

初识量子力学

陈童

2024 年 8 月 26 日

目录

第五章 量子纠缠	2
5.1 两体纠缠态	2
5.2 纠缠态与混态	7
5.3 用例子说明量子纠缠态的神奇	12
5.3.1 量子纠缠能实现超光速信息传递吗?	12
5.3.2 量子密集编码	18
5.3.3 量子隐形传态	19
5.3.4 GHZ态以及为什么爱因斯坦错了	21

第五章 量子纠缠

前面的章节都是成熟的理论体系，但是本章不同，量子纠缠依然是前沿研究的热门内容，因此本章只能算是一个初步的介绍。值得强调的是，对量子纠缠的深入研究无疑将处于整个物理学研究的核心。

5.1 两体纠缠态

有一条量子力学的基本原理，我们在前面的章节中已经凭借着直觉使用了，但却未加深思和检验，本章我们将看到这条原理会带来多少不可思议的事情。

这条原理涉及到两个子系统的复合系统，我们称这两个子系统为 A 和 B 。假设任意为这两个系统分别取一组可确定区分可能性完备集 $\mathcal{I}_A = \{(i_A), i_A = 1, 2, 3, \dots\}$ 以及 $\mathcal{I}_B = \{(i_B), i_B = 1, 2, 3, \dots\}$ ，注意， i_A 和 i_B 是两个相互独立的指标。则可以构造整个复合系统(记作 AB 系统)的一组可确定区分可能性完备集 $\mathcal{I} = \{(i_A, i_B), i_A \in \mathcal{I}_A, i_B \in \mathcal{I}_B\}$ ，由可确定区分性，我们有如下关系

$$\langle j_A, j_B | i_A, i_B \rangle = \delta_{i_A j_A} \delta_{i_B j_B}, \quad (5.1)$$

其中 $i_A, j_A \in \mathcal{I}_A$, $i_B, j_B \in \mathcal{I}_B$ 。当然，这个关系可以解释成复合系统希尔伯特空间矢量基 $|i_A, i_B\rangle$ 的正交归一性。

假设再取 A 和 B 的另一组可确定区分可能性完备集 \mathcal{I}'_A 和 \mathcal{I}'_B ，则又可以构造复合系统 AB 的另一组可确定区分可能性完备集 $\mathcal{I}' = \{(i'_A, i'_B), i'_A \in \mathcal{I}'_A, i'_B \in \mathcal{I}'_B\}$ 。现在我们可以考虑复合系统从可能性 (i_A, i_B) 到可能性 (j'_A, j'_B) 的跃迁过程，很显然，它实际上就是系统 A 从 (i_A) 跃迁到了 (j'_A) ，同时与之

相独立的, 系统 B 从 (i_B) 跃迁到了 (j'_B) , 根据独立事件概率相乘的性质, 我们有

$$P(i_A, i_B \rightarrow j'_A, j'_B) = P(i_A \rightarrow j'_A)P(i_B \rightarrow j'_B). \quad (5.2)$$

而跃迁概率是由跃迁幅的模方给出的, 所以满足上面这一跃迁概率性质的最自然的跃迁幅关系是

$$\langle j'_A, j'_B | i_A, i_B \rangle = \langle j'_A | i_A \rangle \langle j'_B | i_B \rangle. \quad (5.3)$$

实际上, (5.1)式是(5.3)式的特殊情况, 为了看出这一点, 我们取 $\mathcal{I}'_A = \mathcal{I}_A$, $\mathcal{I}'_B = \mathcal{I}_B$, 从而(5.3)式告诉我们

$$\langle j_A, j_B | i_A, i_B \rangle = \langle j_A | i_A \rangle \langle j_B | i_B \rangle = \delta_{i_A j_A} \delta_{i_B j_B}, \quad (5.4)$$

正是(5.1)式。

对(5.3)式的一种自然解读是

$$|i_A, i_B\rangle = |i_A\rangle |i_B\rangle, \quad (5.5)$$

当然, 同样也有 $|j'_A, j'_B\rangle = |j'_A\rangle |j'_B\rangle$, 进而在算希尔伯特空间内积 $\langle j'_A, j'_B | i_A, i_B \rangle$ 时, 应该分别将 A 的态与 A 的态进行内积, 把 B 的态与 B 的态进行内积, 然后再把结果乘起来, 也就有了(5.3)式。这实际上也是对 $|i_A\rangle |i_B\rangle$ 这种乘法的一个定义, 这种乘法我们在第三章讲量子不可克隆定理时就见过了, 当时我们只是凭直觉来理解它, 现在才开始追溯这种乘法到底是怎么来的。文献中通常称这种乘法为张量积, 并记作 $|i_A\rangle \otimes |i_B\rangle$, 本书采用更自然(但是数学上稍微含糊一点)的记号 $|i_A\rangle |i_B\rangle$ 。(5.5)式告诉我们, 复合系统的矢量基可以由两个子系统矢量基的张量积给出, 其物理含义就是, 复合系统的可能性 (i_A, i_B) 由两个子系统相互独立的可能性 $(i_A), (i_B)$ 并置而成。

\mathcal{I} 作为复合系统的一组可确定区分可能性完备集, 则根据跃迁幅乘法, 复合系统的任何量子态 $|\psi\rangle$ 当然都能用 \mathcal{I} 来展开

$$|\psi\rangle = \sum_{(i_A, i_B) \in \mathcal{I}} |i_A, i_B\rangle \langle i_A, i_B | \psi \rangle. \quad (5.6)$$

记跃迁幅 $\langle i_A, i_B | \psi \rangle = \psi_{i_A i_B}$ (为一个复数), 则根据(5.5)式可知

$$|\psi\rangle = \sum_{(i_A, i_B) \in \mathcal{I}} \psi_{i_A i_B} |i_A\rangle |i_B\rangle. \quad (5.7)$$

不难看出, 当且仅当 $\psi_{i_A i_B}$ 具有 $\psi_{i_A i_B} = \phi_{i_A} \varphi_{i_B}$ 的形式时, 复合系统 AB 的量子可能性 $|\psi\rangle$ 才能写成 A 和 B 两个子系统可能性的乘积(张量积), 此时即有

$$|\psi\rangle = \sum_{(i_A, i_B) \in \mathcal{I}} \phi_{i_A} \varphi_{i_B} |i_A\rangle |i_B\rangle = \left(\sum_{i_A \in \mathcal{I}_A} \phi_{i_A} |i_A\rangle \right) \left(\sum_{i_B \in \mathcal{I}_B} \varphi_{i_B} |i_B\rangle \right) = |\phi\rangle |\varphi\rangle,$$

式中 $|\phi\rangle = \sum_{i_A \in \mathcal{I}_A} \phi_{i_A} |i_A\rangle$, $|\varphi\rangle = \sum_{i_B \in \mathcal{I}_B} \varphi_{i_B} |i_B\rangle$. 这时候就称可能性 $|\psi\rangle$ 为可分解可能性, 因为它可以按照子系统进行因式分解, 或者称 $|\psi\rangle$ 为可分量子态。换言之, 复合系统的可分量子可能性是由两个子系统相互独立的可能性 $|\phi\rangle$ 和 $|\varphi\rangle$ 并置而成。

如果 $\psi_{i_A i_B}$ 不具有 $\phi_{i_A} \varphi_{i_B}$ 的形式, 那可能性 $|\psi\rangle$ 就不能按照子系统进行因式分解, 可以称之为不可分解的整体可能性(整体就是指 AB 整体, 子系统 A 和 B 都是这个整体的部分), 不过, 由于历史原因, 文献中通常称这时候的 $|\psi\rangle$ 为量子纠缠态。不可分解的整体可能性不能理解成 A, B 两个部分各自局部可能性的简单并置, 所以它是整体性的。

假设记系统 A 的希尔伯特空间为 \mathcal{H}_A , 设其维数为 $\dim(\mathcal{H}_A) = N_A$, 记系统 B 的希尔伯特空间为 \mathcal{H}_B , 其维数为 $\dim(\mathcal{H}_B) = N_B$. 再记整个复合系统的希尔伯特空间为 \mathcal{H} , 则由于 \mathcal{H} 的基矢量为所有可能的 $|i_A, i_B\rangle$, 很显然一共有 $N_A N_B$ 个不同的基矢量, 所以

$$\dim(\mathcal{H}) = N_A N_B = \dim(\mathcal{H}_A) \dim(\mathcal{H}_B). \quad (5.8)$$

通常称复合系统的希尔伯特空间为两个子系统希尔伯特空间的张量积, 记作 $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. 它的意思就是, \mathcal{H} 中的所有态矢量, 都具有(5.7)的形式, 这样的态矢量由复数 $\psi_{i_A i_B}$ 参数化, 这样的复数有 $N_A N_B$ 个。考虑到态矢量相差一个整体复数因子所描述的是同一个量子态, 也就是 $\lambda|\psi\rangle$ 与 $|\psi\rangle$ 在物理上等价, 即 $\lambda\psi_{i_A i_B} \sim \psi_{i_A i_B}$, 所以, \mathcal{H} 的所有量子态由 $N_A N_B - 1$ 个复数参数化。另一方面, 根据上面的讲述可知, 所有可分量子态由复数 ϕ_{i_A} 和复数 φ_{i_B} 共同参数化, 很显然这样的复数只有 $N_A + N_B$ 个, 但是, 考虑到 $\lambda\phi_{i_A} \sim \phi_{i_A}$ 、 $\eta\varphi_{i_B} \sim \varphi_{i_B}$ 所以实际上只有 $N_A + N_B - 2$ 个复数参数化了不同的可分量子态。

很显然, 只要 $N_A > 1, N_B > 1$, 那么就有 $N_A N_B - 1 > N_A + N_B - 2$, 所以, 复合系统的所有量子可能性中有大量的不可分解整体可能性, 或者换句话说, 希尔伯特空间 \mathcal{H} 中有大量的量子纠缠态。尤其是当 N_A, N_B 都很大时, 量子纠缠态的数目将远远比可分量子态的数目多!

可分量子态和纠缠态有一个本质的区别, 那就是 A, B 两个部分局部的任何操作都无法把一个可分量子态转化为一个纠缠态。为了看清楚这一点, 我们假设有一个可分量子态 $|\phi\rangle|\varphi\rangle$, 我们在 A, B 两个部分上分别进行一个任意的操作, 使得它们分别经历一个么正演化(也叫么正变换), 演化算符分别为 U_A 和 U_B , U_A 只作用在希尔伯特空间 \mathcal{H}_A 上, U_B 则只作用在 \mathcal{H}_B 上, 则很显然, 经过这个演化以后原来的可分量子态变为 $U_A U_B(|\phi\rangle|\varphi\rangle) = U_A|\phi\rangle U_B|\varphi\rangle = |\phi'\rangle|\varphi'\rangle$, 其中 $|\phi'\rangle = U_A|\phi\rangle$ 依然是一个 A 的量子态, 同样 $|\varphi'\rangle = U_B|\varphi\rangle$ 也依然是一个 B 的量子态。操作的最终结果 $|\phi'\rangle|\varphi'\rangle$ 显然依然是可分量子态。所以, 局部的操作无法创造纠缠态, 为了创造出整体的纠缠态, 你需要让 A, B 两部分进行相互作用, 进而产生一个整体的演化。

对纠缠态的刻画可以进一步简化, 为此我们将注意力集中在(5.7)式上, 应用线性代数的奇异值分解定理(这里略过, 感兴趣的读者请自行参考线性代数的书籍)可以证明, 对于每一个给定的 $|\psi\rangle$ 态, 总可以通过合适地选取 \mathcal{I}_A 以及 \mathcal{I}_B , 使得(5.7)式简化成如下形式

$$|\psi\rangle = \sum_i \lambda_i |i\rangle|i\rangle. \quad (5.9)$$

注意到 $|i\rangle_B \sim e^{i\theta_i} |i\rangle_B$, 所以我们只需要合适地调节系统 B 的这些相位 $e^{i\theta_i}$, 就可以让上式中的 $\lambda_i \geq 0$, 进而根据归一化条件 $\langle\psi|\psi\rangle = 1$, 即可以得到 $\sum_i \lambda_i^2 = 1$ 。人们通常令 $\lambda_i^2 = p_i \geq 0$, 所以

$$\sum_i p_i = 1, \quad (5.10)$$

并进而将(5.9)式写成

$$|\psi\rangle = \sum_i \sqrt{p_i} |i\rangle|i\rangle. \quad (5.11)$$

(5.11)式就叫做 A, B 两体复合系统量子态的**施密特分解**, 其中非零的 p_i 数目就称作量子态 $|\psi\rangle$ 的**施密特数**。很显然, 施密特数最小为1, 这时候只有一个非零的 p_i , 不妨设为 p_1 , 根据(5.10)式, 必有 $p_1 = 1$, 从而这时候(5.11)式就相当于

$$|\psi\rangle = |1\rangle|1\rangle, \quad (5.12)$$

从而这时候 $|\psi\rangle$ 必为一个可分量子态(注意 A 的 $|1\rangle$ 和 B 的 $|1\rangle$ 不是一回事)。反过来也一样, 可分量子态必定施密特数为1。所以, 量子态 $|\psi\rangle$ 为可分量子态的充要条件是, 其施密特数为1。从而, 施密特数大于1的量子态都是纠缠态! 从(5.11)式可以看出, 施密特数最大为 $\dim(\mathcal{H}_A)$ 和 $\dim(\mathcal{H}_B)$ 中较小的那个。

因此, 施密特数多少反映了两体纠缠的状况, 施密特数越大就说明纠缠得越厉害。特别的, 如果 $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = d$, 而且所有的 p_i 均相等, 从而 $p_i = 1/d$, 这时候相应的施密特分解即为

$$|\Phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle|i\rangle, \quad (5.13)$$

这样的纠缠态就称作**最大纠缠态**。

多体量子纠缠

读者可以想见, 如果我们的系统是一个多体量子系统, 比方说量子计算机的多量子比特, 再比方说凝聚态物理里面的多体系统(多原子, 多自旋等等), 那么量子纠缠就可能出现在多体之间。可以说多体量子纠缠是整个量子计算和量子信息技术的核心, 比如说, 在量子信息中, 人们总是通过合适的量子编码将量子信息储存在许多量子比特的纠缠态中, 这时候由于量子纠缠态的整体性, 即使存储信息的某些量子比特出现差错, 原来的量子信息也依然能从整体的量子纠缠中得到恢复。不仅如此, 近年来多体量子纠缠也被广泛应用于理论凝聚态甚至量子引力的研究。但是, 如何一般性地刻画多体之间的量子纠缠现在还是一个没有完全解决的问题, 凝聚态物理中常常采用所谓的张量网络来表示多体的量子纠缠态。凝聚态物理学家关心多体量子纠缠的原因在于, 近些年来的研究发现, 有一些量子多体系统的基态其实是一个量子纠缠态, 甚至可能是一个多体长程量子纠缠态, 比方说分数量子霍尔效应的基态就是一个这样的长程量子纠缠态。而处在这种长程量子纠缠态的多体系统常常会有所谓的拓扑序, 会处在某种拓扑相。这种长程量子纠缠和拓扑序近年来引起了理论物理学家们的极大兴趣。

当然也可以仿照着前面关于两体纠缠定义多体量子纠缠态, 不过, 组成整体的部分一多, 就会带来更多的复杂性, 因此多体量子纠缠的刻画和

研究远没有两体量子纠缠那么成熟，因此，我们将不进行一般性的介绍，仅在后文以一个三体量子纠缠态的例子来说明多体纠缠的神奇之处。

5.2 纠缠态与混态

本节我们讲述纠缠态最神奇的一点特性，即如果 AB 整体处于纠缠态，那么你可以完全了解这个整体，但对 A 和 B 这两个部分却必然都带有无知。即，纠缠态是一种可以完全了解整体却无法同时完全了解部分的东西。这种特性当然是经典物理里完全没有的，对于经典的事物，你完全了解了整体必然意味着你同时了解了它的所有部分。但是，量子纠缠态不是这样的。

下面我们先作一些准备。

测量与期望值

在第二章关于量子力学基本原理的讨论中，我们得出过一个重要公式：对某个物理量 A 多次重复实验测得的平均值 $\langle A \rangle$ 等于算符 A 在态上的期望值，即

$$\langle A \rangle = \langle \psi | A | \psi \rangle, \quad (5.14)$$

$|\psi\rangle$ 为系统所处的量子态。我们也说过，物理量 A 的测量值是相应算符 A 的本征值，在单次实验中，我们测得哪个值是随机的，测得本征值 λ_i 的概率为 $p_i = |\langle i | \psi \rangle|^2$ ，式中 $|i\rangle$ 为与本征值 λ_i （请与上文施密特分解中的 λ_i 相区分）相应的本征态。这样算出来的概率 p_i （请与上文施密特分解中的 p_i 区分）当然也可以通过重复多次实验来检验，因此其计算公式应该也能写成期望值的形式，的确，假如定义投影算符 $P_i = |i\rangle\langle i|$ ，则人们很容易验证

$$p_i = \langle \psi | i \rangle \langle i | \psi \rangle = \langle \psi | P_i | \psi \rangle. \quad (5.15)$$

因此，不仅仅物理量的平均值，而且物理量值的概率分布，都可以表达成厄密算符期望值的形式。

以上讨论告诉我们，在量子力学中一切可以通过重复实验来进行检验的量都可以由一个适当厄密算符的期望值来计算，各种厄密算符的期望值就是我们能够从一个量子态中提取的所有信息。

算符求迹

一个矩阵所有对角元的和称为矩阵的迹，我们可以将迹的概念推广到线性算符。对于一个线性算符 \mathcal{O} ，我们记其迹为 $\text{Tr}(\mathcal{O})$ ，定义为

$$\text{Tr}(\mathcal{O}) = \sum_i \langle i | \mathcal{O} | i \rangle, \quad (5.16)$$

式中 $\{|i\rangle\}$ 为希尔伯特空间的一组正交归一矢量基。虽然为了求出算符的迹我们需要选取一个特定的表象，但是利用跃迁元乘法，不难验证算符的迹与具体表象的选取无关，具体证明我们留给读者自行思考。由此可以知道，一个算符的迹就是它在任何一个表象中表示矩阵的迹，特别的，对于厄密算符，我们可以将这个表象选为它的本征表象，这时候算符的迹其实就是所有本征值的和。

假设有两个算符 A 和 B ，利用跃迁元乘法，容易证明算符迹满足如下等式

$$\text{Tr}(AB) = \text{Tr}(BA). \quad (5.17)$$

证明如下， $\text{Tr}(AB) = \sum_i \langle i | AB | i \rangle = \sum_{i,j} \langle i | A | j \rangle \langle j | B | i \rangle = \sum_{i,j} \langle j | B | i \rangle \langle i | A | j \rangle = \sum_j \langle j | BA | j \rangle = \text{Tr}(BA)$ 。不过，值得说明的是，对于无穷维希尔伯特空间，并非所有算符的迹都是定义良好的，因此在无穷维希尔伯特空间上应用(5.17)式时得特别小心，有时候它并不成立。比方说，对于坐标算符和动量算符的对易子来说，如果简单地应用这个公式将会得出 $\text{Tr}([X, P]) = 0$ ，但实际上 $\text{Tr}([X, P]) = i\hbar \text{Tr}(1) \neq 0$ 。在这个例子中，(5.17)式之所以不成立，正是因为式中各算符的迹都不是良好定义的。

利用算符的迹，我们可以把算符的期望值公式重写成

$$\langle \psi | \mathcal{O} | \psi \rangle = \text{Tr}(|\psi\rangle\langle\psi| \mathcal{O}) = \text{Tr}(\rho_\psi \mathcal{O}). \quad (5.18)$$

式中 $\rho_\psi = |\psi\rangle\langle\psi|$ 。要证明这个式子，我们只需注意到

$$\text{Tr}(|\psi\rangle\langle\psi| \mathcal{O}) = \sum_i \langle i | \psi \rangle \langle \psi | \mathcal{O} | i \rangle = \sum_i \langle \psi | \mathcal{O} | i \rangle \langle i | \psi \rangle = \langle \psi | \mathcal{O} | \psi \rangle.$$

可见，为了计算算符的期望值，我们并不需要知道量子态 $|\psi\rangle$ ，而是只需要知道厄密算符 ρ_ψ 。 $|\psi\rangle$ 和 ρ_ψ 的一个重要区别是， $|\psi\rangle$ 可以相差一个非物理的

整体相位因子, 变成 $e^{i\theta}|\psi\rangle$, 而 ρ_ψ 在这种相位变换下不变, 也即是说, 它自动剔除了这一非物理的整体相位信息。

以上讨论告诉我们, 从一个量子系统中能够提取出来的所有物理信息都包含在 $\rho_\psi = |\psi\rangle\langle\psi|$ 这一特殊厄密算符中。通常称这样的 ρ_ψ 为一个纯态密度算符。假设记 U 为时间演化算符, 则由于 $\rho_\psi = |\psi\rangle\langle\psi|$, 并且 $|\psi\rangle$ 会演化为 $|\psi\rangle \rightarrow U|\psi\rangle$ (这里选取的是薛定谔绘景), 从而不难看出 ρ_ψ 的时间演化为

$$\rho_\psi \rightarrow U\rho_\psi U^\dagger. \quad (5.19)$$

纠缠态与混态

下面进入本节的主题。假设我们有一个 AB 复合系统, 它由 A, B 两个子系统复合而成, 两个子系统的希尔伯特分别为 \mathcal{H}_A 和 \mathcal{H}_B 。假设整个复合系统处在 $|\psi\rangle$ 态, 它当然也会对应一个纯态密度算符 ρ_ψ 。假设我们忽略 B 而仅仅只关心 A , 对 A 进行各种测量。比方说我们测量 A 的某个物理量 \mathcal{O}_A , 因此我们就要计算如下期望值,

$$\langle\psi|\mathcal{O}_A|\psi\rangle = \text{Tr}_{AB}(\rho_\psi \mathcal{O}_A). \quad (5.20)$$

式中 Tr_{AB} 表示在整个系统的张量积希尔伯特空间 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上求迹。注意到 $\mathcal{H}_A \otimes \mathcal{H}_B$ 的基矢量 $|ij\rangle_{AB} = |i\rangle_A |j\rangle_B$, 所以 $\text{Tr}_{AB} = \text{Tr}_A \text{Tr}_B$, 式中 Tr_A 和 Tr_B 分别表示在 \mathcal{H}_A 和 \mathcal{H}_B 上求迹。由于 \mathcal{O}_A 只作用在 \mathcal{H}_A 上, 与子系统 B 无关, 所以 Tr_B 就直接作用在 ρ_ψ 上, 根据施密特分解(5.11)式, 即得到

$$\rho_A = \text{Tr}_B(\rho_\psi) = \sum_i p_i |i\rangle_A \langle i|. \quad (5.21)$$

这是一个只作用在 \mathcal{H}_A 上的厄密算符。而期望值公式(5.20)就变成

$$\langle\psi|\mathcal{O}_A|\psi\rangle = \text{Tr}_A(\rho_A \mathcal{O}_A). \quad (5.22)$$

从(5.21)式可以看出, 施密特分解的 p_i 刚好是算符 ρ_A 的本征值, 施密特分解的 $|i\rangle_A$ 则是相应的本征态, 因为很容易验证相应的本征方程成立。

以上讨论告诉我们, 如果仅仅只关心子系统 A , 那就无需知道整体的 $|\psi\rangle$, 只需知道 ρ_A , 忽略 B 以后所有能从子系统 A 提取出来的信息都包含在厄密算符 ρ_A 中。我们称 ρ_A 为系统 A 的密度算符, 也称之为 ρ_ψ 在 A 上的约化

密度算符, 当然它不是纯态密度算符, 因为一般来说现在这个密度算符不能写成 $|\phi\rangle_A\langle\phi|$ 这样的形式。很明显, ρ_A 满足

$$\mathrm{Tr}_A(\rho_A) = \sum_i p_i = 1. \quad (5.23)$$

完全类似的, 如果我们是忽略 A 而仅关心 B , 那就会有

$$\rho_B = \mathrm{Tr}_A(\rho_\psi) = \sum_i p_i |i\rangle_B\langle i|. \quad (5.24)$$

由于 $\rho_A = \mathrm{Tr}_B(\rho_\psi)$, 所以不难看出, B 部分局部的任何么正操作 U_B 都无法影响子系统 A , 因为操作完成之后依然有 $\mathrm{Tr}_B(U_B\rho_\psi U_B^\dagger) = \mathrm{Tr}_B(U_B^\dagger U_B\rho_\psi) = \mathrm{Tr}_B(\rho_\psi) = \rho_A$.

如果原来 AB 整体的量子态 $|\psi\rangle$ 不是一个纠缠态, 也就是说施密特数等于1, 则仅有 $p_1 = 1$ 非零, 则, 由(5.21)可见, 这时候必有

$$\rho_A = |1\rangle_A\langle 1|. \quad (5.25)$$

显然这是一个纯态密度算符, ρ_B 也一样。反过来, 如果原来的 $|\psi\rangle$ 是一个纠缠态, 施密特数大于1, 则从(5.21)式可以看到, 对于忽略了 B 的我们来说, 子系统 A 完全可以看作是以 p_i 的概率随机地处于 $|i\rangle_A$ 态, 由于施密特数大于1, 那就有多个这样的 $|i\rangle_A$, 所以我们说这时候系统 A 处于一个由 ρ_A 描述的混态, 这时候 ρ_A 就是混态密度算符。同样, 这时候 ρ_B 也为混态密度算符。所以, 整个完整系统 AB 的纠缠态和子系统 A 以及 B 的混态是相对应的。特别的, 不难看到与最大纠缠态对应的子系统混态密度算符为 $\frac{1}{\dim(\mathcal{H}_A)} \sum_i |i\rangle\langle i|$, 这时候相应的混态就叫做最大混态。

混态是什么意思呢? 由于它意味着以某个概率分布随机地处于多个态的“混杂”, 所以, 混态就意味着我们对系统有某种无知! 这里多个量子可能性以一定的概率混杂就反映了我们的无知。另一方面, 正如刚刚看到的, 整个复合系统处于纠缠态就意味着作为部分的子系统必定为混态。这就说明, 当整体处于纠缠态时, 即使我们完全了解了整体, 我们对每一个部分也都必然含有无知。特别的, 如果整体处于最大纠缠态, 则我们对部分就最无知。可以完全了解整体却无法同时完全了解部分, 甚至可以对部分完全无知(最大混态), 这就是量子纠缠最奇怪的地方。

密度算符

当然，我们可以完全不提 B 部分，直接定义一个系统的密度算符，而不管它是否源于与另一个系统 B 的纠缠。一个系统的密度算符 ρ 包含了所有我们能从对这个系统的观测中提取出来的信息，根据上面的讨论可以知道，**密度算符 ρ 应该满足如下性质**：1. 它是一个厄密算符。2. 它的本征值都大于等于0，为正定算符。3. $\text{Tr}(\rho) = 1$ 。有了密度算符以后，对任何物理可观测量 \mathcal{O} 期望值的计算就可以表达为

$$\langle \mathcal{O} \rangle = \text{Tr}(\rho \mathcal{O}). \quad (5.26)$$

如果一个密度算符能够写成 $\rho = |\psi\rangle\langle\psi|$ 的形式，就称为纯态密度算符，它描述的系统状态就是纯态，否则就是混态密度算符，描述的状态就是混态。很显然，纯态密度算符额外满足

$$\rho^2 = \rho. \quad (5.27)$$

反过来，如果一个密度算符额外满足上式，则它的本征值必为0或1，由于密度算符所有本征值的和要等于1，因此它就必定能写成 $\rho = |\psi\rangle\langle\psi|$ 的形式($|\psi\rangle$ 为 ρ 的本征态)，从而必为纯态密度算符。对于纯态密度算符，我们必定有

$$\text{Tr}(\rho^2) = \text{Tr}(\rho) = 1. \quad (5.28)$$

对于一个任意的密度算符 ρ ，我们必可以通过求解它的本征方程将它对角化成如下形式

$$\rho = \sum_i p_i |i\rangle\langle i|. \quad (5.29)$$

密度算符的正定性告诉我们 $p_i \geq 0$ ， $\text{Tr}(\rho) = 1$ 的条件则告诉我们 $\sum_i p_i = 1$ ，所以 $p_i \leq 1$ ，等号仅当 ρ 为纯态密度算符时才成立。因此，对于混态密度算符，我们必有 $\text{Tr}(\rho^2) = \sum_i p_i^2 < \sum_i p_i = 1$ ，即对于混态密度算符，必有

$$\text{Tr}(\rho^2) < 1. \quad (5.30)$$

5.3 用例子说明量子纠缠态的神奇

我们来考察双电子系统的自旋量子态，由于态叠加原理，下面这个量子态 $|\phi^+\rangle$ 显然是双电子系统的一个可能自旋态，

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle). \quad (5.31)$$

这个量子态当然是一个量子纠缠态，而且是最大纠缠态。这就意味着处在 $|\phi^+\rangle$ 态上的两个电子共同形成了一个不可分解的整体，而这个不可分割的整体与两个电子之间的距离没有关系，也即是说，即使你将其中一个电子放在南昌，另一个放到天边，这两者遥遥相隔，但是它们却依然处于同一个不可分解的整体之中。

现在，假设你沿着 z 轴测量南昌的这个电子的自旋，那你会得到两种可能的结果， $1/2$ 的概率(由 $|\langle\uparrow\uparrow|\phi^+\rangle|^2 = (1/\sqrt{2})^2$ 决定)你将测到南昌的这个电子自旋向上 \uparrow ， $1/2$ 的可能性你将测到它自旋向下 \downarrow 。但是，奇妙的是，由于南昌的这个电子和天边的那个电子形成了不可分解的整体 $|\phi^+\rangle$ ，因此当你测到南昌的电子自旋向上时就意味着原来的 $|\phi^+\rangle$ 态跃迁到了 $|\uparrow\uparrow\rangle$ 态，而这又意味着天边的电子立即处在 $|\uparrow\rangle$ 态，同样的，当你测到南昌的电子自旋向下时，原来的 $|\phi^+\rangle$ 态就跃迁到了 $|\downarrow\downarrow\rangle$ 态，因此天边的电子立即就处在 $|\downarrow\rangle$ 态。总之，无论你测到南昌的电子自旋向上还是自旋向下，两者的整体就发生量子跃迁了，相应的就立即决定了天边电子的量子态。由于这种你在南昌的测量对天边电子的影响是立即的，所以很多人会说：这意味着在量子力学里信息可以超光速传播，利用量子纠缠态可以超光速地传递信息。情况果真如此吗？

5.3.1 量子纠缠能实现超光速信息传递吗？

为了分析量子纠缠态能否实现超光速传递信息的问题，让我们假设某个实验室中制备了 N 对电子，每一对都处在纠缠态 $|\phi^+\rangle$ ，你和你的她分别持有每一对电子中的一个，你待在南昌，而她去了天边，因此你们分享着 N 个纠缠对，但是你们之间不能通信。在这种情况下，你能用你们之间分享的纠缠对来给她瞬时传递信息吗？比方说，你和她约定，如果你们在南昌养的那只猫死了，你就会对你的电子进行测量，而你的测量立即就会

影响她持有的另一个电子，因此看起来只要她接着对自己持有的那个电子进行测量就能获知猫死的信息。情况真是这样的吗？

现在，假设南昌的猫死了，因此你沿着 z 轴测量了你们共享的 N 个纠缠对中你所持有的那些电子，但是检测所带来的纠缠对的量子跃迁是随机的，因此你有 $1/2$ 的可能性测到某个电子自旋向上， $1/2$ 的可能性测到自旋向下，而你无法决定自己的测量结果，因此完成测量之后，你的 N 个电子大约会有一半自旋向上，另一半自旋向下，哪些自旋向上，哪些自旋向下是完全随机的。接着，她也对自己的电子进行了测量，当然，你的测量立即影响到了她的电子，因此所有你测到你的电子自旋向上的那些纠缠对，她也会测到自己的另一个电子自旋向上，所有你测到自己的电子自旋向下的纠缠对，她也会测到自己的另一个电子自旋向下。但问题是，你们之间不能通信，因此她无从得知你的测量结果，也就是说，她不知道你测到的哪些电子自旋向上，哪些电子自旋向下。对她来说，她唯一能知道的就是，她自己测量的结果是，大约有一半的电子自旋向上，另一半的电子自旋向下，而且在她看来，哪些电子自旋向上，哪些电子自旋向下是完全随机的。而根据纠缠态 $|\phi^+\rangle$ 量子跃迁的随机性，即使你根本没有作任何测量，只有她一个人在天边对她的那些电子进行测量，她也会得到完全类似的结论。也就是说，你的测量根本就不能增加任何她从自己的测量中获取的信息，她甚至根本就无从判断你有没有测量。因此她根本就无从得知你们的猫死了。

看来，你根本就无法利用纠缠对超光速地传递信息，甚至你根本就无法利用这些纠缠对来传递信息。但是，你说且慢，以上只考虑了你沿着 z 轴测量的情况，假设你有两种不同的测量选择，要么你沿 z 轴测量你的所有电子，要么你沿着 x 轴测量你的电子，那能不能通过你的测量对她的即时影响将你的这两种不同选择传递给她呢？如果能的话，那你就可以用你的不同选择来代表猫的两种不同状态(这个你们可以事先约定好)，从而就能将猫死了的信息超光速地传递给她。

为了下一步的分析，我们首先来看一下 x 方向的测量和 z 方向的测量有什么不同。量子力学的基本原理告诉我们，如果我们沿着 x 轴测量电子的自旋态，那么被测的电子就会跃迁到 x 方向上的两个自旋本征态 $|\uparrow_x\rangle \equiv |\rightarrow\rangle$ 和 $|\downarrow_x\rangle \equiv |\leftarrow\rangle$ 中的某一个，根据第三章中的相关讲述，这两

个本征态和 z 方向本征态的关系是

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle + |\downarrow_x\rangle), \quad |\downarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle - |\downarrow_x\rangle). \quad (5.32)$$

当然，反过来也有

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle), \quad |\downarrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle). \quad (5.33)$$

另外，由于 $|\uparrow\uparrow\rangle = |\uparrow\rangle|\uparrow\rangle = \frac{1}{2}(|\uparrow_x\rangle + |\downarrow_x\rangle)(|\uparrow_x\rangle + |\downarrow_x\rangle) = \frac{1}{2}(|\uparrow_x\rangle|\uparrow_x\rangle + |\downarrow_x\rangle|\downarrow_x\rangle + |\uparrow_x\rangle|\downarrow_x\rangle + |\downarrow_x\rangle|\uparrow_x\rangle) = \frac{1}{2}(|\uparrow_x\uparrow_x\rangle + |\downarrow_x\downarrow_x\rangle + |\uparrow_x\downarrow_x\rangle + |\downarrow_x\uparrow_x\rangle)$ ，类似的 $|\downarrow\downarrow\rangle = \frac{1}{2}(|\uparrow_x\uparrow_x\rangle + |\downarrow_x\downarrow_x\rangle - |\uparrow_x\downarrow_x\rangle - |\downarrow_x\uparrow_x\rangle)$ ，所以我们可以知道，原来的纠缠态 $|\phi^+\rangle$ 也可以写成

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\uparrow_x\rangle + |\downarrow_x\downarrow_x\rangle). \quad (5.34)$$

假设你有沿着 z 轴和沿着 x 轴两种测量选择，她也知道你有这两种选择，并且你们约定，如果你沿着 z 轴测量，那就代表猫还活着，如果你沿 x 轴测量那就代表猫死了。由于你们无法正常通信，所以你当然不能直接告诉她你的测量选择是什么，她只能从她自己随后的测量结果中对你的测量方式进行推断，那么她能推断出你的测量方式进而得知猫的死活吗？由于她无法预先知道你的测量方式，所以她自己只能从两种不同测量方式中随机选取一种，比如说，假设她总是选择沿着 z 轴测量她的电子(由于 z 轴和 x 轴对于我们的纠缠态 $|\phi^+\rangle$ 完全对称，所以对于她选择沿 x 轴测量的所有分析将是完全类似的)。当然，我们总是假定她的测量在你的测量完成之后进行，而你有两种测量方式的选择，你沿着 z 轴测量她也沿着 z 轴测量的情况我们已经分析过了，结论是，她将得到大约一半电子自旋向上，另一半电子自旋向下的结论，并且哪些电子自旋向上哪些自旋向下对于她来说是完全随机的。

现在假设你沿着 x 轴测量，之后她再沿着 z 轴进行测量，我们来看她是否能得到不同的结果。由于纠缠态 $|\phi^+\rangle$ 也可以写成(5.34)的形式，所以你沿着 x 轴的测量结果将是，大约有一半你所持有的电子会跃迁到 $|\uparrow_x\rangle$ 态，当然由于纠缠态的性质(5.34)，这时候她相应的另一个电子也会立即跃迁到 $|\uparrow_x\rangle$ 态，同样，你另半数电子会跃迁到 $|\downarrow_x\rangle$ 态，这时候她的相应电子也会立即跃迁到 $|\downarrow_x\rangle$ 态，当然这种跃迁是完全随机的。因此在你的测量完

成以后，她所持有的每一个电子有 $1/2$ 的概率处在 $|\uparrow_x\rangle$ 态， $1/2$ 的概率处在 $|\downarrow_x\rangle$ 态，当然由于她还不知道你的测量方式，所以对于这个结果她是并不知情的。她只是选择沿着 z 轴进行她的测量，由(5.33)式可以知道，这时候如果她测的电子处在 $|\uparrow_x\rangle$ 态，那她的测量将会使得这个电子以 $1/2$ 的可能性跃迁到 $|\uparrow\rangle$ ，还有 $1/2$ 的可能性跃迁到 $|\downarrow\rangle$ ，如果她测的电子处在 $|\downarrow_x\rangle$ 态，结论也是一样的，因此总的来说，对于她所持有的每一个电子，她都有 $1/2$ 的概率测到它自旋向上， $1/2$ 的概率测到它自旋向下。因此，当她完成所有的测量以后，她同样发现，在她所持有的电子中，大约有一半自旋向上，有一半自旋向下，而且这个结果是完全随机的。你已经看到了，她所得到的这个结果和你沿着 z 轴进行测量时她所得到的结果完全一样。也即是说，远在天边的她根本无从推断出你的测量方式，因此当然也就无法得知猫的死活。因此，用这种方式同样无法实现信息的超光速传递。

那么这是不是意味着只要你不通过正常的通信直接告诉她你的测量方式，她就根本无从得知呢？能不能说明，量子纠缠态不仅无法超光速传递信息，甚至根本就无法用来传递信息呢？答案是不能。因为以上的结论都是在假定你和她之间无法进行通常的通信的情形下得到的。如果你们之间能够进行通常的通信，那即使你不直接告诉她你的测量方式，她也有可能推断出这个信息，即是说，如果你们之间能够正常通信，那你们之间共享的量子纠缠对是能够用来传递信息的。我们来看一下这是怎么回事。

假设你们之间能够正常通信，那么即使你不直接告诉她你的测量方式，你也还可以告诉她你的测量结果，也就是说，你也还可以告诉她你所测的每一个电子自旋是沿着你测量轴的正方向，还是沿着你测量轴的反方向，而她得知你的这些信息就能进一步推断出你是沿着 z 轴进行测量，还是沿着 x 轴进行测量。不妨假设你沿着 x 轴进行测量，因此在你的测量完成之后所有电子都跃迁到了某个 x 方向的本征态，这时候如果她也沿着 x 轴进行测量，那么由于纠缠的性质，她会发现她所测的每一个电子结果都和你的测量结果一样(指电子自旋是沿着测量轴还是反着测量轴的结果。注意，你已经告诉她这个测量结果了)。但是，如果她是沿着 z 轴进行测量，这时候由于她的电子已经处在 x 方向的某个本征态，而 x 方向的本征态跃迁到 z 方向的本征态是完全随机的，所以她会发现她所测的电子到底是沿着测量轴的正方向还是反方向，与你告诉她的测量结果之间完全没有关联。所以，

通过这种将她的测量结果和你的测量结果相比较的方式，她就能推断出你的测量方式与她的是否一样，从而也就知道了你是沿着 z 轴测量，还是沿着 x 轴进行测量。这样，关于你的测量方式的信息就成功传递给她了。

可见，利用你和她之间共享的量子纠缠对，你的确有可能向她传递额外的信息。但，前提是，你们之间必须可以进行通常的经典的通信，她必须先得到你用经典方式传递过来的信息，才能进一步获知你用纠缠对传递过来的信息。而经典通信肯定是无法超光速的，因此量子纠缠对也无法用来超光速地传递信息。

如何提取纠缠态中的信息

在量子计算和量子信息科学中，人们将电子自旋这样的例子抽象成了量子比特模型，所谓的量子比特，就是一个只有0和1这两种可确定区分可能性的量子系统，因此，一个量子比特的希尔伯特空间就是两维的，其正交归一基矢量可以记作 $\{|0\rangle, |1\rangle\}$ 。当然，我们可以用电子自旋来实现量子比特，比方说取自旋向上态 $|\uparrow\rangle$ 代表 $|0\rangle$ 态，自旋向下态 $|\downarrow\rangle$ 代表 $|1\rangle$ 态。这样定义的话，那之前第三章中对于电子自旋定义的算符 X 和 Z (其实也就是泡利算符 σ_x 和 σ_z)现在就成了，

$$\begin{aligned} X|0\rangle &= |1\rangle, & X|1\rangle &= |0\rangle \\ Z|0\rangle &= |0\rangle, & Z|1\rangle &= -|1\rangle. \end{aligned} \quad (5.35)$$

X 和 Z 当然都是厄米算符，不仅如此，还容易验证 $X^2 = Z^2 = 1$ (泡利算符的性质)，所以 X 和 Z 还是么正算符。同样也可以验证 ZX 为么正算符。

因此，之前我们所讨论的两电子自旋的纠缠对 $|\phi^+\rangle$ 就可以重写成两个量子比特的纠缠对 $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 。但是两个量子比特的希尔伯特空间是 $2 \times 2 = 4$ 维的，它应该有4个正交归一的基矢量，假设我们将 $|\phi^+\rangle$ 选作其中一个基矢量，那么其余三个基矢量可以怎么选择呢？事实上我们可以将其余三个基矢量也选作纠缠态(并且是最大纠缠态)，

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad (5.36)$$

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (5.37)$$

很容易验证这4个态的确是正交归一的。为了纪念物理学家贝尔在量子纠缠上所做的开创性工作(贝尔不等式),人们通常称这四个态所构成的两量子比特希尔伯特空间矢量基为贝尔基,有时候也称这些量子态为贝尔态。

现在,假定你和你远在天边的她是同一个导师的学生,你们的导师将两比特的重要信息(这就有四种可能性)用这四个贝尔态(它们构造四个可确定区分的不可分解整体可能性)来编码,每种可能性对应一个贝尔态,并且导师将这个贝尔纠缠态中的第一个量子比特发给了南昌的你,而将与之纠缠的另一个量子比特发给了远在天边的她。即是说,如果你们想获知导师给出的具体是什么信息,你们就得确定共享的是四个贝尔态中的哪一个。

你们如何能确定这一点呢? 由于相隔遥远,所以你们首先想到的可能就是各自独立地对手中的那个量子比特进行测量。但是,显然的是,只要你们不相互通信,那你们就不可能从这种测量中获取任何信息,因为从这四个贝尔态的表达式(5.37)可以知道,不管你们共享的是哪一个贝尔态,你的测量将总是以1/2的可能性得到0,以1/2的可能性得到1,结果完全是随机的,你完全无法从中得知贝尔态的任何具体信息,当然她也一样。这是贝尔态和通常的单个量子比特量子态的根本性不同,对于通常的量子比特,如果你存进一比特的信息,比如将它存为 $|0\rangle$ 态,那你只要测量这个量子比特的值,就一定能把这个信息读取出来。但是,现在你导师明明存进了两个比特的信息,但你和她的只要相互保持独立不进行沟通,就什么信息也读取不出来。也即是说,信息是隐藏的,是存储在你们共享的纠缠对的整体之中。

你可能会问,那这四个贝尔态到底如何区分呢? 答案很简单,只要同时测量算符 Z_1Z_2 和算符 X_1X_2 的值,这里写在算符上的下标表示这个算符仅对相应的量子比特进行作用,下标1就表示这个算符仅作用在纠缠对的第1个量子比特上,下标2就表示这个算符仅作用在纠缠对的第2个量子比特上,当然,作用在不同量子比特上的算符是相互对易的。利用 $ZX = -XZ$,人们很容易验证 Z_1Z_2 和 X_1X_2 是对易的,因此可以有共同的本征态,实际上,贝尔基的四个量子态就是它们共同的本征可能性完备集。从贝尔态的表达式(5.37)可以很容易验证, Z_1Z_2 的两个不同本征值可以用来区分四个贝尔态是属于 $|\phi\rangle$ 类型还是属于 $|\psi\rangle$ 类型,而 X_1X_2 的本征值可以用来进一步区分它们在这两个类型中的 \pm 号。但是,正如你已经看到

的，要完成这种区分，就需要对纠缠对中的两个量子比特进行联合测量，比如说，对算符 Z_1Z_2 的值进行测量。注意，这和你测 Z_1 ，她同时测 Z_2 有根本性的不同，因为在联合测量中可以仅仅测得 Z_1Z_2 的值而不必同时知道 Z_1 、 Z_2 分别是多少。实际上，要同时对 X_1X_2 和 Z_1Z_2 进行这种联合测量，就必须首先将你和她的量子比特放到一起来。也即是说，只要你们依然分别持有纠缠对中的一个量子比特，那就无法进行这样的联合测量，从而也就无法完整地读出导师存储的两比特信息。

当然，你们依然可以通过交流各自的测量结果，从而获取部分信息，比方说，你和她分别测量了 Z_1 和 Z_2 ，并将结果进行了比较，由于 Z_1 、 Z_2 都与 Z_1Z_2 对易，所以根据测量结果你们依然可以推断出你们共享的贝尔态是属于 $|\phi\rangle$ 类型还是 $|\psi\rangle$ 类型，但是，由于 Z_1 、 Z_2 都与 X_1X_2 反对易，因此你们的测量必定会干扰 X_1X_2 的本征态信息，因此你们也就不可能进一步获知被测贝尔态的 \pm 号。总之，通过这样的方式你们只能获知两比特信息中的1比特。

5.3.2 量子密集编码

到此为止，实际上我们还没有看到量子纠缠对有什么神奇的用处。实际上，量子纠缠对能大幅度提高我们的通信能力，当然，代价是要额外消耗掉纠缠对，因此在量子信息中，人们通常将量子纠缠态看成是一种会被消耗的资源。下面就让我们来看一下这种资源的一种神奇应用。

还是假定你在南昌，你的她远在天边，假设你要发送两比特的经典信息给她，如果用经典的方式，通过经典信道进行发送，那你得占用两比特的信道。但是，如果你和她之间建立了量子信道，你就可以通过量子信道发送量子比特，并且，假定你和她在前年就分别持有了某个量子纠缠对中的一个量子比特，不妨假定这个纠缠对处在 $|\phi^+\rangle$ 态吧。如果你们有这些资源，那么你只要占用一比特的量子信道，就能完成对两比特经典信息的发送，这就是所谓的量子密集编码。

你如何做到这一点呢？首先，你们之间得事先约定好一种如何用四个贝尔态对应两比特经典信息的编码方式。其次，你注意到可以对自己所持有的量子比特进行四种不同的么正变换，分别为恒等变换 I ，变换 Z_1 ，变换 X_1 ，以及变换 Z_1X_1 （利用泡利算符的性质，你很容易验证这四个算符的

么正性), 变换的结果你也很容易算出来,

$$1|\phi^+\rangle = |\phi^+\rangle, Z_1|\phi^+\rangle = |\phi^-\rangle, X_1|\phi^+\rangle = |\psi^+\rangle, Z_1X_1|\phi^+\rangle = |\psi^-\rangle. \quad (5.38)$$

然后你再根据你们事先约定好的编码方式, 将你要发送的信息对应成四个贝尔态中的某一个, 并对你的量子比特进行相应的么正变换。最后, 完成了合适的么正变换以后, 你将你手中的那个量子比特通过量子信道发送给天边的她。她本来就持有纠缠对中的另一个量子比特, 再接收到你的量子比特以后就拥有整个纠缠对了。为了确定这个纠缠对是四个贝尔态中的哪一个, 她只需要同时进行 Z_1Z_2 和 X_1X_2 两种联合测量就可以了。再根据约定好的编码方式她就能得知你所发送的信息。这样, 你们就完成了仅用1比特的量子信道就传送2比特的经典信息了。这就是量子密集编码的基本思想。注意, 虽然你们前年就共同持有了这对纠缠对, 但那时候的纠缠对中完全不含有你现在要发送的信息, 你的信息发送的确是通过现在传送这一个量子比特完成的。

5.3.3 量子隐形传态

量子纠缠对真正神奇的地方在于, 只要有足够的量子纠缠对, 那么原则上就可能做到将你超空间传送到一个遥远的星球。当然, 这只是原则上, 实际上这个目标对于我们来说可能永远都遥不可及。但原则上并没有什么物理定律禁止我们实现这种科幻场景。因为, 今天在实验室里早就做到将一个量子比特的量子态超空间传送到非常远的地方, 这就是量子隐形传态。

还是假设你在南昌, 你的她远在天边, 你们共同持有一对纠缠的量子比特, 不妨称你持有的那个为量子比特1, 她持有的那个为量子比特2, 这两个量子比特处在纠缠态 $|\phi^+\rangle_{12}$ (式中我们加上了下标12, 这是因为我们即将引入第3个量子比特)。现在, 假设你还有另一个量子比特3, 它处在某个未知的状态 $|\Psi\rangle_3 = \alpha|0\rangle_3 + \beta|1\rangle_3$, 而你想把这第三个量子比特发送给天边的她。你当然可以通过你们之间的量子信道直接进行发送, 但你发送的量子比特很有可能被别人拦截, 从而带来不可预料的结果。当然, 你真正要发送的其实是第三个量子比特的量子态, 因为它包含了某些你想发送给她的的重要未知信息。

那么你们有没有什么绝对安全的量子信息发送方法呢？有。答案就在于充分利用你们之间共享的纠缠对 $|\phi^+\rangle_{12}$ 。为了说清楚这一点，首先由贝尔态的定义式(5.37)，我们很容易得到

$$|00\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle), \quad |11\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle) \quad (5.39)$$

$$|01\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle), \quad |10\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle). \quad (5.40)$$

其次，我们注意到整个系统的量子态可以重写成

$$\begin{aligned} |\Psi\rangle_3 |\phi^+\rangle_{12} &= (\alpha|0\rangle_3 + \beta|1\rangle_3) \frac{1}{\sqrt{2}}(|00\rangle_{12} + |11\rangle_{12}) \\ &= \frac{1}{\sqrt{2}}[\alpha|00\rangle_{31}|0\rangle_2 + \alpha|01\rangle_{31}|1\rangle_2 + \beta|10\rangle_{31}|0\rangle_2 + \beta|11\rangle_{31}|1\rangle_2] \\ &= \frac{1}{2}[(\alpha|0\rangle_2 + \beta|1\rangle_2)|\phi^+\rangle_{31} + (\alpha|0\rangle_2 - \beta|1\rangle_2)|\phi^-\rangle_{31}] \\ &\quad + \frac{1}{2}[(\alpha|1\rangle_2 + \beta|0\rangle_2)|\psi^+\rangle_{31} + (\alpha|1\rangle_2 - \beta|0\rangle_2)|\psi^-\rangle_{31}], \end{aligned} \quad (5.41)$$

式中第三个等号我们利用了公式(5.40)，并且由贝尔态的正交归一性可以知道，第三个等号右边的最终表达式中的4个态相互正交。因此，你只需要将你的第3个量子比特和你所持有的第1个量子比特放在一起，并同时对它们进行 Z_3Z_1 和 X_3X_1 的联合测量，测量的结果是，第3个量子比特和第1个量子比特所构成的系统将会跃迁到它们相应的四个贝尔态中的某一个。然后，你再把你的测量结果用经典的方式发送给天边的她，她如果得知你的结果是 $|\phi^+\rangle_{31}$ ，那就什么也不需要，因为从式(5.41)可以知道，这时候她的量子比特2的量子态已经变成 $\alpha|0\rangle_2 + \beta|1\rangle_2 = |\Psi\rangle_2$ 态了，如果她得知你的结果是 $|\phi^-\rangle_{31}$ ，根据(5.41)式，那她就对她的量子比特进行 Z_2 的么正变换，由于 $Z_2(\alpha|0\rangle_2 - \beta|1\rangle_2) = (\alpha|0\rangle_2 + \beta|1\rangle_2) = |\Psi\rangle_2$ ，因此变换以后她也将得到正确的量子态，同样的，如果你的结果是 $|\psi^+\rangle_{31}$ ，那她就对自己的量子比特进行 X_2 的么正变换，根据(5.41)式，结果也将是正确的量子态，而如果你的结果是 $|\psi^-\rangle_{31}$ ，根据(5.41)式，那她就进行 Z_2X_2 的么正变换，同样会得到正确的量子态。总之，在得知你的测量结果以后，她总可以让自己的量子比特变成 $|\Psi\rangle_2$ 态。这样一来，你的第三个量子比特的未知量子态就成功传送给她了。

这里有几点值得进一步讨论，第一， $|\Psi\rangle$ 态的信息从来也没有在某个量子信道中进行传送！ $|\Psi\rangle$ 态的成功传送完全是超空间的，所以称之为隐形传态。第二，你告知给她的测量结果中也完全不包含 $|\Psi\rangle$ 态的信息，否则根据量子力学的基本原理，你的测量就已经对 $|\Psi\rangle$ 态造成了不可逆的扰动，那此后她也就不可能得到 $|\Psi\rangle$ 态了。同时，正因为你发送给她的测量结果中不包含任何 $|\Psi\rangle$ 态的信息，因此即使有人窃听了你们的通信，他也无法获得 $|\Psi\rangle$ 态。第三，整个过程并没有违反量子不可克隆定理，这是因为，在你进行你的测量之后，你就已经摧毁了第三个量子比特原来的态，因此天边的她后来所做的并不是把你的量子比特3的态复制一份。第四，直到获知你的测量结果之前，天边的她都还无法得到正确的 $|\Psi\rangle$ ，并且由于你的测量结果是完全随机的，因此从概率上来说，这时候她只能得到与 $|\Psi\rangle$ 不相关的态。因此，这里也没有信息的超光速传递，因为你告诉她测量结果时采用的经典通信方式当然是无法超光速的。

如果回顾我们上一节所讨论的量子密集编码和这一节讨论的量子隐形传态，人们就会发现，这两个过程的实现都需要消耗纠缠对。这两个过程无论哪一个，当它成功完成之后，原来由两个人共同持有的纠缠对就被消耗掉了，因此对于你和你远在天边的她来说，你们共享的那些纠缠对是一种稀缺资源。

5.3.4 GHZ态以及为什么爱因斯坦错了

以上我们只讨论了两个量子比特的纠缠，而且实际上我们还只讨论了两个量子比特的那些所谓最大纠缠态，也就是我们所说的贝尔态。人们自然会想到，三个量子比特的纠缠会怎么样呢？这就是我们这一小节想要讨论的问题。当然我们讨论三个量子比特的纠缠，不是因为它有多特殊，而是因为借助于它人们可以了结量子力学发展史上的一段著名公案。

在量子力学刚刚发展起来的时候，爱因斯坦认为量子力学理论是不完备的。因为他认为一个物理量的值总是存在的，或者说任何时候任何物理量总会有一个确定的值，虽然可能因为种种原因你不能测到这个值，但它总存在，爱因斯坦所谓的“即使你没有看月亮，月亮也存在”就是这个意思，由此他指出量子力学里面物理量的值之所以不确定，之所以我们只能测得物理量取值的一个概率分布，是因为我们还缺失了一些信息，爱因斯

坦称之为有一些隐变量，如果我们能进一步掌握这些缺失的信息，那量子力学将和经典力学一样，没有任何不确定性。总之，爱因斯坦认为物理量的值总是存在的，量子力学中的不确定性和概率的起源与我们日常概念中的概率起源一样，都是因为我们缺失了一些信息，因此他强烈反对玻尔和海森堡等人的不确定性和概率是世界的内在属性的观念，认为不确定性在量子力学理论中的存在只不过反映了量子力学理论的不完备性，也即是说量子力学理论没有把所有隐变量都包括进来。

那爱因斯坦的观点到底对不对呢？为此人们曾经长期争论不休，直到物理学家贝尔从爱因斯坦的观念出发推导出了著名的贝尔不等式，贝尔说，你只要用实验检验贝尔不等式是否成立，就能判定爱因斯坦到底对不对。只要爱因斯坦对，那贝尔不等式就一定成立，相反，如果玻尔和海森堡等人的观点对，那贝尔不等式就可以被破坏。后来的实验证明，爱因斯坦的确错了，不过虽然爱因斯坦错了，但是他为了否定量子力学的完备性却提出了今天非常重要的量子纠缠的概念。我们前面对量子纠缠的讨论，以及贝尔的开创性工作都是在量子纠缠的概念上进一步发展而来的。下面我们将要描述的，就是另外一个更为直接了当，比贝尔不等式更简单的可以用于判定爱因斯坦是否正确的情形。

我们要讨论的就是由物理学家Greenberg, Horne, 以及Zeilinger提出来并在实验上实现的一种特殊的三量子比特纠缠态，通常称作GHZ态。假设我们把这三个量子比特分别标记为1、2、3，那么GHZ态可以写成

$$|GHZ\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle_{123} + |111\rangle_{123}). \quad (5.42)$$

利用泡利算符的作用规则，人们很容易验证 $|GHZ\rangle_{123}$ 同时是下面三个相互对易的算符的本征值为1的本征态，这三个算符是

$$Z_1 Z_2, \quad Z_2 Z_3, \quad X_1 X_2 X_3, \quad (5.43)$$

利用泡利算符的反对易性，人们很容易验证这三个算符两两对易。现在我们进一步引入泡利算符 σ_y ，在这里写作 Y ，根据泡利算符的乘法规则我们有 $ZX = iY$ 。由于 $Y_1 Y_2 X_3 = -Z_1 X_1 Z_2 X_2 X_3 = -(Z_1 Z_2)(X_1 X_2 X_3)$ (式中我们已经利用了不同量子比特的算符相互对易的性质)，因此我们可以知道， $|GHZ\rangle_{123}$ 也是 $Y_1 Y_2 X_3$ 的本征值为 -1 的本征态。类似的，我们可以得到，当

作用在 $|GHZ\rangle_{123}$ 上时，下面的等式必定同时成立

$$Y_1 Y_2 X_3 = -1, \quad X_1 Y_2 Y_3 = -1, \quad Y_1 X_2 Y_3 = -1, \quad X_1 X_2 X_3 = 1. \quad (5.44)$$

下面，让我们来假设爱因斯坦的观点也成立，即任何情况下，每一个物理量的值总是存在，我们将三个泡利算符的值分别记作 $v(X), v(Y), v(Z)$ ，当然由于泡利算符的平方等于1，所以它们的值只能取 ± 1 。请注意，作为物理量的值， $v(X), v(Y), v(Z)$ 都是普通的数，因此它们相互之间当然都相互对易。如果 $v(X), v(Y), v(Z)$ 总是存在，虽然可能由于我们不了解隐变量，缺失了信息，导致我们不能完全确定这些取值到底是多少，但按照爱因斯坦的观点，它们总是存在的，总是有定义的。如此一来，根据(5.44)，对于 $|GHZ\rangle_{123}$ 态，我们就必定有

$$v(Y_1)v(Y_2)v(X_3) = -1, \quad v(X_1)v(Y_2)v(Y_3) = -1, \quad (5.45)$$

$$v(Y_1)v(X_2)v(Y_3) = -1, \quad v(X_1)v(X_2)v(X_3) = 1. \quad (5.46)$$

但是，对于普通的数来说，这些式子是自相矛盾的，因为将前三个式子乘起来并利用 $(v(Y))^2 = 1$ ，你很容易得到 $v(X_1)v(X_2)v(X_3) = -1$ ，这和第四个式子矛盾。

因此，这也就是说，要么量子力学是错的，从而(5.44)式不对，要么爱因斯坦就是错的(也就是说我们不能假定 $v(X)$ 这样的量总是存在)，两者必居其一。到底谁错了呢？实验发现，爱因斯坦错了，(5.44)式是成立的。因此，这就从实验上否定了物理量的取值必定存在的观点。也从侧面证明了为什么在量子力学中物理量只能表示成算符，因为算符的值当然只在本征态上有定义，对于叠加态，谈算符的取值是没有意义的，因为它根本就不存在。