量子不可克隆定理与量子克隆

杨佳宇　物理学院　1800011409

摘要: 量子不可克隆定理在量子力学中有极为重要的意义。本文从早期人们对量子不可克隆定理的思考和引入出发，对其定理的内容及证明进行简单的介绍，并讨论了该定理的实际意义和应用。同时，作为量子不可克隆定理的推广，还介绍了量子不可删除定理与不可广播定理。最后讨论了近似量子克隆的技术，并对量子克隆及量子信息的发展进行了展望。

关键词: 量子不可克隆定理　量子克隆　量子密码学　量子信息

目录

1 量子不可克隆定理

1.1 量子不可克隆定理的内容与证明

1.1.1 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 [1]，首次提出了量子不可克隆定理。

爱因斯坦在他 1917 年发表的论文《关于辐射的量子理论》中从理论上提出了受激辐射，大约 10 年后，英国物理学家保罗 · 狄拉克首次实验证明受激辐射的存在。当激励光子打到激发态的原子上时，在辐射场的作用下，原子会跃迁到低能级并辐射出一个光子，辐射的光子和激励光子的频率、偏振态完全相同。从另一个角度来看，受激辐射似乎是一个对光子的量子态进行克隆的过程：向系统输入一个光子，可以输出两个量子态完全相同的光子。

但实际上，在受激辐射的过程中，不可避免地也会存在自发辐射，因此当我们输入一个光子、得到两个光子的时候，我们并不能完全确定另一个光子就是由自发辐射产生的，因此这样的克隆光子的量子态的方法并不能做到绝对的完美克隆。

基于对受激辐射过程的思考，物理学家开始了对量子态的克隆的研究，并最终得到了量子不可克隆定理。

1.1.2 定理的内容及证明

假定量子态是可以被克隆的，那么就应该存在一个完美的克隆机器，这个机器的作用可以用1式来表达。

$$|s\rangle|\Sigma\rangle|M\rangle \longrightarrow |s\rangle|s\rangle|M_s\rangle \tag{1}$$

其中 $|s\rangle$ 为输入的想要克隆的量子态，$|M\rangle$ 和 $|M_s\rangle$ 分别表示克隆机器的初态和末态，$|\Sigma\rangle$ 为一个空白的量子态，也可以形象地理解为得到目标克隆态所需要的“材料”，而这个箭头则是需要在量子克隆机中完成的一个幺正演化。

因为这个克隆过程是遵循薛定谔方程的，所以这个过程具有两个性质：其一为线性性质，因为薛定谔方程本身就是一个线性方程；其二为概率守恒，即幺正变换保内积的性质，进行该过程前的态 $|\phi_0\rangle$ 和完成该过程后的态 $|\phi\rangle$ 满足 $\langle\phi_0|\phi_0'\rangle = \langle\phi|\phi'\rangle$。

对于两个线性独立的归一化量子态 $|a\rangle$ 和 $|b\rangle$，我们所定义的克隆机器都可以对他们进行完美的克隆克隆，即：

$$\begin{aligned} |a\rangle|\Sigma\rangle|M\rangle &\longrightarrow |a\rangle|a\rangle|M_a\rangle \\ |b\rangle|\Sigma\rangle|M\rangle &\longrightarrow |b\rangle|b\rangle|M_b\rangle \end{aligned} \tag{2}$$

同时，对于由 $|a\rangle$ 和 $|b\rangle$ 构成的叠加态 $|s\rangle = \alpha|a\rangle + \beta|b\rangle$，克隆机器也可以对它进行克隆，即：

$$\begin{aligned} |s\rangle|\Sigma\rangle|M\rangle \longrightarrow |s\rangle|s\rangle &= (\alpha|a\rangle + \beta|b\rangle)(\alpha|a\rangle + \beta|b\rangle)|M_s\rangle \\ &= (\alpha^2|a\rangle|a\rangle + \beta^2|b\rangle|b\rangle + \alpha\beta(|a\rangle|b\rangle + |b\rangle|a\rangle))|M_s\rangle \end{aligned} \tag{3}$$

以上仅是根据克隆机的定义表述了这一过程。根据这个过程的线性性质，也可以将该克隆过程表达为：

$$|s\rangle|\Sigma\rangle|M\rangle = \alpha|a\rangle|\Sigma\rangle|M\rangle + \beta|b\rangle|\Sigma\rangle|M\rangle \longrightarrow \alpha|a\rangle|a\rangle|M_a\rangle + \beta|b\rangle|b\rangle|M_b\rangle \tag{4}$$

对比3式和4式，显然得到了矛盾的结果，由反证法，假设不成立，即不存在这样一个可以完美克隆任何一个量子态的克隆机器。

Theorem 1. 完全未知的纯量子态不可以被完美的克隆。

定理1即为量子不可克隆定理的严格表述，从证明过程中可以看出，量子不可克隆定理本质上是量子力学体系线性性质的要求。

1.1.3 关于定理的进一步讨论

1.1.2中对量子不可克隆定理的证明是建立在线性叠加原理的基础上的，换言之，我们默认允许对克隆机提供至少 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。

假定有一个克隆机器仅仅可以完美克隆两个线性独立的归一化量子态 $|a\rangle$ 和 $|b\rangle$，即只有输入 $|a\rangle$ 或 $|b\rangle$ 时才能使用1式。此时利用幺正变换前后内积相同的性质，可以得到：

$$\langle b|a\rangle = \langle b|a\rangle^2 \tag{5}$$

因为 $|a\rangle$ 和 $|b\rangle$ 线性独立，若要满足5式，当且仅当 $\langle a|b\rangle = 0$。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。

1.2 定理的意义与应用

1.2.1 量子密钥分发的安全保障

假设两个自旋 $\frac{1}{2}$ 粒子 A 和 B 处于纠缠态，在 $\hat{S}_z$ 表象下：

$$S = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A \otimes |\uparrow\rangle_B + |\downarrow\rangle_A \otimes |\downarrow\rangle_B) \tag{6}$$

同时通过基变换，在 $\hat{S}_x$ 表象下，我们发现：

$$S = \frac{1}{\sqrt{2}}(|\rightarrow\rangle_A \otimes |\rightarrow\rangle_B + |\leftarrow\rangle_A \otimes |\leftarrow\rangle_B) \tag{7}$$

现在假设 Alice 拿着若干粒子 A，Bob 拿着若干粒子 B，Alice 所及决定测量 A 粒子的 S_z 或是 S_x，如果测量 S_z，得到 $|\uparrow\rangle$ 则记为 1，$|\downarrow\rangle$ 则记为 0；如果测量 S_x，得到 $|\rightarrow\rangle$ 则记为 1，$|\leftarrow\rangle$ 则记为 0。分别测量若干 A 粒子之后，Alice 就得到了一个随机的比特序列。Bob 对这些 B 粒子同样进行随机的测量，在测量完成之后，Bob 和 Alice 在经典信道公开自己每一次测量的是 S_z 还是 S_x，因为测量的方向完全是随机选取的，所以大约会有一半的粒子 Alice 和 Bob 测量了相同方向的自旋。通过对比这些粒子的测量结果是否一致，就可以知道这段信息有没有被窃听。

假设有一个窃听者 Eve，可以在 Alice 测量后，Bob 测量前，对 B 粒子先进行测量。但是因为此时 Alice 测量方向的选取还没有公开，所以 Eve 有几率选取了和 Alice 不同的测量方向，使得量子态 S 坍缩到另外一个态上，此时假如 Bob 对该粒子测量的方向恰好和 Alice 一致，那么他有一半的几率得到和 Alice 不同的结果。此时 Eve 的窃听就会被 Alice、Bob 察觉。

但是如果没有量子不可克隆定理，Eve 有量子克隆技术，可以在 Alice 测量之后对 B 粒子进行克隆，这样的话 Eve 的窃听并不会影响 Bob 手中原本的 B 粒子的量子态。这样一来 Eve 的窃听也就不再能够被察觉。

可见，正是因为有量子不可克隆定理，才能够从理论基础上保障量子密钥分发的安全性。

1.2.2 不确定性关系成立的保障

根据不确定性关系，对于一个粒子，我们无法同时确定它的坐标和动量。实际上，当我们测量它的坐标时，它会坍缩到坐标表象下的一个本征态，此时动量的不确定度发散；当我们测量它的动量时，会坍缩

到动量表象下的一个本征态，此时波函数为一个平面波，坐标在全空间弥散。可见不确定性关系从某种意义上是由于测量对原本的量子态一定会产生干扰导致的。

如果量子不可克隆定理不成立，假设我们可以对量子态进行克隆，那么就能够在测量之前先对要测量的对象进行克隆，只对克隆的量子态进行测量，而并不改变原本的量子态。这样就可以实现“无干扰地测量”，对一部分克隆的量子态测量坐标，一部分克隆的量子态测量动量，就可以同时确定其坐标和动量，打破不确定性关系。

因此，量子不可克隆定理的成立也保证了不确定性关系的正确性。

1.2.3 保证信息不能超光速传递

仍旧使用1.2.1中相互纠缠的 A、B 粒子，Alice 手里有粒子 A，Bob 手里有粒子 B，Alice 可以选择测 S_z，即视为发出为信号 1，或者选择测 S_x，即视为发出信号 0。在 Alice 测量之后，双粒子态 S 会立即坍缩。假设 Alice 测量 S_z，得到了 $|\uparrow\rangle$，此时体系坍缩到 $S = |\uparrow\rangle \otimes |\uparrow\rangle$。在这之后，Bob 如果测量 S_z，只能得到 $|\uparrow\rangle$，与 Alice 未进行测量时的情形不同；如果测量 S_x，有一半的概率得到 $|\rightarrow\rangle$ 或者 $|\leftarrow\rangle$，与 Alice 未进行测量时的情形相同。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。因此即使坍缩过程是是立刻发生的，但这并不能用来帮助我们传递任何信息。

但是，如果量子不可克隆定理不成立，Bob 有克隆任意未知量子态的机器，他就可以在 Alice 测量之后、自己测量之前，将手里的 B 的自旋态克隆若干份，一部分测量 S_z，一部分测量 S_x。其中测量 S_z 只能得到 $|\uparrow\rangle$，测量 S_x 有一半的概率得到 $|\rightarrow\rangle$ 或者 $|\leftarrow\rangle$，由此可以得知 Alice 测量的是 S_z，便可以获知 Alice 传递的信号 1，从而实现信息的超光速传递。

根据量子不可克隆定理，Bob 不可能完美复制粒子 B 的未知的量子态，但是根据1.1.3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 $|\downarrow\rangle$，讨论这种情形下是否能够实现信息的超光速传递。

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 B 粒子之后之后 Bob 得到的是 $|\uparrow\uparrow\uparrow ...\rangle$. 随后 Bob 对这些克隆粒子逐个进行单次测量，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。

再考虑 Alice 选择测量 S_x、发出信号 0 的情况，假如 Alice 得到的是 $|\rightarrow\rangle$，那么 Bob 那里的粒子会坍缩到 $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$. 然而 Bob 还使用那个只能完美克隆 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 的克隆机去克隆，根据线性叠加原理，他会得到：

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

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 $|\uparrow\uparrow\uparrow ...\rangle$ 或者 $|\downarrow\downarrow\downarrow ...\rangle$，之后再测量其他粒子的 S_z，只会得到一种结果。

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 依然无法得知 Alice 要传递什么信息。

综上所述，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，也依然无法实现信息超光速传递。

2 量子不可克隆定理的延伸和推广

2.1 量子不可广播定理

2.1.1 问题的提出

从定理1中可以看出，量子不可克隆定理完全是对于纯态而言的。实际上，我们还会遇到混合态的量子系统，例如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，在这些情形下不知道到底系统处于哪个纯态，只能知道系统处在各个纯态的概率分布。混合态无法用一个 $|a\rangle$ 来表示，只能用密度算符来表示：$\hat{\rho} = \sum_i \omega_i |\psi_i\rangle \langle\psi_i|$ [2]。

一般而言，对于任何一个量子系统，都能够写出它的密度算符，如果密度算符满足8式的条件时，这个系统就是一个纯态。

$$\begin{cases} \hat{\rho}^2 = \hat{\rho} \\ Tr(\hat{\rho}) = 1 \end{cases} \tag{8}$$

对于纯态，已经提出并证明了量子不可克隆定理，物理学家们便开始关心混合态的量子克隆能否实现。在 1996 年，Howard Barnum 等人发表了一篇文章：《*Noncommuting Mixed States Cannot Be Broadcast*》，提出并证明了量子不可广播定理，实现了将量子不可克隆定理从纯态到混合态的推广 [3]。

2.1.2 定理的内容

对纯态 $|\psi\rangle$ 的广播就是产生态 $|\psi\rangle \otimes |\psi\rangle$，即纯态的量子克隆，使得广播的接受者们可以获得克隆的量子态。换言之，纯态的广播和克隆等价。

但是对于混合态 ρ 而言，广播并不一定需要产生态 $\rho \otimes \rho$，当然实现了混合态的克隆是完全可以实现混合态广播的，但混合态的信息并不一定非要克隆出 $\rho \otimes \rho$ 才能广播，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。简而言之，对于混合态而言，克隆是广播的充分不必要条件。

下面我们来严格的对“广播”进行定义。

假设 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 $\mathcal{E}$：

$$\rho_s \otimes \Sigma \longrightarrow \mathcal{E}(\rho_s \otimes \Sigma) = \tilde{\rho}_s \tag{9}$$

其中 $\tilde{\rho}$ 在希尔伯特空间 AB 中且满足：

$$\begin{cases} Tr_A(\tilde{\rho_s}) = \rho_s \\ Tr_B(\tilde{\rho_s}) = \rho_s \end{cases} \tag{10}$$

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。

Theorem 2. *系统 $\{\rho_0, \rho_1\}$ 可以被广播当且仅当算符 ρ_0, ρ_1 对易。*

更进一步，如果系统 $\{\rho_0, \rho_1\}$ 可以被广播，那么算符 ρ_0, ρ_1 是相同的或者是正交的（$\rho_0 \rho_1 = 0$）。

量子不可广播定理是对量子不可克隆定理的延伸和加强，当 ρ_0、ρ_1 为纯态的密度算符时，就从量子不可广播定理回到了量子不可克隆定理。

2.2 量子不可删除定理

2.2.1 量子不可删除定理的提出

在得到定理1之后，人们也开始研究量子克隆过程的时间反演，即已经有两个相同的量子态，是否可以将其变为一个量子态和一个空白态。通俗地讲，即是否可以删除两个相同的量子态中的某一个。

2000 年 A. K. Pati 和 S. L. Braunstein 在 *Nature* 上发表了一篇题为《*Impossibility of Deleting an Unknown Quantum State*》的文章，正式提出并证明了量子不可删除定理 [4]。

Theorem 3. 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。

2.2.2 量子不可删除定理的证明

我们依然采取反证法来证明量子不可删除定理。与1.1.2中的证明类似，假设量子不可删除定理不成立，也就存在一个量子删除机器，它的作用可以用11式中的演化来表示。其中 $|\psi\rangle$ 为任意一个量子态，$|\Sigma\rangle$ 为一个不依赖与输入态的空白态。$|A\rangle$ 和 $|A_\psi\rangle$ 分别为这个量子删除机器的初态和末态。11式中的演化过程物理意义是明确的，相比1式，也确实是量子克隆的时间反演过程。这个空白态的生成可以理解为我们将原本储存在量子态中的信息完全释放掉，原本存放这些信息的存储空间再删除之后闲置出来，就形成了一个空白的量子态，在后续如果允许我们就可以将其他的信息写入到这个存储空间中，即将空白态再转化为其他的量子态。

$$|\psi\rangle|\psi\rangle|A\rangle \longrightarrow |\psi\rangle|\Sigma\rangle|A_\psi\rangle \tag{11}$$

需要说明的是，相比1式对克隆机的定义，11式对量子删除机的定义并不是完备的。1式对克隆机的定义的完备性在于对于任何形式的输入 $|s\rangle$，都可以依据1式来得到相应的输出。但是11式只定义了对量子删除合法的输入，只有将两个相同的量子态 $|\psi\rangle|\psi\rangle$ 作为删除机的输入，才能够根据11式的定义得到相应的输出。但是我们也可以对删除机进行类似于 $|\psi_1\rangle|\psi_2\rangle$ 的输入，尽管不合法，但也应该得到一个输出，即使这个输出没有什么物理意义。而对于不同的量子删除机，也可能对于这些不合法的输入有着不同的输出。因此11式所定义的量子删除机并不是唯一的。

考虑一个光子的偏振态，假设两个本征态为 $|H\rangle$ 和 $|V\rangle$。根据11式的定义，将 $|H\rangle|H\rangle$ 或是 $|V\rangle|V\rangle$ 作为量子删除机的输入，应该得到12式中对应的输出结果。

$$\begin{aligned} |H\rangle|H\rangle|A\rangle &\longrightarrow |H\rangle|\Sigma\rangle|A_H\rangle \\ |V\rangle|V\rangle|A\rangle &\longrightarrow |V\rangle|\Sigma\rangle|A_V\rangle \end{aligned} \tag{12}$$

同时我们也对将 $\frac{1}{\sqrt{2}}(|H\rangle|V\rangle+|V\rangle|H\rangle)$ 作为不合法输入的情形进行13式中的单独定义，其中 $|\phi\rangle$ 不依赖于 α 和 β。

$$\frac{1}{\sqrt{2}}(|H\rangle|V\rangle+|V\rangle|H\rangle)|A\rangle \longrightarrow |\phi\rangle \tag{13}$$

现在假设 $|\psi\rangle=\alpha|H\rangle+\beta|V\rangle$，其中该 (α,β) 为该量子态所存储的信息。将 $|\psi\rangle|\psi\rangle$ 输入到量子删除机中，根据12式的定义，得到的输出应为14式。

$$|\psi\rangle|\psi\rangle|A\rangle \longrightarrow |\psi\rangle|\Sigma\rangle|A_\psi\rangle = \alpha|H\rangle|\Sigma\rangle|A_\psi\rangle+\beta|V\rangle|\Sigma\rangle|A_\psi\rangle \tag{14}$$

但同时结合线性叠加原理，注意到 $|\psi\rangle|\psi\rangle=\alpha^2|H\rangle|H\rangle+\beta^2|V\rangle|V\rangle+\sqrt{2}\alpha\beta\frac{1}{\sqrt{2}}(|H\rangle|V\rangle+|V\rangle|H\rangle)$，因此将 $|\psi\rangle|\psi\rangle$ 输入删除机得到的输出也可以表示为15式。

$$|\psi\rangle|\psi\rangle|A\rangle \longrightarrow \alpha^2|H\rangle|\Sigma\rangle|A_H\rangle+\beta^2|V\rangle|\Sigma\rangle|A_V\rangle+\sqrt{2}\alpha\beta|\phi\rangle \tag{15}$$

如果要让14式和15式得到的两个结果相同，需要满足的条件如16式所示。根据 $|H\rangle$ 和 $|V\rangle$ 的正交性可以得知 $|A_V\rangle$ 与 $|A_H\rangle$ 也是正交的。从16式中可以看出，量子态 $|\psi\rangle$ 中的信息并没有被完全删除，而是转移到了量子删除机 $|A_\psi\rangle$ 中。因此这和我们对量子删除机功能的定义相违背。所以并不存在我们所期望的量子删除机，量子不可删除定理也得到了证明。

$$\begin{aligned} |A_\psi\rangle &= \alpha\,|A_H\rangle + \beta\,|A_V\rangle \\ |\phi\rangle &= \frac{1}{\sqrt{2}}(|H\rangle\,|\Sigma\rangle\,|A_V\rangle + |V\rangle\,|\Sigma\rangle\,|A_H\rangle) \end{aligned} \tag{16}$$

在量子计算机中，量子不可删除定理对于量子文件的安全存储提供了理论保障，也是量子计算机发展的一块基石。

3 近似量子克隆技术

3.1 量子复制机

3.1.1 量子复制机概要

量子不可克隆定理告诉我们对任意未知的量子态的完美克隆是不可能的。但量子不可克隆定理并没有彻底否定对量子态的克隆技术，因为很多时候我们并不需要完美的精确克隆一个量子态，我们只需要“大致”克隆它，使其和原来的量子态近似相等。基于这一点，人们开始关注近似量子克隆技术，其中首要的就是对量子复制机的研究。

量子复制机不同于量子克隆机，允许输入态与输出态之间存在偏差，这时就需要一个衡量量子复制相似程度的标准。对于一个量子复制机，可以用17式来表示。

$$|s\rangle_A\,|\Sigma\rangle_B\,|M\rangle_C \longrightarrow |\phi\rangle_{ABC} \tag{17}$$

量子不可克隆定理告诉我们，$|\phi\rangle_{ABC} \neq |s\rangle_A\,|s\rangle_B\,|M_s\rangle_C$，此时考虑输出结果的约化密度矩阵，定义为18式，并要求 ρ_A、ρ_B 相等，且它们和完美克隆时输出态密度矩阵 ρ_{id} 尽可能的接近。当完全相等的时候，就回到10式，也就是量子“广播”的条件。

$$\begin{aligned} \rho_A &= Tr_{BC}(|\phi\rangle_{ABC\ ABC}\,\langle\phi|) \\ \rho_B &= Tr_{AC}(|\phi\rangle_{ABC\ ABC}\,\langle\phi|) \end{aligned} \tag{18}$$

为了表征两个密度矩阵的接近程度，人们分别定义了施密特距离 D 和保真度 F。在量子复制机的性能评判中，近年来人们更常用的是保真度 F。而在输入态为纯态 $|\psi\rangle$ 的定义可以化简为 $F = \langle\psi|\,\hat{\rho}\,|\psi\rangle$。

$$\begin{aligned} D_a &= Tr[\hat{\rho}_a^{(id)} - \hat{\rho}_a^{(out)}]^2 \\ F &= Tr(\hat{\rho}_1^{1/2}\hat{\rho}_2\hat{\rho}_1^{1/2})^{1/2} \end{aligned} \tag{19}$$

在最早 Wootters 和 Zurek 提出量子不可克隆定理时，它们在证明中所提出的量子克隆机，虽然被证明无法实现完美克隆，但却可以实现近似的量子复制，这时最早的量子复制机，被后人称为 Wootters-Zurek 型量子复制机。

1996 年，V. Buzek 和 M. Hillery 发表了文章《*Quantum copying: Beyond the no-cloning theorem*》，首次提出量子复制的概念，并分析了 Wootters-Zurek 型量子复制机的性能，同时他们提出了另外一个量子复制机，也被称为通用量子复制机，因为他们所提出的量子复制机的保真度并不依赖于输入态，为一个常数。[5]

1997 年，Gisin 和 Massar 在文章《*Optimal quantum cloning machines*》中提出了 M-N 型通用量子复制机，即输入 N 个相同的初始态，可以得到 M 个复制态的量子复制机，，并得到其保真度仅仅依赖与 N、M 而不依赖于输入态。这是对 V. Buzek 和 M. Hillery 的通用量子复制机的推广。[6] 在之后还有很多其他的量子复制机的构造方案被提出，不过 Bruss 等人证明了 Gisin 和 Massar 的 N-M 型通用量子复制机的保真度是所有通用量子复制机中的上限。[7]

3.1.2 Wootters-Zurek 型量子复制机

在1.1.2和1.1.3中，利用1式给出了量子克隆机的定义，并提出了精确克隆两个相互正交的量子态对量子克隆机是可能的。而 Wootters-Zurek 型量子复制机实际上就是一个仅能精确复制两个相互正交的量子态的量子克隆机。假设量子克隆机可以精确复制 $|0\rangle$ 和 $|1\rangle$ 这两个相互正交的量子态，克隆过程可以有20式来表示。

$$\begin{aligned} |1\rangle|\Sigma\rangle|M\rangle &\longrightarrow |1\rangle|1\rangle|M_1\rangle \\ |0\rangle|\Sigma\rangle|M\rangle &\longrightarrow |0\rangle|0\rangle|M_0\rangle \end{aligned} \tag{20}$$

输入态设为 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$，将其输入到 Wootters-Zurek 型量子复制机中，根据线性叠加原理可以得到输出态 $|phi\rangle_{ABC} = \alpha|0\rangle|0\rangle|M_0\rangle + \beta|1\rangle|1\rangle|M_1\rangle$. 根据18式的定义，可以求出约化密度矩阵，结果由21表示。很显然，满足了 $\rho_A = \rho_B$。

$$\begin{aligned} \rho_A &= |\alpha|^2 |0\rangle_{A\ A}\langle 0| + |\beta|^2 |1\rangle_{A\ A}\langle 1| \\ \rho_B &= |\alpha|^2 |0\rangle_{B\ B}\langle 0| + |\beta|^2 |1\rangle_{B\ B}\langle 1| \end{aligned} \tag{21}$$

再利用19的定义计算保真度，考虑到输入态为一个纯态，可以计算得到保真度 $F = |\alpha|^4 + |\alpha|^4$. 可以看出，对于 Wootters-Zurek 型量子复制机，其保真度是依赖于输入态的，因此这并不是一个通用量子复制机。

考虑到归一化条件 $|\alpha|^2 + |\alpha|^2 = 1$，F 可以化为仅关于 $|\alpha|^2$ 的二次函数：$F = 2(|\alpha|^2 - 0.5)^2 + 0.5$。可见在输入态更接近于 $|0\rangle$ 或者 $|1\rangle$ 时，保真度可以接近 1，实际上也就是 Wootters-Zurek 型量子复制机本身按照定义可以完美克隆 $|0\rangle$ 和 $|1\rangle$ 这两个态，而当输入态更接近于 $\frac{1}{\sqrt{2}}|0\rangle \pm \frac{1}{\sqrt{2}}|1\rangle$ 时，保真度会达到最小值 0.5。

3.1.3 Buzek 和 Hillery 提出的通用量子复制机

Buzek 和 Hillery 提出的量子复制机试图解决保真度不稳定的问题，他们希望能够构造一个量子复制机，使得对于任何输入，其保真度都能维持稳定。他们假设量子复制机的变换可以定义如22式所示，其中包含 $|Y_0\rangle_C$ 和 $|Y_1\rangle_C$ 的项为对完美克隆的偏离项。

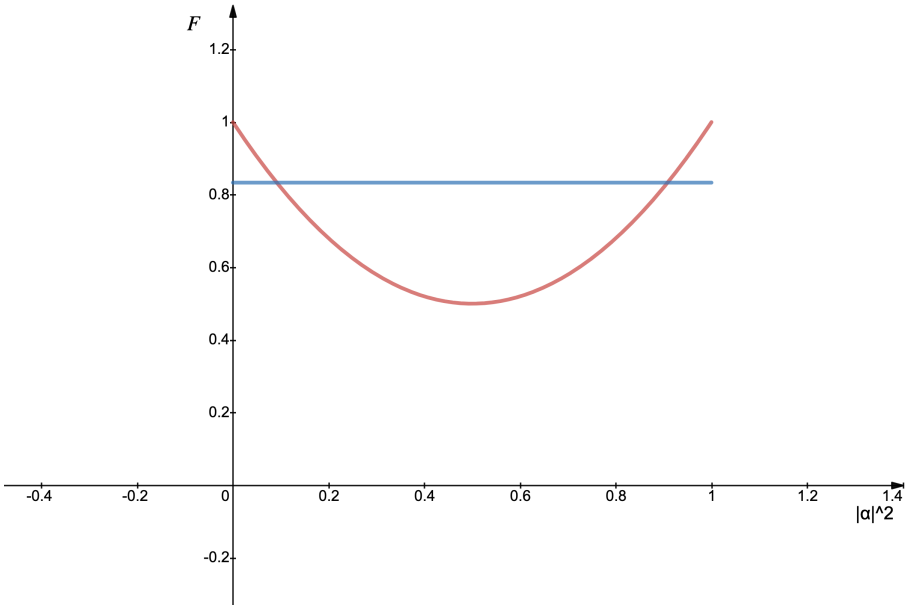
$$\begin{aligned} |0\rangle_A|\Sigma\rangle_B|M\rangle_C &\longrightarrow |0\rangle_A|0\rangle_B|M_0\rangle_C + (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)|Y_0\rangle_C \\ |1\rangle_A|\Sigma\rangle_B|M\rangle_C &\longrightarrow |1\rangle_A|1\rangle_B|M_1\rangle_C + (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)|Y_1\rangle_C \end{aligned} \tag{22}$$

根据幺正变换保内积的性质，我们可以得到 $\langle M_i|M_i\rangle + 2\langle Y_i|Y_i\rangle = 1$（对 $i = 0, 1$ 均成立）以及 $\langle Y_0|Y_1\rangle = \langle Y_1|Y_0\rangle = 0$。同时我们再引入一个假设：$\langle M_0|Y_0\rangle = \langle M_1|Y_1\rangle = \langle M_1|M_0\rangle = 0$。这一假设的引入仅仅是对复制机本身性质的要求。基于以上结论，再计算输入 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 时输出的约化密度算符，从而计算约化密度算符和完美克隆时的输出态密度算符的施密特距离 D。当 $\frac{\partial D}{\partial \alpha^2} = 0$ 的时候，可以求出 $|M_0\rangle$、$|M_1\rangle$、$|Y_0\rangle$、$|Y_1\rangle$ 之间的关系，从而将这一关系代入到22中，得到一个通用量子复制机的定义。这就是 Buzek 和 Hillery 构造量子复制机的基本思路。

进一步假设复制机态所在的希尔伯特空间 C 中的一组单位正交基为 $|\uparrow\rangle$ 和 $|\downarrow\rangle$，可以得到通用量子复制机的定义如23式所示。其中 $ketM$ 可以由 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 线性表出。

$$\begin{aligned}|0\rangle_A|\Sigma\rangle_B|M\rangle_C &\longrightarrow \sqrt{\frac{2}{3}}|0\rangle_A|0\rangle_B|\uparrow\rangle_C+\sqrt{\frac{1}{6}}(|0\rangle_A|1\rangle_B+|1\rangle_A|0\rangle_B)|\downarrow\rangle_C\\ |1\rangle_A|\Sigma\rangle_B|M\rangle_C &\longrightarrow \sqrt{\frac{2}{3}}|1\rangle_A|1\rangle_B|\downarrow\rangle_C+\sqrt{\frac{1}{6}}(|0\rangle_A|1\rangle_B+|1\rangle_A|0\rangle_B)|\uparrow\rangle_C\end{aligned} \tag{23}$$

对这一通用量子复制机输入 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ 时，可以求出其输出的约化密度矩阵为 $\rho_A=\rho_B=\frac{2}{3}\langle\psi|\psi\rangle+\frac{1}{6}I$，由此可以计算出保真度为 $F=\frac{5}{6}$。



与前面3.1.2中的 Wootters-Zurek 型量子复制机保真度进行对比，如图3.1.3所示，红线表示 Wootters-Zurek 型量子复制机保真度，蓝线表示通用量子复制机的保真度。可以看出在绝大多数情况下通用量子复制机的保真度都更高，当然最重要的是其保真度足够稳定。

3.1.4 N-M 型通用量子复制机

Gisin 和 Massar 构造的 N-M 型通用量子复制机定义如24所示。其构造思路与 Buzek 和 Hillery 的思路基本一致，只是将输入一个态、输出两个态推广位输入 N 个态、输出 M 个态。其中 $|Q\rangle$ 为机器的初始状态，$|Q_j\rangle$ 为某一种机器的末态，$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$，而 $|\psi^{\perp}\rangle=\beta^*|0\rangle-\alpha^*|1\rangle$，与 $|\psi\rangle$ 正交。

$$|N\psi\rangle|(M-N)\Sigma\rangle|Q\rangle\longrightarrow\sum_{j=0}^{M-N}\alpha_j|(M-j)\psi,j\psi^{\perp}\rangle|Q_j\rangle \tag{24}$$

对于 N-M 型通用量子复制机，可以求出 $\alpha_j=\sqrt{\frac{N+1}{M+1}}\sqrt{\frac{(M-N)!(M-j)!}{(M-N-j)!M!}}$.

输入 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$，其单个输出态的保真度 $F_{N,M}=\frac{M(N+1)+N}{M(N+2)}$，特别地，取 $N=1,M=2$，此时 $F=\frac{5}{6}$，即回归到 Buzek 和 Hillery 的通用量子复制机。

3.2 概率量子克隆机

在1.1.3中讨论过，一个量子克隆机可以精确克隆两个相互正交的量子态。但如果是两个非正交的量子态呢？我国量子信息学家段路明和郭光灿在 1998 年提出了概率量子克隆机的概念。[8]

概率量子克隆机与量子复制机不同，概率量子克隆机将克隆的幺正演化过程和测量的坍缩过程相结合，来进行克隆。克隆机虽然允许有一定概率克隆失败，但是一旦克隆成功，得到的一定是完全精确的克隆结果。

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25式所表示的演化，且该演化对 $s=1,2$ 均成立。而 $|0\rangle_P$ 和 $|1\rangle_P$ 是模 P 的某个可观测量 $\hat{A}_P$ 的正交的本征态。

$$|\psi_s\rangle_A |S_0\rangle_{BP} \longrightarrow \sqrt{\eta_s}\,|\psi_s\rangle_A |\psi_s\rangle_B |0\rangle_P + \sqrt{1-\eta_s}\,|\psi_{AB}\rangle_{AB} |1\rangle_P \tag{25}$$

在克隆过程过程之后，再对模 P 的可观测量 A_P 进行一次测量。这次测量有 η_s 的概率得到 0，有 $1-\eta_s$ 的概率得到 1。如果得到的结果是 0，AB 系统将随之瞬间坍缩到我们需要的精确复制态。如果得到的结果是 1，那么 AB 系统坍缩到我们不想要的非复制态，此时克隆机无输出，克隆失败。可见，概率量子克隆机实现的关键在于要设计合适的幺正演化，同时能够联系一个合适的测量过程。

段路明和郭光灿还证明了，对于输入态为 $\{|\psi_1\rangle, |\psi_2\rangle\}$ 的情况，一定有26式的关系。特别地，当 $\eta_1 = \eta_2 = \eta$ 时，有 $\eta_{max} = \frac{1}{1+\langle\psi_1|\psi_2\rangle}$，可见，只有输入态相互正交的时候，$\eta$ 才可能达到 1，即实现完美克隆。

$$\frac{\eta_1+\eta_2}{2} \leq \frac{1}{1+\langle\psi_1|\psi_2\rangle} \tag{26}$$

4 总结与展望

在 1982 年 Wootters 和 Zurek 提出量子不可克隆定理之后，量子克隆逐渐步入物理学家们的视野，在上世纪的最后几年，量子克隆成为一大研究热点，人们对它的研究进展十分迅速，近似量子克隆的理论基础也愈加完善，近似量子克隆的新方案也层出不穷，例如相位不变量子克隆 [9]、非对称量子克隆 [10] 等等。在完善的理论框架下，人们开始着眼于量子克隆机的物理实现，例如 Cummins、Jones 和 Furze 利用核磁共振系统实现了 Buzek 和 Hillery 的通用量子复制机 [11]。一直到近几年，量子克隆领域一直十分活跃。人们依然在探寻量子克隆的方方面面，例如更高维度的量子克隆 [12]、各种物理系统中的量子克隆的实现等等。

目前人们在量子信息学中的种种研究，其实都是在为建造一台通用的量子计算机而作出贡献。近几十年量子信息这一领域一直是人们目光的焦点，我们应该相信，在不懈的努力之下，我们的理论与技术一定会日臻成熟，我们也一定能够一步一步接近并最终实现我们的目标，使得我们的科技水平上升到一个新的高度。

$$\hat{a}_X^\dagger |Y\rangle$$

$$\hat{a}_Y^\dagger |X\rangle$$

参考文献

[1] W. K. Wootters and W. H. Zurek, Nature 299, 802(1982).

[2] https://en.wikipedia.org/wiki/Quantum_state#Mixed_states

[3] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa and B. Schumacher, Phys. Rev. Lett. 76, 2818(1996).

[4] A. K. Pati and S. L. Braunstein, Nature 404, 164(2000).

[5] V. Buzek and M. Hillery, Phys. Rev. A 54, 1844 (1996).

[6] N. Gisin and S. Massar, Phys. Rev. Lett. 79, 2153 (1997).

[7] D. Bruss and A. Ekert, Phys. Rev. Lett. 81, 2598-2601(1998).

[8] Lu-Ming Duan and Guang-Can Guo, Phys. Lett. A 243,261-264(1998).

[9] D. Bruss and M. Cinchetti, Phys. Lett. A 62:012302(2000).

[10] N. J. Cerf, Phys. Rev. Lett. 84, 4497-4500(2000).

[11] H. K. Cummins, C. Jones and A. Furze, Phys. Rev. Lett. 88:187901(2002).

[12] F. Bouchard and R. Fickler, Sci. Adv. 3: e1601915(2017)

[13] https://en.wikipedia.org/wiki/No-cloning_theorem