

LIANGZI SUANFA
YU BIANCHENG RUMEN

量子算法与编程入门

主 编 傅 鹏 向 宏 向 涛

非
外
借



重庆大学出版社

内容简介

LIANGZI SUANFA YU BIANCHENG RUMEN

量子算法与编程入门

主编 傅 鹏 向 宏 向 涛



重庆大学出版社

内容提要

量子计算与传统计算在概念上有着巨大差异,理解较困难。本书阐述了量子算法与编程,按照通用量子计算所需的知识线索,循序渐进,环环相扣,扫除了理解障碍。量子系统的刻画和相关数学基础都是以这种需求逻辑进行安排的。解析的几种量子算法具有问题和算法的双重清晰性,算法分析则揭示了算法的奥秘。量子编程部分详细介绍了量子编程语言和一些已出现的实验平台,并展示了算法的编程实现。

本书既可用于量子算法与编程的教学,也可用于量子计算自学的引导。

图书在版编目(CIP)数据

量子算法与编程入门/傅鹏,向宏,向涛主编. --

重庆:重庆大学出版社,2018.5

新工科系列.软件工程类教材

ISBN 978-7-5689-1076-7

I. ①量… II. ①傅…②向…③向… III. ①程序设计—高等学校—教材 IV. ①TP311.1

中国版本图书馆 CIP 数据核字(2018)第 099971 号

量子算法与编程入门

主编 傅 鹏 向 宏 向 涛

策划编辑:何 梅 范 琪

责任编辑:李定群 版式设计:何 梅 范 琪

责任校对:关德强 责任印制:张 策

*

重庆大学出版社出版发行

出版人:易树平

社址:重庆市沙坪坝区大学城西路 21 号

邮编:401331

电话:(023) 88617190 88617185(中小学)

传真:(023) 88617186 88617166

网址:<http://www.cqup.com.cn>

邮箱:fxk@cqup.com.cn (营销中心)

全国新华书店经销

重庆市正前方彩色印刷有限公司印刷

*

开本:787mm×1092mm 1/16 印张:11.25 字数:168 千

2018 年 5 月第 1 版 2018 年 5 月第 1 次印刷

印数:1—2 000

ISBN 978-7-5689-1076-7 定价:48.00 元

本书如有印刷、装订等质量问题,本社负责调换
版权所有,请勿擅自翻印和用本书
制作各类出版物及配套用书,违者必究

前言

量子世界有着十分奇异的现象，与人们的直觉相去甚远。例如，量子叠加，薛定谔猫处于既是死的又是活的状态，尽管这只是一个思想实验，仍让人们不能接受其中直指的量子状态叠加概念。其实，量子态的叠加本身毫不奇怪，简言之，波函数所满足的薛定谔方程是线性的，函数空间是向量空间，进而在典则内积下成为希尔伯特空间，量子态可由特征态的线性组合表达，这就是叠加的源头。超越单纯的量子叠加，令人称奇的是波函数坍缩，就是系统虽然可处于多态叠加，但只要一测量，立即就坍缩到仅是一个特征态，且还不是确定地坍缩到某个特征态，而是按照概率分布行事。这意味着两点：一是系统的状态从某种意义上讲永远无法知晓；二是相同叠加态的每次测量结果都可能完全不同。又如，量子纠缠，若说纠缠只不过是两个东西密切地关联着，这不奇特；若进一步说两个关联着的东西即便被分开到天各一方还是有关联，这也不奇怪，就像被分开的一双鞋，仍因本是一双鞋而有关联。但是，量子纠缠是讲，如两个纠缠的粒子，无论分开多远，即便各处银河系的两端，不仅还有关联，而且一旦测量一个粒子坍缩到一个特征态，就能立即确定地预知银河系另一端那个尚未测量的粒子态的测量结果，就好像是完全无需时间的信息传输。尽管人们也用一双鞋来打比方解释量子纠缠，但为什么会纠缠成如此状况就不是一件清楚的事情了。因此，连爱因斯坦也不信，即便他作为量子纠缠的发现者，也从未信服，称之为鬼魅的超距作用。

这就决定了量子理论确实更难懂，也决定了量子计算与传统计算必有概念上的鸿沟。因此，本书虽是一本入门书，但需要读者尽可能已经扫除了量子领域最基本的知识障碍，包括量子力学和量子计算中最具原生性的一些概念。换言之，书中并非从头讲述一切，那样反而分散了本应集中于量子算法和编程上的力量。因此，书中按照此种要求进行安排，在适当的层面上找到若干逻辑起点，使得逻辑链条脉络清晰，建立利于学习的系统，使步步

向前的推进得以流畅。

即便是一本小书，也是在多方的默契与支持下才会顺利地面世。衷心感谢各方以各种方式给予的有效配合与帮助。特别要提到的包括信息物理社会可信服务计算教育部重点实验室的张鑫、何湘、张亚妮等，他们不仅在实验素材和相关事务等方面提供了充分、直接的协助，而且在为尽可能减少工作环境的硬软干扰方面默默地做了大量事情，这些都是本书能够以所需效率完成和出版的不可忽视的原因。

由于知识在任何时候的无法穷尽，作者在任何阶段的认知局限，即便是一本小书，也难免存在笔误、瑕疵、疏漏，甚至可能有未及时发现之差错和谬误，恳请读者指正。

编者

2017年12月

目 录

第 1 章 相关基础	1
1.1 量子系统的理解	1
1.1.1 量子系统的抽象描述	2
1.1.2 可观测量及其与状态的关系	4
1.1.3 量子状态演化与量子计算	7
1.1.4 复合量子系统的状态	9
1.2 有限维复希尔伯特空间	10
1.2.1 n -维复坐标空间	10
1.2.2 n -维复希尔伯特空间	12
1.2.3 狄拉克符号	17
1.3 线性变换与变换矩阵	19
1.3.1 一般线性映射	19
1.3.2 线性算子	21
1.3.3 酉算子和酉矩阵	22
1.3.4 其他特殊算子和矩阵	25
1.4 克罗内克积与张量积	28
1.4.1 克罗内尔积	29
1.4.2 张量积	31
1.4.3 状态简写与基态编码	35
第 2 章 量子算法	40
2.1 量子计算概要	40
2.1.1 量子门	41
2.1.2 量子线路及通用量子门	43

2.1.3	量子门常用结果	46
2.2	量子算法和量子黑箱的实现	48
2.2.1	计算问题与布尔函数	49
2.2.2	布尔函数的实现	52
2.2.3	量子黑箱实现示例	56
2.3	Deutsch 算法解析	60
2.3.1	问题与算法描述	61
2.3.2	实现的讨论与简单示例	63
2.3.3	算法分析	64
2.4	Deutsch-Jozsa 算法解析	67
2.4.1	问题与算法描述	67
2.4.2	实现的讨论与简单示例	69
2.4.3	算法分析	71
2.5	Grover 算法解析	77
2.5.1	问题与算法描述	77
2.5.2	实现的讨论与简单示例	79
2.5.3	算法分析	85
第 3 章	量子编程	98
3.1	量子编程概述	99
3.1.1	两个引例	99
3.1.2	量子编程的概念	101
3.1.3	数据叠加与程序叠加	103
3.2	量子编程语言	106
3.2.1	量子线路图	107
3.2.2	量子汇编语言	108
3.2.3	高级量子编程语言	111

3.3 量子计算实验平台	119
3.3.1 IBM Quantum Experience	120
3.3.2 LIQui ⟩	126
3.3.3 ProjectQ	133
3.3.4 其他平台简介	138
第 4 章 量子算法的编程实现	143
4.1 Deutsch 算法	143
4.1.1 IBM Quantum Experience	144
4.1.2 LIQui ⟩	146
4.1.3 ProjectQ	147
4.2 Deutsch-Jozsa 算法	150
4.2.1 IBM Quantum Experience	150
4.2.2 LIQui ⟩	152
4.2.3 ProjectQ	155
4.3 Grover 算法	157
4.3.1 IBM Quantum Experience	158
4.3.2 LIQui ⟩	160
4.3.3 ProjectQ	161
附 录	165
附录 A 命题 2.2 的证明	165
附录 B 部分练习提示	167
参考文献	169

第 1 章 相关基础

如果是为了理解量子计算机——确切地说，本书仅限于通用量子计算机，忽略仍然可能是非常重要的专用量子计算机——那么，看待量子系统的角度、层面和重心，必定与研究量子力学本身有所不同。结果是，为了更好地理解量子计算、量子算法和编程，更应该站在抽象的层面看问题，而不能过分陷入细枝末节。这样，最需要的基础是什么，应该以怎样的步骤去深入，就会变得更加鲜明起来。

1.1 量子系统的理解

量子系统的行为是量子计算的物理基础。在传统电子计算机领域，算法设计者和软件开发对电子计算机硬件的基本原理有足够的了解是应该的，不然就会只知其然而不知其所以然，终究会在不同程度上影响专业效率和水准。因此，在量子计算领域，同样应该适当了解由量子力学描述的量子现象，在物理层面上掌握所需的那些基本原理。

但仅仅停留在这个层面还不够。在某种意义上，应该反过来强调，更重要的是从抽象的层面去把握事物的本质，而不是过分陷入烦琐的枝节。例如，当今电子计算机在物理层面的核心原理，与晶体管的特性密切相关，由此构造各种逻辑器件。然而对算法和软件设计者而言，在对物理细节有了所需的了解之后，应该尽快上升到抽象模型的认识层次。以三态逻辑门为例，它有代表 1 的高电平、代表 0 的低电平和高阻态 3 种状态，其本质是可由控制端的信号是 1 还是 0 来控制线路处于接通和断开状态。这本质上就是

一个逻辑控制开关，接通时可传送 0 或 1 信号，断开时就隔离了信号传递。到了这一层，就不必去操心到底电压多少伏是高电平，多少伏是低电平；不必去操心到底每单位电压的电流低到多少微安才是高阻态。

在量子计算领域也是如此。通用量子计算机虽然是植根于具有纷繁细节的量子物理规律，但在了解了所需最基本的量子特性之后，也应该尽快上升到抽象化的本质层面。正如传统的三态逻辑门抽象模型是一个那么明确的抽象，只有到了那样的抽象层面，意思反而才会变得更加明白。

1.1.1 量子系统的抽象描述

从何开始？就从波恩 (Born, 1926)、狄拉克 (Dirac, 1930) 和冯·诺依曼 (von Neumann, 1932) 等先驱的奠基性成果开始。下面讨论量子系统可以如何抽象地刻画。

要刻画任何一个动态系统，首先要明确系统状态及其演化规律；而状态可能是不便于直接观测的，就像一个人的内心世界；然后要明确系统的可观测量是（些）什么，它（们）是如何关联到状态的，就像一个人的外在行为。

在量子力学里，状态并不是直接由具体的物理量组成的，如粒子的位置、速度、动量、角动量、能量及时间等，这些物理量并不直接构成量子系统的状态；准确地说，量子系统状态是某些物理量的函数，包括时间；而系统的一个可观测量则是一个状态的函数，这是因为状态不便直接观测，只能观测某些状态的函数来获得状态信息——这等于说一个可观测量就是一个状态的函数。这有一点抽象了，但还不够；为理解量子计算，起码要超越物理量这个层面，只聚焦以下 3 点：

①量子系统每一时刻处于一个状态。

②系统的状态不便于直接观测，只能通过某些可观测量（为状态的函数）来获得其信息。

③系统的状态从这一刻到下一刻有特定的演化规律。

这里已经没有提到任何一种具体的物理量，而系统的状态则成为核心。

为了让这种抽象明确化，现来看看抽象描述量子系统的狄拉克-冯·诺依曼公理集 (Dirac, 1930; von Neumann, 1932)，下面是其大致内容。

设 H 是可数维复希尔伯特空间。

①量子系统的状态是 H 中的单位向量 $|\psi\rangle$ ，它乘以任一相位因子 $e^{i\theta}$ 仍是同一状态，即 $e^{i\theta}|\psi\rangle$ 与 $|\psi\rangle$ 是同一个状态。

②量子系统的每个可观测量 A 是 H 上的自伴算子，该算子可以是无界的。

③量子系统的一个可观测量 A 在状态 $|\psi\rangle$ 下的期望值等于 $|\psi\rangle$ 与 $A|\psi\rangle$ 的内积，即 $\langle|\psi\rangle, A|\psi\rangle\rangle = \langle\psi|A|\psi\rangle$ 。

先粗略地解释一下这套公理。

首先，可数维复希尔伯特空间就是量子系统的状态空间，也就是说，系统的状态作为该空间的向量就在那个空间里变化。可数维太广泛了，实际意义下的量子计算，有限维就够了，而且更方便。复希尔伯特空间就是复数域上的希尔伯特空间，这是量子力学所需；实数域是不够的，而其他域连保证内积的正定性都困难，完备性也成问题。有限维加上复数域的完备性，已经能保证整个内积空间的完备性，自然就是希尔伯特空间。因此，有限维复希尔伯特空间才是我们刚好需要的。

接下来的第一条，状态为单位向量是归一化条件要求，因为所有可能的测量结果的概率之和必为1；但总相位因子并无任何可区分的物理意义，故在特别包括量子计算在内的有关分析中，总是可以忽略的。

第二条，系统的一个可观测量本质上是状态的一个函数，而在复希尔伯特空间这个线性空间里，这样一个函数就是一个线性算子。复希尔伯特空间中的一个线性算子 A ，通过由内积关系表现的线性函数关系，唯一地对应着一个线性算子 A^* ，称为 A 的伴随算子；当恰好 A 的伴随算子等于自己时，它就是自伴算子。作为可观测量的自伴算子，允许是无界的。但当仅限于已够用的有限维复希尔伯特空间时，任何线性算子都是有界的。此时，自伴算子则变得非常明确，就是一个埃尔米特矩阵，即其共轭转置等于自身的矩阵。

第三条，暗示了一个可观测量是随机量；又因它是状态的函数，其实是反映了量子系统的状态是随机量这个本源。明确地说，给定一个可观测量 A ，对于同一个状态 $|\psi\rangle$ ，每次通过 A 观测 $|\psi\rangle$ 都可能会（按某种概率分布）得到不同的值，而观测结果的期望值为 $\langle\psi|A|\psi\rangle$ 。

在公理化的鼻祖欧几里得那里，公理作为推理的起点，是不证自明的。后来，不证自明并不作为公理的必要属性，因为把系统归结为若干推理起点才是本，不必在无法兼顾的情况下强求不证自明性，所以现代的公理并不一定是显然的，量子力学的公理也是或更是如此。但无论如何，上述 3 条公理是量子力学先驱们为我们奠定的坚实基础。当然，要继续为理解量子计算、量子算法扫清障碍，还需要更多、更细的知识。例如，这套公理中没有细化可观测量与状态的具体关系，没有直接提到量子状态的演化规律，更没有量子计算所需的复合系统构成法则，等等。这是本节的后续小节要解决的问题，让我们沿着抽象化的路子，依据波恩定则、狄拉克-冯·诺依曼公理提供的线索，针对量子计算、量子算法和编程的需求范围，对量子系统的抽象数学框架给出明确化的描述和阐释 (Hall, 2013)。

下面设某个量子系统的状态空间 H 是一个复希尔伯特空间，并且只要需要，可默认它是一个有限维复希尔伯特空间，而不一定每次都特地去声明这一点。

1.1.2 可观测量及其与状态的关系

量子叠加原理表明若干量子态的线性组合仍是量子态。反过来说，一个量子态 $|\psi\rangle$ 也可表示为若干量子态 $|\psi_i\rangle$ 的叠加，具体就是

$$|\psi\rangle = \sum_i c_i |\psi_i\rangle,$$

此式可称为量子态叠加表达式，或简称量子态叠加式。不过，最为重要的不是这个一般的叠加式，而是当 $\{|\psi_i\rangle\}$ 为状态空间 H 的规范正交基的情况。这就与量子系统的可观测量密切相关了。

一个量子系统，其状态在每个时刻只有一个 $|\psi\rangle \in H$ ，但其可观测量可以有多个，每一个都是状态 $|\psi\rangle$ 的一个函数。具体地，就是 $A: H \rightarrow H$ 这样一个线性算子，并且它是一个自伴算子，即 $A = A^*$ 。在有限维空间的情况下，自伴算子对应的变换矩阵为埃尔米特矩阵 $A = A^\dagger$ 。这样一个自伴算子 A 的特征值和特征向量（也称**特征态**）具有很好的性质：它的特征值都是实数，更重要的是它必存在一组正交的单位特征向量，构成 H 的一组**规范正交基**。

下面考虑这样一个可观测量 A 。设状态空间 H 的维数为 N 。

首先, A 的特征值 $\{\lambda_0, \lambda_1, \dots, \lambda_{N-1}\}$ 均为实数, 允许重根——单位矩阵就是明显例子; A 必有一组对应的正交的单位特征向量 $\{|a_0\rangle, |a_1\rangle, \dots, |a_{N-1}\rangle\}$, 构成 H 的一组规范正交基, 因此, 对 $i, j = 0, 1, \dots, N-1$, 有:

$$A|a_i\rangle = \lambda_i|a_i\rangle;$$

$$\langle a_i|a_j\rangle = \delta_{ij} = \begin{cases} 1 & \text{若 } i = j \\ 0 & \text{若 } i \neq j \end{cases}.$$

其中, δ_{ij} 为克罗内克函数, 会经常用到。

在量子计算中, 这里的规范正交基向量 $|a_i\rangle$ 又称**计算基态**(Nielsen et al, 2010)。如语境中清楚时, 可简称**基态**。有了这样一组规范正交基之后, 一切将会变得明朗起来。在这组基下, 系统的状态可表示为基态的叠加:

$$|\psi\rangle = \sum_{i=0}^{N-1} c_i|a_i\rangle.$$

这个表达式可称为 $|\psi\rangle$ 的**基态叠加式**。其中, 幅值 c_i 还可以具体地由 A 和 $|\psi\rangle$ 给出:

$$\begin{aligned} \langle a_i|\psi\rangle &= \sum_{j=0}^{N-1} \langle a_i|c_j|a_j\rangle \\ &= \sum_{j=0}^{N-1} c_j \langle a_i|a_j\rangle = \sum_{j=0}^{N-1} c_j \delta_{ij} = c_i. \end{aligned}$$

故有时也将基态叠加式直接写为

$$|\psi\rangle = \sum_{i=0}^{N-1} \langle a_i|\psi\rangle|a_i\rangle.$$

可见, 一个观测量 A 以规范正交基的形式为被观测的系统状态提供了一个观测框架, 一个“坐标系”。现在以此坐标系为基准, “观测”一下系统的状态 $|\psi\rangle$, 具体就是看看状态的这个函数 $|\phi\rangle = A|\psi\rangle$ 在这个坐标系下是什么样子:

$$\begin{aligned} |\phi\rangle &= A|\psi\rangle \\ &= \sum_{i=0}^{N-1} c_i A|a_i\rangle \end{aligned}$$

$$= \sum_{i=0}^{N-1} c_i \lambda_i |a_i\rangle。$$

到了这里，往下会发生什么呢？量子系统的本性是，真正物理上的测量，其结果将为：系统状态 $|\psi\rangle$ 随机坍缩到 A 的一个特征向量，即基态 $|a_i\rangle$ ，同时得到对应的某个物理量（不妨就以 ϕ 记之）的测量值，这个值就是 $|a_i\rangle$ 对应的特征值 λ_i ；而得到 $|a_i\rangle$ 和 λ_i 的概率由 $c_i = \langle a_i|\psi\rangle$ 决定，具体就是：

$$\Pr(|\psi\rangle = |a_i\rangle) = \Pr(\phi = \lambda_i) = |c_i|^2 = |\langle a_i|\psi\rangle|^2 \quad (i = 0, 1, \dots, N-1)。$$

这里物理量 ϕ 的测量值是一个具体的实数，代表具体的物理量（如位置、动量等）的测量结果。注意， A 的特征值都是实数。

这就是波恩定则。这个定则清晰地表明了系统状态 $|\psi\rangle$ 和物理量 ϕ 的随机性，并且在给定可观测量 A 提供的坐标系之下，具有确定的概率分布：

$ \psi\rangle:$	$ a_0\rangle$	$ a_1\rangle$	\dots	$ a_{N-1}\rangle$
$\phi:$	λ_0	λ_1	\dots	λ_{N-1}
Pr:	$ c_0 ^2$	$ c_1 ^2$	\dots	$ c_{N-1} ^2$

其中

$$\langle \psi|\psi\rangle = \sum_{i=0}^{N-1} |c_i|^2 = 1$$

为概率分布自然需要满足的归一化要求，这也解释了为什么系统状态必须是单位向量。

有了这个明确的概率分布之后，物理量 ϕ 这个随机量的期望值 $E\phi$ 就可以求得。由于

$$A|\psi\rangle = \sum_{i=0}^{N-1} c_i \lambda_i |a_i\rangle，$$

所以

$$\begin{aligned} \langle \psi|A|\psi\rangle &= \sum_{i=0}^{N-1} |c_i|^2 \lambda_i \\ &= \sum_{i=0}^{N-1} \Pr(\phi = \lambda_i) \lambda_i = E\phi。 \end{aligned}$$

这正是狄拉克-冯·诺依曼公理集中的第三条。

现在总结要点如下：

① 系统状态 $|\psi\rangle$ 这个随机量的值域是可观测量 A 的特征向量集 $\{|a_0\rangle, |a_1\rangle, \dots, |a_{N-1}\rangle\}$ ，这也是状态空间的规范正交基；而物理量 ϕ 这个随机量的值域是对应的 A 的特征值集 $\{\lambda_0, \lambda_1, \dots, \lambda_{N-1}\}$ 。

② 这两个随机量的分布相同，都具有同样的概率质量 $\{|c_0|^2, |c_1|^2, \dots, |c_{N-1}|^2\}$ 。

③ 对系统进行测量就是对此概率分布进行一次随机试验。试验结果就是系统状态 $|\psi\rangle$ 必为样本空间 $\{|a_0\rangle, |a_1\rangle, \dots, |a_{N-1}\rangle\}$ 的元素之一，而物理量 ϕ 是样本空间 $\{\lambda_0, \lambda_1, \dots, \lambda_{N-1}\}$ 的元素之一。测量之后，系统状态坍缩到某个基态，并无再次测量先前状态的机会，除非重新制备，这一点与一般随机变量可立即重复试验有所不同。

④ 量子系统的一个可观测量，其根本作用是为系统测量提供了一个规范正交基作为“坐标系”，使得测量结果，尽管是随机的，但有了一个明确的概率分布。换一个可观测量，就是换一个“坐标系”，虽然概率分布不同了，但彼此是等价的，不改变量子系统及其测量的本质。

⑤ 至此，就抽象地理解量子计算的这个需求而言，反倒可以忘掉可观测量，同时也忘掉具体的物理量，只需聚焦量子系统的状态本身，心中清楚状态空间具有规范正交基，状态可在该基下明确表示出来；一旦测量，状态就按照确定的概率分布坍缩到一个基态。

1.1.3 量子状态演化与量子计算

现在聚焦量子系统的状态本身。设系统的状态空间为 N -维复希尔伯特空间 H ，系统的状态为 $|\psi\rangle \in H$ ，可不管可观测量具体是什么，总之有一组规范正交基 $\{|x\rangle \mid x = 0, 1, \dots, N-1\}$ 。注意，这里开始采用了更简洁的记法，后面将专门讲述。状态的基态叠加式为

$$|\psi\rangle = \sum_{x=0}^{N-1} c_x |x\rangle。$$

其中, $|\psi\rangle$ 是满足归一化条件的单位向量。既然 $|\psi\rangle$ 是单位向量, 则对任意相位因子 $e^{i\theta}$, 称为总相位因子, $e^{i\theta}|\psi\rangle$ 也是单位向量, 表示同一个状态。与总相位因子不同, 一个状态叠加式, 如

$$\sum_k e^{i\theta_k} |\psi_k\rangle$$

内部的相位因子 $e^{i\theta_k}$, 如果无法提到求和式之外, 则称为相对相位因子。总相位因子总是可以忽略的, 因为代表的是同一状态; 而相对相位因子则是不可忽略的, 因为一个状态如果改变了其相对相位因子, 就成了不同的状态。例如, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 与 $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 就是两个不同的状态。

量子系统的状态演化规律是什么? 答案是, 状态演化是由酉算子确定的。酉算子就是不改变内积的算子, 即一个酉算子 U 满足, 对任意的 $|\psi\rangle, |\phi\rangle$

$$\langle U|\psi\rangle, U|\phi\rangle \rangle = \langle |\psi\rangle, |\phi\rangle \rangle。$$

酉算子对应的变换矩阵是酉矩阵, 即满足 $U^\dagger U = I$ 的矩阵。因此, 系统的状态演化就是一系列酉算子 U_k 的作用:

$$|\psi_{k+1}\rangle = U_k |\psi_k\rangle。$$

量子计算的实质, 就是量子系统状态的演化过程, 也就是一系列的酉变换。量子算法的设计就是精心构造这些酉算子, 使得称为量子寄存器的量子系统, 其状态一步步演化, 最终达到需要的状态。而所谓需要的状态, 粗略地说, 就是对应正确输出的基态, 其概率幅决定的概率要充分大; 换言之, 就是使得系统状态一旦测量, 将以充分大的概率坍缩到对应正确输出的基态。这也意味着, 量子计算是概率性的而非确定性的, 除了十分特殊的情况外。

这显示了量子计算与传统计算、量子算法与传统算法的根本差异。传统计算中, 算法的形态与它所解决的计算问题不会相差太远; 而量子计算中, 一切计算问题的算法都必须由一系列酉算子体现, 因此, 量子算法与它所解决的计算问题可能显得相去甚远。这就是为什么要找到一个有价值的量子算法, 其难度也比传统算法更大。同时, 量子计算普遍的概率性, 也使之与

传统计算的差异更突出。

酉算子在量子计算中具有根本的作用。正因为如此，酉算子和酉矩阵必将在后续多个小节中予以详述。

1.1.4 复合量子系统的状态

通用量子计算机必定是由系列标准部件构成的。它由一些简单的标准部件，构成复杂的计算系统。因此，我们关心若干量子系统构成一个更大的量子系统是什么情形。具体而言，在量子计算中，一个 n -量子比特系统是由 n 个单量子比特系统构成的复合系统。量子比特也译量子位元，简称量子位。但是，量子比特与传统计算领域的比特截然不同。

一个传统比特就代表一个值域为 $\{0,1\}$ 的布尔变量，而一个量子比特则是2-维复希尔伯特空间中的向量，它代表一个双态量子系统的状态。双态量子系统就是只有两个特征态的量子系统，这两个特征态构成其状态空间的规范正交基，两个基向量即基态，通常记为 $|0\rangle$ 和 $|1\rangle$ 。因此，单个量子比特的状态可表示为两个基态的叠加。其一般形式为

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad (|c_0|^2 + |c_1|^2 = 1).$$

这是最简单的量子系统。有比它更简单的吗，如“单态量子系统”，其状态为 $|\psi\rangle = c_0|0\rangle$ ($|c_0|^2 = 1$)，即 $|\psi\rangle = e^{i\theta}|0\rangle$ ？这样的系统，每次测量必然都以概率 $|e^{i\theta}|^2 \equiv 1$ 坍缩到唯一可能的状态 $|0\rangle$ ，完全没有量子态的随机性，也就是完全没有任何“量子性”，它根本就是一个经典系统。不存在这样的“单态量子系统”。

因此，通用量子计算机可由若干最简的单量子比特系统复合而成。由 n 个单量子比特构成一个大小为 n 的量子比特系统，可称为 n -量子比特或量子位寄存器。现在需要回答的是，一个 n -量子位寄存器的状态表达式是怎样的，它的状态空间是怎样的？

答案是张量积。任何复合量子系统的状态是其构成系统的张量积，复合系统的状态空间是其构成系统状态空间的张量积。由若干量子位构成量子寄存器也是如此。