

量子密码学 (II)

——量子不可克隆定理

物理学院 2018 级 杨佳宇

2020 年 4 月 29 日

目录

Contents

- 量子不可克隆定理的证明
- 定理的意义与应用
- 定理的延伸与推广
- 近似量子克隆

量子不可克隆定理的提出

1982 年 10 月, W. K. Wootters 和 W. H. Zurek 在 *Nature* 刊登了一篇题目为 *A single quantum cannot be cloned* 的文章, 提出了量子不可克隆定理。

引入: 光子打到激发态的原子上的时候可能会发生受激辐射, 这样的受激辐射产生的光子和原来的光子有着相同的偏振态。

思考: 是否可以像这样, 或者有其他方式, 来将一个未知的量子态复制很多份, 得到若干个完全相同的量子态?

量子不可克隆定理的证明

W. K. Wootters 和 W. H. Zurek 使用了光子的偏振态进行证明，这里采用另一种更为直观的等价的证明方式。

假定存在一个完美的克隆机器，这个机器的作用为：

$$|s\rangle |M\rangle \longrightarrow |s\rangle |s\rangle \quad (1)$$

这个克隆过程是一个符合薛定谔方程的量子演化，它有两个性质：

1. 因为薛定谔方程是一个线性方程，所以这个过程也具有线性性质
2. 么正变换保内积：克隆前的态 $|\phi_0\rangle$ 和克隆后的态 $|\phi\rangle$ 满足 $\langle\phi_0|\phi'_0\rangle = \langle\phi|\phi'\rangle$

量子不可克隆定理的证明

对于两个线性独立的归一化量子态 $|a\rangle$ 和 $|b\rangle$ ，这个克隆机器都可以对他们进行克隆：

$$\begin{aligned}|a\rangle |M\rangle &\longrightarrow |a\rangle |a\rangle \\|b\rangle |M\rangle &\longrightarrow |b\rangle |b\rangle\end{aligned}$$

同时，对于由 $|a\rangle$ 和 $|b\rangle$ 构成的叠加态 $|s\rangle = \alpha |a\rangle + \beta |b\rangle$ ，也可以进行克隆：

$$\begin{aligned}|s\rangle |M\rangle &\longrightarrow |s\rangle |s\rangle = (\alpha |a\rangle + \beta |b\rangle)(\alpha |a\rangle + \beta |b\rangle) \\&= \alpha^2 |a\rangle |a\rangle + \beta^2 |b\rangle |b\rangle + \alpha\beta(|a\rangle |b\rangle + |b\rangle |a\rangle)\end{aligned}$$

量子不可克隆定理的证明

但是，根据线性性质，这个克隆的过程可以表达为：

$$|s\rangle |M\rangle = \alpha |a\rangle |M\rangle + \beta |b\rangle |M\rangle \longrightarrow \alpha |a\rangle |a\rangle + \beta |b\rangle |b\rangle$$

显然得到了不同的结果。说明这个机器并不能完美复制任何一个未知的量子态。

至此已经完成了对量子不可克隆定理的证明。

量子不可克隆定理

完全未知的纯量子态不可以被完美的克隆

这是量子力学体系线性性质的要求。

对受激辐射的解释：不可避免的存在自发辐射。

量子不可克隆定理的讨论

前面的证明是基于线性叠加原理的，也就是说需要对克隆机有至少 3 个可能的输入： $|a\rangle$ 、 $|b\rangle$ 和 $|s\rangle$ 。

因此量子不可克隆定理并没有完全排除克隆量子态的可能性——仅仅是完全未知的量子态不可以完美克隆。

假定这个机器仅仅可以完美克隆量子态 $|a\rangle$ 和 $|b\rangle$ ，我们限定输入只能是 $|a\rangle$ 和 $|b\rangle$ ：

$$\begin{aligned}|a\rangle |M\rangle &\longrightarrow |a\rangle |a\rangle \\ |b\rangle |M\rangle &\longrightarrow |b\rangle |b\rangle\end{aligned}$$

此时考虑性质 2：变换前后内积相同

$$\langle b|a\rangle \langle M|M\rangle = \langle b|a\rangle^2$$

因为 $|a\rangle$ 和 $|b\rangle$ 是独立的量子态，所以只能为 $\langle a|b\rangle = 0$

量子不可克隆定理的讨论

所以一个克隆机器对一组相互正交的量子态实现完美克隆是可能的。
这并不违反量子不可克隆定理。

Question:

为什么这个克隆过程是一个么正变换？

According to quantum mechanics this transformation should be representable by a linear (in fact unitary) operator. It therefore follows that if the incoming photon has the polarization given by the linear combination $\alpha|\uparrow\rangle + \beta|\leftrightarrow\rangle$ —for example, it could be linearly polarized in a direction 45° from the vertical, so that $\alpha = \beta = 2^{-1/2}$ —the result of its interaction with the apparatus will be the superposition of equations (2) and (3):

量子不可克隆定理的意义与应用

1. 量子隐形传态的安全保障
2. 不确定性关系成立的保障
3. 保证了信息不能超光速传递

量子不可克隆定理的意义与应用

信息不能超光速传递

以粒子的自旋为例，如果两个粒子处于纠缠态：

$$S = \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\uparrow\rangle + |\downarrow\rangle \otimes |\downarrow\rangle)$$

在 \hat{S}_x 的本征态下展开：

$$\begin{cases} |\uparrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\leftarrow\rangle) \\ |\downarrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\leftarrow\rangle) \end{cases}$$

可以得到：

$$S = \frac{1}{\sqrt{2}}(|\rightarrow\rangle \otimes |\rightarrow\rangle + |\leftarrow\rangle \otimes |\leftarrow\rangle)$$

量子不可克隆定理的意义与应用

信息不能超光速传递

Alice 有粒子 1, Bob 有粒子 2, Alice 可以选择测 S_z , 即为信号 1, 或者测 S_x , 即为信号 0.

在 Alice 测量之后, 双粒子态坍缩。假设 Alice 测量 S_z , 得到了 $|\uparrow\rangle$, 此时体系坍缩到 $S = |\uparrow\rangle \otimes |\uparrow\rangle$ 。

此时 Bob 如果测量 S_z , 只能得到 $|\uparrow\rangle$, 如果测量 S_x , 有一半的概率得到 $|\rightarrow\rangle$ 或者 $|\leftarrow\rangle$, 与 Alice 测量前相同。

但是没有经典信道的信息传递, Bob 是不知道 Alice 什么时候做了怎样的测量的, 他只能测量一次, 之后量子态又会被他的测量影响。

但是, 如果 Bob 有克隆任意未知量子态的机器, 会发生什么?

量子不可克隆定理的意义与应用

信息不能超光速传递

根据量子不可克隆原理，Bob 不可能完美复制粒子二的未知量子态，但是根据之前的讨论，Bob 可以拥有一个克隆机器，只能完美克隆一组相互正交的量子态。

不妨假设 Bob 的克隆机器只能完美克隆 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ ，看看会发生什么：如果 Alice 选择的是测量 S_z ，得到了 $|\uparrow\rangle$ ，那么 Bob 的克隆机可以完美运作，在克隆之后 Bob 得到的是：

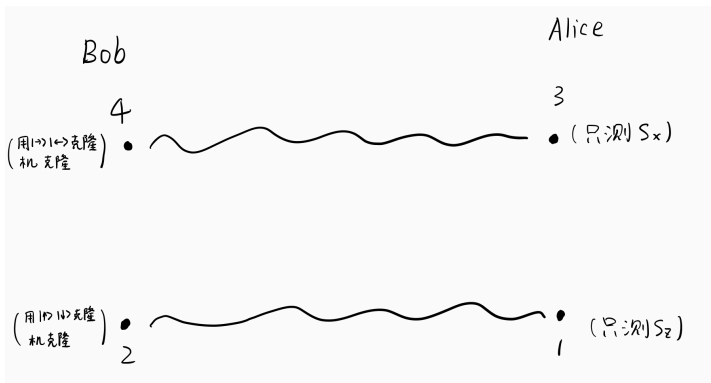
$$|\uparrow\uparrow\uparrow \dots\rangle$$

然后 Bob 对这些态逐个进行单次测量，测量 S_z 只能得到 $|\uparrow\rangle$ ，测量 S_x 有一半的概率得到 $|\rightarrow\rangle$ 或者 $|\leftarrow\rangle$ ，Bob 认为 Alice 测量了 S_z ，由此得到信号 1。

量子不可克隆定理的意义与应用

信息不能超光速传递

看似信息超光速传递得到了实现。尽管看起来只能传递信号 1，但是是否可以用四个粒子、两台单独的克隆机实现 1 和 0 的传递？



量子不可克隆定理的意义与应用

信息不能超光速传递

实际上是不可能的，两个粒子甚至不能仅仅传递信号 1.

我们再考虑 Alice 选择测量 S_x 的情况，假如得到的是 $|\rightarrow\rangle$ ，那么 Bob 那里的粒子会坍缩到 $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$.

Bob 还使用那个只能完美克隆 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 的克隆机去克隆，他会得到：

$$\frac{1}{\sqrt{2}}(|\uparrow\uparrow\uparrow \dots\rangle + |\downarrow\downarrow\downarrow \dots\rangle)$$

如果这些克隆的粒子是相互纠缠的，如果去测量某个粒子的 S_x ，会有一半的概率得到 $|\rightarrow\rangle$ 或者 $|\leftarrow\rangle$ ，并没有影响其他粒子的测量结果。但是如果去测量某个粒子的 S_z ，整个体系会坍缩到 $|\uparrow\uparrow\uparrow \dots\rangle$ 或者 $|\downarrow\downarrow\downarrow \dots\rangle$ ，之后再测量其他粒子的 S_z ，只会得到一种结果。

量子不可克隆定理的意义与应用

信息不能超光速传递

所以对 Bob 而言, 无论 Alice 测量的是什么, 他用只能完美克隆 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 的克隆机去克隆并进行测量, 得到的结果是一样的: 测量 S_z 只能得到一种结果, 测量 S_x 等概率出现 2 种结果。

因此 Bob 无法得知 Alice 要传递什么信息, 甚至连仅仅传递 1 都无法做到。

也就是说, 量子不可克隆原理保证了信息超光速传递是不可能的, 即使根据量子不可克隆原理有可能克隆一组已知的相互正交量子态。

量子不可克隆定理的延伸与推广

量子不可克隆定理

完全未知的纯量子态不可以被完美的克隆

完全未知？

允许存在可以完美复制已知的一组相互正交的量子态的克隆机器

纯态？

1996 年的一篇 PRL: *Noncommuting Mixed States Cannot Be Broadcast*

提出了量子不可广播定理。从纯态到混合态的推广。

时间反演？

2000 年 A. K. Pati 和 S. L. Braunstein 在 *Nature* 上发表:
Impossibility of Deleting an Unknown Quantum State
提出并证明了量子不可删除定理。

量子不可克隆定理的延伸与推广

不可广播定理

混合态：并不是叠加态，无法用一个 $|a\rangle$ 来表示，可以用密度算符来表达一个混合态。

$$\hat{\rho} = \sum_i \omega_i |\psi_i\rangle \langle \psi_i|$$

混合态量子系统出现的案例包括，处于热力学平衡或化学平衡的系统、制备历史不确定或随机变化的系统（因此不知道到底系统处于哪个纯态）。

对于一个纯态 $|\psi\rangle$ ，其密度算符为 $\hat{\rho} = |\psi\rangle \langle \psi|$ 。

一般而言，对于一个量子系统，如果密度算符满足：

$$\begin{cases} \hat{\rho}^2 = \hat{\rho} \\ \text{Tr}(\hat{\rho}) = 1 \end{cases}$$

那么它就是一个纯态。

量子不可克隆定理的延伸与推广

不可广播定理

为什么是 Broadcast:

对纯态 $|\psi\rangle$ 的广播就是产生纠缠态 $|\psi\rangle \otimes |\psi\rangle$, 即纯态的量子克隆, 广播的接受者可以获得克隆的量子态。

对混合态 ρ 的广播并不一定要产生 $\rho \otimes \rho$.

例如 ρ 的谱分解为 $\rho = \sum_b \lambda_b |b\rangle \langle b|$, 如果可以产生: $\sum_b \lambda_b |b\rangle |b\rangle \langle b| \langle b|$, 就能够实现对这个混合态的广播。

量子不可克隆定理的延伸与推广

量子不可广播定理

A 系统: $\{\rho_0, \rho_1\}$ 中的一个混合态, B 系统: 标准量子态 Σ 。
系统 AB 初始态为 $\rho_s \otimes \Sigma$. 其中 $s = 0, 1$, 指定了被广播的态。
我们希望存在一个符合量子力学的物理过程 \mathcal{E} :

$$\rho_s \otimes \Sigma \longrightarrow \mathcal{E}(\rho_s \otimes \Sigma) = \tilde{\rho}_s$$

其中 $\tilde{\rho}$ 在希尔伯特空间 AB 中且满足:

$$\begin{cases} \text{Tr}_A(\tilde{\rho}_s) = \rho_s \\ \text{Tr}_B(\tilde{\rho}_s) = \rho_s \end{cases}$$

如果这个物理过程 \mathcal{E} 存在且对 $s = 0, 1$ 均成立, 这个量子系统 A 就是可以被广播的。

量子不可克隆定理的延伸与推广

不可广播定理

当 $\tilde{\rho}_s = \rho_s \otimes \rho_s$, 就从“广播”回到了所谓的“克隆”。

A. K. Pati 和 S. L. Braunstein 在文章中证明了系统 A 可广播当且仅当 ρ_0, ρ_1 两个算符对易。

另外, 他们还指出, 系统 A 可克隆当且仅当 ρ_0, ρ_1 是相同的或者是正交的 ($\rho_0 \rho_1 = 0$) 。

可见当 ρ_0, ρ_1 是纯态的密度算符时, 就回到了纯态的量子不可克隆定理。因此量子不可广播定理更具有普适性。

量子不可克隆定理的延伸与推广

量子不可删除定理

量子不可删除定理

给定任意未知量子态的两个副本，不可能完全删除其中一个。

如果有一个量子删除机器，它的作用可以用下面的演化表示：

$$|\psi\rangle |\psi\rangle |A\rangle \longrightarrow |\psi\rangle |\Sigma\rangle |A_\psi\rangle$$

对于一个光子，处于偏振态 $|H\rangle$ 或者 $|V\rangle$ ，可以有：

$$|H\rangle |H\rangle |A\rangle \longrightarrow |H\rangle |\Sigma\rangle |A_H\rangle$$

$$|V\rangle |V\rangle |A\rangle \longrightarrow |V\rangle |\Sigma\rangle |A_V\rangle$$

我们注意到对这个删除机的定义是不完备的。在 W. K. Wootters 和 W. H. Zurek 对量子不可克隆定理最早的证明中，对克隆机做了如下完备定义：

$$|A_0\rangle |s\rangle \longrightarrow |A_s\rangle |ss\rangle$$

量子不可克隆定理的延伸与推广

量子不可删除定理

删除机的不完备性在于，将相同态输入体现了其功能含义，但如果进行如下输入也应该有一个相对应的结果：

$$\frac{1}{\sqrt{2}}(|H\rangle|V\rangle + |V\rangle|H\rangle)|A\rangle \longrightarrow |\phi\rangle$$

现在假设 $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ ，可以得到：

$$|\psi\rangle|\psi\rangle|A\rangle \longrightarrow |\psi\rangle|\Sigma\rangle|A_\psi\rangle = \alpha|H\rangle|\Sigma\rangle|A_\psi\rangle + \beta|V\rangle|\Sigma\rangle|A_\psi\rangle$$

但同时结合：

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

还可以得到：

$$|\psi\rangle|\psi\rangle|A\rangle \longrightarrow \alpha^2|H\rangle|\Sigma\rangle|A_H\rangle + \beta^2|V\rangle|\Sigma\rangle|A_V\rangle + \sqrt{2}\alpha\beta|\phi\rangle$$

量子不可克隆定理的延伸与推广

量子不可删除定理

如果要想这两个结果相同，并注意到 $|\phi\rangle$ 不依赖于 α 和 β ，需要满足：

$$\begin{aligned} |A_\psi\rangle &= \alpha |A_H\rangle + \beta |A_V\rangle \\ |\phi\rangle &= \frac{1}{\sqrt{2}}(|H\rangle |\Sigma\rangle |A_V\rangle + |V\rangle |\Sigma\rangle |A_H\rangle) \end{aligned}$$

根据 $|H\rangle$ 和 $|V\rangle$ 的正交性： $|A_V\rangle$ 与 $|A_H\rangle$ 也是正交的。

可见，量子态 $|\psi\rangle$ 并没有被完全删除，只是将自身携带的信息转移到了删除仪器中。

量子不可删除定理在量子计算机中对量子文件的安全存储提供了保护作用。

近似量子克隆

量子不可克隆定理

完全未知的纯量子态不可以被完美的克隆

“不完美”的克隆是否可能？

——近似量子克隆

1996 年，V. Buzek 和 M. Hillery 发表了 *Quantum copying: Beyond the no-cloning theorem*，提出了量子复制机。

后来，人们还提出了概率量子克隆机的原理。

近似量子克隆

"universal" quantum-copying machine

量子复制机：要求低于克隆，允许输入与输出存在偏差。

人们的研究集中在寻找一个性能最佳的量子复制机，可以尽可能精确地复制所有输入态。

表征两个态接近程度的量：施密特距离 D 和保真度 F 。

$$D_a = \text{Tr}[\hat{\rho}_a^{(id)} - \hat{\rho}_a^{(out)}]^2$$

$$F = \text{Tr}(\hat{\rho}_1^{1/2} \hat{\rho}_2 \hat{\rho}_1^{1/2})^{1/2}$$

在输入态为纯态 $|\psi\rangle$ 的时候，保真度 $F = \langle \psi | \hat{\rho} | \psi \rangle$

人们后来证明得到，对于 N 个处于相同态的输入模和 M 个处于相同状态的输出模 ($M > N$)，保真度最高可以达到：

$$F_{N,M} = \frac{M(N+1) + N}{M(N+2)}$$

当输入 1 个态输出 2 个相同态时，保真度最大可达到 $F = \frac{5}{6}$

近似量子克隆

概率量子克隆机

一个量子克隆机可以精确克隆两个相互正交的量子态，如果是两个非正交的量子态呢？

概率量子克隆机将克隆的么正演化过程和测量的坍缩过程相结合，来进行克隆。

假设有两个态 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ ，克隆机操作的体系包括原始输入 A、复制模 B 和附加模 P，并能够进行如下演化：

$$|\psi_s\rangle_A |S_0\rangle_{BP} \longrightarrow \sqrt{\eta} |\psi_s\rangle_A |\psi_s\rangle_B |0\rangle_P + \sqrt{1-\eta} |\psi_{AB}\rangle_{AB} |1\rangle_P$$

这个演化对 $s = 1, 2$ 均成立，且 η 不依赖输入态。 $|0\rangle_P$ 和 $|1\rangle_P$ 是模 P 的某个力学量 \hat{A}_P 的正交的本征态。

近似量子克隆

概率量子克隆机

对模 P 的力学量 A_P 进行一次测量，有 η 的概率得到 0，这个时候 AB 系统坍缩到我们需要的精确复制态。

如果得到了 1，那么 AB 系统坍缩到我们不想要的非复制态，克隆机无输出。

概率量子克隆机的关键：设计合适的么正演化，联系合适的测量过程。可以证明，对于输入态为 $\{|\psi_1\rangle, |\psi_2\rangle\}$ 的情况，概率量子克隆机的克隆效率 η 可达到的最大值为：






$$\eta_{max} = \frac{1}{1 + \langle \psi_1 | \psi_2 \rangle}$$

可见，只有输入态相互正交的时候， η 才可能达到 1。

另外，对于不止 2 个输入态的情形，概率量子克隆技术依然适用， η_{max} 的形式也更为复杂。

参考资料

References

-  W. K. Wootters and W. H. Zurek, Nature 299, 802(1982).
-  H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa and B. Schumacher, Phys. Rev. Lett. 76, 2818(1996) .
-  V. Buzek and M. Hillery, Phys. Rev. A 54, 1844 (1996).
-  Lu-Ming Duan and Guang-Can Guo, Phys. Lett. A 243,261-264(1998) .
-  A. K. Pati and S. L. Braunstein, Nature 404, 164(2000).
https://en.wikipedia.org/wiki/Density_matrix

Thanks for listening!!

Thanks for listening!!



Questions?