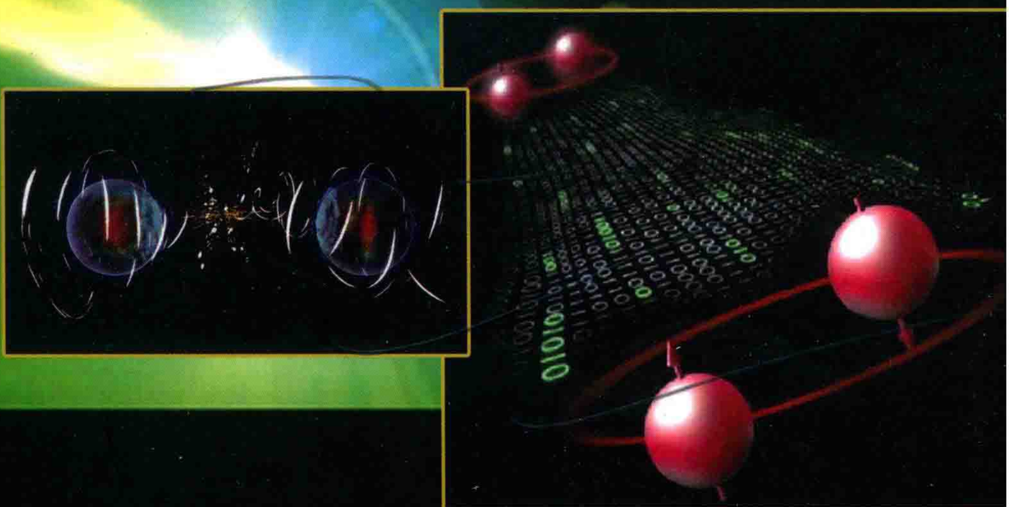
量子信息的多角度解析

Liangzi Xinxi de Duojiaodu Jiexi

许 丽◎著



中国农业大学出版社
China Agricultural University Press

量子信息的多角度解析

许 丽 著

中国农业大学出版社
·北京·

内容简介

本书对量子信息技术各个热点研究分支的发展进行了介绍，涉及量子密码、量子通信、量子计算、量子模拟、量子度量学等各个领域。此外，也讨论了腔量子电动力学和金刚石 NV 色心系统在量子信息技术中的应用和发展。本书的特色是对量子信息技术做一个总体性的介绍，在阐述各个学科方向的历史以及国际发展动态的同时，展现中国近年来量子信息科学技术发展的概貌，提炼了近年来中国量子信息科学技术在国际上取得的成就。

本书内容深入浅出，层次分明，参考文献丰富，适合具有物理学、信息科学、数学等不同学科背景的读者阅读参考，了解量子信息技术的相关知识。

图书在版编目(CIP)数据

量子信息的多角度解析/许丽著．—北京：中国农业大学出版社，2018.5

ISBN 978-7-5655-2040-2

Ⅰ.①量…　Ⅱ.①许…　Ⅲ.①量子力学-信息技术　Ⅳ.①O413.1

中国版本图书馆 CIP 数据核字(2018)第 113439 号

书　　名　量子信息的多角度解析

作　　者　许　丽　著

策划编辑　赵　中　李卫峰　　　**责任编辑**　韩元凤

封面设计　郑　川

出版发行　中国农业大学出版社

社　　址　北京市海淀区圆明园西路 2 号　　　**邮政编码**　100193

电　　话　发行部 010-62818525，8625　　　读者服务部 010-62732336

　　　　　　编辑部 010-62732617，2618　　　出　版　部 010-62733440

网　　址　http：// www.caupress.cn　　　**E-mail** cbsszs @ cau.edu.cn

经　　销　新华书店

印　　刷　北京时代华都印刷有限公司

版　　次　2018 年 10 月第 1 版　　2018 年 10 月第 1 次印刷

规　　格　787×1 092　　16 开本　　18.5 印张　　340 千字

定　　价　58.00 元

前　言

量子信息科学，以量子计算研究为开篇，以量子力学规律来改造经典信息的表征，向人们展示出一幅奇妙的未来信息技术的图景。经过近 30 年的发展，人们调控微观世界的能力获得了显著的提高。这一领域在理论和技术方面获得突飞猛进发展的同时，依然展示着勃勃的生机。虽然迄今为止，人们距离制造出一台可实用化的、超越当前经典计算极限的量子计算机的目标依然遥远，有若干瓶颈技术仍需克服，但毋庸置疑的是，人们调控微观世界的能力获得了显著的提高：量子密码技术已经接近实用化；长程量子通信的原理性验证也不存在原则上的障碍；量子模拟技术快速发展，已经接近经典计算机可以模拟的极限；量子计量学也获得了快速的发展。这些都酝酿并孕育着崭新的量子信息时代。而尤为可喜的是，中国的研究人员在这一领域已经跟上了世界的步伐，成为量子信息世界版图中一股不可或缺的力量。

本书的主要目的是对量子信息技术做一个总体性的介绍，在阐述各个学科方向的历史以及国际发展动态的同时，展现中国近年来量子信息科学技术发展的概貌，提炼了近年来中国量子信息科学技术在国际上取得的成就。本书主要对量子信息技术各个热点研究分支的发展进行了介绍，涉及量子密码、量子通信、量子计算、量子模拟、量子度量学等各个领域。此外，也讨论了腔量子电动力学和金刚石 NV 色心系统在量子信息技术中的应用和发展。

第 1 章量子信息基础，主要介绍了量子信息的数学基础和量子力学基础，介绍了量子纠缠相关概念、密度算符与约化密度矩阵、常见的量子操作和常见的量子技术。

第 2 章量子密码学，详述了量子密码相关技术的理论研究状况，包括量子密钥分配、量子认证、量子签名、量子秘密共享和量子加解密等方面的进展，介绍了量子保密通信系统和量子密码分析技术的相关理论。

第 3 章量子通信，介绍量子安全直接通信和量子机密共享以及其中涉及的几个重要原理、方案。

第 4 章量子计算，简要介绍了量子计算发展史、基本概念，并对几个主要实验体系进行简单的介绍，还介绍了几个重要的量子计算模式。

第 5 章量子模拟，介绍了量子模拟的具体定义、分类以及物理系统和具体应用。其中量子模拟可能的物理系统介绍了冷原子系统、微腔系统、离子阱系统和核磁共振系统。

第 6 章量子度量学，就是使用量子系统或利用量子力学特性来进行参数估计的过程。本章主要介绍了量子度量学概况、量子 Fisher 信息、Cramér-Rao 不等式和 Mach-Zehnder 干涉仪。

第 7 章量子克隆，是量子信息学的一个重要分支。本章主要介绍了量子克隆、纯态量子克隆和混合态量子克隆。

第 8 章两个常用的物理系统，主要介绍了腔量子电动力学和金刚石 NV 色心这两个常用的物理系统。分别介绍了腔量子电动力学和 Jaynes-Cummings 模型，以及腔量子电动力学实验系统；而金刚石 NV 色心中则介绍了金刚石 NV 色心的研究历史、性质与制备、研究进展和能级理论研究。

量子信息学涉及经典信息论、计算机科学和量子物理学等诸多方面，其中还用到了数学知识，涉及面甚广，再加上该领域发展非常迅速，使本书不能将所有论题都深度展开，请大家谅解。

参考文献列出书中引用的大部分文献，同时向由于疏漏而未被引用的作者表示歉意。

山西工程技术学院为本书的出版和相关研究工作提供了资金支持。

特别强调的是，量子信息技术尚未成熟，且是一个发展迅速的领域，要概括出它的全貌，对于作者来说实在是一件十分困难的任务，加之作者水平有限，不妥之处在所难免，殷切期待给予批评指正。

许　丽

2017 年 8 月

目　录

第1章 量子信息基础

量子信息从物理本质来讲，是利用了量子力学中的一些特殊的原理来完成经典信息无法完成的事情。因而，对量子信息的理解，首先需要对一些量子力学的基本原理和一些特殊的量子特性和量子效应有一个大体的了解。当然，量子信息是一个不断发展的交叉学科，在自身的发展过程中，也会不断地涌现出一些新的量子技术。本章主要介绍在量子信息中常用的部分量子力学原理和量子门；也将介绍部分量子技术，譬如量子离物传态(quantum teleportation)、量子纠缠转移(quantum entanglement swapping)、量子密集编码(quantum dense coding)等。

1.1 预备知识

1.1.1 数学基础

1. 向量空间与希尔伯特空间

微观粒子的运动是在一定的时空中进行的，为了更好地描述和分析其运动状态，需要在向量空间内研究量子力学问题。而线性代数是研究向量空间和线性算子的，因而线性代数是研究量子力学的重要基础。通常，在由 n 元复数构成的向量空间内研究量子力学问题。

在数学领域，希尔伯特空间是欧几里得空间的推广，不再局限于有限维的情形，即希尔伯特空间是无穷维的欧几里得空间。在量子力学中经常使用希尔伯特空间，而在量子计算与量子信息中遇到的有限维复向量空间类中，希尔伯特空间和内积空间是完全相同的，无穷维希尔伯特空间需要在内积空间基础上附加一些限制条件，在此不考虑这种情况。

2. 狄拉克符号

量子力学中的一个量子态可以用希尔伯特空间中的一个矢量来标记，而力学量对应线性厄米算符。也就是说，量子态这个物理概念用数学中的矢量描述，而力学量这个物理概念用数学中的一个算符描述。狄拉克首先使用符号“$|\rangle$”来标记量子态，称为右矢。

3. 内积、外积、张量积

(1)内积

内积是向量空间上的二元复函数，两个向量$|v\rangle$和$|w\rangle$的内积在量子力学中的标准符号写成$\langle v|w\rangle$，符号$\langle v|$表示向量$|v\rangle$的对偶向量。将带有内积的向量空间称为内积空间。

若$|v\rangle=[x_1,\cdots,x_n]^{\mathrm{T}}$，$|w\rangle=[y_1,\cdots,y_n]^{\mathrm{T}}$，则$\langle v|w\rangle$表示$C^n$中的一个内积，即$\langle v|w\rangle=[x_1,\cdots,x_n][y_1,\cdots,y_n]^{\mathrm{T}}$。

如果向量$|v\rangle$和$|w\rangle$的内积为0，则称它们正交。向量$|v\rangle$的范数定义为$\||v\rangle\|=\sqrt{\langle v|v\rangle}$。如果$\||v\rangle\|=1$，则称$|v\rangle$为归一化的；任意非零向量除以其范数，则称为向量的归一化。不难看出，两个向量内积的结果应该是一个数。

(2)外积

两个向量$|v\rangle$和$|w\rangle$的外积在量子力学中的标准符号写成$|v\rangle\langle w|$，表示C^n中的一个外积，即$|v\rangle\langle w|=[x_1,\cdots,x_n]^{\mathrm{T}}[y_1,\cdots,y_n]$。

不难看出，两个向量$|v\rangle$和$|w\rangle$的外积$|v\rangle\langle w|$是内积定义$\langle v|w\rangle$中左矢变为右矢、右矢变为左矢的结果，因此，两个向量外积的结果应该是一个算符。设为$|i\rangle$向量空间C^n的任意标准正交基，对任意向量$|v\rangle$可写为$|v\rangle=\sum\limits_i v_i|i\rangle$。式中，$v_i$是一组复数(为基本状态$|i\rangle$的概率幅)，取$|i\rangle=\big[\overbrace{0,\cdots,0}^{i-1个0},1,\overbrace{0,\cdots,0}^{n-i个0}\big]^{\mathrm{T}}$，$|v\rangle=[v_1,\cdots,v_i,\cdots,v_n]^{\mathrm{T}}$，由内积定义可得$\langle i|v\rangle=v_i$，于是$\left(\sum\limits_i|i\rangle\langle i|\right)|v\rangle=\sum\limits_i|i\rangle\langle i|v\rangle=\sum\limits_i v_i|i\rangle=|v\rangle$，而$\sum\limits_i|i\rangle\langle i|=I$，称为向量空间$C^n$的标准正交基的完备性关系，由该完备关系可以把任意算子表示成外积形式。

(3)张量积

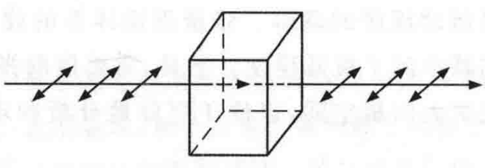
为了用数学方法描述微观粒子在一定时空中的运动规律，必须建立空间坐标系。描述同一运动规律的方程在不同坐标系中的形式不同，这种形式上的差

异严重阻碍了人们对运动规律的理解。张量理论体系的建立，把坐标系对描述运动方程形式的影响减小到了最低程度。于是，需要借助张量积的方法，将向量空间结合在一起构成更大向量空间，以便于更好地分析和理解量子力学多粒子系统。

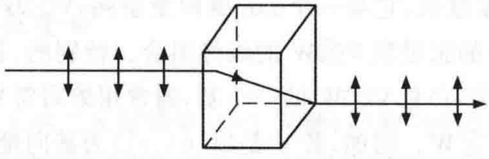
设 V 和 W 分别是 m 和 n 维的向量空间，并假设 V 和 W 是希尔伯特空间，称 $V\otimes W$ 是 V 和 W 的张量积，它是一个 mn 维向量空间，$V\otimes W$ 的元素是 V 的元素 $|v\rangle$ 和 W 的元素 $|w\rangle$ 的张量积 $V\otimes W$ 的线性组合。特别的，若 $|i\rangle$ 和 $|j\rangle$ 是 V 和 W 的标准正交基，则 $|i\rangle\otimes|j\rangle$ 是 $V\otimes W$ 的一个基，通常用缩写符号 $|v\rangle|w\rangle$、$|v,w\rangle$ 或 $|vw\rangle$ 来表示张量积 $V\otimes W$。例如，若 V 是以 $|0\rangle$、$|1\rangle$ 为基向量的二维向量空间，则 $|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle$ 是张量积 $V\otimes W$ 的一个元素。

1.1.2　测量基

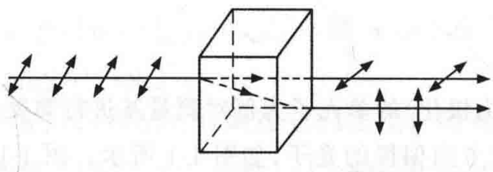
以偏振（或称之为极化）的单光子为例对测量基进行简要的说明。假设用方解石来区分水平与垂直方向偏振的光子，如图 1-1 所示。图 1-1(a)表示沿水平方向偏振的光子垂直方解石表面入射通过方解石后传播方向不变；图 1-1(b)表示沿垂直方向偏振的光子垂直方解石表面入射通过方解石后传播方向发生偏转，即出射光子相对于入射光子在传播方向上发生一定的向下平移；图 1-1(c)表示斜向 45°方向偏振的光子垂直方解石表面入射通过方解石后，光子的传播方向可能发生偏转，也可能不发生偏转，二者的发生概率各占 50%。由于图 1-1 所示放置的方解石对于水平和垂直偏振方向的光子通过后方向是否发生偏转是完全确定的，即水平偏振不偏转，垂直偏振发生偏转，将这样的测量装置称为水平垂直测量基，简称为水平垂直基，用符号$\oplus$标识。如果把方解石沿光子水平偏振方向和传播方向组成的平面旋转 45°，这样的装置称之为 45°与 135°基，用符号$\otimes$标识，如图 1-2 所示。用$\otimes$基去测量 45°或 135°方向偏振的光子可以得到一个完全确定的结果，即 45°方向偏振的光子通过后不发生偏转，135°方向偏振的光子通过后发生偏转。用$\oplus$基去测量 45°或 135°方向偏振的光子，以及用$\otimes$基去测量水平或垂直方向偏振的光子均无法事先得到确定的结果，即是否偏转是完全随机的。在量子通信中，通常用测量基来标识一个力学量，譬如对于电子的自旋，可以将$\oplus$和$\otimes$分别对应电子沿 z 与 x 方向的自旋 σ_z 与 σ_x。从量子力学的角度上看，测量基就是将要对量子系统进行测量的某一个物理量。



(a)水平偏振的光子直接通过方解石晶体



(b)垂直偏振的光子通过方解石晶体后要发生偏转



(c)斜偏振(45°)的光子通过方解石晶体后可能发生偏转,也可能不发生偏转

图 1-1　不同偏振方向的光子通过方解石得到不同结果示意图

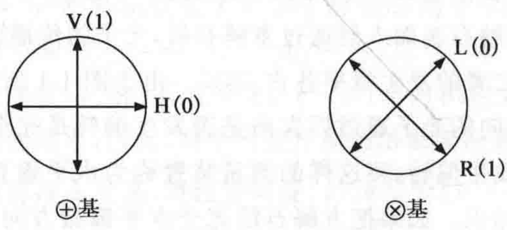


图 1-2　不同的测量基及其编码

1.1.3　量子比特

比特(bit)是经典计算和经典信息的基本概念,量子计算与量子信息建立在类似的概念——量子比特[1](quantum bit 或 qubit)的基础上。就像经典比特有一个状态:0 或 1,量子比特也有一个状态:|0⟩或|1⟩。符号"|⟩"称为狄拉克符号,在量子力学中表示状态。

1.1.4　多量子比特

对于两个经典比特而言，共有四种可能状态：00，01，10，11。相应的，一个双量子比特有四个基态，记作$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$。一对量子比特也可以处于这四个基态的叠加，因而双量子比特的量子状态包含相应基态的复系数，称为幅度（概率幅 amplitude）。描述双量子比特的状态向量为：

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{1-1}$$

类似于单量子比特情形，测量结果 x（$=00,01,10$ 或 11）出现的概率是$|\alpha_x|^2$，测量后，量子比特处于$|x\rangle$状态。概率之和为 1，归一化条件可表示为：

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1 \tag{1-2}$$

其中$\{0,1\}^2$ 表示长度为 2，每个字母从 0 和 1 中任取的字符串的集合。对于一个双量子比特系统，只测量其中一个量子比特，例如，单独测量第一个量子比特，得到 0 的概率为$|\alpha_{00}|^2+|\alpha_{01}|^2$，而测量后的状态为：

$$|\Psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}} \tag{1-3}$$

注意，测后状态被因子$\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}$重新归一化后，仍满足归一化条件。

考虑 n 量子比特系统。这个系统的基态形如：$|x_1x_2x_3\cdots x_n\rangle$，并且量子状态由 2^n 个幅度所确定。$n=500$ 时，这数就已超过了整个宇宙原子的估算总数，在传统计算机上存储所有这些复数是不可想象的。量子力学具有超越经典系统的信息处理能力。

1.2　量子信息的量子力学基础

量子信息以量子力学为基础，是量子力学与信息科学相结合的交叉学科，因此在介绍量子信息前有必要简要地介绍一些量子力学的基本原理。

1.2.1　量子力学的基本假设

量子力学是研究微观粒子系统运动变化规律的理论。它是一门相当成熟的学

科,它的全部内容可以从少数几个基本原理出发,用逻辑推理的方法推演出来。可以将这些原理大体上归纳为五个基本假设[2]:

①微观量子系统的物理状态可以用 Hilbert 空间的一个态矢量$|\Psi(t)\rangle$来描述。

②微观量子系统的每一个力学量对应 Hilbert 空间中的一个线性厄米算符,力学量的取值是相应算符的本征值。

③微观系统的状态$|\Psi(t)\rangle$随时间演化的动力学方程为 schrödinger 方程:

$$i\hbar\frac{\partial}{\partial t}\Psi(t)=\hat{H}\Psi(t) \tag{1-4}$$

式中$\hat{H}=H(\hat{X},P,t)$是系统的哈密顿算符。

④测量与塌缩:假定力学量算符A的本征值为a_1和a_2,对应的本征态分别为ϕ_1和ϕ_2;如果微观体系处于A算符的两本征态ϕ_1和ϕ_2的叠加态$\Psi=c_1\phi_1+c_2\phi_2$,那么对微观体系的力学量A进行测量,将以$|c_1|^2$的概率获得结果a_1,以$|c_2|^2$的概率获得结果a_2;测量后,体系的量子态塌缩到测量所得本征值对应的本征态。

⑤描写全同粒子系统的态矢量,对于任意一对粒子的交换,是对称的或反对称的;服从前者的粒子称为玻色子,服从后者的粒子称为费米子。

1.2.2 量子态叠加原理

量子信息中使用的量子态与经典信息中使用的经典物理态有一些不同的地方。可以说,经典物理态是量子态的一个子集,是量子态的一类特例。对经典物理态的测量,其结果通常是确定的;而对量子态的测量并不一定是完全确定的,即可能是某一些测量结果的概率分布。这是因为量子态可以是测量算符的一些本征态的叠加[2]。

从逻辑上讲,态叠加原理可以由量子力学的第一条基本假设推演出来,因此通常人们并不把它作为量子力学的基本假设。态叠加原理[2]的内容为:如果$|\Psi_1\rangle$,$|\Psi_2\rangle$,$|\Psi_3\rangle$,…,$|\Psi_n\rangle$是量子系统的可能的态,那么它们的任意线性叠加态:

$$|\Psi\rangle=\sum_i c_i\ |\Psi_i\rangle,(i=1,2,\cdots,n) \tag{1-5}$$

也是系统的一个可能的态。

量子力学中的态叠加原理在量子信息中有着广泛的应用,也给量子信息赋予了与经典信息截然不同的丰富内容。当然,这也体现了量子力学中的态叠加原理与经典物理中的叠加原理的不同:两个相同的态的叠加在经典物理中代表一个新

的态，但在量子物理中仅表示同一个态；经典物理中的叠加是概率的叠加，而量子物理中的叠加是概率幅的叠加。

1.2.3 测不准原理与非克隆定理

根据量子力学的基本假设，微观体系的一个力学量用一个线性厄米算符表示。处于某一给定状态 $\Psi(t)$ 的量子系统，其各力学量并不总是取确定值[2]。例如力学量 A，假设其本征值为 a_i，对应的本征态为 $|a_i\rangle$，

$$A|a_i\rangle = a_i|a_i\rangle \tag{1-6}$$

则在 $|\Psi(t)\rangle$ 态下对力学量 A 进行测量得到取值 a_i 的概率是 $|\langle a_i|\Psi(t)\rangle|^2$。

定义力学量 A 在态 $\Psi(t)$ 中的平均值 $\overline{A}$：

$$\overline{A} = \langle\Psi(t)|A|\Psi(t)\rangle \tag{1-7}$$

力学量 A 在态 $\Psi(t)$ 中的不确定度定义为 ΔA，满足[2]

$$\begin{aligned}
(\Delta A)^2 &= \overline{(a_i - \overline{A})^2} \\
&= \sum_i \langle\Psi(t) \mid (a_i - \overline{A})^2 \mid a_i\rangle\langle a_i \mid \Psi(t)\rangle \\
&= \sum_i \langle\Psi(t) \mid [(a_i^2 - 2a_i\overline{A} + (\overline{A})^2] \mid a_i\rangle\langle a_i \mid \Psi(t)\rangle \\
&= \langle\Psi(t) \mid [A^2 - (\overline{A})^2] \mid \Psi(t)\rangle \\
&= \overline{A^2 - (\overline{A})^2}
\end{aligned} \tag{1-8}$$

定义力学量算符 A 与 B 的对易子 $[A,B]= AB-BA$，则力学量 A 和 B 在同一量子态 $\Psi(t)$ 下的不确定度关系为：

$$\Delta A\Delta B \geqslant \frac{1}{2}\overline{|[A,B]|} \tag{1-9}$$

这就是测不准原理，或测不准关系。

非克隆定理[3]可以看作是测不准原理的一个推论。非克隆定理的内容为：一个未知的量子态不能被完全拷贝。事实上，正是因为未知的量子态可能来自不对易算符的本征态，而由某一个确定的算符去测量量子系统，可能会导致不完备的测量，从而得不到量子态的全部信息。

当然，根据 Hilbert 空间是一个线性空间的特点，不难证明非克隆定理，用反证法证明如下。

假设存在一个克隆机，它能克隆任意一个量子态。用一个幺正算符 U_c 来表

示它，即

$$U_c(|\Psi\rangle|0\rangle)=|\Psi\rangle|\Psi\rangle$$

对于$|\Psi\rangle=|0\rangle$，有$U_c(|0\rangle|0\rangle)=|0\rangle|0\rangle$；对于$|\Psi\rangle=|1\rangle$，有$U_c(|1\rangle|0\rangle)=|1\rangle|1\rangle$；对于叠加态$|\Psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$：

一方面，根据克隆机的克隆效果有

$$\begin{aligned}U_c\left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle\right]&=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)-\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\\&=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle+|01\rangle+|10\rangle)\end{aligned}\tag{1-10}$$

另一方面，根据 Hilbert 空间的线性性质，有

$$\begin{aligned}U_c\left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle\right]&=\frac{1}{\sqrt{2}}[U_c(|0\rangle|0\rangle)+U_c(|1\rangle|1\rangle)]\\&=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\end{aligned}\tag{1-11}$$

显然，式(1-10)与式(1-11)是不相等的。由此可见，假设是错误的，即不存在克隆机U_c能克隆一个未知的态。

测不准原理和非克隆定理在量子信息，特别是量子通信中起着很重要的作用，将在以后的章节中提及。

1.2.4 量子态的演化与幺正算符

根据量子力学假设，孤立量子系统态矢量随时间演化的动力学方程为 schrödinger 方程：$i\hbar\frac{\partial}{\partial t}\Psi(t)=\hat{H}\Psi(t)$，同时，在量子力学中，孤立系统态矢量$|\Psi(t)\rangle$随时间的演化还可以通过演化算符$U(t,t_0)$来描述[2]。

$$|\Psi(t)\rangle=U(t,t_0)|\Psi(t_0)\rangle\tag{1-12}$$

将态矢量$|\Psi(t)\rangle$代入 schrödinger 方程，可以得到演化算符$U(t,t_0)$满足的微分方程：

$$i\hbar\frac{\partial}{\partial t}U(t,t_0)=\hat{H}U(t,t_0)\tag{1-13}$$