



西安电子科技大学

XIDIAN UNIVERSITY

雷达信号处理国家级重点实验室

National Laboratory of Radar Signal Processing

## 2.1 数学基础

## 2.2 量子力学的假设

## 2.3 密度算子

## 2.4 EPR和Bell不等式

## 2.5 量子超密编码

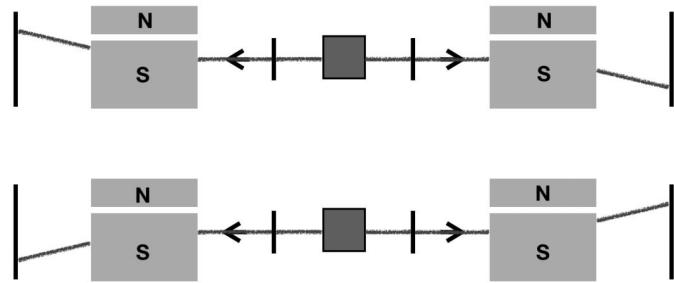


# 纠缠态

## ● 经典 VS 量子

一副手套，随机抽出一只，不看，直接寄给北京的同学A，另一只寄给上海的同学B。

➤ 问题：当A同学打开包裹，看到是“左手”手套时，他瞬间能知道什么？



$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\text{左}} \otimes |1\rangle_{\text{右}} + |1\rangle_{\text{左}} \otimes |0\rangle_{\text{右}})$$

把手套换成两个纠缠的光子。我们制造一对处于“纠缠态”的光子，一个发给A，一个发给B。

· 关键点：在A测量之前，每个光子都处于一种“既是0又是1”的叠加态，而且它们的状态是关联在一起的。这种关联，与手套有本质区别。



## ● 两个单量子比特构成复合系统

左

$$|\phi_1\rangle = a_1|0\rangle + b_1|1\rangle$$

右

$$|\phi_2\rangle = a_2|0\rangle + b_2|1\rangle$$

$$\begin{aligned} |\psi\rangle &= |\phi_1\rangle \otimes |\phi_2\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \\ &= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle \end{aligned}$$

- 左边是0，右边可能是0，也可能是1
- 左边是1，右边可能是0，也可能是1

**不具备强关联特性！！！**



## ● 什么是纠缠态

- 当量子比特的叠加态无法用各量子比特的张量积表示时，这种叠加态称为量子纠缠态。例如，

$$\frac{1}{\sqrt{2}} \{ |00\rangle + |10\rangle \} = \frac{1}{\sqrt{2}} |0\rangle |0\rangle + \frac{1}{\sqrt{2}} |1\rangle |0\rangle \rightarrow \frac{1}{\sqrt{2}} |0\rangle |0\rangle + \frac{1}{\sqrt{2}} |1\rangle |0\rangle = \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) |0\rangle$$

以上的态就不是纠缠态！！！

$$\frac{1}{\sqrt{2}} \{ |01\rangle + |10\rangle \} = \frac{1}{\sqrt{2}} |0\rangle |1\rangle + \frac{1}{\sqrt{2}} |1\rangle |0\rangle$$

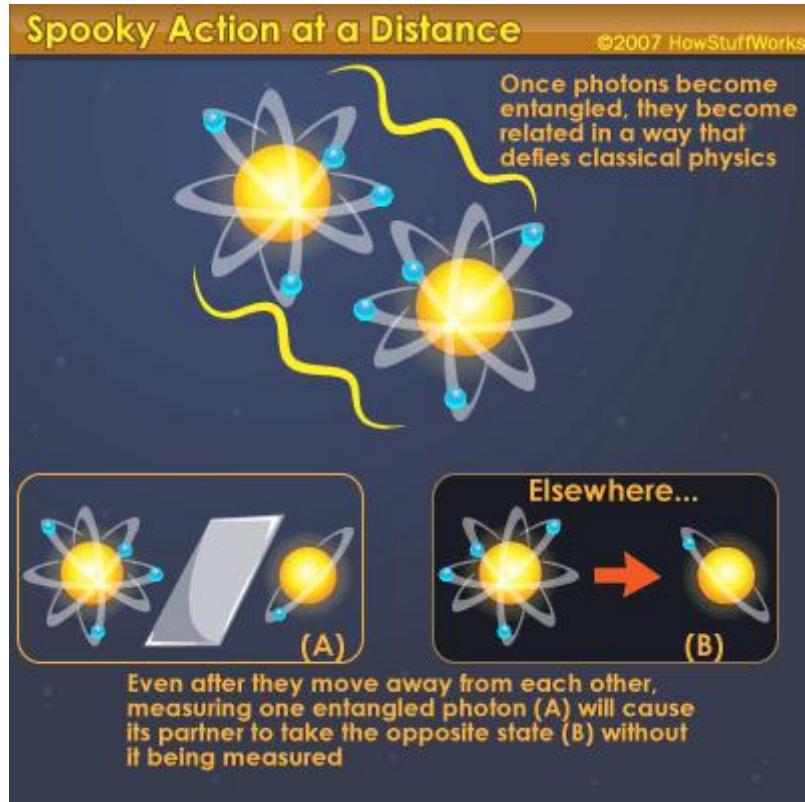
不能够写为同一个矢量与一个叠加态的张量积，称为纠缠态

- $|01\rangle$ ：表示粒子1处于0状态，粒子2处于1状态。
- $|10\rangle$ ：表示粒子1处于1状态，粒子2处于0状态。
- $\frac{1}{\sqrt{2}}$ ：是概率幅，保证总概率为1。
- 加号 +：关键所在！它代表的是相干叠加，而不是经典的“要么...要么...”。



# 纠缠态

- 纠缠是量子力学所特有的一个基本性质，它是两体或多体量子系统之间存在非定域、非经典的强关联
  - (无论子系统相隔多远) 一个子系统的塌缩会影响另一个子系统的状态



$$|\varphi\rangle_{12} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{12}$$

若用 $\{|0\rangle, |1\rangle\}$ 基测1(或2)系统，测得 $|0\rangle$ 和 $|1\rangle$ 的概率各为 $1/2$

当测量1系统得到 $|0\rangle$ 时，意味着复合系统整体状态塌缩为 $|00\rangle$ ，即2系统的状态也变成了 $|0\rangle$

塌缩效应是瞬时的（与距离无关），  
但这并不能做通信！



- 纠缠特性在量子通信、量子密码、量子计算中均有重要应用
- 前面说过，同一量子态在不同基下有多种不同表示
- 纠缠态中，用某个基测量1系统，可使2系统塌缩到相应基态之一

$$|\varphi\rangle_{12} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{12} = \frac{1}{\sqrt{2}} (|++\rangle + |--\rangle)_{12}$$

用 $\{|0\rangle, |1\rangle\}$ 基测1，可使2塌缩到 $|0\rangle$ 或 $|1\rangle$ ，用 $\{|+\rangle, |-\rangle\}$ 基测1，可使2塌缩到 $|+\rangle$ 或 $|-\rangle$

更一般地：  $|\varphi\rangle_{12} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{12} = \frac{1}{\sqrt{2}} (|B_1\rangle|B_1\rangle + |B_2\rangle|B_2\rangle)$

$$|B_1\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \quad |B_2\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$$

$$|0\rangle = \cos\theta|B_1\rangle + \sin\theta|B_2\rangle, \quad |1\rangle = \sin\theta|B_1\rangle - \cos\theta|B_2\rangle$$

性质：用不同基测1，可控制2塌缩到（连续变化的）不同基的基态



## ● 贝尔态

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\{|01\rangle + |10\rangle\} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\{|00\rangle - |11\rangle\} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

贝尔态用于描述两个量子比特 (Qubit) 系统的四种最大纠缠态。它得名于爱尔兰物理学家，著名的贝尔不等式的提出者约翰·斯图尔特·贝尔

也可以简写为

$$\left\{ \begin{array}{l} |\Psi^{(\pm)}\rangle = \frac{1}{\sqrt{2}}\{|01\rangle \pm |10\rangle\} = \frac{1}{\sqrt{2}}\{|0\rangle \otimes |1\rangle \pm |1\rangle \otimes |0\rangle\} \\ |\Phi^{(\pm)}\rangle = \frac{1}{\sqrt{2}}\{|00\rangle \pm |11\rangle\} = \frac{1}{\sqrt{2}}\{|0\rangle \otimes |0\rangle \pm |1\rangle \otimes |1\rangle\} \end{array} \right.$$



## ● Bell态的产生

在量子光学实验中，产生纠缠的双光子态最常见的方法是自发参量下转换（SPDC）的方案。在II型 SPDC 中，信号光子和闲置光子的偏振相互垂直，其中一个称为 $\circ$ 光，另一个称为 $e$ 光，晶体的双折射效应使得信号光子和闲置光子的出射方向分布在两个轴线不同的圆锥面上，如下图所示：

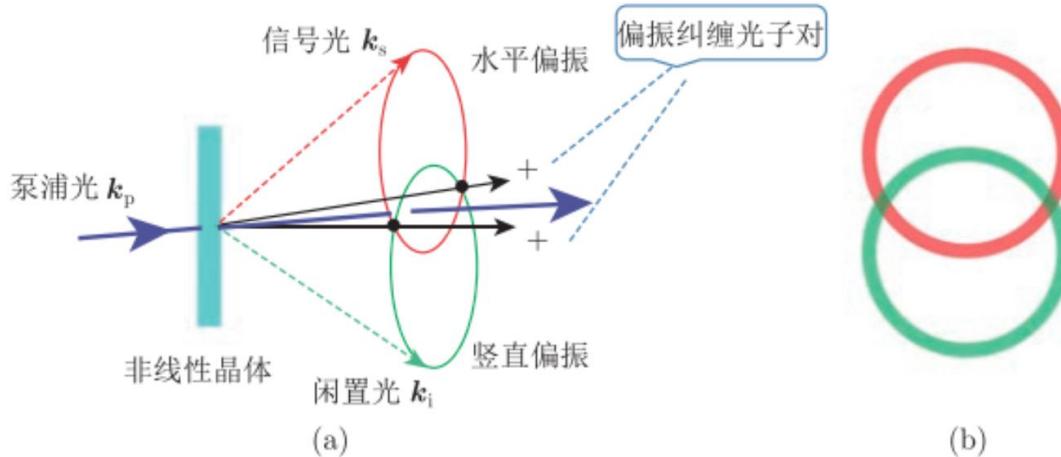


图 3.16 II-型 SPDC 对应的光路示意图 (a) 及出射光对应光锥的截面图 (b)



## ● Bell态的产生

➤ 对于图中两个光锥的交叠区域，我们无法分辨光子是 e 偏振还是 o 偏振，因此这一不可区分性为实验生成偏振纠缠的光子对提供了一种方案，对于这样的 SPDC 过程，可以引入下述的哈密顿量来描述纠缠光子对的生成：

$$\hat{H}_{II} = \frac{1}{\sqrt{2}} \hbar \eta \left( \hat{a}_{Hs}^\dagger \hat{a}_{Vi}^\dagger + \hat{a}_{Vs}^\dagger \hat{a}_{Hi}^\dagger \right) + h.c.$$

- 其中， $\hat{a}_{Hs}^\dagger$ 、 $\hat{a}_{Vs}^\dagger$  对应水平和竖直偏振信号光子的产生算子； $\hat{a}_{Vi}^\dagger$ 、 $\hat{a}_{Hi}^\dagger$  对应水平和竖直闲置光子的产生算符； $\eta$  为对应的非线性耦合系数。
- 对于初始状态  $|\psi(0)\rangle = |0_H, 0_V\rangle_s |0_H, 0_V\rangle_i$ ，若考虑一级近似，得到输出状态为

$$\begin{aligned} |\psi(t)\rangle &\sim (1 - it\hat{H}_{II}t) |\psi(0)\rangle \\ &= |\psi(0)\rangle - i\eta t \frac{1}{\sqrt{2}} \left( |1_H, 0_V\rangle_s |0_H, 1_V\rangle_i + |0_H, 1_V\rangle_s |1_H, 0_V\rangle_i \right) \end{aligned}$$

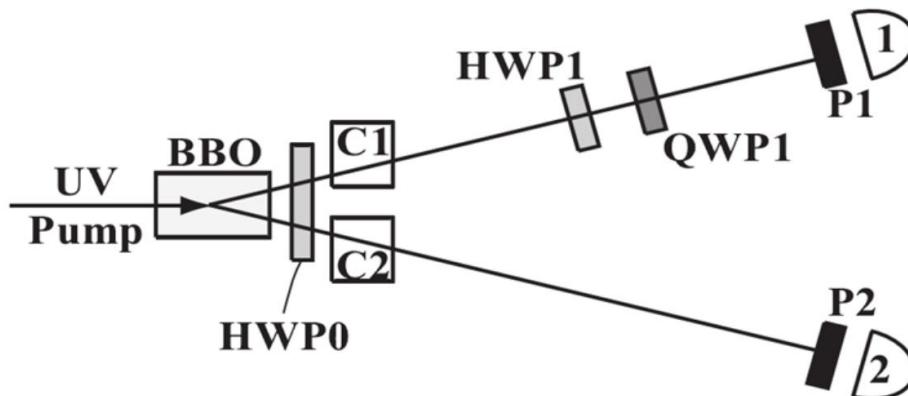


## ● Bell态的产生

➤ 定义  $|H\rangle_{s(i)} = |1_H, 0_V\rangle_{s(i)}$ ,  $|V\rangle_{s(i)} = |0_H, 1_V\rangle_{s(i)}$ , 则上述方程第二项可以记为:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|V\rangle_i + |V\rangle_s|H\rangle_i)$$

● 显然, 上述等式为标准的 Bell 态。通过调节半波片 HWP1 和四分之一波片 QWP1 也可以很容易地得到四个 Bell 态中的任意一个。



其余三个 Bell 态可表示为:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|V\rangle_i - |V\rangle_s|H\rangle_i),$$
$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|H\rangle_i \pm |V\rangle_s|V\rangle_i)$$



## ● EPR佯谬

1935年，爱因斯坦、波多尔斯基和罗森提出了著名的EPR佯谬。

➤ 他们的逻辑（基于定域实在论）：

1. 实在性：如果一个物理量的值可以被精确预测而不扰动系统，那么它必然对应着一个客观存在的元素。
2. 定域性：不存在超光速的信号传递。
3. 推论：既然我测量A粒子能瞬间确定B粒子的状态，那么B粒子的状态必然是早就确定好的（存在一个“隐变量”）。所以，量子力学是不完备的！

➤ 爱因斯坦认为：量子力学背后应该有一个更深刻的、满足定域实在论的理论。



## ● 贝尔不等式

约翰·贝尔提出了一个天才的想法。他设计了一个数学不等式——贝尔不等式。

- 核心思想：这个不等式是所有定域隐变量理论都必须遵守的。如果量子力学的预测违背了这个不等式，就证明爱因斯坦的“定局实在论”是错的。
- 比喻：就像一场审判。贝尔不等式是“经典理论”必须遵守的法律。量子力学是否“违法”了呢？

从20世纪80年代开始，阿斯佩等人的一系列精妙实验给出了最终判决。

- 结果：实验数据明确地违背了贝尔不等式，并以极高的精度与量子力学的预言相符。
- 结论：
  1. 量子纠缠是非定域的。两个纠缠粒子之间存在一种超越空间的关联。
  2. 这种关联不能用于超光速传递信息。因为B方看到的结果是随机的，他无法判断这个随机结果是自身固有的，还是因为A测量了远方粒子导致的。没有信息的传递，不违背相对论。
  3. “鬼魅般的超距作用”是真实存在的！这揭示了自然界一个深刻的本质：在量子层面，宇宙是一个不可分割的整体。



## ● 贝尔不等式（知识拓展）

假设两个观察者A和B分别对光子对的个别光子做偏振测量，两个人可以任意选择各种不同测量的基底。假设A选择a和a' 两种基底，B选择b和b' 为基底。用  $E(a,b)$  表示A用a，B用b为基底时，经过反复多次测量后的，统计平行和垂直两种几率差（即期望值），那么经典理论的预测总是有以下不等式

$$-2 \leq E(a,b) - E(a,b') + E(a',b) - E(a',b') \leq 2$$

**这就是贝尔不等式！！！** [潘建伟新年演讲：量子革命](#)

用某个算符  $\hat{B}$  （贝尔算符）表示在一定量子态上的平均值将贝尔不等式表示为

$$-2 \leq \langle \psi | \hat{B} | \psi \rangle \leq 2$$



# 纠缠态

## 两粒子纠缠态

$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$$

如果测量结果是预先确定的，沿a, b, c三个方向进行测量的所有结果都在这里

	粒子1			粒子2			
测量方向	a	b	c	a	b	c	概率
“预先确定的”测量结果	0	0	0	1	1	1	$P_1$
	0	0	1	1	1	0	$P_2$
	0	1	0	1	0	1	$P_3$
	0	1	1	1	0	0	$P_4$
	1	0	0	0	1	1	$P_5$
	1	0	1	0	1	0	$P_6$
	1	1	0	0	0	1	$P_7$
	1	1	1	0	0	0	$P_8$

▷ 粒子1沿a方向的测量结果为“0”，同时粒子2沿b方向的测量结果为“0”的概率为

$$P(a0, b0) = P_3 + P_4$$

▷ 粒子1沿a方向的测量结果为“0”，同时粒子2沿c方向的测量结果为“0”的概率为

$$P(a0, c0) = P_2 + P_4$$

▷ 粒子1沿c方向的测量结果为“0”，同时粒子2沿b方向的测量结果为“0”的概率为

$$P(c0, b0) = P_3 + P_7$$

▷ 定域实在论要求：

$$P_3 + P_4 \leq P_3 + P_4 + P_2 + P_7$$

$$P(a0, b0) \leq P(a0, c0) + P(c0, b0)$$

$$\parallel \\ P_3 + P_4$$

$$\parallel \\ P_2 + P_4$$

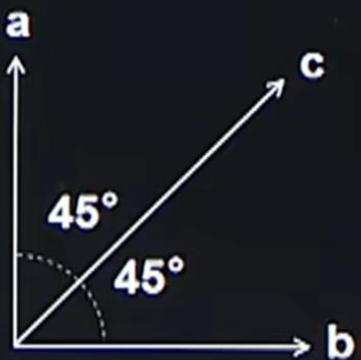
$$\parallel \\ P_3 + P_7$$



## ▷ 量子力学预言:

$$P(a0, b0) = \frac{1}{2} \sin^2 \left( \frac{a-b}{2} \right)$$

选取这样三个测量方向:



$$P(a0, b0) = \frac{1}{2} (\sin^2 45^\circ)$$

$$P(a0, c0) = \frac{1}{2} (\sin^2 22.5^\circ)$$

$$P(c0, b0) = \frac{1}{2} (\sin^2 22.5^\circ)$$

## ▷ 按照定域实在论:

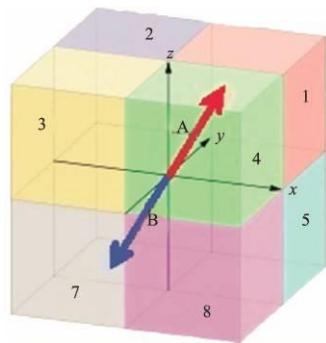
$$\frac{1}{2} \sin^2 45^\circ \leq \frac{1}{2} \sin^2 22.5^\circ + \frac{1}{2} \sin^2 22.5^\circ$$

即是  $0.2500 \leq 0.1464$



表1 AB纠缠态自旋矢量的8种可能性以及4个相关函数的值

$L$	$A_x$ $A_y$ $A_z$ (红矢)	$B_x$ $B_y$ $B_z$ (蓝矢)	$P$	$P_{xx}(L)$	$P_{xz}(L)$	$P_{zy}(L)$	$P_{xy}(L)$
1	+++	- - -	$n_1$	-1	-1	-1	-1
2	-++	+ - -	$n_2$	-1	+1	-1	+1
3	--+	+ + -	$n_3$	-1	+1	+1	-1
4	+ - +	- + -	$n_4$	-1	-1	+1	+1
5	+ + -	- - +	$n_5$	-1	+1	+1	-1
6	- + -	+ - +	$n_6$	-1	-1	+1	+1
7	-- -	+ + +	$n_7$	-1	-1	-1	-1
8	+ - -	- + +	$n_8$	-1	+1	-1	+1



$$P_{xx} = -n_1 - n_2 - n_3 - n_4 - n_5 - n_6 - n_7 - n_8 = -1,$$

$$P_{xz} = -n_1 + n_2 + n_3 - n_4 + n_5 - n_6 - n_7 + n_8,$$

$$P_{zy} = -n_1 - n_2 + n_3 + n_4 + n_5 + n_6 - n_7 - n_8,$$

$$P_{xy} = -n_1 + n_2 - n_3 + n_4 - n_5 + n_6 - n_7 + n_8.$$



$$\begin{aligned}|P_{xz} - P_{zy}| &= 2|n_2 - n_4 - n_6 + n_8| \\ &= 2|(n_2 + n_8) - (n_4 + n_6)| . \quad (1)\end{aligned}$$

$$\begin{aligned}2|(n_2 + n_8) - (n_4 + n_6)| &\leq 2(n_2 + n_4 + n_6 + n_8) \\ &= (n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8) + \\ &\quad (-n_1 + n_2 - n_3 + n_4 - n_5 + n_6 - n_7 + n_8) \\ &= 1 + P_{xy} . \quad (2)\end{aligned}$$

$$|P_{xz} - P_{zy}| \leq 1 + P_{xy} . \quad (3)$$



## ● 纠缠态的应用

- 量子隐形传态
- 量子计算：纠缠是量子并行计算的资源。多个量子比特纠缠在一起，可以同时处理海量信息，实现指数级加速。（例如：秀尔算法破解RSA密码）
- 量子密码术：利用纠缠的关联性和测量的坍缩特性，可以实现量子密钥分发。任何窃听行为都会破坏纠缠态，从而被通信双方发现，原理上绝对安全。
- 量子计量：利用纠缠态，可以超越经典极限的测量精度，例如制造更精确的原子钟和干涉仪。



## ● 总结

### ➤ · 核心思想：

- 量子纠缠是一种非定域的、强大的量子关联。
- 它源于多粒子系统的波函数不可分。
- 它通过了贝尔实验的检验，否定了定域实在论。
- 关键特性：非定域性、不可克隆、作为资源。
- 应用：量子通信、量子计算、量子精密测量的核心资源。

### ➤ 思考：

- 纠缠的度量有多少种？
- 多粒子纠缠有多复杂？
- 纠缠与时空本质有什么联系？

理解量子纠缠，不仅是掌握一门技术，更是对我们世界观的一次革新。它告诉我们，宇宙在最基本的层面上，是相互连接、不可分割的。



西安电子科技大学

XIDIAN UNIVERSITY

雷达信号处理国家级重点实验室

National Laboratory of Radar Signal Processing

## 2.1 数学基础

## 2.2 量子力学的假设

## 2.3 密度算子

## 2.4 EPR和Bell不等式

## 2.5 量子超密编码

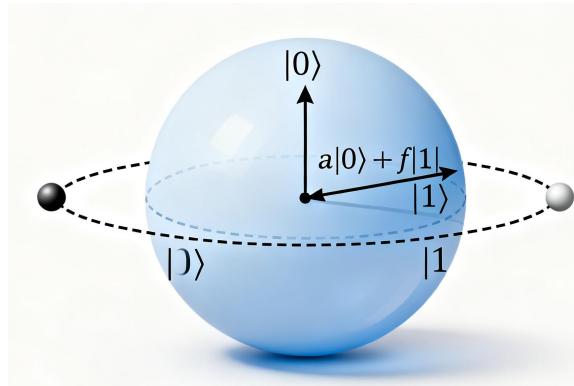


## ● 核心思想

用量子纠缠的资源，实现“一个量子比特传输两个经典比特信息”的神奇效果

**经典信息：**0 或 1，一个比特只能携带一个比特信息

**量子信息：**量子比特 ( $|0\rangle$ ,  $|1\rangle$ , 或叠加态  $a|0\rangle + b|1\rangle$ )。神奇之处在于叠加和纠缠！



**纠缠：**两个或多个粒子状态高度关联，无法单独描述。

◆ 关键特性：

- ✓ 强关联：测量一个粒子状态，瞬间确定另一个粒子状态（即使相隔遥远）。
- ✓ 资源共享：纠缠对是一个整体资源！这是超密编码的核心资源。

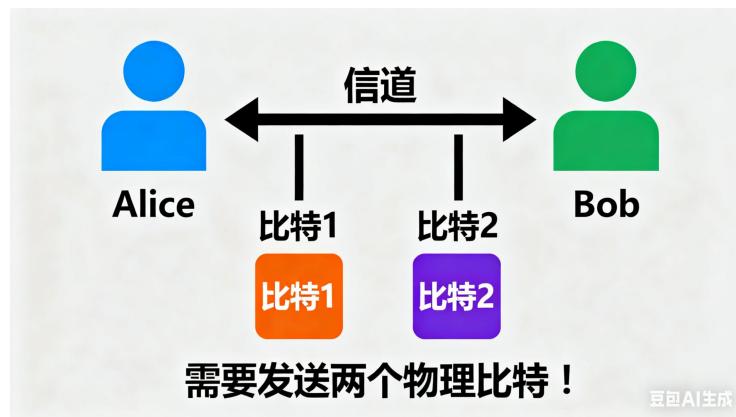


## ● 经典通信的局限性

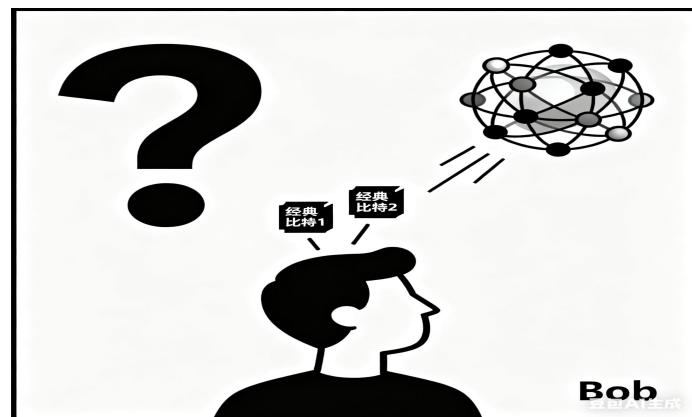
**场景：**Alice想发送两个经典比特的信息（00, 01, 10, 11）给Bob

### ■ 经典通信任务：

无论信息内容是什么，Alice都必须通过信道发送两个独立的物理载体（比特）给Bob。效率受限。

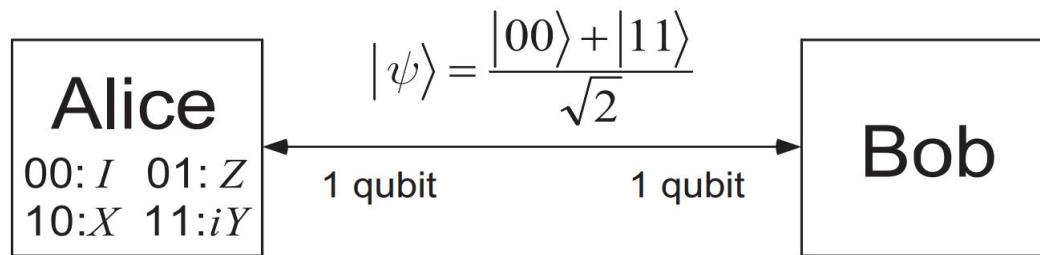


- **量子挑战：**能否做得更好？
  - ◆ **问题：**利用神奇的量子资源（尤其是纠缠），Alice能否只发送一个量子比特，就让Bob获得两个经典比特的信息？
- 答案是：YES! 这就是**量子超密编码** (Superdense Coding)!





## ● 量子超密编码协议1



1. 第三方（常叫Charlie或源）制备一对处于Bell态  $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$  的纠缠粒子。将粒子A发给Alice，粒子B发给Bob。

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left\{ |0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B \right\}$$

Alice和Bob提前共享一个纠缠对（特定Bell态）。这是协议的前提和关键资源！



## ● 量子超密编码协议2

2. Alice根据她想发送的两个经典比特信息，对她手中的粒子A施加特定的幺正操作。**(变成4个BELL态中的一个)**

### ■ 00 不做操作 (I)

$$\begin{aligned} I_A I_B |\beta_{00}\rangle &= |\beta_{00}\rangle \\ &= \frac{1}{\sqrt{2}} \left\{ |0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B \right\} \end{aligned}$$

### ■ 10 应用 Z 门 (相位翻转)

$$\begin{aligned} Z_A I_B |\beta_{00}\rangle &= \frac{1}{\sqrt{2}} \left\{ Z_A |0\rangle_A \otimes I_B |0\rangle_B + Z_A |1\rangle_A \otimes I_B |1\rangle_B \right\} \\ &= \frac{1}{\sqrt{2}} \left\{ |0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B \right\} \end{aligned}$$

### ■ 01 应用 X 门 (比特翻转)

$$\begin{aligned} X_A I_B |\beta_{00}\rangle &= \frac{1}{\sqrt{2}} \left\{ X_A |0\rangle_A \otimes I_B |0\rangle_B + X_A |1\rangle_A \otimes I_B |1\rangle_B \right\} \\ &= \frac{1}{\sqrt{2}} \left\{ |1\rangle_A \otimes |0\rangle_B + |0\rangle_A \otimes |1\rangle_B \right\} \end{aligned}$$

### ■ 11 应用 iY 门 (X+Z组合)

$$\begin{aligned} (ZX)_A I_B |\beta_{00}\rangle &= \frac{1}{\sqrt{2}} \left\{ (ZX)_A |0\rangle_A \otimes I_B |0\rangle_B + (ZX)_A |1\rangle_A \otimes I_B |1\rangle_B \right\} \\ &= \frac{1}{\sqrt{2}} \left\{ |1\rangle_A \otimes |0\rangle_B + |0\rangle_A \otimes |1\rangle_B \right\} \end{aligned}$$

Alice的本地操作巧妙地利用纠缠，将两个比特的信息编码到了整个纠缠对的状态变化中。她只需要操作自己这一个粒子！



## ● 量子超密编码协议3/4

3. Alice发送: Alice将她操作后的粒子A通过量子信道发送给Bob。

(仅一个量子比特)

Alice只需将她手中的单个量子比特发送给Bob。

4. Bob的解读: 贝尔态测量

- Bob现在拥有什么? 他原本的粒子B + Alice刚发来的粒子A。
- Bob需要做什么? 对这两个粒子进行贝尔基测量 (Bell State Measurement, BSM)。

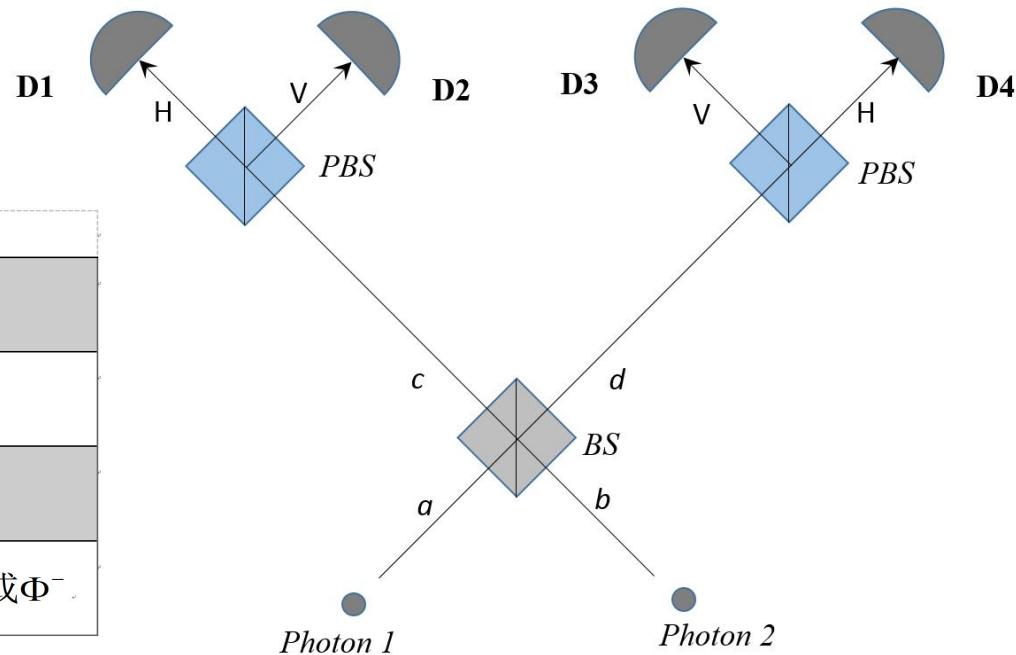
Bob通过BSM确定纠缠对现在的状态, 这个状态直接唯一对应Alice想发送的两个比特信息。Bob成功解码!



## ● 知识拓展：如何测量Bell态

一种偏振编码下Bell态的区分方法（实现部分Bell态分辨）

	D1	D2	D3	D4
D1	$\Phi^+$ 或 $\Phi^-$	$\Psi^+$	$\Psi^-$	fail
D2	$\Psi^+$	$\Phi^+$ 或 $\Phi^-$	fail	$\Psi^-$
D3	$\Psi^-$	fail	$\Phi^+$ 或 $\Phi^-$	$\Psi^+$
D4	fail	$\Psi^-$	$\Psi^+$	$\Phi^+$ 或 $\Phi^-$



探测器的响应组合所对应的贝尔态形式。上表中fail的元素表示测量失败，即理论上是无法出现的结果，若实验中出现则说明是探测器的暗计数所致。

测量偏振编码的bell态装置图。PBS为偏振分束器，规定H光通过，V光反射；BS为普通50/50分束器，D1、D2、D3、D4为探测器。



## ● 总结

### ➤ 量子超密编码流程图



### 1. 关键点总结

- **输入**: Alice的两个经典比特。
- **核心资源**: 一个共享的纠缠对。
- **量子通信量**: Alice只发送了一个量子比特。
- **输出**: Bob成功获得两个经典比特。
- **核心**: 利用纠缠作为“信道”或“资源”，Alice的本地操作将信息“写入”纠缠态的变化，Bob通过联合测量读取。

### 2. 量子优势何在？

- **突破了经典信道容量限制！** 用“一个量子比特的传输”完成了“两个经典比特信息”的传递。体现了量子信息处理的强大威力。



## 3. 为什么安全？

- 窃听者Eve如果截获Alice发送的那个量子比特，她无法从中直接读取信息，因为那只是一个粒子，处于叠加态的一部分，单独看是随机的。
- Eve如果想干扰（比如测量它），会破坏纠缠态或引入错误，容易被Alice和Bob通过后续校验发现（虽然超密编码本身不直接提供无条件安全，但结合其他技术如量子密钥分发QKD的思想，体现了量子通信的安全性潜力）。
- 量子不可克隆定理保证了Eve无法完美复制那个量子比特来窃听。

## 4. 现实与展望

### • 挑战：

- ✓ 制备和维持高质量纠缠困难（退相干）。
- ✓ 贝尔态测量 (BSM) 效率和高保真度实现是技术难点（尤其在光子系统中）。
- ✓ 需要可靠的量子信道传输量子比特。

### • 意义：

- ✓ 量子信息基本原理的绝佳演示（纠缠、操作、测量）。
- ✓ 未来量子通信网络（如量子互联网）的关键技术组件之一，用于高效节点间信息传输。
- ✓ 展示了量子资源（纠缠）如何赋能信息处理。



## ● 思考问题

1. 量子超密编码中，信息主要存储在什么地方？

(答案：编码在纠缠对的状态变化中)

2. 如果Alice和Bob没有提前共享纠缠对，超密编码还能工作吗？

(答案：不能，纠缠是核心资源)

3. Bob需要测量什么才能解码信息？

(答案：贝尔基测量BSM)

4. 经典通信能实现发送1个物理比特传递2个比特信息吗？

(答案：不能，香农极限)