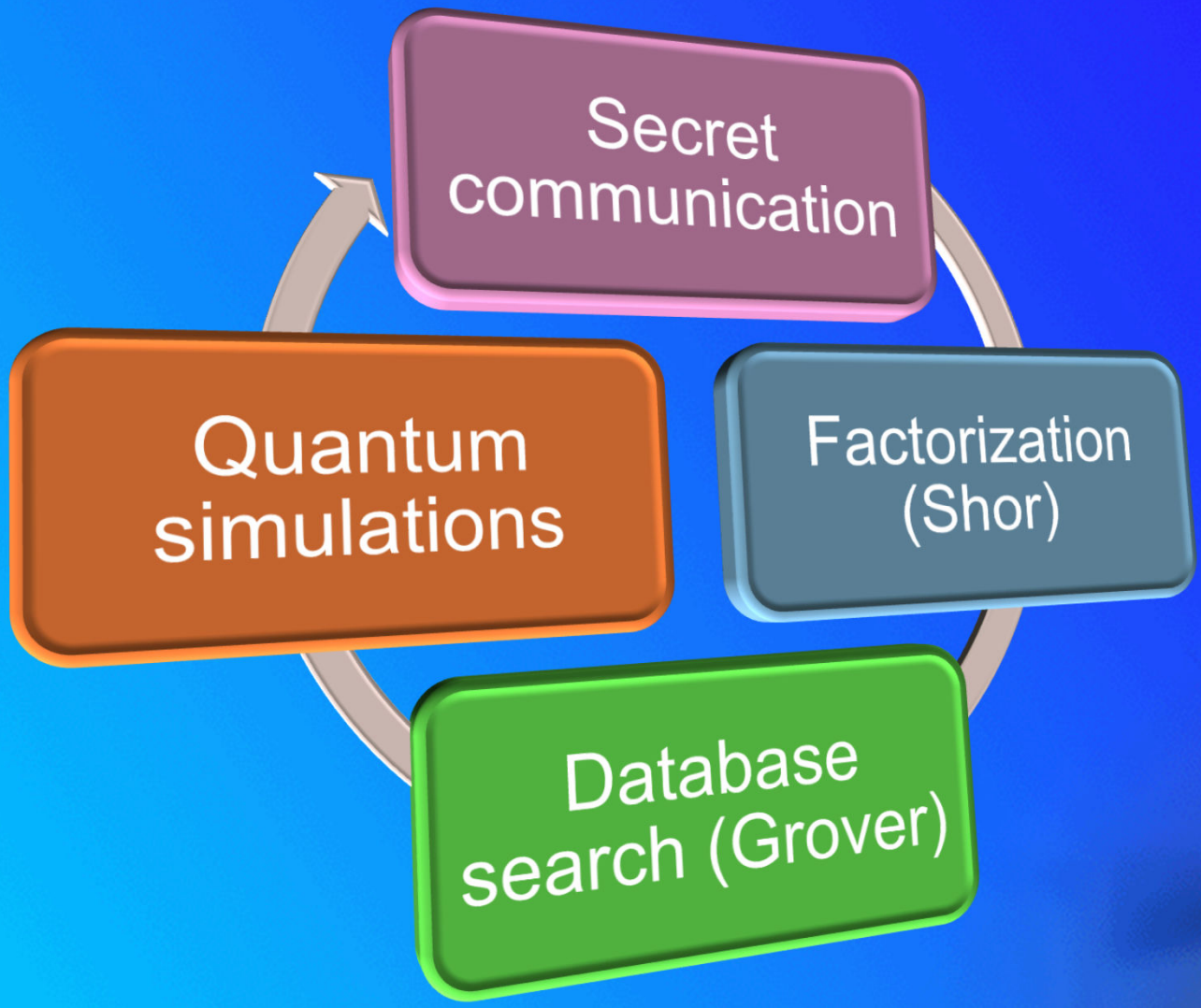
$$00 : |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$01 : |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

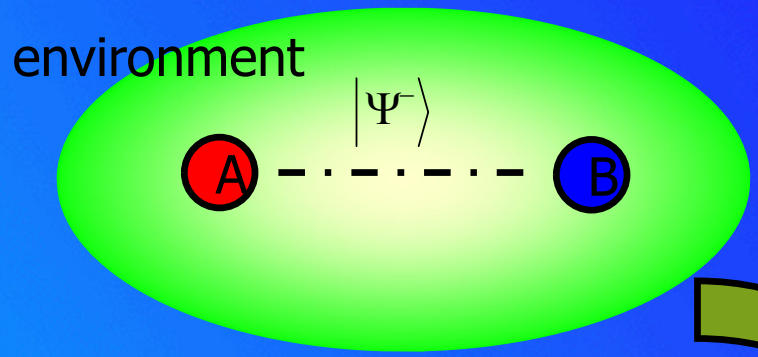
$$10 : |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$11 : |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

量子纠缠应用


Secret communication
Factorization (Shor)
Database search (Grover)
Quantum simulations

Decoherence



The separability problem:
one of the basic and emergent problem in present and future quantum information processing

Is a quantum state entangled?

How entangled is it still after interacting

with a noisy environment?

Density matrix of quantum states

A number of states $|\psi_i\rangle$ with respective probabilities p_i

define: $$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

we call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states,
where

$$\rho \geq 0, tr\rho = 1, \rho = \rho^\dagger$$

Pure states: $$\rho^2 = \rho = |\psi_i\rangle\langle\psi_i|$$

Mixed states: $$\rho^2 \neq \rho$$

Separability

entangled?

Pure states

- Product states(separable):

$$|\Psi_{AB}\rangle = |\psi_A\rangle|\psi_B\rangle$$

density matrix $\quad \rho_{AB} = \rho_A \otimes \rho_B, \rho_A = |\psi\rangle_A\langle\psi|, \rho_B = |\psi\rangle_B\langle\psi|$

- Examples:

Product state: $|\Psi\rangle = |00\rangle$

Entangled state: $|\Psi\rangle = c_0|00\rangle + c_1|11\rangle$ $\quad c_0, c_1 \neq 0$

Mixed states

Physical definition:

a separable state is a quantum state which can be prepared in a *local* or *classical* way (Local operations and classical communications: LOCC),

this is equivalent to:

$$\rho_{AB\cdots Z} = \sum_i p_i \rho_i^A \otimes \rho_i^B \otimes \cdots \otimes \rho_i^Z$$

(Werner 89)

Otherwise, it is entangled

Problem：there are infinite possible decomposition,

$$\rho_{AB} = \sum_i q_i \rho_{AB}^i$$

does there exist decomposition like formula ?

Separability criterion for multipartite pure state

A pure state is separable if and only if

$$\rho_{AB\cdots Z} = \rho_A \otimes \rho_B \otimes \cdots \otimes \rho_Z$$

where

$$\begin{aligned}
\rho_A &= Tr_{B,C,\cdots,Z}(\rho_{AB\cdots Z}),\\
\rho_B &= Tr_{A,C,\cdots,Z}(\rho_{AB\cdots Z}),\\
&\vdots\\
\rho_Z &= Tr_{A,B,\cdots,Y}(\rho_{AB\cdots Z}),
\end{aligned}$$

are the reduced density matrices for the subsystems A,B,...,Z respectively.

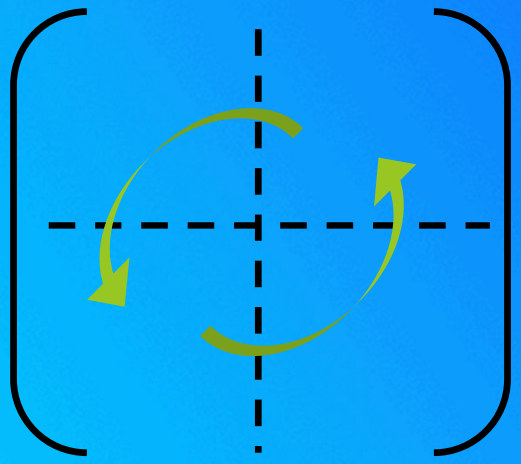
A strong separability criterion for mixed state

Positive partial transpositions(PPT)

Peres PRL **77**, 1413 (1996)

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i \geq 0 \quad \rightarrow \quad \rho^{T_A} = \sum_i p_i (\rho_A^i)^T \otimes \rho_B^i \geq 0$$

An example of 2x2 state:



$$\rho = \begin{pmatrix} \rho_{11} & \rho_{12} & \rho_{13} & \rho_{14} \\ \rho_{21} & \rho_{22} & \rho_{23} & \rho_{24} \\ \rho_{31} & \rho_{32} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{42} & \rho_{43} & \rho_{44} \end{pmatrix}$$

$$\rho^{T_A} = \begin{pmatrix} \rho_{11} & \rho_{12} & \rho_{31} & \rho_{32} \\ \rho_{21} & \rho_{22} & \rho_{41} & \rho_{42} \\ \rho_{13} & \rho_{14} & \rho_{33} & \rho_{34} \\ \rho_{23} & \rho_{24} & \rho_{43} & \rho_{44} \end{pmatrix}$$

例子

量子态 $\Psi = |00\rangle + |11\rangle$ 其密度矩阵为

$$\rho = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix}$$

部分转置给出

$$\rho = \begin{pmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

为非正半定的。本征值为{-1/2, 1/2, 1/2, 1/2}

重要结果

Horodecki *et al*. (PLA,1996)

$2 \otimes 2$, $2 \otimes 3$ cases: PPT $\Leftrightarrow$ Separable

Horodeckis, Phys. Lett. A **223**,1 (1996)

部分转置的量子态可表为

$$\langle m|\langle \mu|\varrho_{AB}^{T_B}|n\rangle|\nu\rangle \equiv \langle m|\langle \nu|\varrho_{AB}|n\rangle|\mu\rangle$$

对于可分离态，也应为一个密度矩阵，应有非负的本征谱

更一般的结果

Necessary and Sufficient Condition for Separability

For any positive (P) but not completely positive (CP) map,

$$\Lambda : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_{A'})$$

one should have $[I_A \otimes \Lambda_B](\varrho_{AB}) \geqslant 0$

for any separable states.

$$[I_A \otimes \Lambda_B](\varrho_{AB}) = \begin{pmatrix} \Lambda(\varrho_{00}) & \cdots & \Lambda(\varrho_{0d_A-1}) \\ \Lambda(\varrho_{10}) & \cdots & \Lambda(\varrho_{1\,d_A-1}) \\ \cdots & \cdots & \cdots \\ \Lambda(\varrho_{d_A-10}) & \cdots & \Lambda(\varrho_{d_A-1d_A-1}) \end{pmatrix}$$

Here $\varrho_{ij} \equiv \langle i| \otimes \mathrm{I} |\varrho_{AB}| j\rangle \otimes I$

Majorization判据

If a state is separable then the inequalities

$$\lambda(\rho) \prec \lambda(\rho_A), \quad \lambda(\rho) \prec \lambda(\rho_B)$$

Holds.

Here $\lambda(\rho)$ is a vector of eigenvalues of ρ ; $\lambda(\rho_A)$ and $\lambda(\rho_B)$ are defined similarly.

$x \prec y$ means $\sum_{i=1}^{k} x_i^{\downarrow} \leqslant \sum_{i=1}^{k} y_i^{\downarrow}, \ 1 \leqslant k \leqslant d$

Nielsen, M. A., and J. Kempe, 2001, Phys. Rev. Lett. 86, 5184

Reduction criterion

定义映射

$$\Lambda^{red}(\varrho) = I\,\mathrm{Tr}(\varrho) - \varrho$$

对于可分态应有

$$[I_A \otimes \Lambda_B^{\mathrm{red}}](\varrho_{AB}) \geqslant 0$$

化简后，即得

$$\varrho_A \otimes I - \varrho_{AB} \geqslant 0$$

- 此判据弱于PPT准则，但是强于Majorization判据
- 违背此准则，一定是可提纯的

Cerf *et al.*, 1999; Horodecki and Horodecki, 1999

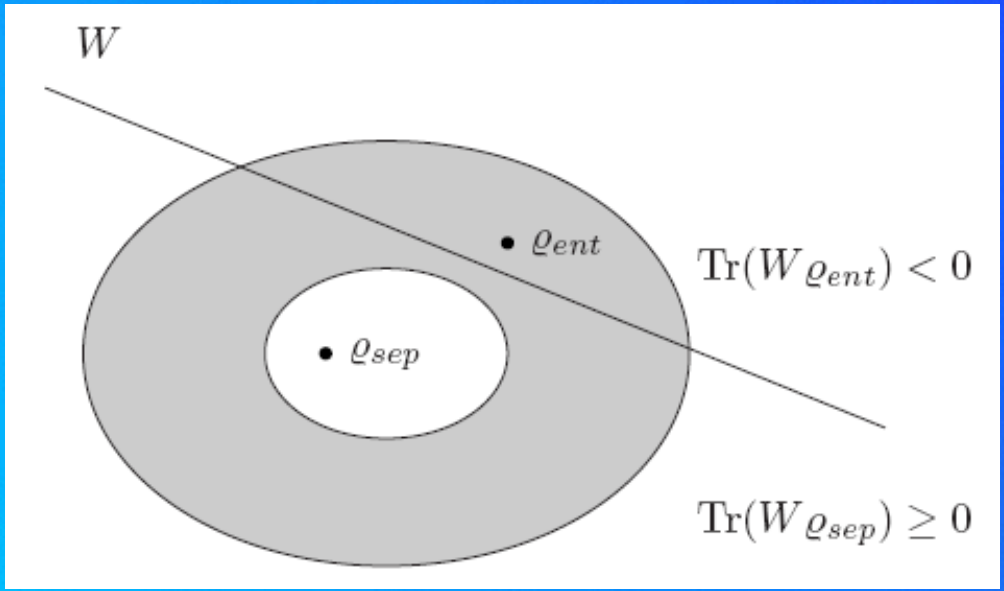
Entanglement witness (EW)

定义映射

$$\mathrm{Tr}(W\varrho_{AB}) \geqslant 0$$

W为可观测量，满足

- 至少有一个负本征值
- 对于所有直积态，应有 $\langle\psi_A|\langle\phi_B|W|\psi_A\rangle|\phi_B\rangle \geqslant 0$



Terhal, B. M., 2000, Phys. Lett. A 271, 319

Entanglement witness例子

交换算符

$$V=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|j\rangle\langle i|$$

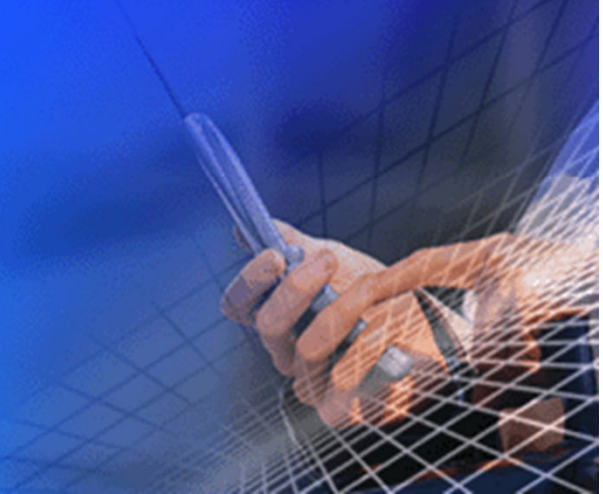
$$\langle\psi_A|\langle\phi_B|V|\psi_A\rangle|\phi_B\rangle=|\langle\psi_A|\phi_B\rangle|^2\geqslant 0$$

$$V=P^{(+)}-P^{(-)}$$

对称子空间和反对称子空间

$$P^{(+)}=\tfrac{1}{2}(I+V)\quad\text{and}\quad P^{(-)}=\tfrac{1}{2}(I-V)$$

具有本征值-1



Entanglement witness例子

四体cluster态

$$|C_4\rangle = \frac{(|0000\rangle_{1234} + |0011\rangle_{1234} + |1100\rangle_{1234} - |1111\rangle_{1234})}{2}$$

构造

$$\mathcal{W} = \frac{[4I^{\otimes 4} - (XXIZ + XXZI + IIZZ + IZXX + ZIXX + ZZII)]}{2}$$

只需要两个实验settings即可

$$XXZZ \text{ and } ZZXX$$

<W>的负值意味着真正的4体纠缠

A Matrix Realignment Method for Recognizing Entanglement

Define realignment operation:

If Z is an mxm block matrix with block size nxn,

$$Z=\begin{pmatrix} Z_{11} & \cdots & Z_{1m} \\ \vdots & \ddots & \vdots \\ Z_{m1} & \cdots & Z_{mm} \end{pmatrix} \rightarrow \tilde{Z}=\begin{pmatrix} vec(Z_{11})^T \\ \vdots \\ vec(Z_{m1})^T \\ \vdots \\ vec(Z_{1m})^T \\ \vdots \\ vec(Z_{mm})^T \end{pmatrix}$$

A 2x2 example:

$$A=[a_{ij}] \rightarrow vec(A)=\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \\ \vdots \\ a_{1m} \\ \vdots \\ a_{mm} \end{pmatrix}$$

$$\rho=\left(\begin{array}{cc:cc} \rho_{11} & \rho_{12} & \rho_{13} & \rho_{14} \\ \rho_{21} & \rho_{22} & \rho_{23} & \rho_{24} \\ \hdashline \rho_{31} & \rho_{32} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{42} & \rho_{43} & \rho_{44} \end{array}\right) \rightarrow \tilde{\rho}=\left(\begin{array}{cccc} \rho_{11} & \rho_{21} & \rho_{12} & \rho_{22} \\ \hdashline \rho_{31} & \rho_{31} & \rho_{32} & \rho_{42} \\ \hdashline \rho_{13} & \rho_{23} & \rho_{14} & \rho_{24} \\ \hdashline \rho_{33} & \rho_{43} & \rho_{34} & \rho_{44} \end{array}\right)$$

The realignment criterion

For any bipartite separable state, we have

$$\|\tilde{\rho}\| \leq 1$$

necessary criterion for separability

Here $\|\tilde{\rho}\|$ is the sum of all the singular values of $\tilde{\rho}$, or sum of the square roots of eigenvalue for $\tilde{\rho}\tilde{\rho}^{\dagger}$.

Kai Chen, Ling-An Wu, *Quantum Information and Computation* 3, 193-202 (2003)

Recognizing entangled states

$$\|\tilde{\rho}\| > 1 \quad \Rightarrow \quad \rho \text{ is entangled}$$

sufficient criterion for entanglement

This criterion is strong enough to distinguish most of BES in the literature!

Examples

Distinguish completely

- d＝2 Werner state
- the Bell diagonal states
- isotropic states in arbitrary dimensions
- most of BES (PPT fails）

1. d＝2 Werner state

$$\rho = x|\Psi^-\rangle\langle\Psi^-| + (1-x)\frac{Id}{4}, 0 \le x \le 1$$

$$\rho = \begin{pmatrix} \frac{1-x}{4} & 0 & 0 & -\frac{x}{2} \\ 0 & \frac{1+x}{4} & 0 & 0 \\ 0 & 0 & \frac{1+x}{4} & 0 \\ -\frac{x}{2} & 0 & 0 & \frac{1-x}{4} \end{pmatrix},$$

ρ is entangled iff

$$\frac{1}{3} < x \le 1 \quad \Leftrightarrow \quad \|\tilde{\rho}\| > 1$$

Positive maps connected to entanglement witnesses (EW)

Jamiołkowski isomorphism

$$W_\Lambda = [I \otimes \Lambda](P_d^+)$$

$$P_d^+ = |\Phi_d^+\rangle\langle\Phi_d^+|$$

$$|\Phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle, \quad d = \dim \mathcal{H}_A$$

其中

$$\Lambda(|i\rangle\langle j|) = \langle i|W|j\rangle$$

不满足

$$(Id_A \otimes \Lambda)\rho \geq 0 \quad \Longrightarrow \quad \rho \text{ 纠缠的}$$

纠缠量化

Good entanglement measures

- 对于可分离态为0
- **No increase under LOCC**

$$E(\Lambda_{LOCC}(\varrho)) \leq E(\varrho)$$

- **Continuity**

$$E(\varrho) - E(\sigma) \to 0 \quad \text{for} \quad ||\varrho - \sigma|| \to 0$$

纠缠量化

Good entanglement measures

- **Convexity**

$$E(\lambda\varrho + (1-\lambda)\sigma) \leq \lambda E(\varrho) + (1-\lambda)E(\sigma)$$

- **Normalization**

$$E(P_+^d) = \log d$$

纯态纠缠度量

定义纯态的纠缠度量
Entropy of Entanglement

$$E(|\psi\rangle\langle\psi|) := S(\mathrm{tr}_A|\psi\rangle\langle\psi|) = S(\mathrm{tr}_B|\psi\rangle\langle\psi|)$$

其中

$$S(\rho) = -\mathrm{tr}[\rho \log_2 \rho]$$

为von-Neumann entropy

对于纯态 $E_D(\rho)$ and $E_C(\rho)$ are identical

混合态纠缠

定义混合态的量子纠缠度量

$$E(\varrho)=\inf\sum_i p_i E(\psi_i),\quad \sum_i p_i=1,\quad p_i\geqslant 0$$

$\{p_i,\psi_i\}$ 满足 $\varrho=\Sigma_i p_i|\psi_i\rangle\langle\psi_i|$

Uhlmann, 1998

纠缠最常用的度量Entanglement of F

$$E_F(\rho):=\inf\{\sum_i p_i E(|\psi_i\rangle\langle\psi_i|)\ :\ \rho=\sum_i p_i|\psi_i\rangle\langle\psi_i|\}$$

其中 $E(|\psi\rangle\langle\psi|)=S(\mathrm{tr}_B\{|\psi\rangle\langle\psi|\})$

Bennett, DiVincenzo, *et al.* 1996

Two qubits纠缠度量

定义纯态的concurrence

$$C=\sqrt{2(1-\mathrm{Tr}\rho^2)}$$

$$C(\psi)=2a_1a_2$$ 其中a_1,a_2为Schmidt系数

等价地

$$C=\langle\psi|\theta|\psi\rangle$$

$$\theta\psi=\sigma_y\otimes\sigma_y\psi^*$$

Hill and Wootters 1997

Two qubits纠缠度量

定义

$$\tilde{\rho} = \theta\rho\theta \qquad \omega = \sqrt{\rho}\sqrt{\tilde{\rho}}$$

则混合态的concurrence

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$$

其中$\lambda_1, \lambda_2, \lambda_3, \lambda_4$为$\omega$的以递减顺序排列的奇异值

则Entanglement of Formation (EoF)为

$$E_F(\rho) = H\left(\frac{1+\sqrt{1-C^2(\rho)}}{2}\right)$$

Wootters 1998

其中

$$H(x) = -x\log_2 x - (1-x)\log_2(1-x)$$

其它纠缠度量

Negativity

$$N(\rho) := \frac{||\rho^{T_B}|| - 1}{2}$$

其中 $||X|| := \mathrm{tr}\sqrt{X^\dagger X}$

或者Logarithmic Negativity

$$E_N(\rho) := \log_2 ||\rho^{T_B}||$$

均是Entanglement Monotones,但是后者非凸。

纠缠度量的一般构造
—Convex roof measures

混合态的纠缠度量

$$E(\varrho)=\inf\sum_i p_i E(\psi_i),\quad \sum_i p_i=1,\quad p_i\geqslant 0$$

Monotonicity under LOCC: Entanglement cannot increase under local operations and classical communication.

For any LOCC operation, we have

$$E(\Lambda(\rho))\leqslant E(\rho)$$

$$\Lambda(\rho)=\sum_i A_i\otimes B_i(\rho)A_i^{\dagger}\otimes B_i^{\dagger}$$

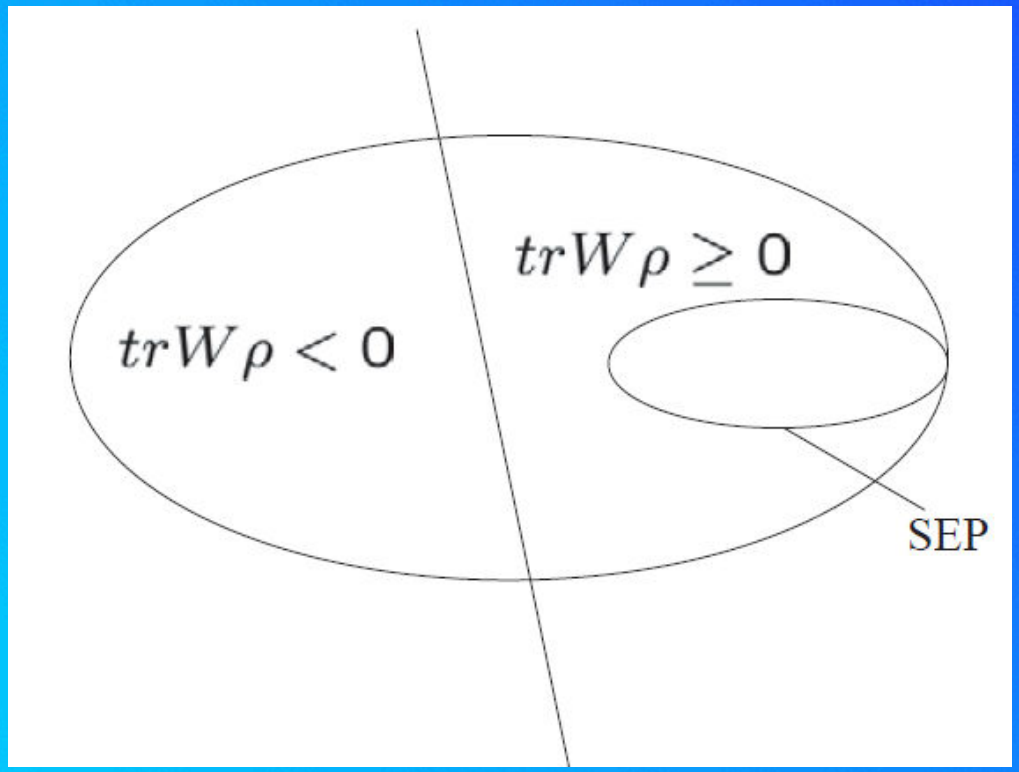
Entanglement Witness Monotones

Entanglement Witness

$$\forall\ \rho \in SEP \qquad \mathrm{tr}\{W\rho\} \geq 0$$

$$and$$

$$\exists \rho \ \text{s.t.} \qquad \mathrm{tr}\{W\rho\} < 0.$$



定义度量

$$E_{wit}(W) = \max\{0, -\mathrm{tr}\{W\rho\}\}$$

纠缠度量大小如何计算？

推广的Concurrence

$$C(|\psi\rangle) = \sqrt{2(1 - \mathrm{Tr}\rho_A^2)}$$

$$C(\rho) \equiv \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i C(|\psi_i\rangle)$$

纯态

$$|\psi\rangle = \sum_i \sqrt{\mu_i}\, |a_i b_i\rangle$$

$$C^2(|\psi\rangle) = 2\left(1 - \sum_i \mu_i^2\right) = 4\sum_{i<j} \mu_i \mu_j$$

where $\sqrt{\mu_i}\ (i = 1, \ldots, m)$ are the Schmidt coefficients

结论

Theorem.—For any $m \otimes n (m \leq n)$ mixed quantum state ρ, the concurrence $C(\rho)$ satisfies

$$C(\rho) \geq \sqrt{\frac{2}{m(m-1)}} (\max(\|\rho^{T_A}\|, \|\mathcal{R}(\rho)\|) - 1).$$

K. Chen, S. Albeverio, S.M. Fei, Phys. Rev. Lett. 95 (2005) 040504

Shannon entropy

Operationally as the minimum number of bits needed to communicate a message produced by a classical statistical source associated to a random variable X.

- *The Shannon entropy of X quantifies how much information we gain, on average, when we learn the value of X.*
- *The entropy of X measures the amount of uncertainty about X before we learn its value.*

Shannon entropy

A measure of our uncertainty before we learn the value of X

A measure of how much information we have gained after we learn the value of X.

$$H(X) \equiv H(p_1, \ldots, p_n) \equiv -\sum_x p_x \log p_x$$

Shannon's noiseless coding theorem:

It can be used to quantify the resources needed to store information

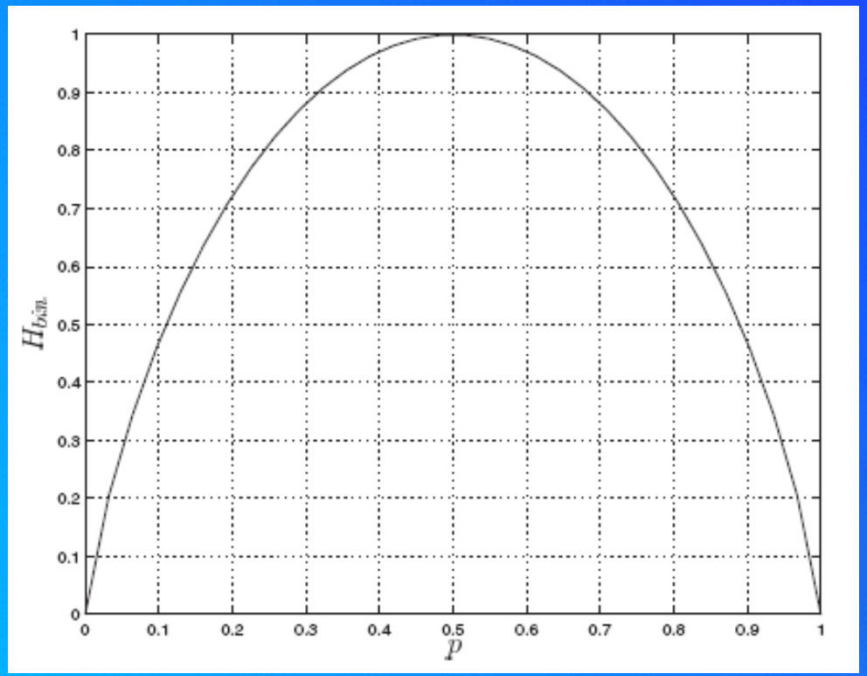
熵的基本性质

定义binary entropy

$$H_{\text{bin}}(p) \equiv -p \log p - (1-p) \log(1-p)$$

concavity

$$H(qp_{\text{U}} + (1-q)p_{\text{A}}) \geq qH(p_{\text{U}}) + (1-q)H(p_{\text{A}})$$



熵的变体

Joint entropy

$$H(X,Y) \equiv -\sum_{x,y} p(x,y) \log p(x,y)$$

The joint entropy measures our total uncertainty about the pair (X, Y).

Conditional entropy

$$H(X|Y) \equiv H(X,Y) - H(Y)$$

A measure of how uncertain we are, on average, about the value of X, given that we know the value of Y.

熵的变体

Mutual information

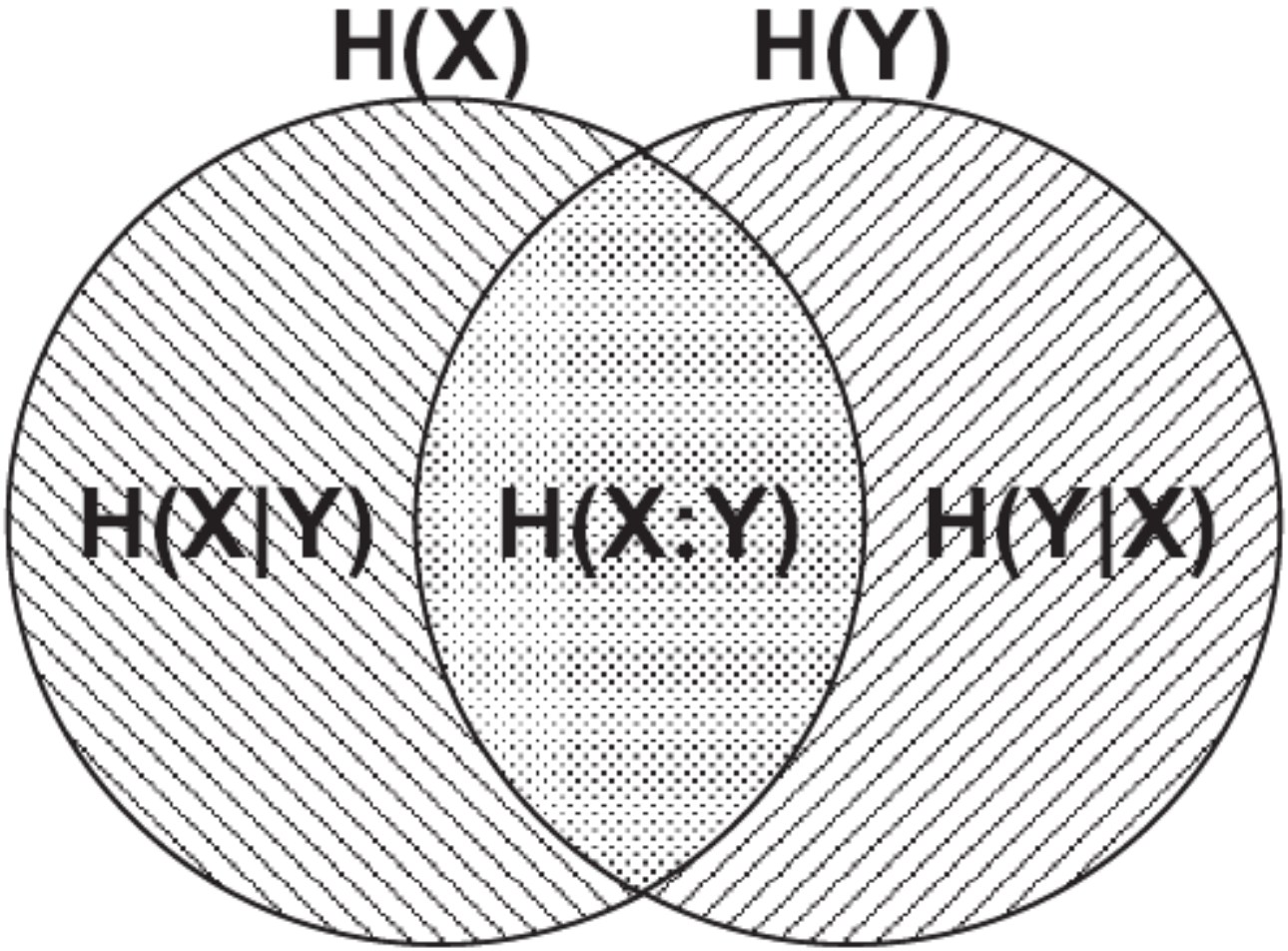
$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y)$$

Measuring how much information X and Y have in common.

Useful equality

$$H(X:Y) = H(X) - H(X|Y)$$

Shannon系列熵关系图



Von Neumann entropy

$$S(\rho) = -\mathrm{tr}[\rho \log_2 \rho]$$

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x$$

λ_x are the eigenvalues of ρ

Relative entropy

$$S(\rho||\sigma) \equiv \mathrm{tr}(\rho \log \rho) - \mathrm{tr}(\rho \log \sigma)$$

Von Neumann entropy和测量

A projective measurement described by projectors P_i

则有

$$\rho' = \sum_i P_i \rho P_i$$

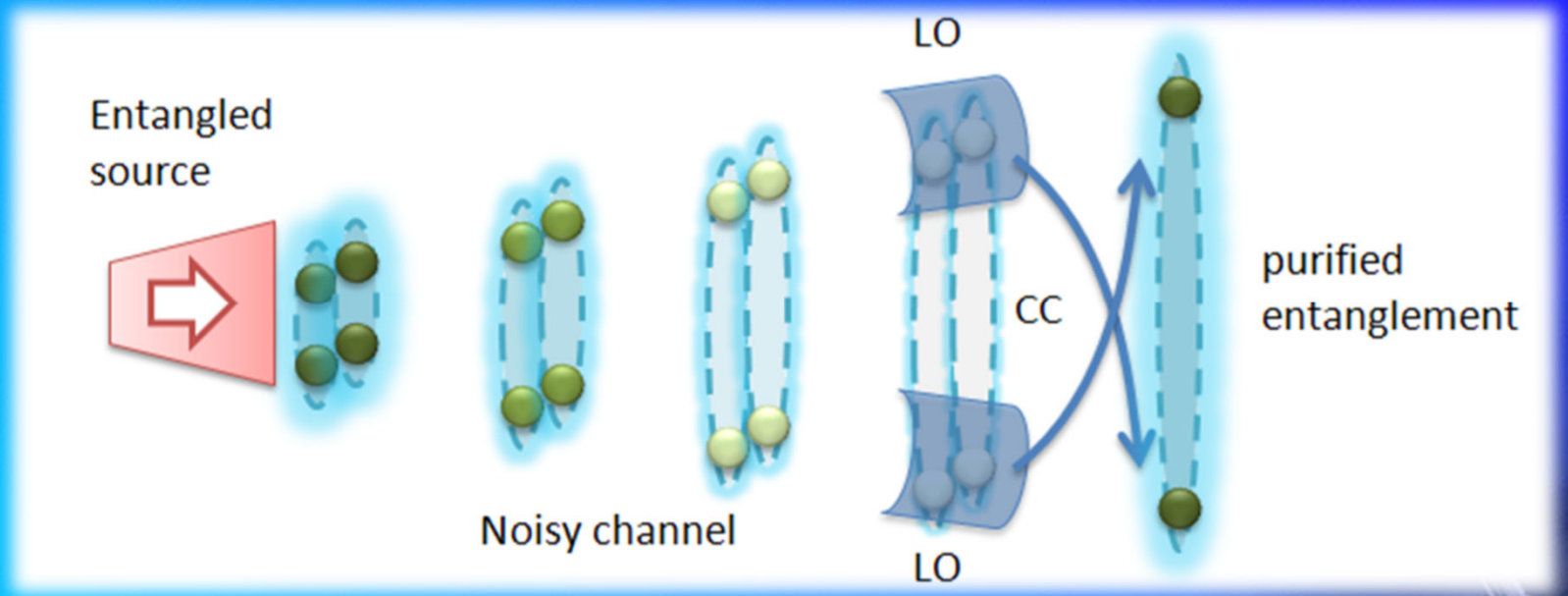
The system after the measurement is at least as great as the original entropy

$$S(\rho') \geq S(\rho)$$

with equality if and only if $\rho = \rho$.

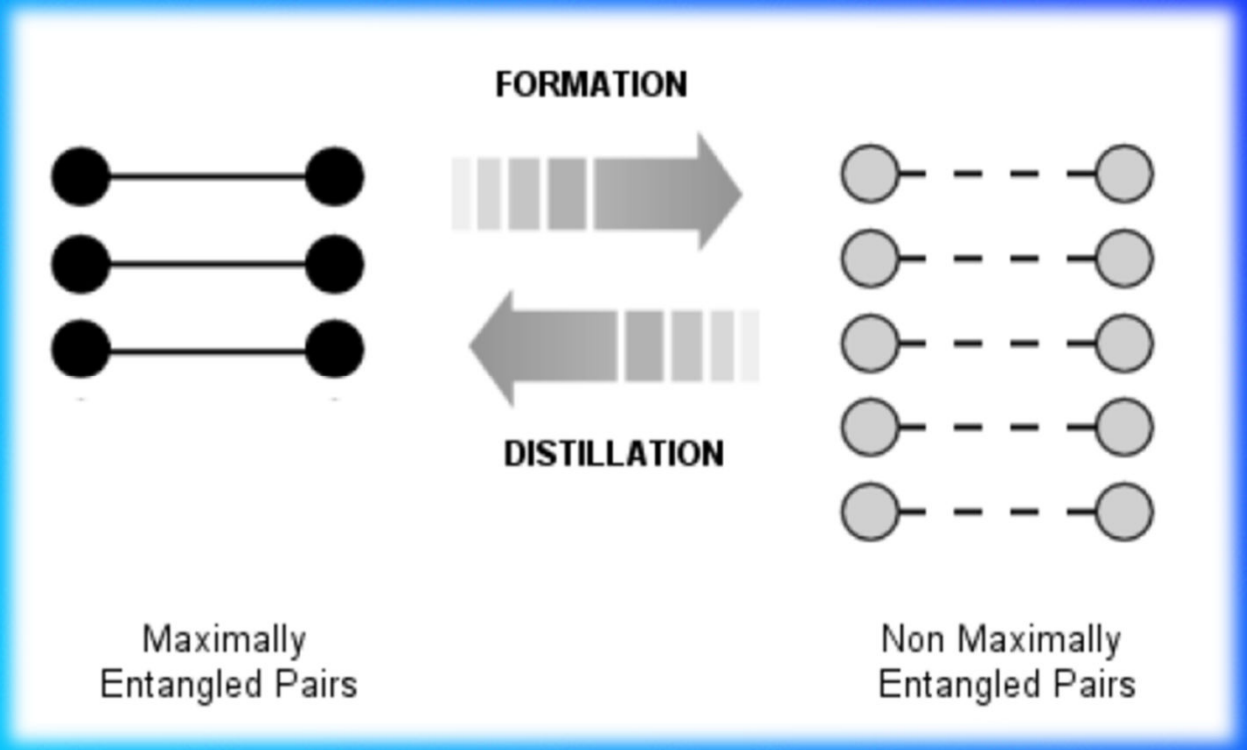
Entanglement distillation

- 应用LOCC操作 (局域操作和经典通信)
  - 利用一对或者多对纠缠资源
  - 牺牲一部分纠缠资源
- 在噪声信道分发和长距离的量子通信后



Entanglement distillation

A certain number of maximally entangled EPR pairs is manipulated by local operations and classical communication and converted into pairs in some state. The asymptotic conversion rate is known as the entanglement of formation.



Vlatko Vedral, Introduction to Quantum Information Science, Oxford University Press, 2006

The converse of formation is the distillation of entanglement. The asymptotic rate of conversion of pairs in the state into maximally entangled states is known as the entanglement of distillation.

纠缠提纯方法

One-way hashing distillation protocol

Bell diagonal states B_{diag} are naturally parametrized by the probability distribution of mixing p.

$$E_D(\rho_{B\,\text{diag}}) \geqslant 1 - H(\{p\})$$

The n copies of the two-qubit Bell diagonal state Bdiag can be viewed as a classical mixture of strings of n Bell states. Typically, there are only about $2^{nH(\{p\})}$ such strings that are likely to occur (Cover and Thomas, 1991).

纠缠提纯方法

Two-way recurrence distillation protocol

Two-step procedure:

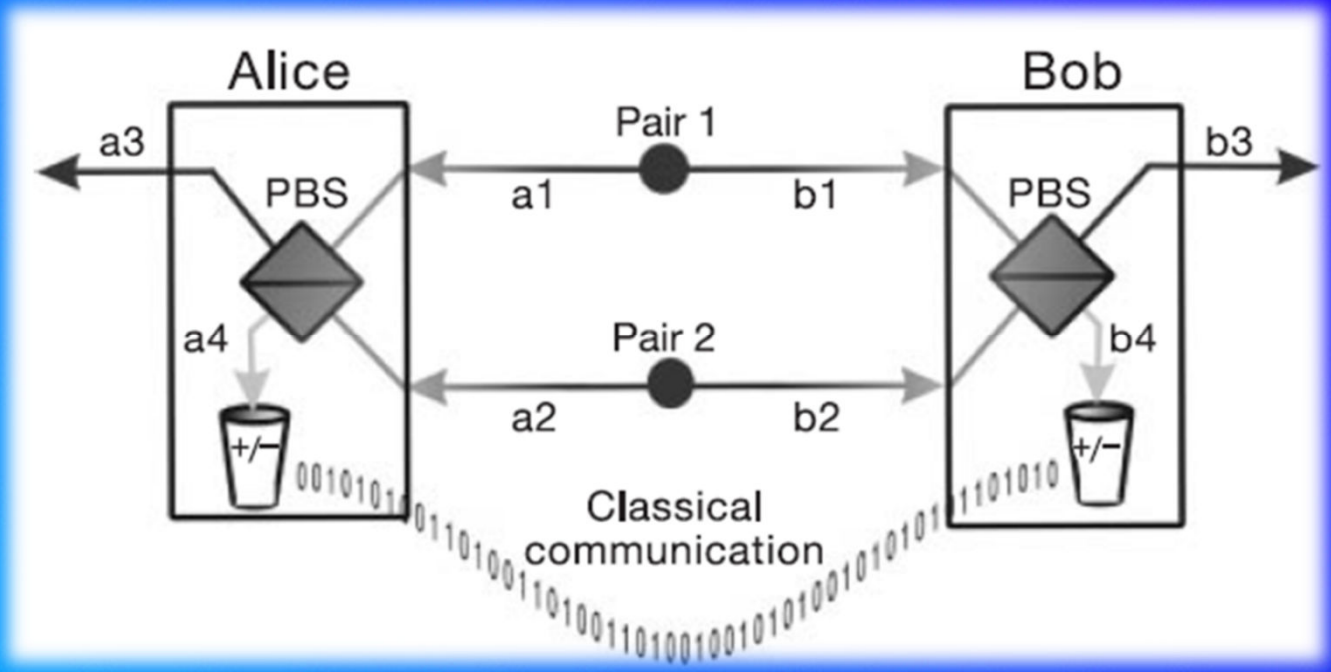
- In the first step Alice and Bob take two pairs, and apply locally a controlled NOT gate. Then they measure the target pair in a bit basis. If the outcomes are different they discard the source pair failure, otherwise they keep it.
- In the latter case, a second step can be applied: they twirl the source pair to the Werner state.

$$F'(F) = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}$$

$$F = \mathrm{Tr}\ \rho |\phi^+\rangle\langle\phi^+|$$

If only $F>1/2$, the above recursive map converges to 1 for a sufficiently large initial number of copies.

纯化纠缠实验



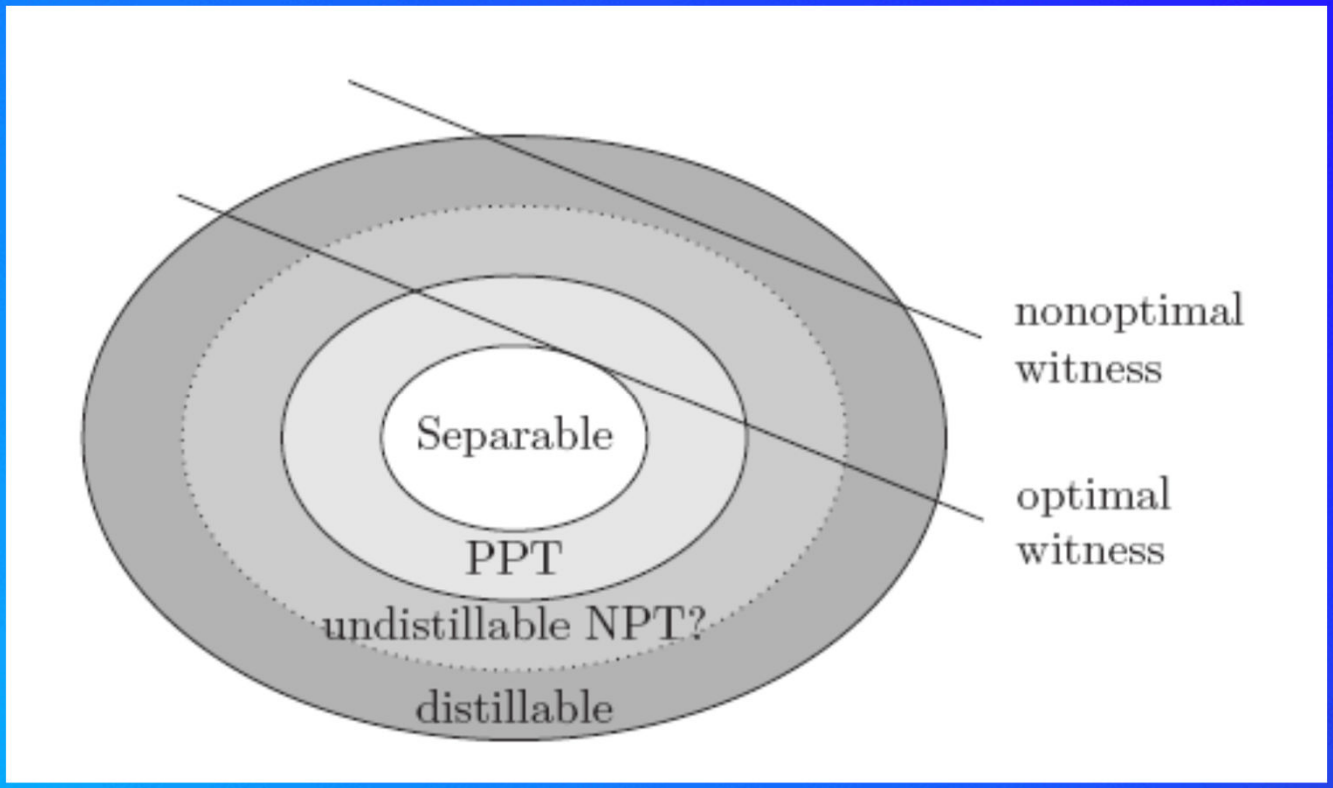
$$\rho_{ab} = F|\Phi^+\rangle_{ab}\langle\Phi^+| + (1-F)|\Psi^-\rangle_{ab}\langle\Psi^-|$$

$$|\Phi^\pm\rangle_{ab} = \frac{1}{\sqrt{2}}(|H\rangle_a|H\rangle_b \pm |V\rangle_a|V\rangle_b)$$

$$|\Psi^\pm\rangle_{ab} = \frac{1}{\sqrt{2}}(|H\rangle_a|V\rangle_b \pm |V\rangle_a|H\rangle_b)$$

Jian-Wei Pan *et al.* Nature 423, 417 (2003)

纠缠提纯总结



- 所有两比特纠缠态可提纯
- 需要发展更好的可提纯协议
- One-way and two-way
- 多个copies

Bell不等式

$$|E(A_1,B_1)+E(A_1,B_2)+E(A_2,B_1)-E(A_2,B_2)|\leqslant 2$$

$E(A_i,B_j)$ is the expectation value of the correlation experiment A_i,B_j.

$$|\mathrm{Tr}(\mathcal{B}_{\mathrm{CHSH}}\rho)|\leqslant 2$$

$$\mathcal{B}_{\mathrm{CHSH}}=\mathbf{A}_1\otimes(\mathbf{B}_1+\mathbf{B}_2)+\mathbf{A}_2\otimes(\mathbf{B}_1-\mathbf{B}_2)$$

$$\mathbf{A}_1=\mathbf{a}_1\cdot\sigma,\ \mathbf{A}_2=\mathbf{a}_2\cdot\sigma\ (\text{similarly for } \mathbf{B}_1 \text{ and } \mathbf{B}_2)$$

Quantum formalism predicts the Cirel'son inequality (Cirel'son, 1980)

$$|\langle\mathcal{B}_{\mathrm{CHSH}}\rangle_{QM}|=|\mathrm{Tr}(\mathcal{B}_{\mathrm{CHSH}}\rho)|\leqslant 2\sqrt{2}$$

Bell不等式

Bell made two key assumptions:

1. *Each measurement reveals an objective physical property of the system. This means that the particle had some value of this property before the measurement was made, just as in classical physics. This value may be unknown to us (just as it is in statistical mechanics), but it is certainly there.*

2. *A measurement made by Alice has no effect on a measurement made by Bob and vice versa. This comes from the theory of relativity, which requires that any signal has to propagate at the (finite) speed of light.*

纯态和Bell不等式

$$\left|\psi^{AB}\right\rangle = a\left|00\right\rangle + b\left|11\right\rangle$$

$$\left|\psi^{AB}\right\rangle = a(\left|00\right\rangle + \left|11\right\rangle) + (b-a)\left|11\right\rangle$$

引入幺正变换和辅助量子态

$$|0^A\rangle|\psi^{AB}\rangle$$

$$\begin{aligned} U^A|0\rangle|0\rangle &= |0\rangle|0\rangle\,, \\ U^A|0\rangle|1\rangle &= \alpha|0\rangle|1\rangle + \beta|1\rangle|0\rangle \end{aligned}$$

混合态和Bell不等式

Mixed states may not violate Bell's inequalities

The Werner states are defined as mixtures of Bell states, where the degree of mixing is determined by a parameter F (which really stands for "fidelity"):

$$\varrho_{\mathrm{W}} = F|\Psi^-\rangle\langle\Psi^-| + \frac{1-F}{3}(|\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|)$$

where $0 \le F \le 1$. When $F = 1/2$, we can write it as

$$\begin{aligned}\varrho_{\mathrm{W}} &= \frac{1}{6}(|\Psi^-\rangle\langle\Psi^-| + |\Psi^+\rangle\langle\Psi^+|) + \frac{1}{6}(|\Psi^-\rangle\langle\Psi^-| + |\Phi^+\rangle\langle\Phi^+|) \\ &+ \frac{1}{6}(|\Psi^-\rangle\langle\Psi^-| + |\Phi^-\rangle\langle\Phi^-|)\end{aligned}$$

混合态和Bell不等式

Mixed states may not violate Bell's inequalities

The Werner states for F=1/2 is separable.

An equal mixture of any two maximally entangled states is a separable state.

$$(1/2)(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|)$$

is equivalent to

$$(1/2)(|00\rangle\langle 00| + |11\rangle\langle 11|)$$

The Werner states are entangled for F > ½,
The Werner states violates Bell's inequalities when F > 0.78.

Bell不等式检验: two-qubit

An 2-qubit state can be written as

$$\varrho = \frac{1}{4}\left(I \otimes I + \boldsymbol{r}\cdot\boldsymbol{\sigma} \otimes I + I \otimes \boldsymbol{s}\cdot\boldsymbol{\sigma} + \sum_{n,m=1}^{3} t_{nm}\sigma_n \otimes \sigma_m \right)$$

$$\mathcal{B}_{\mathrm{CHSH}} = \hat{\boldsymbol{a}}\cdot\boldsymbol{\sigma} \otimes (\hat{\boldsymbol{b}} + \hat{\boldsymbol{b}}')\cdot\boldsymbol{\sigma} + \hat{\boldsymbol{a}}'\cdot\boldsymbol{\sigma} \otimes (\hat{\boldsymbol{b}} - \hat{\boldsymbol{b}}')\cdot\boldsymbol{\sigma}$$

$$|\langle \mathcal{B}_{\mathrm{CHSH}} \rangle_\varrho| \leqslant 2$$

One has

$$2\sqrt{M(\varrho)} = \langle \mathcal{B}_{\max} \rangle_\varrho = \max_{\mathcal{B}_{\mathrm{CHSH}}} |\langle \mathcal{B}_{\mathrm{CHSH}} \rangle_\varrho|$$

$$M(\varrho) := \max_{\hat{\boldsymbol{c}},\hat{\boldsymbol{c}}'} (\|T_\varrho \hat{\boldsymbol{c}}\|^2 + \|T_\varrho \hat{\boldsymbol{c}}'\|^2) = u + \tilde{u}$$

Here u and ũ are the two largest eigenvalues of $T^T{}_\rho T_\rho$

Horodecki, R.; Horodecki, P.; Horodecki, M.
Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition,
Physics Letters A, Volume 200, Issue 5, May 1995, Pages 340-344

Bell's theorem without inequalities

$$|\Psi\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B |0\rangle_E - |1\rangle_A |1\rangle_B |1\rangle_E\right)$$

$$\begin{aligned}
X_A \otimes X_B \otimes X_E |\Psi\rangle_{\mathrm{GHZ}} &= -|\Psi\rangle_{\mathrm{GHZ}}, \\
X_A \otimes Y_B \otimes Y_E |\Psi\rangle_{\mathrm{GHZ}} &= |\Psi\rangle_{\mathrm{GHZ}}, \\
Y_A \otimes X_B \otimes Y_E |\Psi\rangle_{\mathrm{GHZ}} &= |\Psi\rangle_{\mathrm{GHZ}}, \\
Y_A \otimes Y_B \otimes X_E |\Psi\rangle_{\mathrm{GHZ}} &= |\Psi\rangle_{\mathrm{GHZ}}.
\end{aligned}$$

$$\begin{aligned}
x_A x_B x_E &= -1, \\
x_A y_B y_E &= +1, \\
y_A x_B y_E &= +1, \\
y_A y_B x_E &= +1.
\end{aligned}$$

But these relations are not mutually consistent!

Bell test

Correlation functions

$$E(a_i, b_j) = \langle \psi | \vec{\sigma} \cdot \hat{n}_{a_i} \otimes \vec{\sigma} \cdot \hat{n}_{b_j} | \psi \rangle$$

For a maximally entangled state $|\psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$

$$E(a_i, b_j) = -\cos\theta_{a_i b_j} = -\cos(\theta_i^a - \theta_j^b)$$

With appropriate angles $\theta_1^a = \frac{\pi}{2}, \theta_2^a = 0, \ \theta_1^b = \frac{\pi}{4}, \theta_2^b = \frac{3\pi}{4}$

Bell test

$$E_{11}(\theta_1^a,\theta_1^b)=-\cos(\theta_1^a-\theta_1^b)=-\cos\frac{\pi}{4}=-\frac{1}{\sqrt{2}}$$

$$E_{12}(\theta_1^a,\theta_2^b)=-\cos(\theta_1^a-\theta_2^b)=-\cos\left(-\frac{\pi}{4}\right)=-\frac{1}{\sqrt{2}}$$

$$E_{21}(\theta_2^a,\theta_1^b)=-\cos(\theta_2^a-\theta_1^b)=-\cos\left(-\frac{\pi}{4}\right)=-\frac{1}{\sqrt{2}}$$

$$E_{22}(\theta_2^a,\theta_2^b)=-\cos(\theta_2^a-\theta_2^b)=-\cos\left(-\frac{3\pi}{4}\right)=\frac{1}{\sqrt{2}}$$

$$E_{11}+E_{12}+E_{21}-E_{22}=-2\sqrt{2}$$

One verifies that the CHSH inequality is violated!

Bohr-Einstein debates

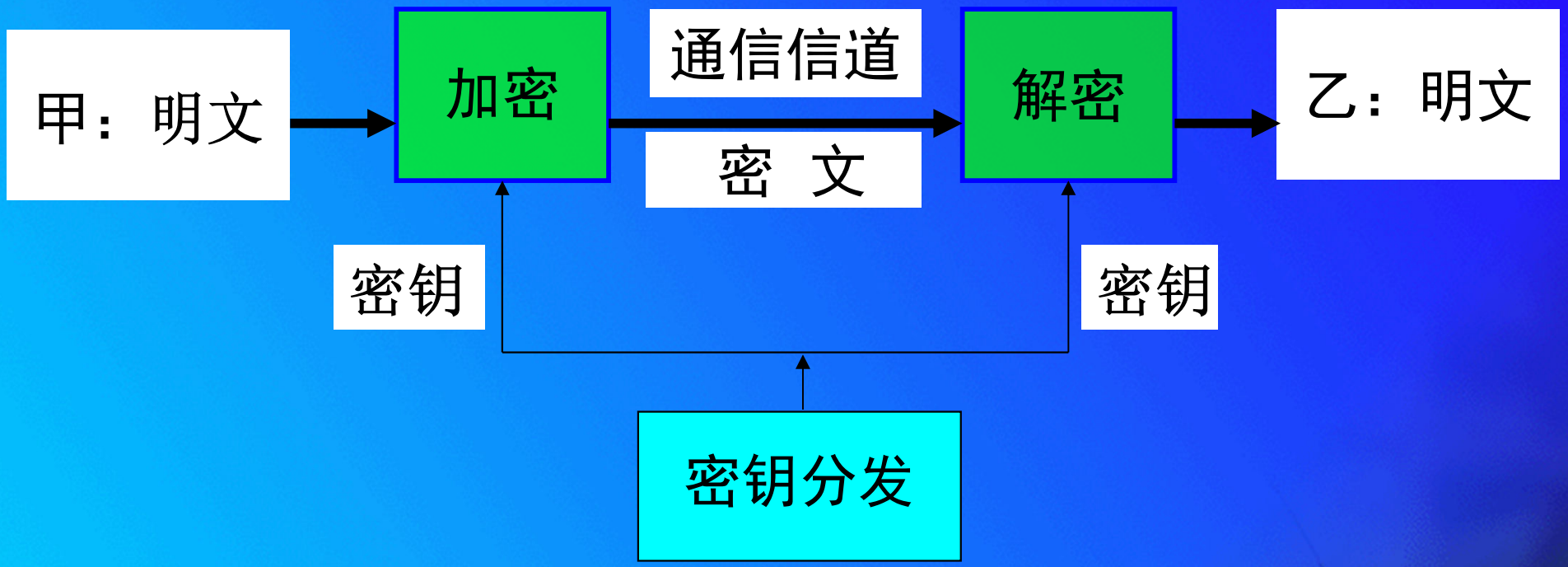
Einstein:

I can't believe God plays dice with the universe.

Bohr:

Albert, stop telling God what to do.

常规保密通信体系

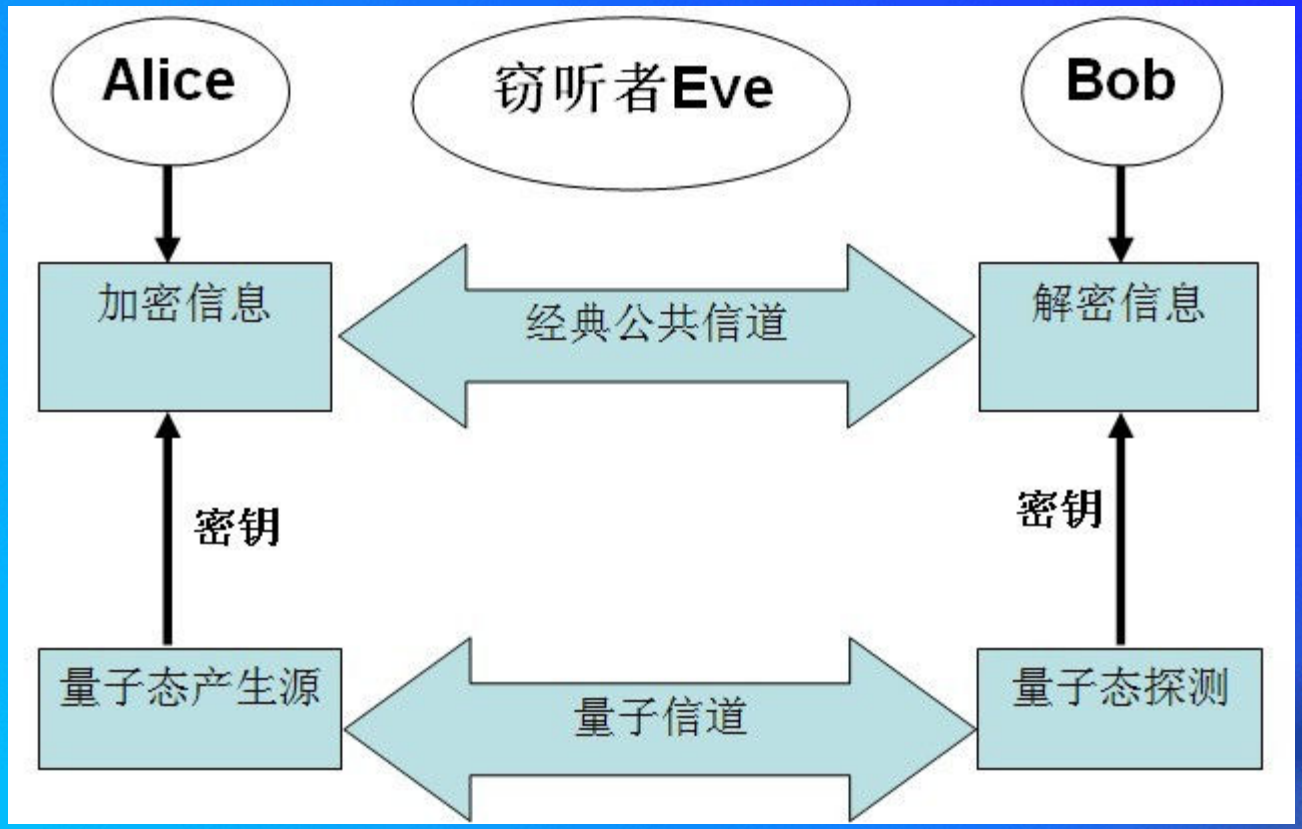


保密原理：系统保密性完全依赖于密钥的安全性，
不依赖于加密体制或算法

然而现有的保密通信体系不存在无条件安全的方案来分发密钥！

量子密钥分发

基于量子力学原理，1984年Bennett和Brassard在印度举行的一个IEEE会议上提出了世界上第一个量子密钥分发协议，俗称BB84协议



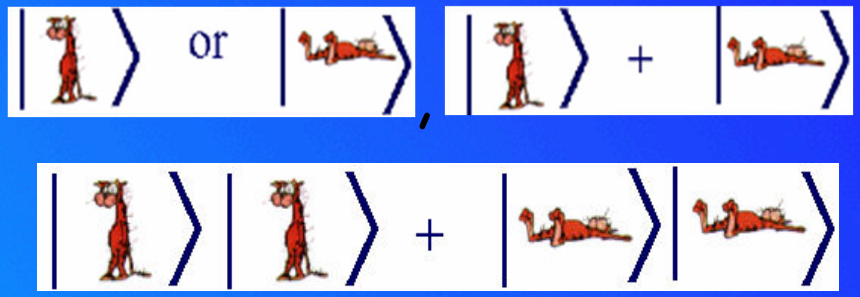
BB84协议示意图

What is QKD?

- Quantum Key Distribution is simultaneous generation of identical bit sequences in two distinct locations with quantum physical methods
- Quantum technology guarantees unconditional security
- QKD enables the implementation of a perfectly secure secret channel

量子密钥分配保密原理

量子态的相干叠加



单光子量子态不可克隆原理

未知量子态

$|\psi\rangle$

X 不可能的

复制到
另一量子体系

在不破坏原来量子态的前提下

单光子是安全的，不可分割，也不可克隆！

量子密钥分发安全性

窃听方式：截取　　单光子不可分割

甲方 ⟶ ⇢ 乙方

被窃取光子
不产生密钥

无条件安全
密钥分发
依然可以
完成

甲方 ⟶ ⟶ 乙方

窃听方式：“复制”
再分发

单光子不可克隆

被复制光子
不产生密钥

- 实现了无条件安全密钥分发的物理通道
- 彻底解决了经典密钥分发体系的安全漏洞

Quantum key distribution

A protocol that enables Alice and Bob to set up a secure secret key, provided that they have:

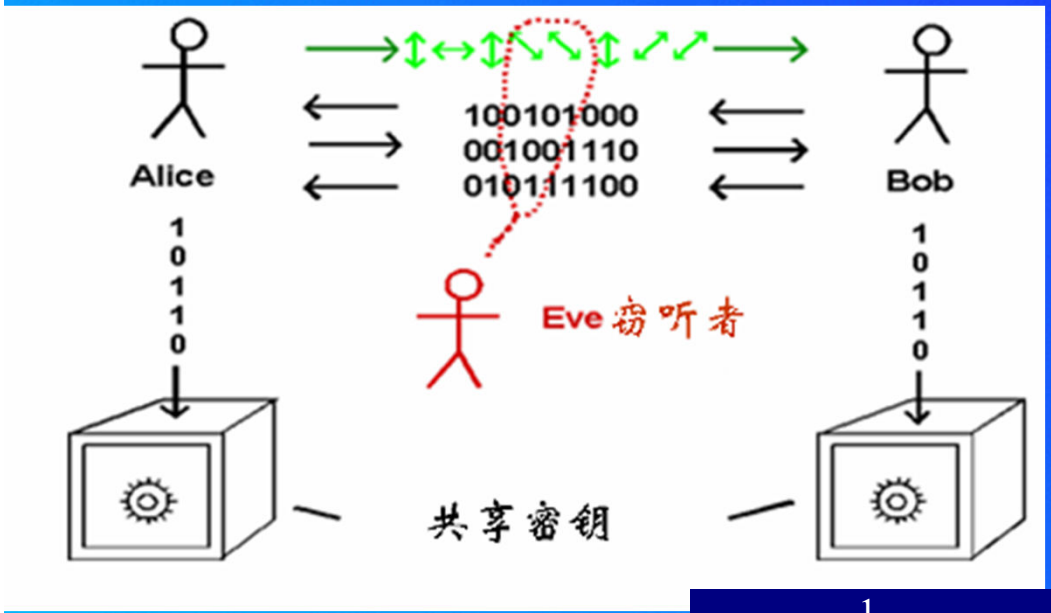
- A ***quantum channel***, where Eve can read and modify messages
- An ***authenticated classical channel***, where Eve can read messages, but cannot tamper with them (the authenticated classical channel can be simulated by Alice and Bob having a ***very short*** classical secret key)

BB84协议执行流程

The BB84 QKD protocol

1: Alice chooses $(4+\delta)n$ random data bits.
2: Alice chooses a random $(4+\delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.
3: Alice sends the resulting state to Bob.
4: Bob receives the $(4+\delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis at random.
5: Alice announces b.
6: Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.
7: Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8: Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
9: Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

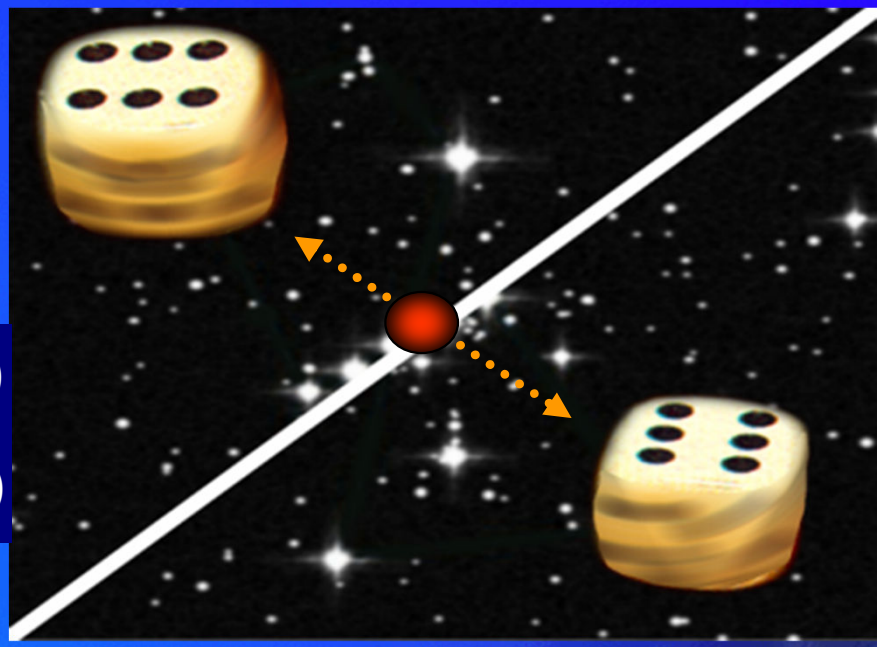
量子通信技术:量子加密术



无条件安全的密钥生成

纠缠态方案

Ekert, PRL 67, 661 (1991)



单粒子方案

Bennett & Brassard (1984)

$$|\Phi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2\pm|\updownarrow\rangle_1|\updownarrow\rangle_2\right)$$

$$|\Psi^{\pm}\rangle_{12}=\frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_1|\updownarrow\rangle_2\pm|\updownarrow\rangle_1|\leftrightarrow\rangle_2\right)$$

量子不可克隆定理

量子不可分割

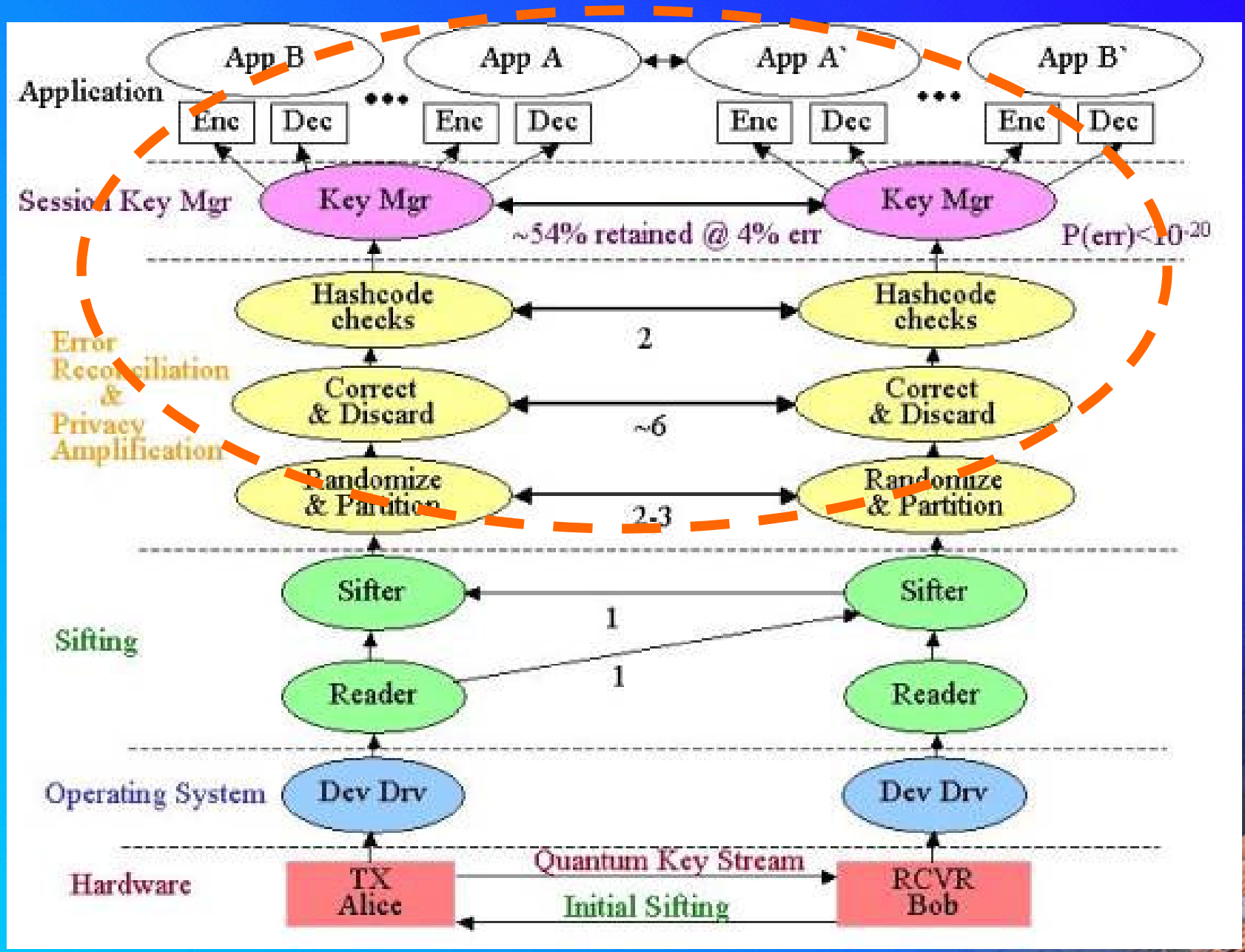
一次一密，完全随机

无条件安全

Distillation procedure of secure keys

- real-time data acquisition
- key sifting
- error estimation
- error detection and correction (reconciliation) one-way, two-way
- privacy amplification

NIST QKD Protocol Stack



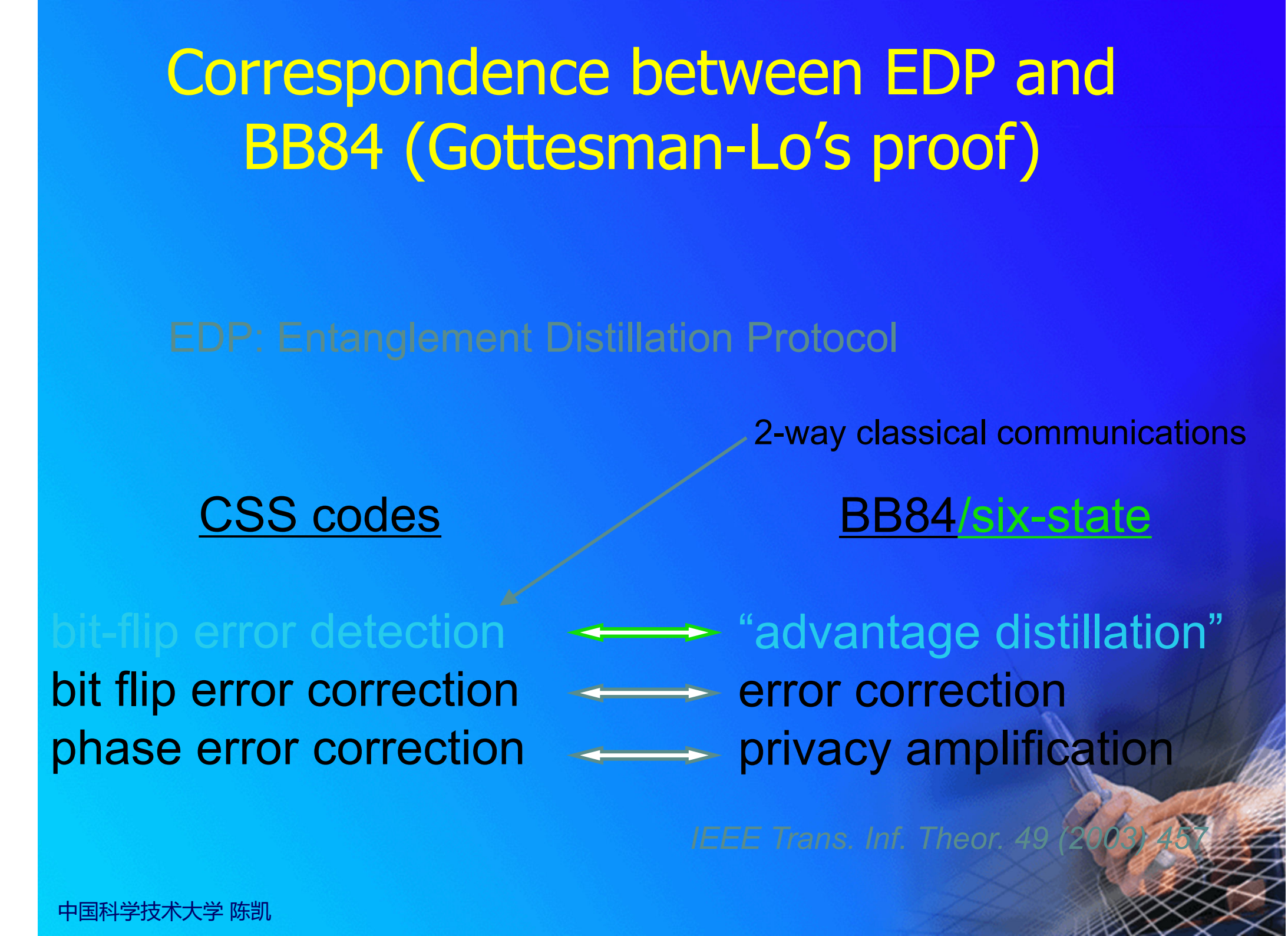
Correspondence between EDP and BB84 (Gottesman-Lo's proof)

EDP: Entanglement Distillation Protocol

2-way classical communications

CSS codes		BB84/six-state
bit-flip error detection	⟺	"advantage distillation"
bit flip error correction	⟺	error correction
phase error correction	⟺	privacy amplification

IEEE Trans. Inf. Theor. 49 (2003) 457



Quantum Distribution of Keys

- Produces raw classical key
- Observed error rate indicates amount of eavesdropper information and channel noise
- Error-correction is used to fix errors
- Random hash function is used to distill a smaller secret classical key

GLLP Formula for key generation rate

$$S \geq \tfrac{1}{2}\{-Q_\mu \cdot f(E_\mu) \cdot H_2(E_\mu) + Q_1 \cdot [1 - H_2(e_1)]$$

Error correction | Privacy amplification

Q_μ is total # of detection events of signals.

E_μ is overall bit error rate of signals.

Q_1 is # of detection events due to single photon states.

e_1 is the bit error rate for single photon state.

$f(e) \geq 1$ is the error correction efficiency.

To prove security, one needs to lower bound Q_1 and upper bound e_1.

GLLP: D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Information and Computation. **4** (5) 2004 325-360, quant-ph/0212066

Combining Decoy with GLLP

$$S \geq \tfrac{1}{2}\{-Q_{Signal} \cdot f(E_{Signal}) \cdot H_2(E_{Signal}) + Q_1 \cdot [1 - H_2(e_1)]\}$$

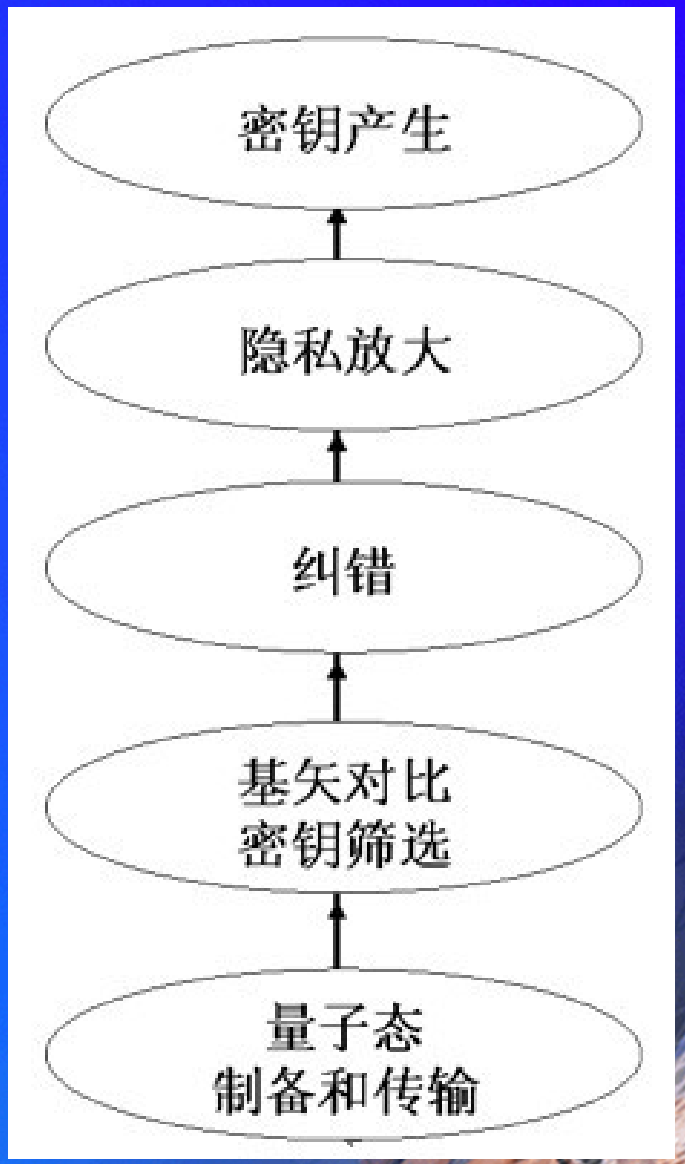
Error correction　　Privacy amplification

- With the knowledge of yields $\{Y_n\}$, Alice can choose a much higher average photon number $\mu = O(1)$.
- Key generation rate $R = O(\eta)$ ☺

η : transmittance ~ 10^{-3}

QKD Protocols

- Sifting –Unmatched Bases; “stray” or “lost” qubits
- Error Correction – Noise & Eaves-dropping detected – Uses “cascade” protocol – Reveals information to Eve so need to track this.
- Privacy Amplification – reduces Eve’s knowledge obtained by previous EC
- Authentication – Continuous to avoid man-in-middle attacks – not required to initiate using shared keys



BOUNDS ON THE BIT ERROR RATE FOR BB84 AND THE SIX-STATE SCHEME

TABLE I

BOUNDS ON THE BIT ERROR RATE FOR BB84 AND THE SIX-STATE SCHEME USING ONE-WAY AND TWO-WAY CLASSICAL POST-PROCESSING. THE LOWER BOUNDS FOR TWO-WAY POST-PROCESSING, 18.9% FOR BB84 AND 26.4% FOR THE SIX-STATE SCHEME, COME FROM THE CURRENT WORK

BB84

	one-way	two-way
Upper bound	14.6%	1/4
Lower bound	11.0%	18.9%

Six-state Scheme

	one-way	two-way
Upper bound	1/6	1/3
Lower bound	12.7%	26.4%

Daniel Gottesman and Hoi-Kwong Lo, Proof of Security of Quantum Key Distribution With Two-Way Classical Communications, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 49, 457-475 (2003)

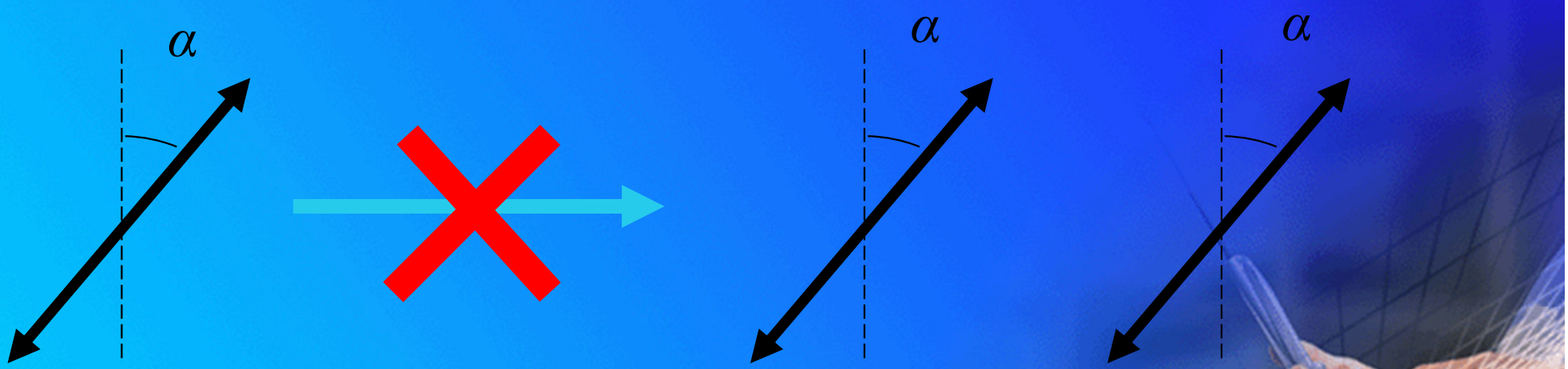
Decoy-state quantum key distribution with both source errors and statistical fluctuations

Xiang-Bin Wang, C.-Z. Peng, J. Zhang, L. Yang, Jian-Wei Pan
General theory of decoy-state quantum cryptography with source errors
Phys. Rev. A 77, 042311 (2008)

Xiang-Bin Wang, Lin Yang, Cheng-Zhi Peng, Jian-Wei Pan, Decoy-state quantum key distribution with both source errors and statistical fluctuations, New. J. Phys., 11, 075006 (2009)

量子不可克隆定理

- 任意量子态不能被精确克隆。因此窃听者不能够获取到和接收方同样的信息。
- 单光子信号是安全的



不可能的

QUANTUM TELEPORTATION

Teleportation of unknown quantum state encompasses the complete transfer of information from one particle to another

Unknown quantum state

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

EPR source

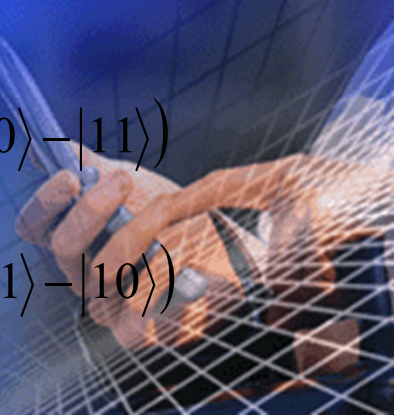
$$|EPR-pair\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Total state

$$|\psi\rangle|EPR-pair\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right)$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$



QUANTUM TELEPORTATION

The joint state of three particles

$$|\psi\rangle|EPR-pair\rangle=\frac{1}{\sqrt{2}}\left(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle\right)$$

can be rephrased as follows:

$$|\psi\rangle|EPR-pair\rangle=|\Phi^{+}\rangle\frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)+|\Psi^{+}\rangle\frac{1}{\sqrt{2}}\left(\beta|0\rangle+\alpha|1\rangle\right)$$

$$+|\Phi^{-}\rangle\frac{1}{\sqrt{2}}\left(\alpha|0\rangle-\beta|1\rangle\right)+|\Psi^{-}\rangle\frac{1}{\sqrt{2}}\left(-\beta|0\rangle+\alpha|1\rangle\right)$$

Therefore Bell measurements on the first two particles would project the state of Bob's particle into a variant of $|\psi_1\rangle$ of the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where

$|\psi_1\rangle$ = either $|\psi\rangle$ or $\sigma_x|\psi\rangle$ or $\sigma_z|\psi\rangle$ or $\sigma_x\sigma_z|\psi\rangle$

The unknown state $|\psi\rangle$ can therefore be obtained from $|\psi_1\rangle$ by applying one of the four operations

$$I, \sigma_x, \sigma_y, \sigma_z,$$

and the result of the Bell measurement provides two bits specifying which of the above four operations should be applied.

Alice can send to Bob these two bits of classical information using a classical channel (by phone, email for example).

Entanglement Swapping: Entangling Photons That Never Interacted

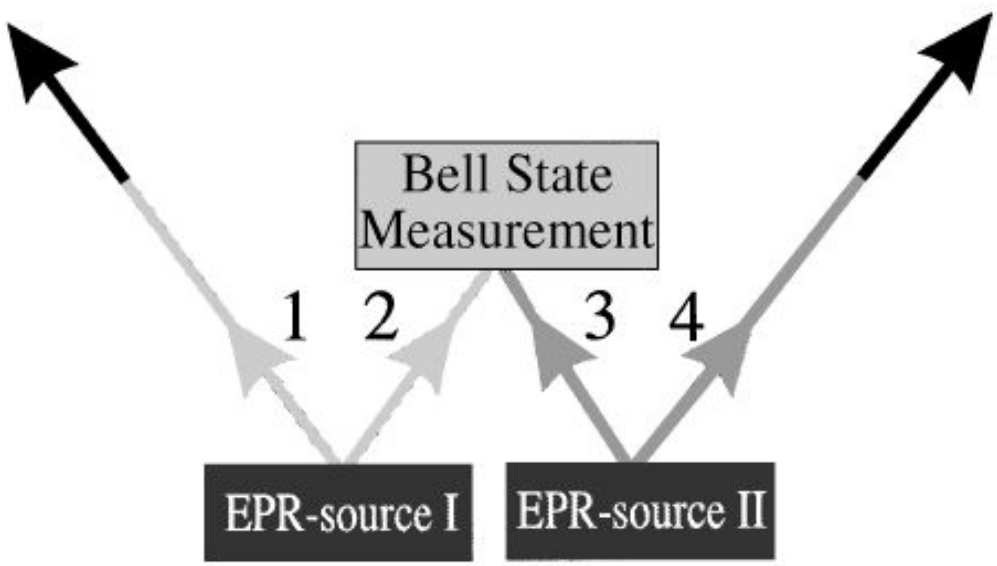


FIG. 1. Principle of entanglement swapping. Two EPR sources produce two pairs of entangled photons, pair 1-2 and pair 3-4. One photon from each pair (photons 2 and 3) is subjected to a Bell-state measurement. This results in projecting the other two outgoing photons 1 and 4 onto an entangled state. Change of the shading of the lines indicates the change in the set of possible predictions that can be made.

Jian-Wei Pan *et al.*, Phys. Rev. Lett. 80, 3891-3894 (1998)

Entanglement Swapping: Entangling Photons That Never Interacted

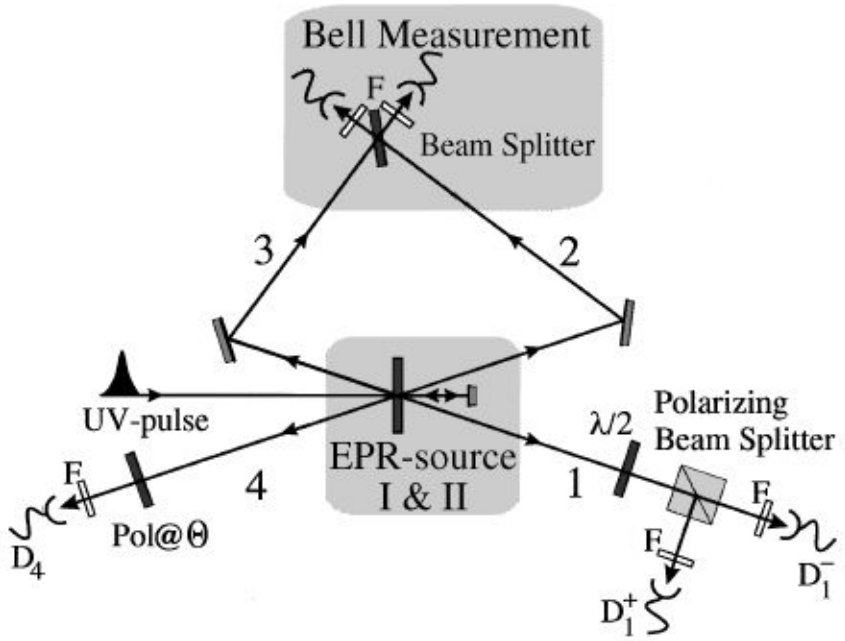


FIG. 2. Experimental setup. A UV pulse passing through a nonlinear crystal creates pair 1-2 of entangled photons. Photon 2 is directed to the beam splitter. After reflection, during its second passage through the crystal the UV pulse creates a second pair 3-4 of entangled photons. Photon 3 will also be directed to the beam splitter. When photons 2 and 3 yield a coincidence click at the two detectors behind the beam splitter, they are projected into the $|\Psi^-\rangle_{23}$ state. As a consequence of this Bell-state measurement the two remaining photons 1 and 4 will also be projected into an entangled state. To analyze their entanglement we look at coincidences between detectors D_1^+ and D_4, and between detectors D_1^- and D_4, for different polarization angles Θ. By rotating the $\lambda/2$ plate in front of the two-channel polarizer we can analyze photon 1 in any linear polarization basis. Note that, since the detection of coincidences between detectors D_1^+ and D_4, and D_1^- and D_4 are conditioned on the detection of the Ψ^- state, we are looking at fourfold coincidences. Narrow bandwidth filters (F) are positioned in front of each detector.

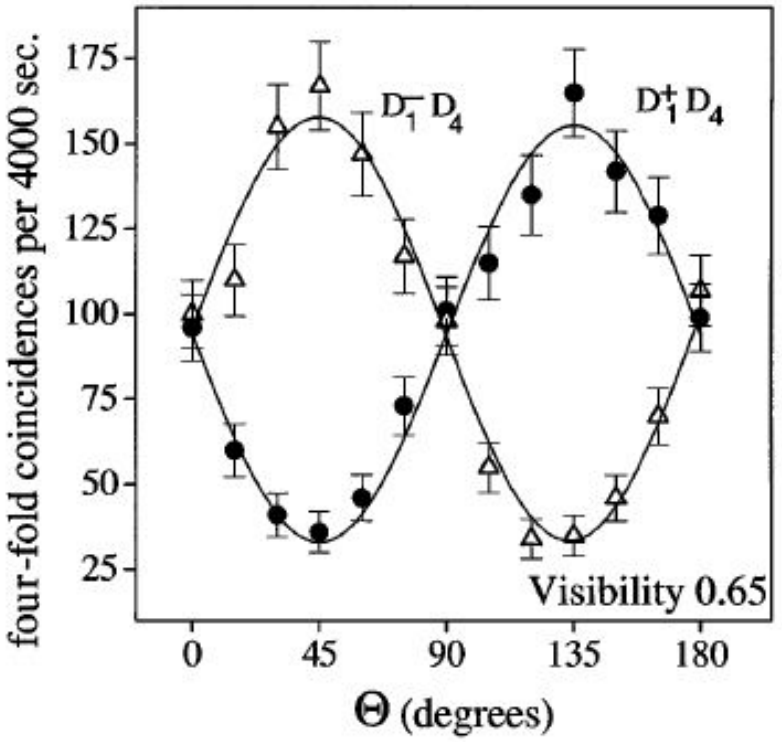


FIG. 3. Entanglement verification. Fourfold coincidences, resulting from twofold coincidence $D1^+D4$ and $D1^-D4$ conditioned on the twofold coincidences of the Bell-state measurement, when varying the polarizer angle Θ. The two complementary sine curves with a visibility of 0.65 ± 0.02 demonstrate that photons 1 and 4 are polarization entangled.

Jian-Wei Pan *et al.*, Phys. Rev. Lett. 80, 3891-3894 (1998)

作业

Entanglement Swapping的原理推导

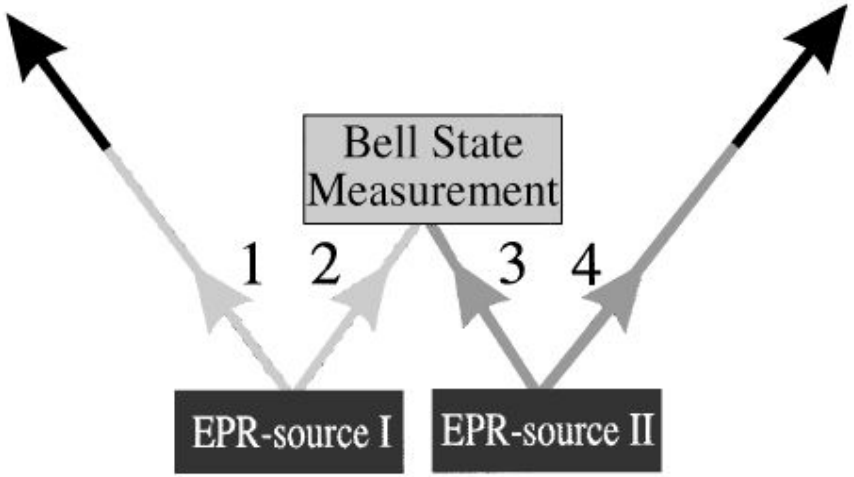


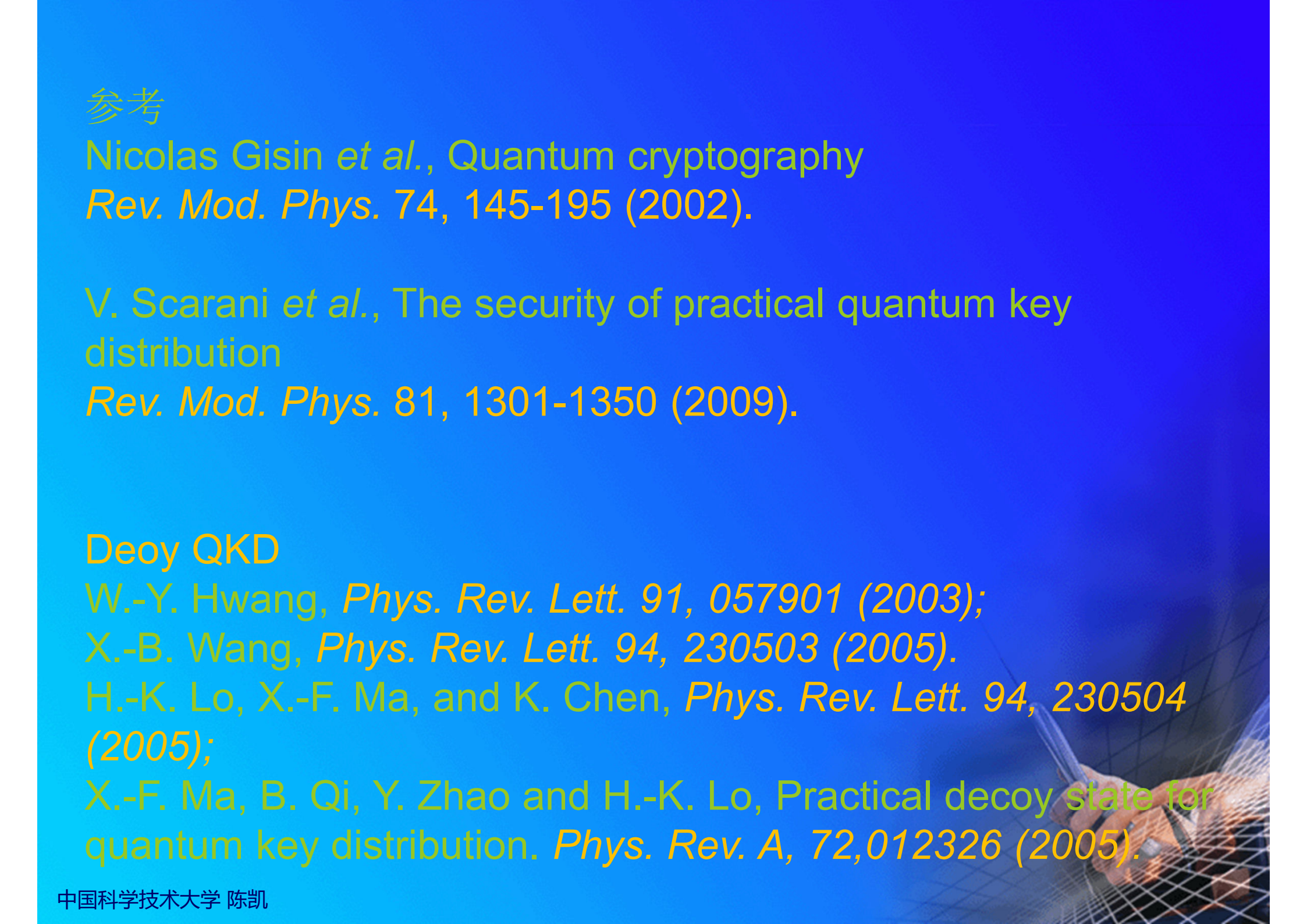
FIG. 1. Principle of entanglement swapping. Two EPR sources produce two pairs of entangled photons, pair 1-2 and pair 3-4. One photon from each pair (photons 2 and 3) is subjected to a Bell-state measurement. This results in projecting the other two outgoing photons 1 and 4 onto an entangled state. Change of the shading of the lines indicates the change in the set of possible predictions that can be made.

参考

Nicolas Gisin *et al.*, Quantum cryptography
Rev. Mod. Phys. 74, 145-195 (2002).

V. Scarani *et al.*, The security of practical quantum key distribution
Rev. Mod. Phys. 81, 1301-1350 (2009).

Deoy QKD
W.-Y. Hwang, *Phys. Rev. Lett. 91, 057901 (2003);*
X.-B. Wang, *Phys. Rev. Lett. 94, 230503 (2005).*
H.-K. Lo, X.-F. Ma, and K. Chen, *Phys. Rev. Lett. 94, 230504 (2005);*
X.-F. Ma, B. Qi, Y. Zhao and H.-K. Lo, Practical decoy state for quantum key distribution. *Phys. Rev. A, 72,012326 (2005).*



Shor码

量子信息：将单量子比特编码

$$\alpha|0\rangle+\beta|1\rangle \longrightarrow \alpha|000\rangle+\beta|111\rangle$$

（原量子比特）　　（通过3个量子比特编码后）

注：量子比特的编码方式不是克隆而是直接制造，比如上述量子态编码可以通过3光子纠缠来实现。

方法

由$Z_1 Z_2$与$Z_2 Z_3$测量

Z_1Z_2测量目的是比较第1量子比特与第2量子比特

$$Z_1 Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I,$$

若1与2相同，则给出+1，若不同给出-1

Z_1Z_2测量目的是比较第2量子比特与第3量子比特

若2与3相同，则给出+1，若不同给出-1

由此，可以判断出错误类型，却不测量有关编码后量子状态的幅值α β

纠单比特错误量子码

$$|0\rangle_L = |000\rangle$$
$$|1\rangle_L = |111\rangle$$

code states

$$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$$

$\alpha|000\rangle + \beta|111\rangle$ **Even Even**

No error $I \otimes I \otimes I$

Bit flip on first qubit $X \otimes I \otimes I$

$\alpha|100\rangle + \beta|011\rangle$

Odd Even

Parity of pairs 12 and 23

$Z \otimes Z \otimes I$ and $I \otimes Z \otimes Z$

Error syndrome

Bit flip on second qubit $I \otimes X \otimes I$

Bit flip on third qubit $I \otimes I \otimes X$

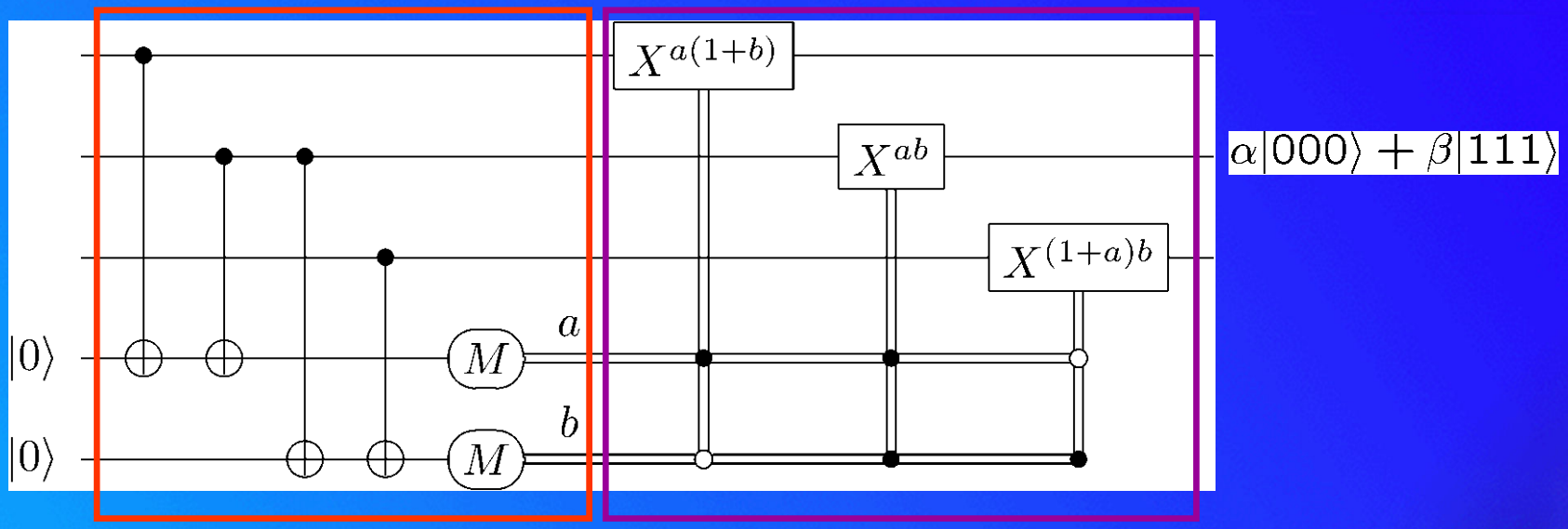
$\alpha|010\rangle + \beta|101\rangle$

Odd Odd

$\alpha|001\rangle + \beta|110\rangle$ **Even Odd**

Quantum error correction

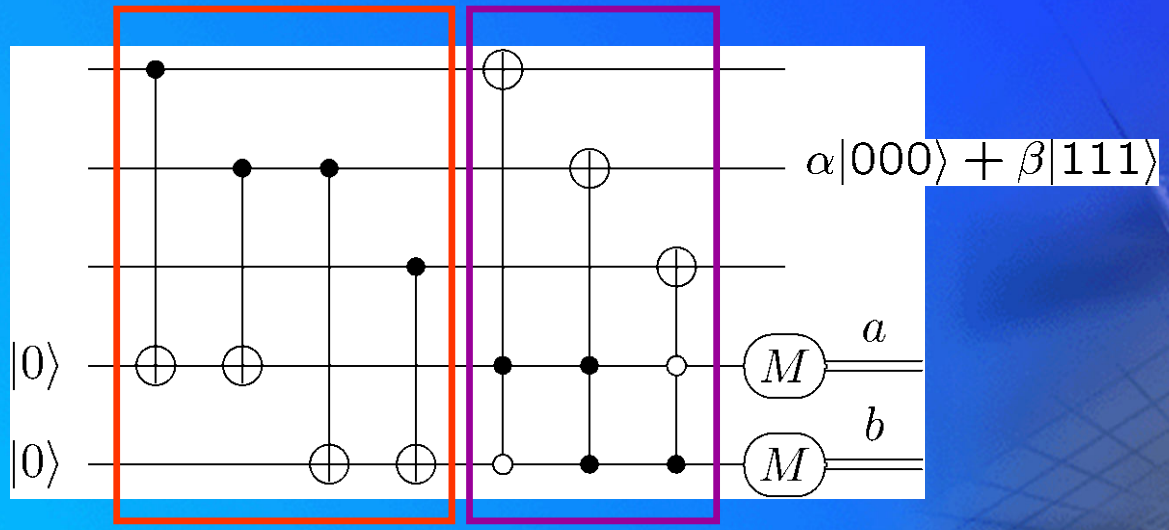
Single bit flip correction circuit



Syndrome measurement

Error correction

Coherent version



From Caves

相位翻转

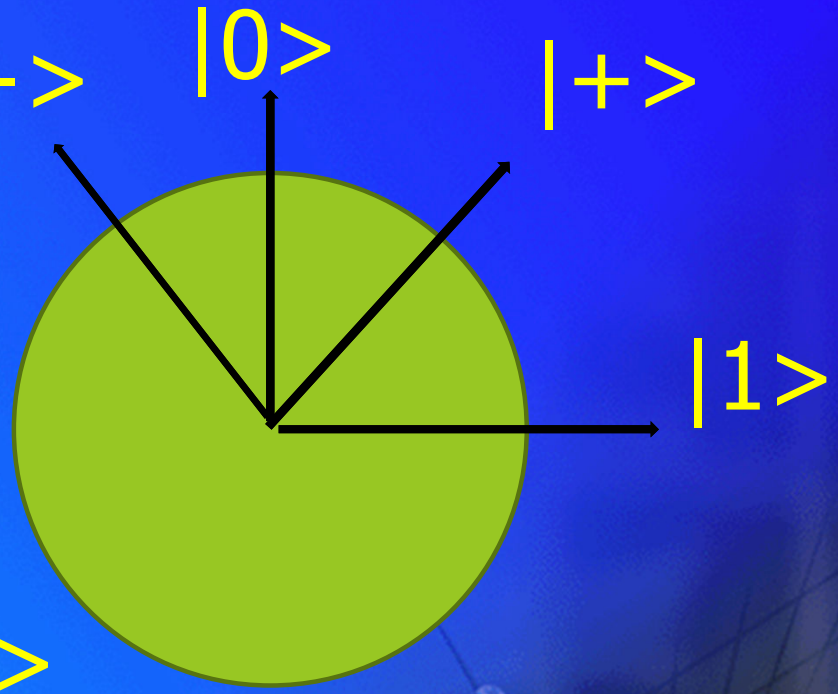
由$\alpha|0\rangle+\beta|1\rangle \longrightarrow \alpha|0\rangle-\beta|1\rangle$（相位翻转）

处理方式：将相位翻转转化为比特翻转

设

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

$$|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}.$$



得出

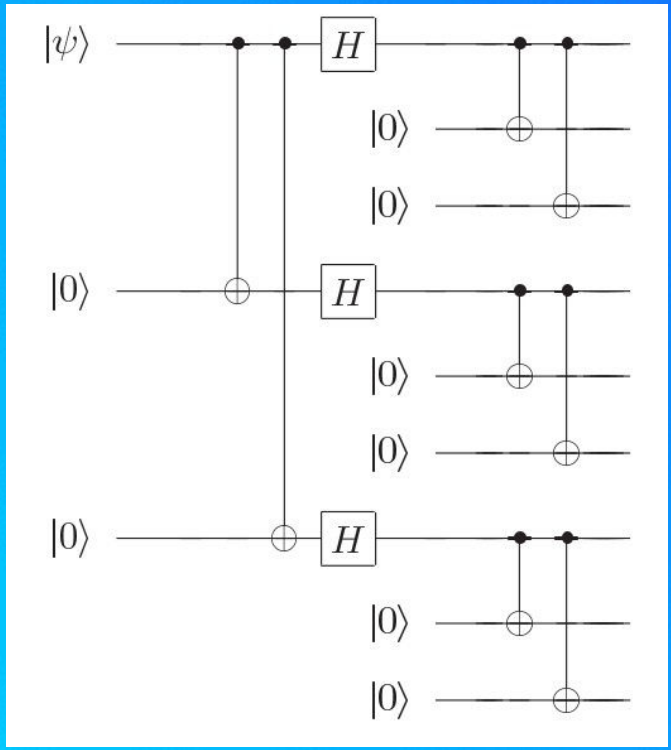
$|0_L\rangle=|000\rangle$ $|0_L\rangle=|+++\rangle$

$|1_L\rangle=|111\rangle$ $|1_L\rangle=|---\rangle$

Shor量子码：
三量子比特 相位翻转码与比特翻转码的组合

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$



Shor码编码线路

Hadamard门可以实现|0>，|1>基与|+>，|−>之间的转换

Shor码推广--可对完全任意的差错进行保护

设噪声为$\{E_i\}$,编码后的量子比特态为

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

噪声$\{E_i\}$作用后:

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger$$

假设把纠错集中到一个单项式 $E_i|\psi\rangle\langle\psi|E_i^\dagger$

量子状态$E_i|\psi\rangle$可以写成

$|\psi\rangle$，$X_1|\psi\rangle$，$Z_1|\psi\rangle$，$X_1Z_1|\psi\rangle$的叠加

测量差错症状会将这个叠加结果

塌缩到上述4个状态之一

恢复过程由相应的逆运算而执行，

并成功恢复状态$|\psi\rangle$，

这种方法对于所有运算元E_i都是正确的

量子错误描述

A general quantum error is a superoperator that is of form:

$$\rho \rightarrow \Sigma\, A_k\, \rho\, A_k^{\dagger}$$

Examples of single-qubit errors:

Bit Flip X: $X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle$

Phase Flip Z: $Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle$

Complete dephasing: $\rho \rightarrow (\rho + Z\rho Z^{\dagger})/2$ (decoherence)

Depolarizing channel : $\rho \rightarrow ((1-p)\rho + p/3(X\rho X + Y\rho Y + Z\rho Z)$

Rotation: $R_\theta|0\rangle = |0\rangle,\ R_\theta|1\rangle = e^{i\theta}|1\rangle$

Correcting All Single-Qubit Errors

Theorem: If a quantum error-correcting code (QECC) corrects errors A and B, it also corrects $\alpha A + \beta B$.

Any 2x2 matrix can be written as $\alpha I + \beta X + \gamma Y + \delta Z$.

A general single-qubit error $\rho \rightarrow \sum A_k \rho A_k^\dagger$ acts like a mixture of $|\psi\rangle \rightarrow A_k |\psi\rangle$, and A_k is a 2x2 matrix.

Any QECC that corrects the single-qubit errors X, Y, and Z (plus I) corrects every single-qubit error.

Correcting all t-qubit X, Y, Z on t qubits (plus I) corrects all t-qubit errors.

From Gottesman

量子纠错一般性

假定：噪声是由量子运算$\mathcal{E}$所描述，整个纠错方法（纠错运算）由保迹量子运算$\mathcal{R}$承担

量子纠错条件：令C为一个量子码，P为到C的投影算子设$\mathcal{E}$为具有运算元$\{E_i\}$的量子运算，则纠正C上的$\mathcal{E}$纠错运算$\mathcal{R}$存在的充分必要条件为，对某个复数Hermitian矩阵α成立

$$PE_i^{\dagger}E_jP = \alpha_{ij}P,$$

称为$\{E_i\}$组成一个可就成的差错集合

每个运算元$\{E_i\}$都可以被写成Pauli矩阵的线性组合。所以只需要满足

$$P\sigma_i^1\sigma_j^1P = \alpha_{ij}P,$$

便可以确定Shor码可以对单量子比特进行纠错

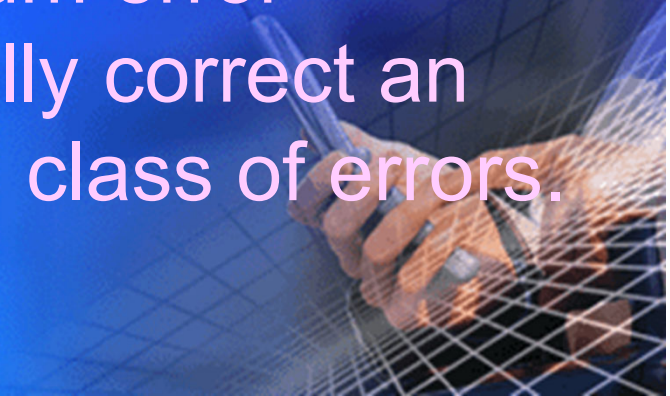
量子纠错的实质：如何构造码空间C以及相应的纠错运算R

Discretization of the errors

Any QECC that corrects the single-qubit errors X, Y, and Z (plus I) corrects every single-qubit error.

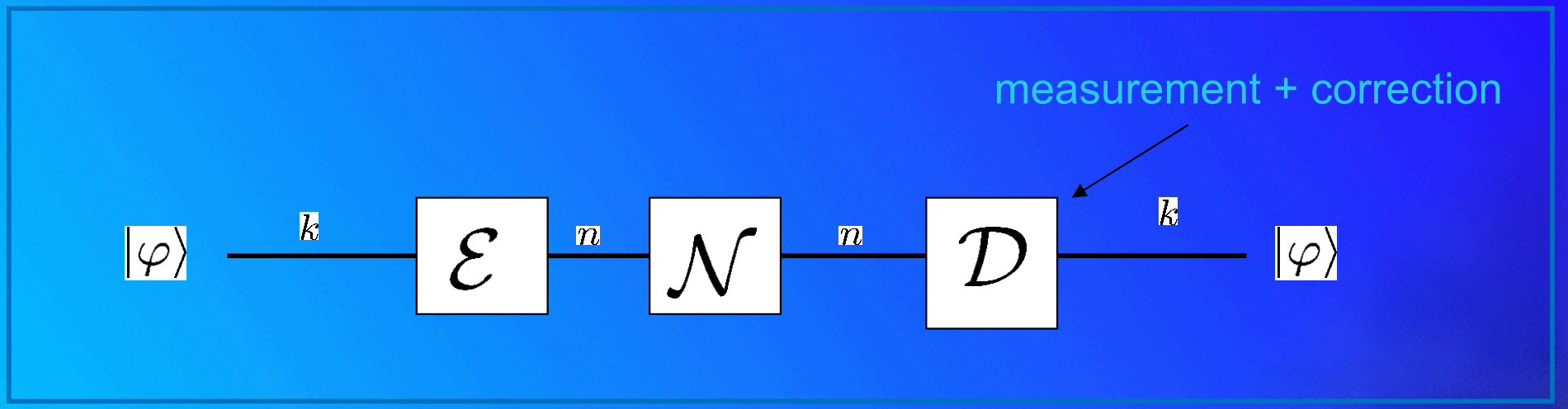
Correcting all t-qubit X, Y, Z on t qubits (plus I) corrects all t-qubit errors.

This is a fundamental and deep fact about quantum error-correction, that by correcting just a discrete set of errors – the bit flip, phase flip, and combined bit–phase flip, in this example – a quantum error-correcting code is able to automatically correct an apparently much larger (continuous!) class of errors.



量子纠错过程

[[n,k]] quantum error correcting code



线性编码

- We encode a k bits codeword x, into a n bits codeword c using a [*n* by k] generator matrix ***G*** as follows:

$$c \equiv G \bullet x$$

- Error correction for linear codes is done using a [(*n-k*) by *n*] *parity matrix*.

Parity Check 过程

- Parity check matrix ***H*** is such that:

$$\boldsymbol{H c = 0} \quad \text{and} \quad \boldsymbol{H G = 0}$$

- The receiver gets the codeword ***r***, which incorporates an error ***e***:

$$\boldsymbol{r = c + e}$$

- Then, the syndrome ***s*** is given by:

$$\boldsymbol{s = H r = H e}$$

Error Correction & Recovery

- Once we detect the syndrome ***s***, we can find the error that occurred ***e***.
- Now we can correct the error as:

$$c = r - e$$

- And finally one can recover the original message

量子码的构造

经典线性码

优势为节省资源：用n个比特编码k个比特

线性码：kn 个比特 刻画生成矩阵

一般码：$n2^k$ 个比特 刻画生成矩阵

奇偶检验矩阵：Hx=0 (H)为奇偶检验矩阵

H矩阵为(n-k)×n

H与G之间可进行相互转换，例如

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

n-k

n

奇偶检验矩阵使差错检测和恢复变得十分明显

H与G之间可进行相互转换

奇偶检验矩阵具体的运作方式

设　编码消息x ⟶ y=Gx

对y造成影响的噪声 ⟶ e

出错后的码字 ⟶ y′=y+e　(+为模二加)

Hy=0 ⟶ Hy′=He

Hy′为差错症状。
- 当没有差错出现的情况下为0
- 当差错出现在第j个比特时为He_j

假设最多只会出现一个量子比特的错误，则通过比较Hy′与 He_j 的值，确定哪个比特需要被纠正。

Hamming距离

距离标示可执行线性纠错码

设 x和y为n比特的字，

则d(x,y)为差异位置数目 ➡ Hamming距离

举例：d((1,1,0,0),(0,1,0,1))=2

Wt(x)=d(x,0)为X中非零位置数目➡Hamming权重

$$d(x,y)=Wt(x+y)$$

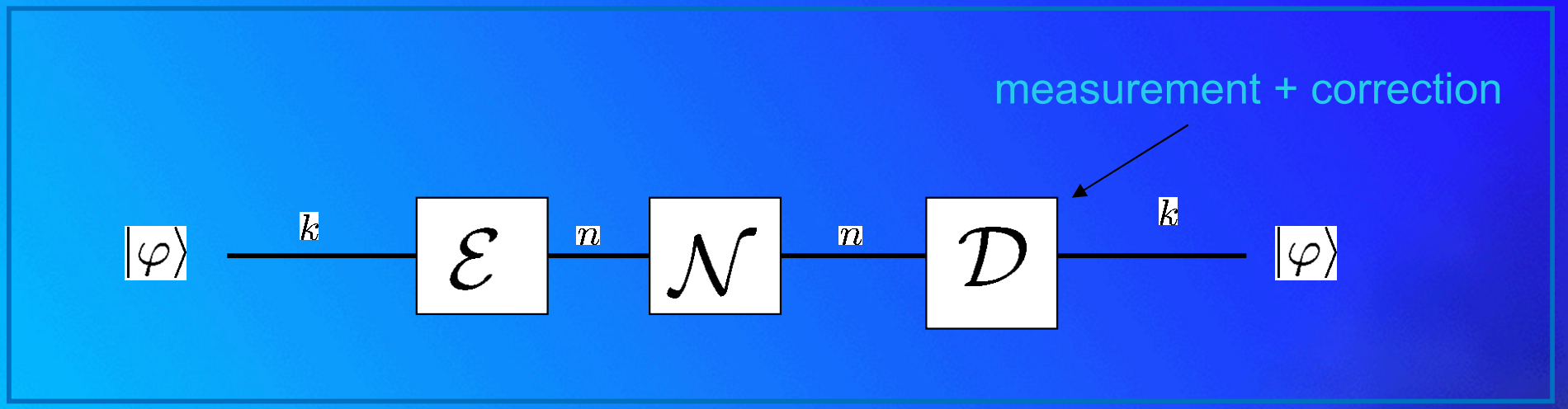
距离的重要性在于，对某个整数t，简单的通过解码变坏的编码消息y′为满足d(y,y′)≤t的唯一码字y，具有距离至少为2t+1的一个码就能纠正最多t个比特上的差错。

量子纠错码特征

- Quantum Error Correction Codes are characterized by the triplet [n,k,d], where:
  - n is the length of the resulting codeword.
  - k is the number of qubits to be encoded.
  - d is the *minimum distance*.
- Data redundancy implies $n>k$
- A code with minimal distance $d=2t+1$ is able to correct errors on up to t bits.

量子纠错过程

[[n,k]] quantum error correcting code



Basic framework for quantum error correction

After encoding the code is subjected to noise, following which a syndrome measurement is performed to diagnose the type of error which occurred, that is, the error syndrome. Once this has been determined, a recovery operation is performed, to return the quantum system to the original state of the code. The basic picture is illustrated in Figure 10.5: different error syndromes correspond to undeformed and orthogonal subspaces of the total Hilbert space. The subspaces must be orthogonal, otherwise they couldn't be reliably distinguished by the syndrome measurement. Furthermore, the different subspaces must be undeformed versions of the original code space, in the sense that the errors mapping to the different subspaces must take the (orthogonal) codewords to orthogonal states, in order to be able to recover from the error.

检测错误，而不是量子信息

Through the information from the error syndromes, one can determine whether there is an error and where it is:

E.g., measurements of Z_1Z_2 and Z_2Z_3 for $\alpha|010\rangle + \beta|101\rangle$ give syndrome 11, which means the second bit is different. Correct it with a X operation on the second qubit. Note that the syndrome does not depend on α and β.

We have learned about the error without learning about the data, so quantum superpositions are still alive!

The Pauli Group

The general Pauli group G_n on n qubits is defined to consist of all n-fold tensor products of up to n operators I, X, Y, or Z with overall phase $\pm 1, \pm i$

For a single quantum bit

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

that G_1 is closed under multiplication, and thus forms a legitimate group.

Any pair M, N of Pauli operators either commutes (MN = NM) or anticommutes (MN = -NM).

The Pauli Group G_n on n qubits is given by the n-fold tensor product of Pauli matrices.

The Pauli group spans the set of all n-qubit errors.

Stabilizer

Suppose S is a subgroup of G_n and define V_S to be the set of n qubit states which are fixed by every element of S.

V_S is the *vector space stabilized by* S, and S is said to be the *stabilizer* of the space V_S, since every element of V_S is stable under the action of elements in S.

Properties of a Stabilizer

The stabilizer is a group:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then $MN|\psi\rangle = |\psi\rangle$.

The stabilizer is Abelian:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then

$$(MN-NM)|\psi\rangle = MN|\psi\rangle - NM|\psi\rangle = 0$$

(For Pauli matrices) ⟹ $MN = -NM$

Stabilizer 例子

The EPR state of two qubits

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

It is easy to verify that this state satisfies the identities

$$X_1 X_2 |\psi\rangle = |\psi\rangle$$
$$Z_1 Z_2 |\psi\rangle = |\psi\rangle$$

We say that the state |ψ> is *stabilized* by the operators X_1X_2 and Z_1Z_2.
In addition, the state |ψ> is the unique quantum state (up to a global phase) which is stabilized by these operators X_1X_2 and Z_1Z_2.

Stabilizer 例子

- Such a state is *unique*, as it is the only one (up to a global phase) to be stabilized by both X_1X_2 and Z_1Z_2.
- The basic idea of using the stabilizer group is to work with the stabilizer operators as group generators rather than with the states.
- The *group theoretical formalism* of the stabilizer codes offers a more compact description of the quantum error correction codes.

Stabilizer 例子

For the classical repetition code, one can see the error syndromes

first two bits have even parity (an even number of 1's), and similarly for the 2nd and 3rd bits, with correctly-encoded state 000 or 111

For state with error on one of the first two bits: odd parity for the first two bits.

One can rephrase this by observing that a codeword is a +1 eigenvector of $Z \otimes Z \otimes I$ and that a state with an error on the 1st or 2nd bit is a -1 eigenvector of $Z \otimes Z \otimes I$.

典型的错误探测

For the three-qubit phase error correcting code, a codeword has eigenvalue +1 for X⊗X⊗I, whereas a state with a phase error on one of the first two qubits has eigenvalue -1 for X⊗X⊗I.

Measuring Z⊗Z detects bit flip (X) errors, and measuring X⊗X detects phase (Z) errors.

Measuring enough operators find locations of errors.

Error Correction Conditions

Theorem: Let *S* be the stabilizer of the stabilizer code *C(S)*. Suppose $\{E_i\}$ is a set of operators in *Gn* such that:

$$E_j^\dagger E_k \notin N(S) - S$$

for all j and k. Then, $\{E_i\}$ is a correctable set of errors for the code *C(S)*.

The normalizer of *S*, denoted *N*(*S*), which is defined to consist of all elements *E* of G_n such that $EgE^\dagger \in S$ for all $g \in S$.

Error Detection

- Suppose $g_1,\ldots,g_{n-k}$ is the set of generators for the stabilizer of an [n,k] stabilizer code, and that $\{E_j\}$ is the set of correctable errors for the code.
- Error detection is performed by measuring the generators of the stabilizer in turn, to obtain the error syndrome, which consists of the results of the measurements $\beta_1,\ldots,\beta_{n-k}$.
- If the error E occurred then the error syndrome is given by β_l such that:

$$E g_l E^\dagger = \beta_l g_l$$

Recovery (1)

- In the case where E is the unique error operator having this syndrome, recovery is done by applying $E^{\dagger}$.
- In the case where there there are two distinct errors E and E' giving rise to the same error syndrome, it follows that:

  $EPE^{\dagger} = E'PE'^{\dagger}$ and then $E^{\dagger}E'PE'^{\dagger}E = P$

  and therefore $E^{\dagger}E'$ is part of S.

Recovery (2)

- Thus applying $E^{\dagger}$ after the error E' has occurred results in a successful recovery.
- Thus, for each possible error syndrome we simply pick out a single error E with that syndrome, and apply $E^{\dagger}$ to achieve recovery when that syndrome is observed.

The three qubit bit flip code

Consider the familiar three qubit bit flip code spanned by the states $|000\rangle$ and $|111\rangle$, with stabilizer generated by Z_1Z_2 and Z_2Z_3. By inspection we see that every possible product of two elements from the error set $\{I, X_1, X_2, X_3\}$ – $I, X_1, X_2, X_3, X_1X_2, X_1X_3, X_2X_3$ – anti-commutes with at least one of the generators of the stabilizer (except for I, which is in S), and thus by Theorem 10.8 the set $\{I, X_1, X_2, X_3\}$ forms a correctable set of errors for the three qubit bit flip code with stabilizer $\langle Z_1Z_2, Z_2Z_3\rangle$.

Error-detection and correction

Z_1Z_2	Z_2Z_3	Error type	Action
+1	+1	no error	no action
+1	−1	bit 3 flipped	flip bit 3
−1	+1	bit 1 flipped	flip bit 1
−1	−1	bit 2 flipped	flip bit 2

The three qubit bit flip code

g_1	Z	Z	I
g_2	I	Z	Z
$\overline{X}$	X	X	X
$\overline{Z}$	Z	Z	Z

The nine qubit Shor code

Name	Operator
g_1	$ZZIIIIIII$
g_2	$IZZIIIIII$
g_3	$IIIZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIIZZI$
g_6	$IIIIIIIZZ$
g_7	$XXXXXXIII$
g_8	$IIIXXXXXX$
$\bar{Z}$	$XXXXXXXXX$
$\bar{X}$	$ZZZZZZZZZ$

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

The nine qubit Shor code

Name	Operator
g_1	$ZZIIIIIII$
g_2	$IZZIIIIII$
g_3	$IIIZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIIZZI$
g_6	$IIIIIIIZZ$
g_7	$XXXXXXIII$
g_8	$IIIXXXXXX$
$\bar{Z}$	$XXXXXXXXX$
$\bar{X}$	$ZZZZZZZZZ$

$g_1, g_2, \ldots, g_8$ generate a group, the *stabilizer* of the code, consisting of all Pauli operators M with the property that $M|\psi\rangle = |\psi\rangle$ for all encoded states $|\psi\rangle$.

More about Stabilizer

The stabilizer is a group:

The stabilizer is Abelian:

Given any Abelian group S of Pauli operators, define a code space $T(S) = \{ |\psi\rangle \text{ s.t. } M|\psi\rangle = |\psi\rangle \ \forall\ M \in S\}$. Then T(S) encodes k logical qubits in n physical qubits when S has n-k generators (so size 2^{n-k}).

Stabilizer Elements Detect Errors

Suppose $M \in S$ and Pauli error E anticommutes with M. Then:

$$M (E |\psi\rangle) = - EM |\psi\rangle = - E |\psi\rangle,$$

so $E |\psi\rangle$ has eigenvalue -1 for M.

Conversely, if M and E commute for all $M \in S$,

$$M (E |\psi\rangle) = EM |\psi\rangle = E |\psi\rangle \quad \forall M \in S,$$

so $E |\psi\rangle$ has eigenvalue +1 for all M in the stabilizer.

The eigenvalue of an operator M from the stabilizer detects errors which anticommute with M.

From Gottesman

Error Syndromes and Stabilizers

To correct errors, we must accumulate enough information about the error to figure out which one occurred.

The error syndrome is the list of eigenvalues of the generators of S: If the error E commutes with M $\in$ S, then M has eigenvalue +1; if E and M anticommute, M has eigenvalue -1.

We can then correct a set of possible errors if they all have distinct error syndromes.

From Gottesman

Stabilizer Codes Summary

- Choose an Abelian subgroup of the Pauli group. This will be the stabilizer S of the QECC.
- The codewords: $\{ |\psi\rangle \text{ s.t. } M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$
- If S has r generators on n qubits, the QECC has k = n-r encoded qubits.
- The codes corrects errors if $E^\dagger F \notin N(S) \setminus S$ for all pairs (E, F) of possible errors. The distance d is the minimum weight of $N(S) \setminus S$.

From Gottesman

Summary: Stabilizer Codes

- We can describe a quantum stabilizer code by giving its stabilizer, an Abelian subgroup of the Pauli group.
- By looking at the stabilizer, we can learn all of the most interesting properties of a QECC, including the set of errors it can correct.
- One interesting and useful class of stabilizer codes is the family of CSS codes, derived from two classical codes. The 7-qubit code is the smallest example.

From Gottesman

Summary of QECCs

- Quantum error-correcting codes exist which can correct very general types of errors on quantum systems.
- A systematic theory of QECCs allows us to build many interesting quantum codes.
- Quantum error correction can be formalized in terms of quantum states and projectors, stabilizer subspaces or the stabilizer group.
- All these formalizations are equivalent.
- The theory of quantum error correction is quite elegant and simple.
- The implementation is really a nontrivial task.

DiVincenzo's Criteria

DiVincenzo, Fortschr. Phys. **48**, 771 (2000)

1. ***Scalability:*** A scalable physical system with well characterized parts, usually qubits.

2. ***Initialization:*** The ability to initialize the system in a simple fiducial state.

3. ***Control:*** The ability to control the state of the computer using sequences of elementary universal gates.

4. ***Stability:*** Decoherence times much longer than gate times, together with the ability to suppress decoherence through error correction and fault-tolerant computation.

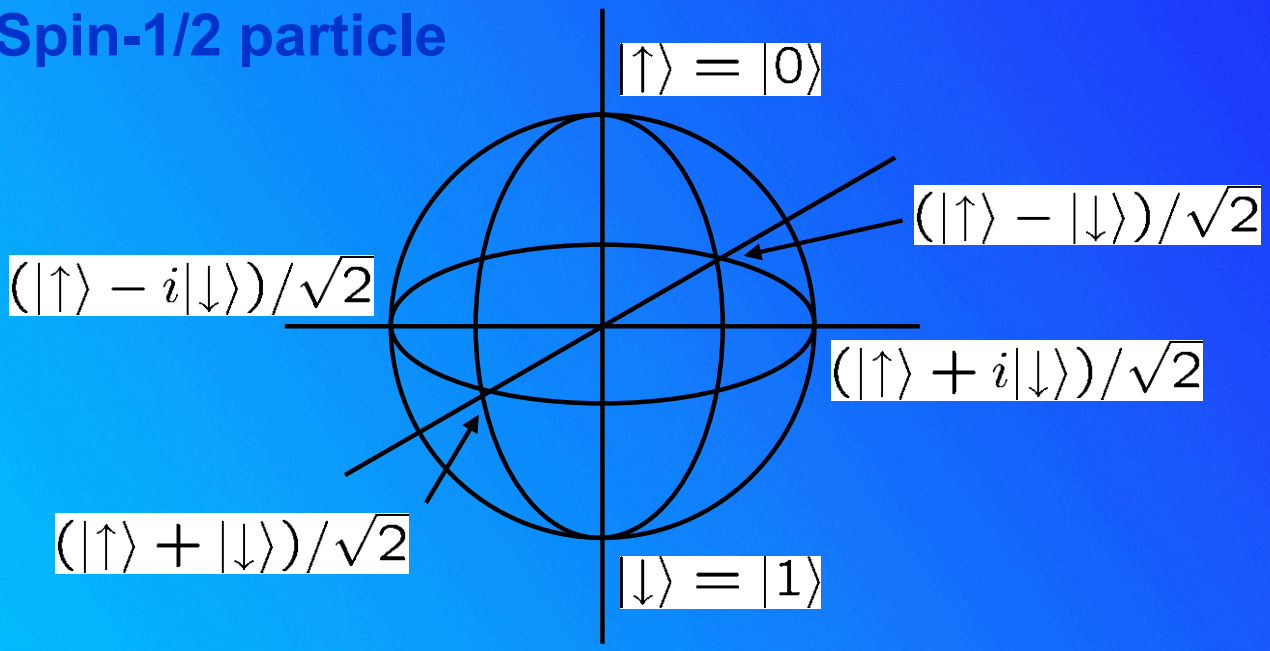
5. ***Measurement:*** The ability to read out the state of the computer in a convenient product basis.

Qubitology. States

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

Direction of spin

Spin-1/2 particle



Bloch sphere

From Caves

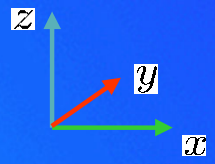
$$|\mathbf{n}\rangle\langle\mathbf{n}| = \frac{1}{2}(I + \sigma_x n_x + \sigma_y n_y + \sigma_z n_z)$$
$$= \frac{1}{2}(I + \mathbf{n}\cdot\sigma)$$

Pauli representation

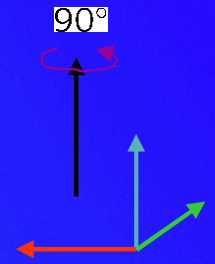
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X$$
$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y$$
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

Qubitology. Gates and quantum circuits

Single-qubit gates



$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = T^2$$

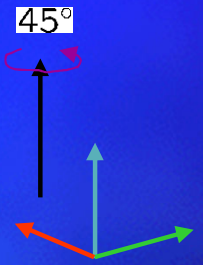


$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S^2$$

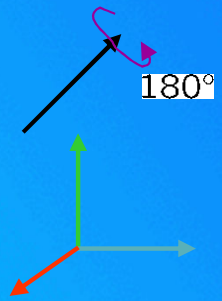
Phase flip

$$|a\rangle \text{ —}\boxed{S}\text{— } i^a|a\rangle$$

$$|a\rangle \text{ —}\boxed{Z}\text{— } (-1)^a|a\rangle$$



$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$



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

Hadamard

$$|a\rangle \text{ —}\boxed{T}\text{— } e^{ia\pi/4}|a\rangle$$

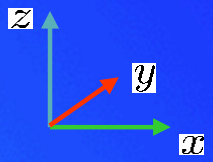
$$|a\rangle \text{ —}\boxed{H}\text{— } (|0\rangle + (-1)^a|1\rangle)/\sqrt{2}$$

$$Z^2 = H^2 = I$$

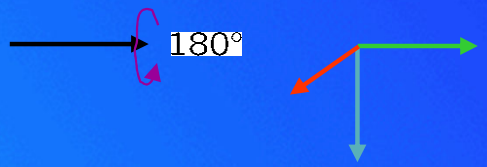
From Caves

Qubitology. Gates and quantum circuits

More single-qubit gates



$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = HZH$$

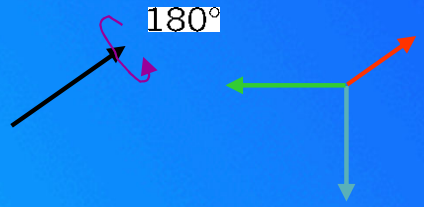


Bit flip

$$|a\rangle \text{ —[}X\text{]— } |a \oplus 1\rangle = \text{ —[}H\text{]—[}Z\text{]—[}H\text{]—}$$

$$X^2 = Y^2 = I$$

$$iY = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = ZX$$



Phase-bit flip

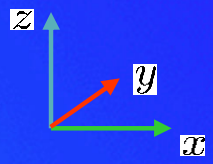
$$|a\rangle \text{ —[}iY\text{]— } (-1)^{a+1}|a \oplus 1\rangle$$

$$= \text{ —[}X\text{]—[}Z\text{]— } = \text{ —[}H\text{]—[}Z\text{]—[}H\text{]—[}Z\text{]—}$$

From Caves

Qubitology. Gates and quantum circuits

Control-target two-qubit gate

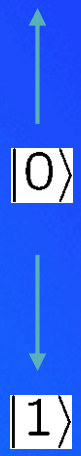


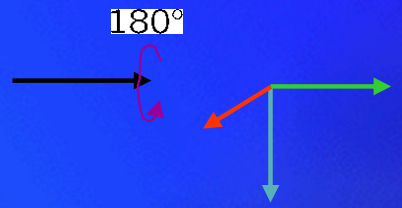
Control

Target

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

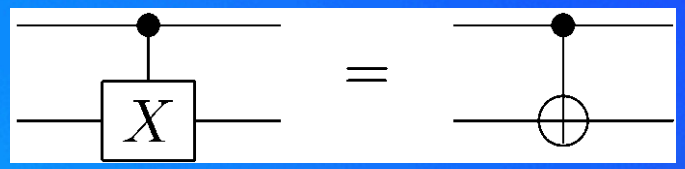
$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

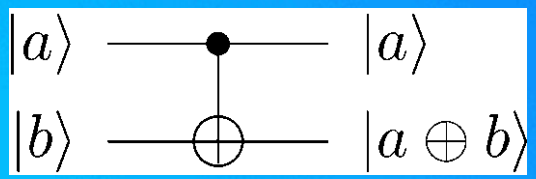




Control

Target





$$(\text{C-NOT})^2 = I$$

From Caves

Qubitology. Gates and quantum circuits

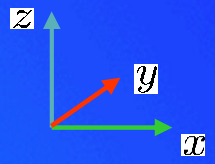
Universal set of quantum gates

- *T* (45-degree rotation about *z*)
- *H* (Hadamard)
- C-NOT

From Caves

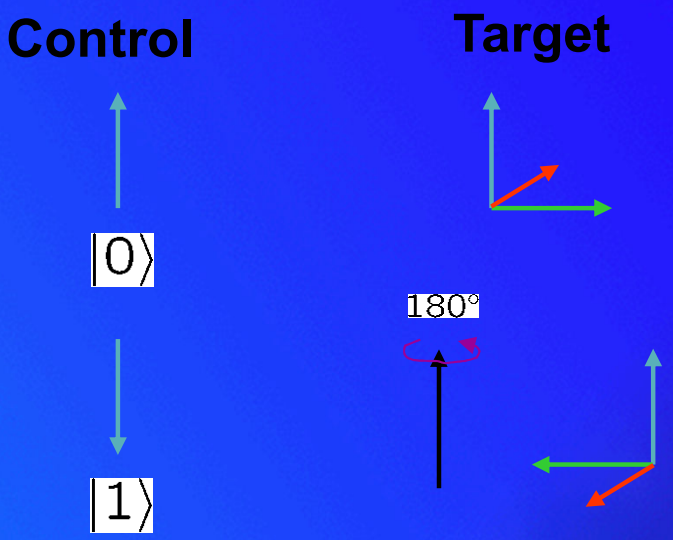
Qubitology. Gates and quantum circuits

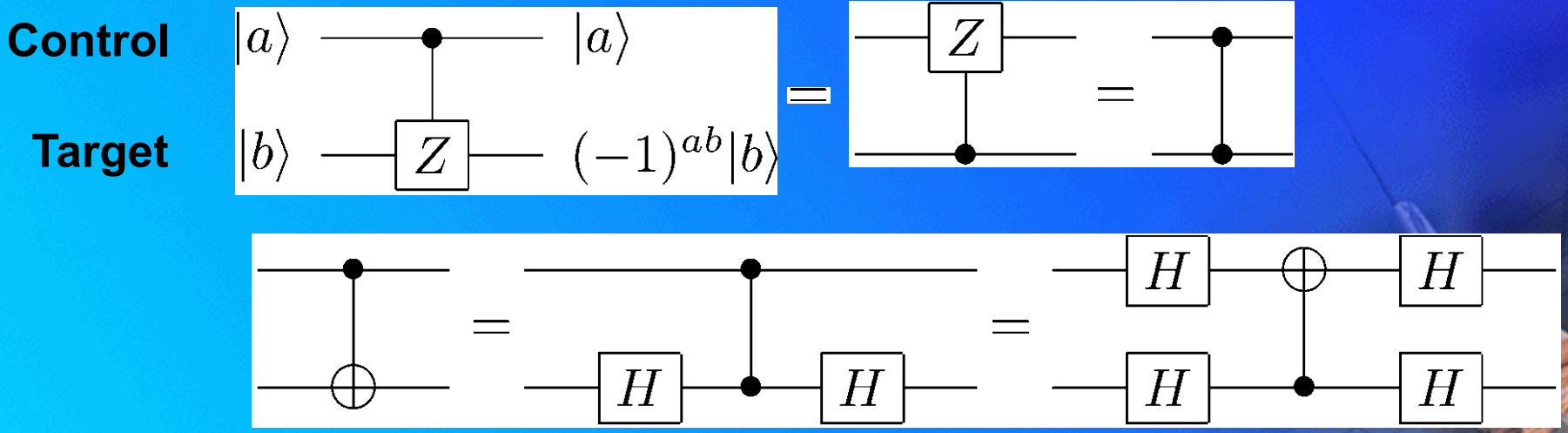
Another two-qubit gate



$$\text{C-PHASE} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

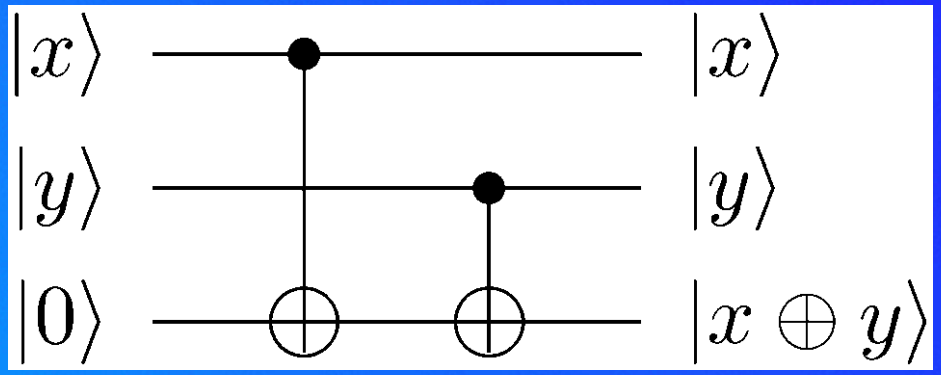




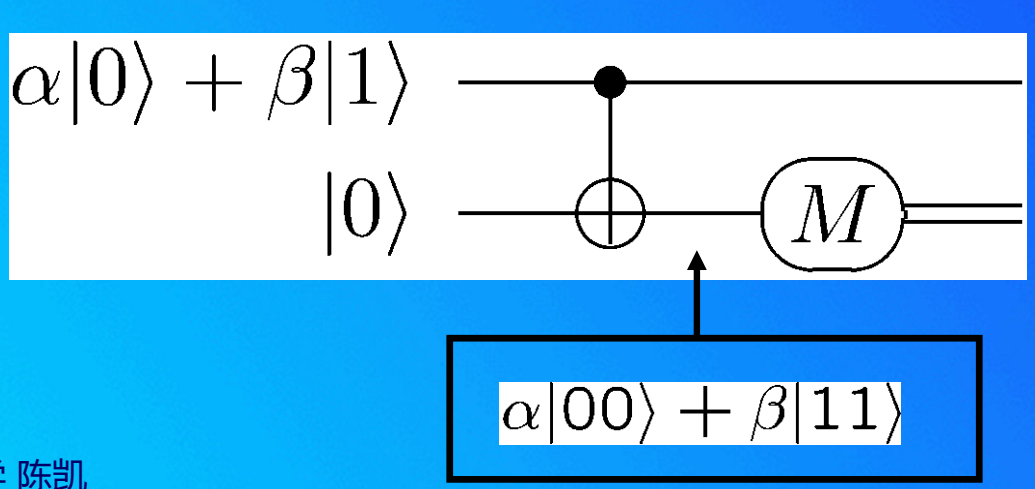
From Caves

Qubitology. Gates and quantum circuits

C-NOT as parity check



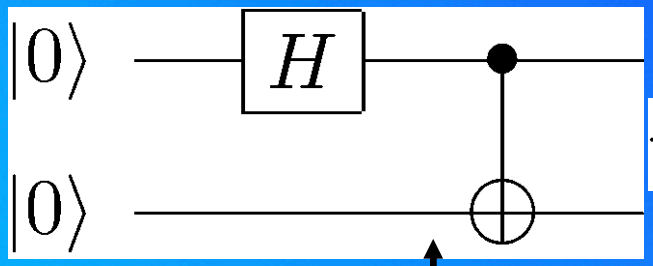
C-NOT as measurement gate



From Caves

Qubitology. Gates and quantum circuits

Making Bell states using C-NOT



$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

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

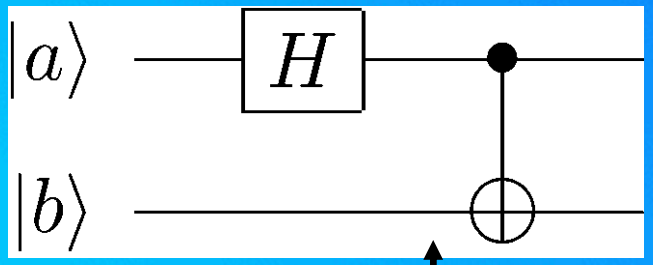
Bell states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



$$\frac{1}{\sqrt{2}}(|0b\rangle + (-1)^a|1, b \oplus 1\rangle) \equiv |\beta_{ab}\rangle$$

phase bit

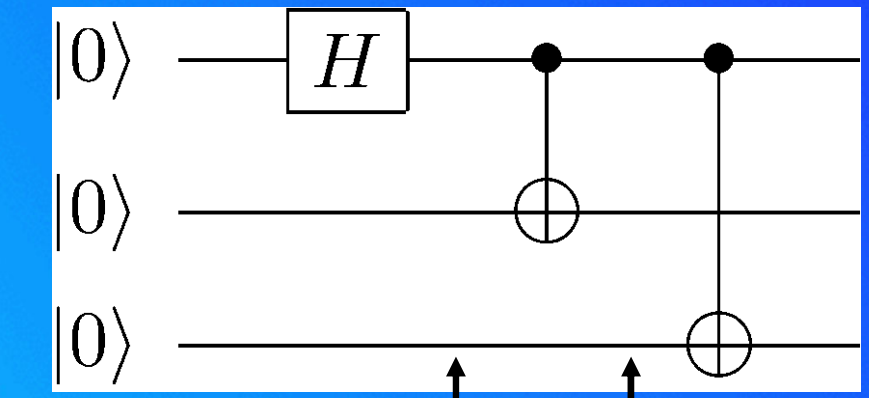
parity bit

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

From Caves

Qubitology. Gates and quantum circuits

Making cat states using C-NOT



GHZ (cat) state

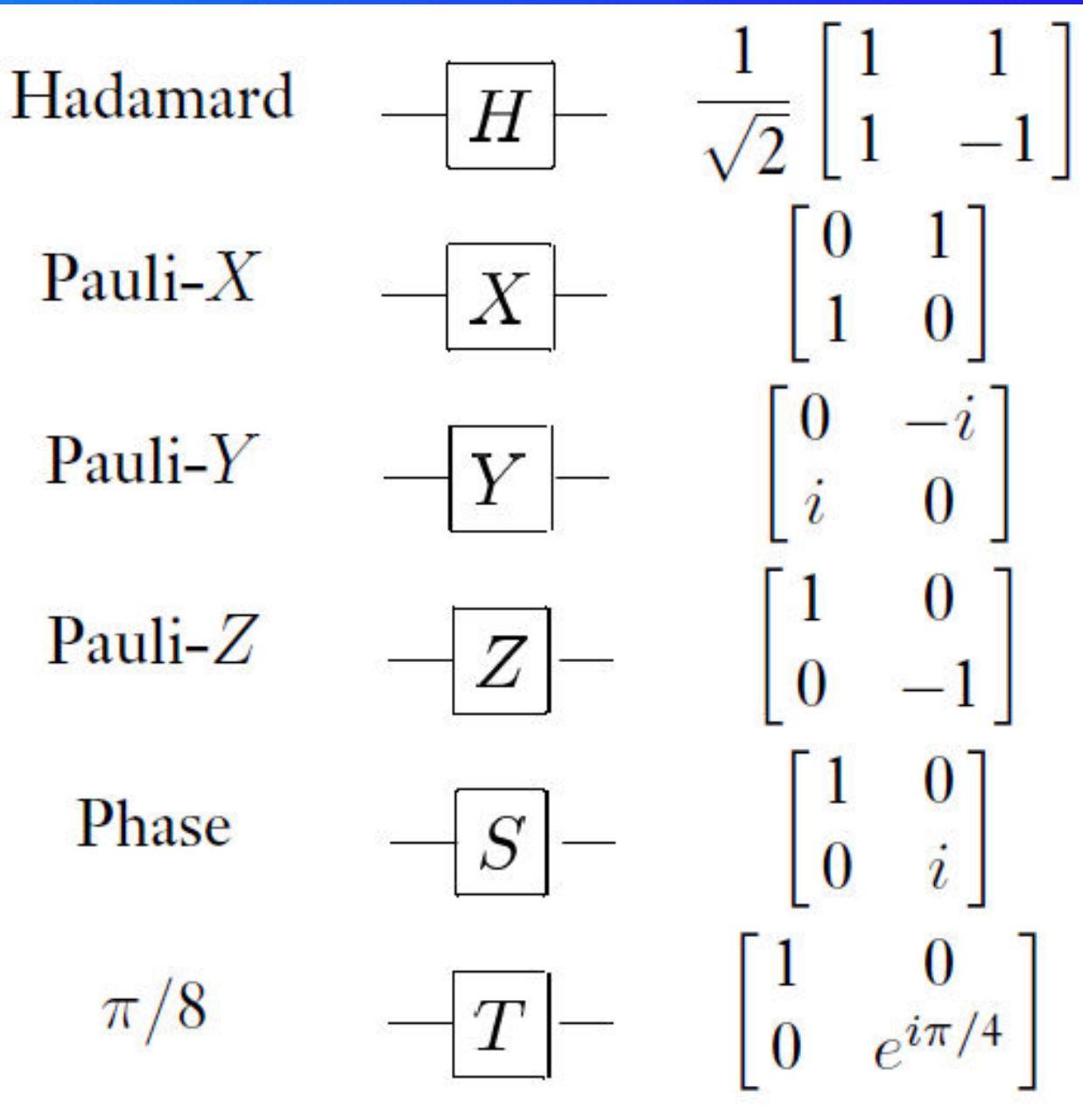
$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$$

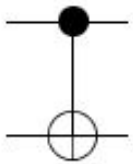
From Caves

典型的单比特量子门


Hadamard
H
$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X
X
$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y
Y
$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z
Z
$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase
S
$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$
T
$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

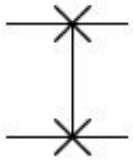
典型的多比特量子门

controlled-NOT



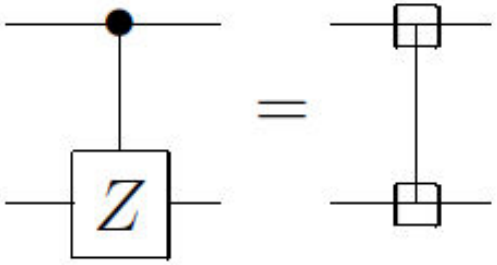
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

swap



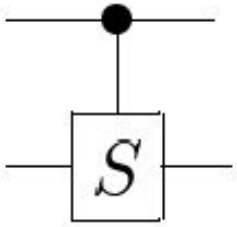
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

controlled-Z



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

controlled-phase



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

Decomposing single qubit operations

Arbitrary 2 ×2 unitary matrix may be decomposed as

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

where α, β, γ, and δ are real-valued.

Swap gate

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

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

Control-U gate

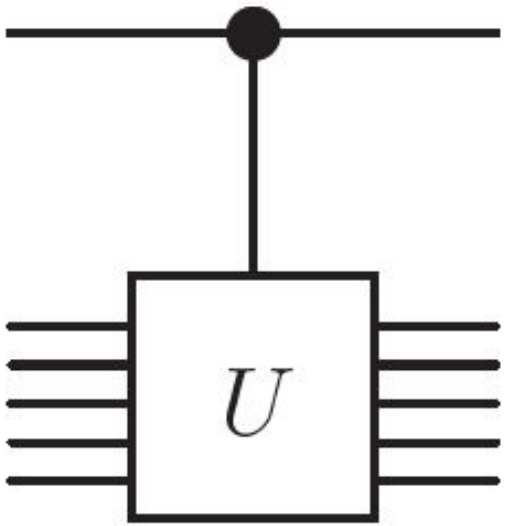


Figure 1.8. Controlled-U gate.

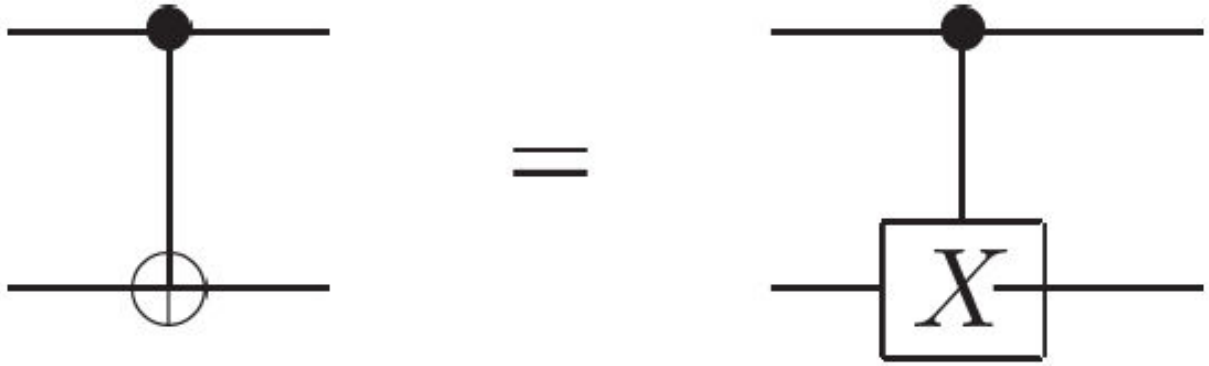


Figure 1.9. Two different representations for the controlled-NOT.

Circuit for measurement

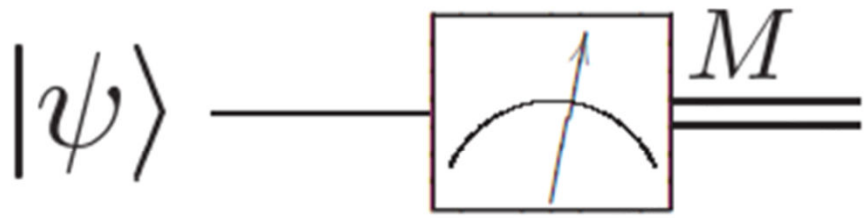


Figure 1.10. Quantum circuit symbol for measurement.

This operation converts a single qubit state $|\psi\rangle = a|0\rangle + \beta|1\rangle$ into a probabilistic classical bit M (distinguished from a qubit by drawing it as a double-line wire), which is 0 with probability $|a|^2$, or 1 with probability $|\beta|^2$.

Bell态产生

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

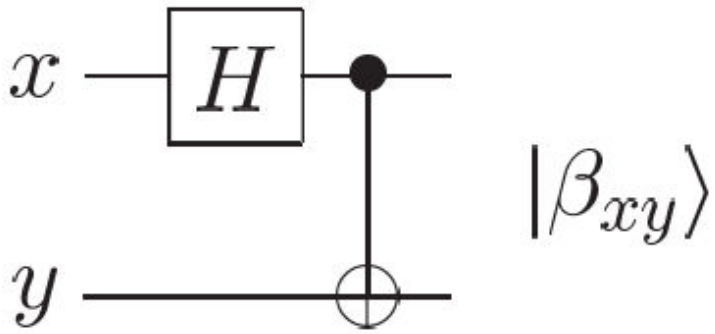


Figure 1.12. Quantum circuit to create Bell states, and its input–ouput quantum 'truth table'.

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

Quantum teleportation

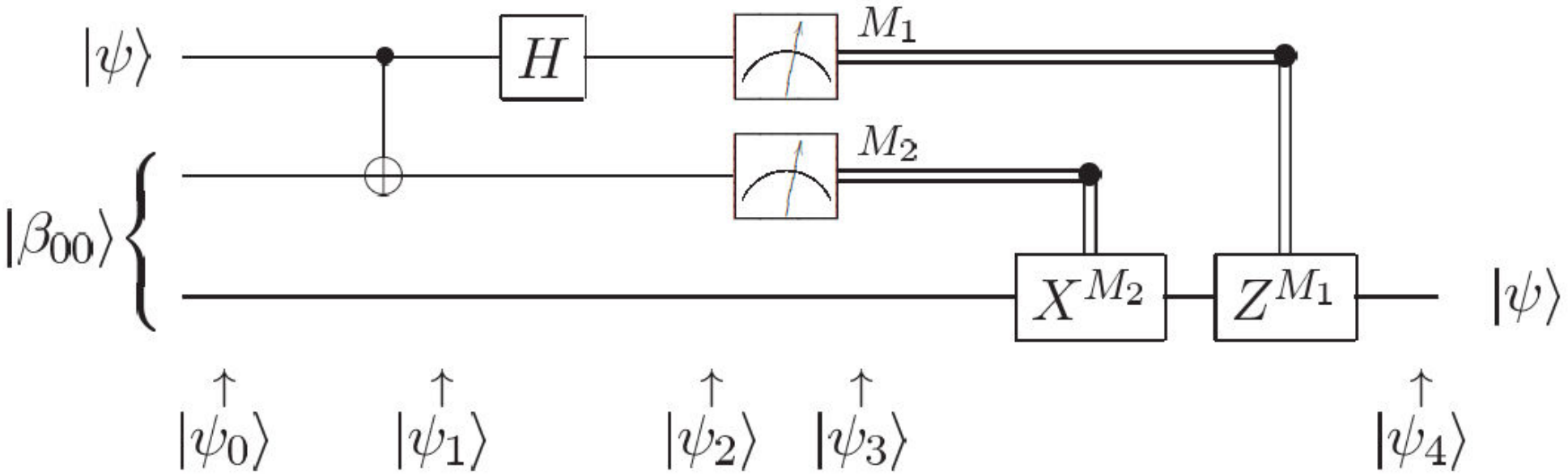
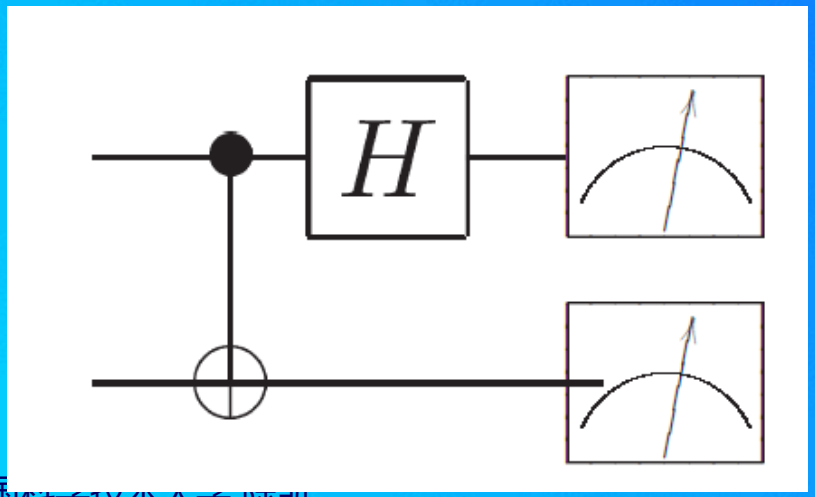
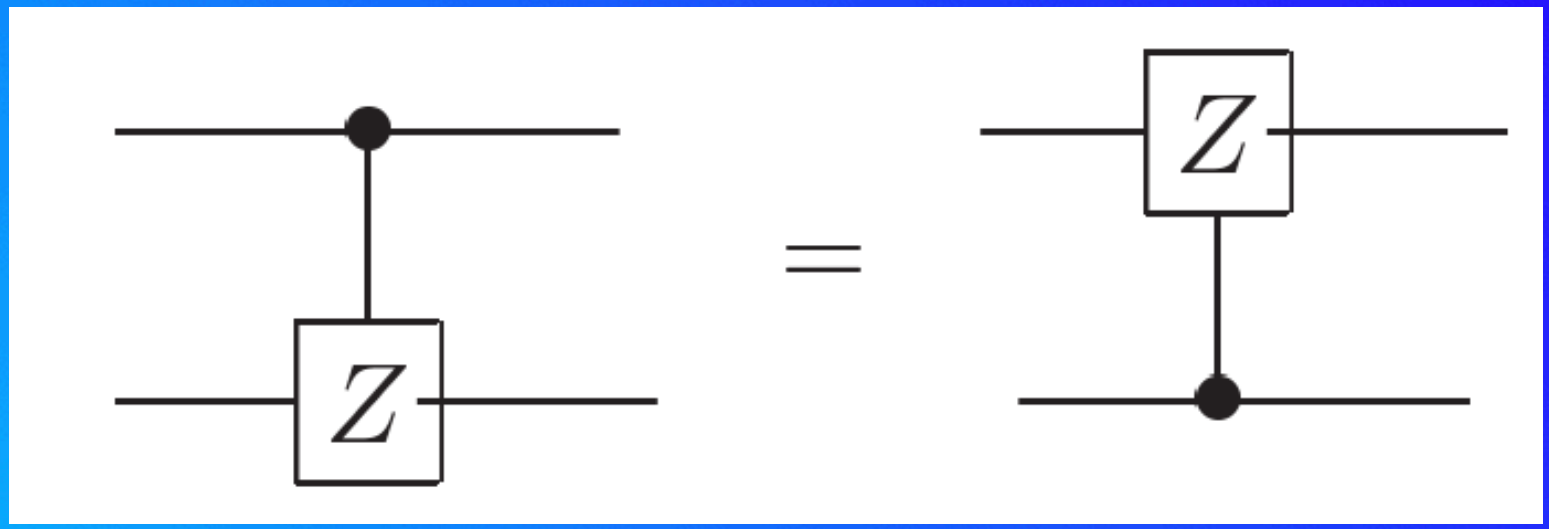


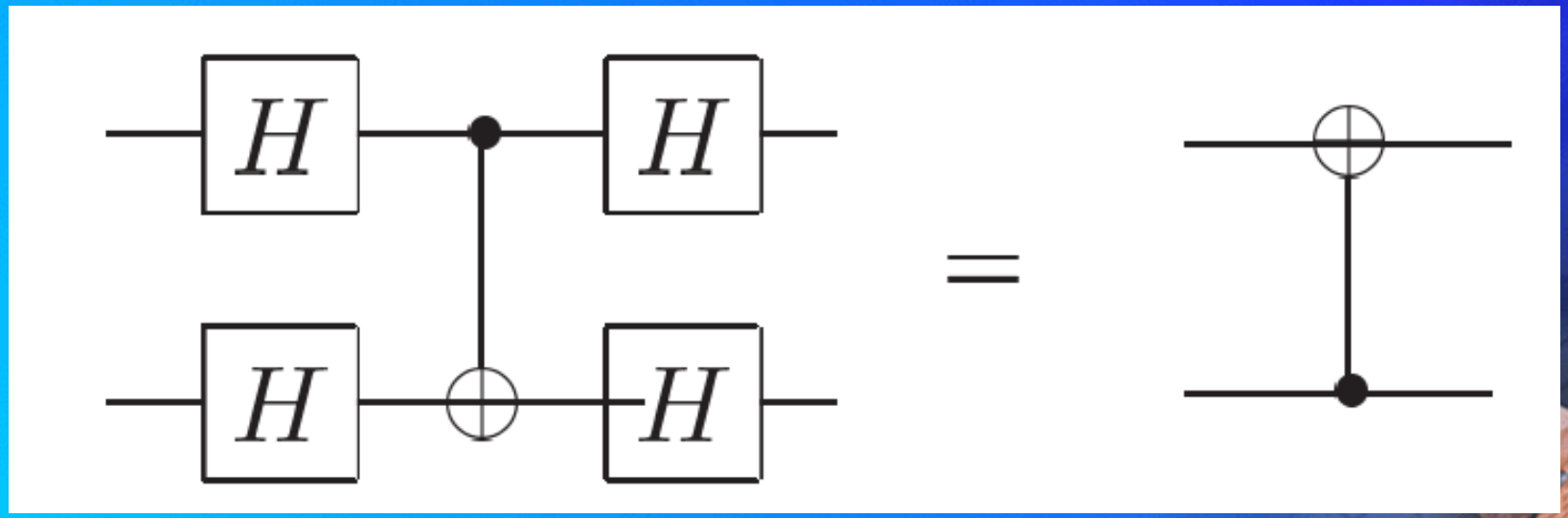
Figure 1.13. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).



Measurement in the basis of the Bell states

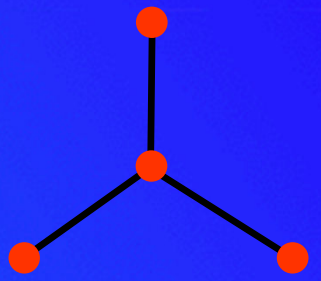
等价的量子线路



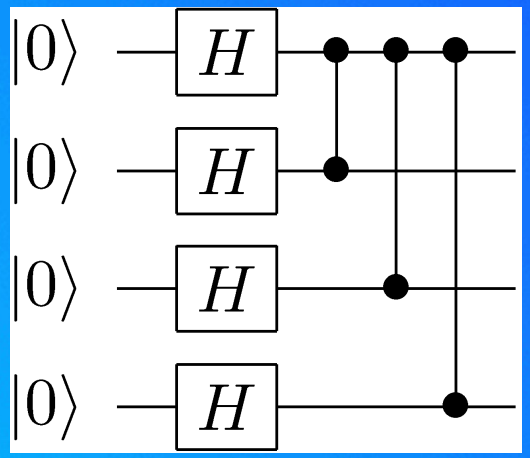


Graph states

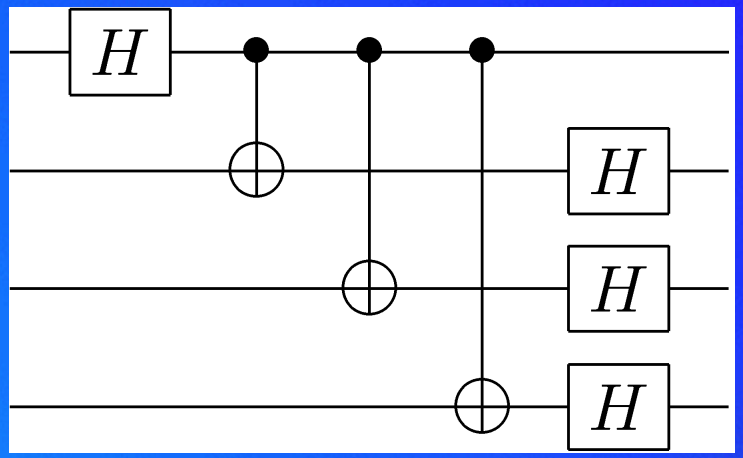
4-qubit GHZ graph state



$$\begin{matrix} ZIII \\ IZII \\ IIZI \\ IIIZ \end{matrix}$$



=



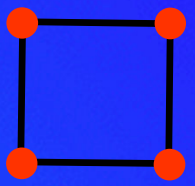
$$\begin{matrix} XZZZ \\ ZXII \\ ZIXI \\ ZIIX \end{matrix}$$

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

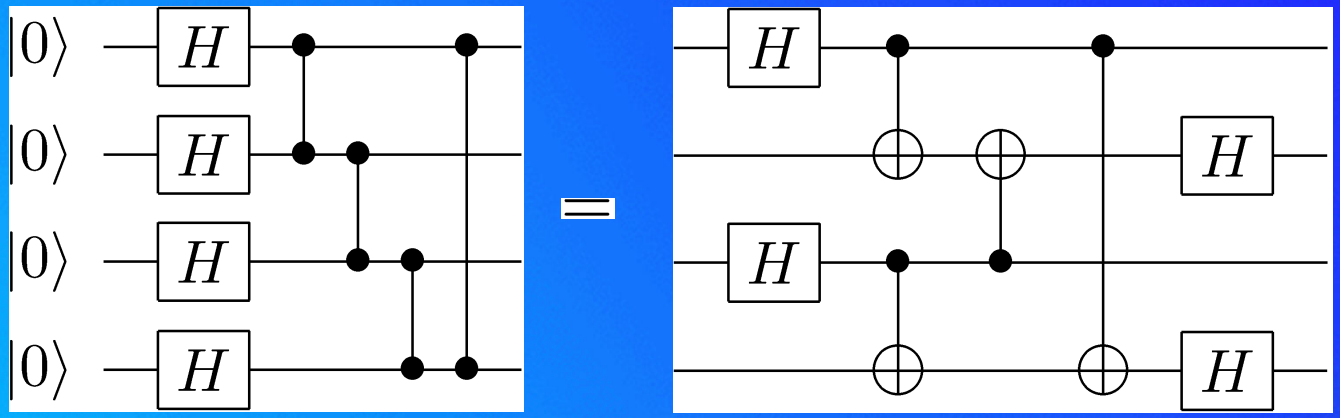
From Caves

Graph states

2 x 2 cluster state



$$\begin{matrix} ZIII \\ IZII \\ IIZI \\ IIIZ \end{matrix}$$



$$\begin{matrix} XZIZ \\ ZXZI \\ IZXZ \\ ZIZX \end{matrix}$$

$$|\psi\rangle = \frac{1}{2}\left(|0\bar{0}0\bar{0}\rangle + |1\bar{1}0\bar{1}\rangle + |0\bar{1}1\bar{1}\rangle + |1\bar{0}1\bar{0}\rangle\right)$$

From Caves

参考书目

教材

- Quantum computation and quantum information by M.A. Nielsen and I.L. Chuang, Cambridge University Press, 2010

其他参考书

- 量子信息

马雄峰、张行健、黄溢智，《量子信息简明教程》，清华大学出版社，2023.

- 量子力学

王向斌、沈艺鑫、于云龙、秦季茜、徐海，《量子力学基础教程》，清华大学出版社，2023.

谢谢

中国科学技术大学 陈凯