1

叠加态、纠缠和可逆性

1.1. 前言

什么是量子计算机？[1] 回答这个问题涵盖了量子力学（Quantum mechanics，QM）、量子信息理论（Quantum Information Theory，QIT）和计算机科学（Computer Science，CS）。

现今的计算机，不论是理论上的图灵机如图1.1，还是实际上的个人电脑、高性能计算机、笔记本电脑、平板电脑、智能手机等，都是基于经典物理学的。它们受到地域性的限制（操作只有局部影响），并受到经典物理学[1]实际的限制，即“**系统在任何时刻只能处于一个状态**”。

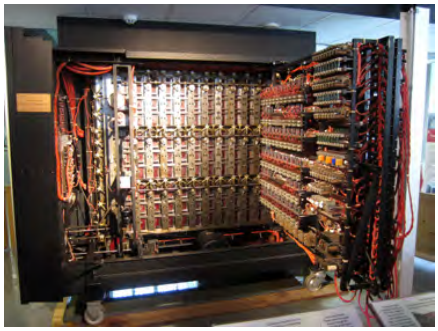


图 1.1: 在 Bletchley Park 的早期图灵机。Bletchley Park 是英国政府机构，位于英格兰中部的 Buckinghamshire 郡。该机构成立于第二次世界大战期间，旨在破译德国和其它敌方国家的加密通信。在战争期间，Bletchley Park 聚集了一批英国最聪明的数学家、工程师、语言学家和密码学家，他们的任务是破解德国的加密通信，为盟军提供重要情报支持。在 Bletchley Park，使用了各种技术手段，包括电子机械装置、密码机和语言学分析等，以破译加密通信。该机构最为著名的成就之一是破解 Enigma 密码系统，这是纳粹德国用于保护军事通信的一种机械密码机，使用了一系列复杂的密码方法。通过对 Enigma 密码系统的破解，Bletchley Park 帮助盟军获取了大量的战略情报，对于战争的胜利进程起到了重要作用。Bletchley Park 的历史是英国在二战期间的一个重要组成部分，同时也为现代密码学、计算机科学和信息技术的发展做出了贡献。目前，Bletchley Park 已成为一个开放的博物馆和教育中心，向公众展示和解释这段历史，并向人们展示这个时期的科技成就和创新精神。图片由 Douglas Hoyt 拍摄：https://www.flickr.com/photos/douglashoyt/8235850748/

[1] 经典物理学是指在相对论和量子力学出现之前，对物理现象进行研究的传统物理学分支。经典物理学主要涉及物理学中最基本的领域，包括力学、电学、热学、光学和声学等。经典物理学的研究对象通常是宏观物体和宏观现象，其中最为著名的经典物理学理论包括牛顿力学、电磁学马克思韦尔方程、热力学第一、二定律和光的波动理论等。尽管经典物理学被相对论和量子力学所替代，但它仍然是物理学中重要的基础和入门学科，也是许多实际应用的基础。

然而，现代量子物理告诉我们，世界的运行方式可能大不相同。量子系统认为可以处于多个不同状态的“超位置”，其演化过程中会表现出干涉效应。另外，空间上分离的量子系统之间可能会发生纠缠，操作可能会因此具有“非局部”效应[2]。

量子计算是研究基于量子力学原理的计算机的计算能力和其他特性的领域。它结合了 20 世纪最重要的两个科学领域：**量子力学**[3]和**计算机科学**[4]。探索量子力学的一个重要的目标是寻找比解决同样问题的任何经典算法快得多的量子计算方法或者量子计算范式。

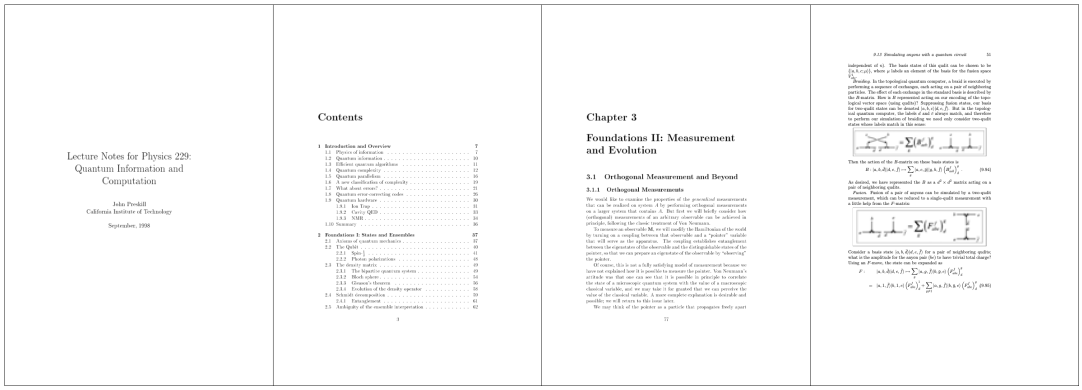


图 1.2: 《Lecture notes for physics 229: Quantum information and computation》图1.1。这是一篇关于量子信息和计算的讲义的文献引用，作者为 John Preskill，发表于 1998 年，发表在《加州理工学院》期刊上。该文献记录了作者在加州理工学院教授的物理学 229 课程的讲义。这门课程介绍了量子信息和计算的基本概念，包括量子比特、量子纠缠、量子电路、量子算法等内容，并讨论了量子计算的应用前景。这门课程对后来量子计算和量子信息领域的发展产生了重要影响，被认为是这一领域的经典教材之一。该文献可以被视为介绍量子计算和量子信息领域的重要文献之一，对这一领域的初学者和研究者都有很大的参考价值。感兴趣的同学可以问赵老师索要改讲义 xifizhao@gmail.com。

量子计算始于 20 世纪 80 年代初，由**尤里 · 伊万诺维奇 · 马宁**[5] [3, 4]、**理查德 · 费曼**[6] [5, 6] 和

[2]“非局部”效应是指在某个系统中，两个或多个空间上分离的部分之间存在相互作用或联系，这种联系是通过超距离传递信息或作用而发生的。这种联系并不依赖于空间上的距离，而是通过某种非局部的方式进行传递。

在物理学中，“非局部”效应的概念经常出现在量子力学中，例如量子纠缠效应。量子纠缠是指当两个或多个量子系统处于纠缠状态时，它们之间的相互作用是非局部的，即它们之间的相互作用并不受到它们之间距离的影响。这意味着当一个量子系统发生测量时，它可能会影响与之纠缠的另一个量子系统，即使它们之间的距离非常远，这种现象被称为“非局部”效应。非局部效应在量子信息学和量子计算等领域有重要应用。

[3]由普朗克、爱因斯坦、玻尔、海森堡、薛定谔等人于 1900 年至 1925 年间发展

[4]其诞生可以追溯到图灵 1936 年的论文 [2]

[5]尤里 · 伊万诺维奇 · 马宁（Yuri Ivanovich Manin）是一位著名的数学家，生于 1937 年，是苏联和俄罗斯的国家科学院院士，也是美国国家科学院外籍院士。他是数学领域中的重要人物，对代数几何、数论、数学物理等领域作出了卓越的贡献，他也是现代数学的一些基本概念和理论的奠基人之一。

马宁在代数几何和数论领域的研究成就非常突出，他对于椭圆曲线、数域、代数簇、模形式、保型形式等领域都做出了杰出的贡献，他也在数学物理领域中的工作取得了重要成果。马宁获得了多项国际数学奖项，包括 1982 年的菲尔兹奖和 1993 年的沃尔夫数学奖等。此外，他还是国际数学界著名杂志《数学年刊》（Annals of Mathematics）的编辑之一。

[6]理查德 · 费曼（Richard Feynman）是一位著名的美国理论物理学家，生于 1918 年，逝世于 1988 年。他是 20 世纪最具影响力的物理学家之一，同时也是一位杰出的教育家、科学普及者和散文家。费曼在量子电动力学和粒子物理学的研究方面作出了重要贡献，并因此获得了 1965 年的诺贝尔物理学奖。

费曼的贡献涉及许多领域，包括量子电动力学、强相互作用、拓扑物理学、计算机科学等。他发明了一种著名的计算方法，称为费曼图，这种图形方法能够清晰地表示物理过程，为理解粒子物理学提供了强有力的工具。此外，他也在物理学教育领域作出了杰出的贡献，他的讲授风格幽默诙谐、生动活泼，深受学生和同行们的喜爱。他的讲义和书籍，如《费曼物理学讲义》等，在物理学教育中被广泛使用。

保罗·贝尼奥夫[7] [7] 提出了模拟量子计算机的建议。在 1985 年，**大卫·迪奥克**[8]定义了通用量子图灵机 [8]，将其应用扩展到数字领域。加州理工学院量子信息研究所主任**约翰·普雷斯基尔** (John Preskill) 教授的教材讲义《Lecture notes for physics 229: Quantum information and computation》[9, 10] 中有更多关于量子计算机早期历史的介绍，有兴趣的同学可以去阅读。再接下来的几年中，**大卫·迪奥克**和**理查德·约瑟夫**[9] [11]、**丹尼尔·西蒙** [12] 首先提出的量子算法以及由**伊桑·伯恩斯坦**和**乌梅什·瓦齐拉尼** [13] 发展出的量子复杂性理论。然而，在 1994 年**彼得·肖尔**非常意外地发现了整数因子分解和离散对数问题的有效量子算法——肖尔算法（关于这段历史，有一段非常不错的彼得 · 肖尔本人采访的视频以及根据此段视频制作的动画片，感兴趣的同学可以联系赵老师组织观看）[14]，肖尔算法是建立在 Simon 的工作之上，他的意义在于由于我们现在的大多数经典密码学是基于这两个问题的计算难度来保证的，因此实际构建和使用量子计算机将使我们能够破解大多数当前的经典密码系统，尤其是基于 RSA 系统 [15, 16] 。当然，**查尔斯·贝内特**和**吉尔·布拉萨** [17] 提出的量子密码学形式即使对于量子计算机也是不可破解的。以下是探索量子计算的三个原因，包括了解决实际问题和哲学层面上的：

- 使现有的经典计算机已经很强大和廉价的微型化过程（摩尔定律）已经达到了量子效应要发生的微观水平。
- 利用量子效应可以极大地加速某些计算（有时呈指数级），甚至使某些经典计算机无法实现的事情成为可能。本课程的主要目的是详细解释量子计算编程（算法、密码学等）的这些优点。
- 最后，可以说理论计算机科学的主要目标是“研究自然界允许我们使用的最强大的计算设备的能力和限制”。由于我们对自然的当前理解是量子力学的，理论计算机科学应该研究量子计算机的能力，而不是经典计算机的能力。

在开始这门课程之前，让我们问一个实践方面的问题：建造量子计算机需要什么条件？此时此刻，还为时过早？第一台小型 2 比特量子计算机是在 1997 年建造的，2001 年一台 5 比特量子计算机被用来成功因式分解“15”[18]。此后，对不同技术路线的实验进展稳步但依旧缓慢。目前最先

[7] 保罗 · 贝尼奥夫（Paul Benioff）是一位美国计算机科学家和量子物理学家，生于 1934 年，逝世于 2021 年。他是计算机科学中量子计算理论的先驱之一，并且是最早研究量子计算机的科学家之一。

在 20 世纪 80 年代初，贝尼奥夫就开始研究量子计算机的理论，并在 1982 年提出了著名的“量子图灵机”（quantum Turing machine）概念，为后来的量子计算机研究提供了基础。他也是第一批认识到量子计算机在某些领域将优于传统计算机的人之一，并且他的工作启发了后来量子计算领域的发展。

此外，贝尼奥夫还在物理学中作出了重要贡献，他是最早将量子力学与信息理论相结合的科学家之一，他的研究在量子信息理论、量子算法和量子物理学的交叉领域有广泛应用。他还是一位出色的教育家，在科学教育和科学普及方面也做出了贡献。

[8] **大卫 · 迪奥克**（David Deutsch）是一位英国物理学家和量子计算机科学家，生于 1953 年。他是量子计算理论的先驱之一，也是量子信息科学的奠基人之一。

迪奥克在 20 世纪 80 年代初开始研究量子计算理论，提出了著名的“量子图灵机”（quantum Turing machine）模型，并在 1985 年提出了量子并行性的概念，这些成果对后来量子计算机的发展产生了深远的影响。此外，他还提出了量子误差纠正的概念，这在保护量子信息方面起到了重要作用。

迪奥克还在物理学中作出了贡献，尤其是在量子力学的基本问题和哲学方面。他提出了“多世界诠释”（Many-worlds interpretation）的量子力学解释，认为量子力学中的不确定性并不是真正的随机，而是来自于各种可能性的同时发生。他的工作在哲学、科学和文化领域都产生了广泛的影响。

迪奥克获得了多项国际奖项，包括 2002 年的欧洲物理学会量子电子学奖和 2010 年的英国皇家学会皇家奖章等。他还是多本著作的作者，其中包括《量子计算机和量子通信》（Quantum Computation and Quantum Communication）等经典著作。

[9] 理查德 · 约瑟夫（Richard Jozsa）是一位英国数学家和计算机科学家，生于 1957 年。他是量子计算和量子信息领域的重要人物之一，同时也是量子算法领域的奠基人之一。

Jozsa 在 20 世纪 90 年代提出了著名的 Jozsa 算法，该算法可以判断任意的黑盒量子函数是否为恒等函数或者平衡函数，是量子计算领域中最早的重要算法之一。此外，他还提出了其他一些著名的量子算法，如 Grover 搜索算法的一种变体，以及求解线性方程组的量子算法等。

Jozsa 也是量子信息理论领域的重要研究者，他的研究工作涉及量子信息压缩、量子纠错等领域，并发展了许多经典信息理论的量子版本。他还曾获得过多个重要奖项，包括 2005 年的欧洲物理学会量子电子学奖和 2007 年的英国皇家学会皇家奖章等。

进的实现方式使用超导量子比特和离子阱量子比特。在撰写本文的时候，据英国《新科学家》周刊网站 11 月 9 日报道，国际商用机器公司（IBM）已经制造出迄今为止最大的量子计算机。这台名为“鱼鹰”（Osprey）的计算机包含 433 个量子比特，是该公司此前打破纪录的 127 个量子比特计算机的 3 倍多，是谷歌公司包含 53 个量子比特的“西克莫”计算机[10]的 8 倍多。

图 1.3: IBM Osprey 芯片组的示意图。IBM Osprey 是一种用于构建量子计算机的芯片组，是 IBM 量子计算机的核心部件之一。这个芯片组包括多个量子位和多个控制电路，用于在量子计算机中执行量子门操作，从而实现量子算法的运行。图片来源：IBM 官网 www.ibm.com

在理论上，一个 433 量子比特的处理器可以处理 2^{433} 的复数希尔伯特空间，远远超出任何经典系统。但是在量子计算过程中，处理器内部的大量数据（被称为“状态向量”）需要使用单量子位门和双量子位门进行处理。大多数量子算法都需要至少运行同样大量的门循环，这导致门数量远大于算法深度。错误在量子计算中也会迅速增加，因此需要错误纠正和错误缓解技术。

以 99% 的双量子比特错误率为例（没有错误缓解），使用具有 422 个双量子比特门的算法时，您有 1.28% 的机会获得良好的结果。而在 99.9% 的错误率下，这个数字将会下降到 65%。这表明错误率的高低对于量子计算的结果至关重要。因此，需要开发出更加可靠的量子硬件和量子错误纠正技术来提高量子计算的准确性和可靠性。

物理实现量子计算机所面临的实际问题似乎十分严峻。噪声[11]和退相干问题[12]在理论上在一定

[10]” 西克莫” 是指 Google Quantum AI 实验室在 2019 年推出的一款量子计算机处理器，该处理器包含了 53 个超导量子比特。这是谷歌目前推出的量子计算机处理器中最大的一个，也是在公共领域中可用的最大量子计算机之一。

” 西克莫” 处理器的目标是实现量子优势，即通过利用量子计算的优势解决经典计算难以处理的问题。与传统的二进制计算机不同，量子计算机使用量子比特作为基本计算单元，可以在同一时间处理多个计算，从而具有处理大规模数据的能力。这种能力使得量子计算机在解决一些特定问题时具有优势，如优化、模拟和密码学等领域。

” 西克莫” 处理器的推出标志着谷歌在量子计算领域取得了重大进展，并成为了该领域的领军者之一。

[11]在量子计算中，噪声问题是一个非常严重的挑战。由于量子计算机中的量子比特是非常脆弱的，很容易受到周围环境的影响，例如温度、电磁干扰和量子比特之间的相互作用等。这些环境因素会导致量子比特产生误差和失真，从而对量子计算机的准确性和可靠性产生影响，这就是量子计算机的噪声问题。

在实际的量子计算机中，错误的来源是多种多样的。例如，有些量子比特可能会因为与环境的相互作用而失去相干性；有些量子比特可能会因为与其他量子比特的相互作用而发生失真；还有些量子比特可能会因为随机性引起的噪声而产生错误。

噪声问题不仅会影响量子计算机的运行速度，还会对算法的正确性和可靠性产生严重影响。为了解决这个问题，需要采用各种技术来对量子比特进行纠错和缓解。其中一些技术包括量子错误纠正（Quantum Error Correction，QEC）、量子优化和量子模拟等。这些技术可以帮助我们提高量子计算机的准确性和可靠性，并进一步推动量子计算的发展

[12]在量子计算中，” 相干性”（Coherence）是指一个量子比特能够保持在一个明确定义的状态（例如，$|0\rangle$ 或 $|1\rangle$ 或它们的叠加态 $|\rangle$ 的时间长度。量子计算中的” 退相干”（Decoherence）问题是指量子比特在和环境相互作用时，失去它的相干性和纠缠状态，导致量子计算的错误和失效。

在量子计算中，相干性是实现量子算法所必需的，因为它允许量子比特之间的纠缠和相互作用。相干性的丢失是由于量子比特与它周围的环境（如热噪声、振动、磁场等）相互作用而引起的。这种相互作用会导致量子比特的相位和振幅失真，从而使得量子比特不能维持其原有的纠缠状态，而是演化成经典态。

退相干问题对于量子计算的实现非常关键，因为它限制了量子计算机的规模和精度。如果不能有效地控制和抑制退相干，量子计算机就不能够进行准确和可靠的计算。因此，为了解决退相干问题，研究者们采用了多种技术，如使用量子错误纠正码来保护量子比特，使用量

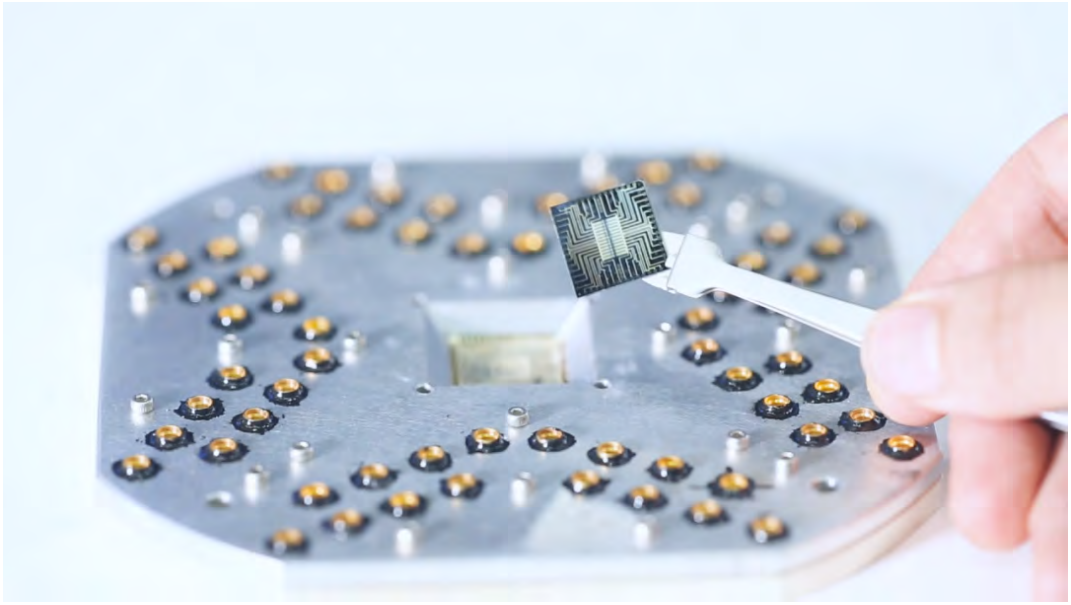


图 1.4: 本源超导 24 比特量子芯片。图片来源：https://www.guancha.cn/

程度上已经被量子纠错码和容错计算的发现所解决，但这些问题在实践中并没有被完全解决。另一方面，科学家认识到，物理实现量子计算机的领域仍处于起步阶段，而经典计算机也曾面临和解决过许多艰巨的技术问题，有趣的是，这些在经典计算机发展中遇到的问题甚至与现在量子计算机面临的问题相同（例如，噪声抑制和纠错）。另外，尽管实现完整量子计算机面临的困难似乎令人望而却步，但涉及量子通信的更有限的应用已经在一定程度上取得了成功，例如通过纠缠和经典通信发送量子比特的传送（teleportation），以及 BB84 量子密钥分发的一些版本现在甚至已经商业化。

即使量子计算的理论永远不会实现为现在像手机、笔记本电脑一样真正的大规模物理计算设备，量子计算机仍然是一个极为有趣的想法，将在计算之外产生一系列成果。

- 在物理学方面，它可能会改善我们对量子力学的理解。关于纠缠和哈密顿复杂度的新兴理论已经在某种程度上做到了这一点。
- 在计算机科学方面，量子计算理论扩展和丰富了经典复杂性理论，可能有助于解决其中的一些问题虽然实现完整的量子计算机面临的实际问题似乎十分艰巨。

总结：说量子计算是涉及最广泛的大学学科可能有些夸张，但它确实跨足了许多学科领域。量子计算的研究和应用在诸多领域中都发挥着重要作用，这使得量子计算成为了一个高度跨学科的领域。以下是一些量子计算涉及的主要学科：

- **物理学**：量子计算的基础建立在量子力学之上，这是现代物理学的一个重要分支。量子计算机的设计、构建和实现都需要对量子力学和相关物理概念有深入的理解。
- **计算机科学**：量子计算机使用量子比特（qubits）作为基本信息单位，与传统计算机使用的比特（bits）不同。因此，量子计算需要独特的算法和计算方法，这使得计算机科学家在量子计算领域具有关键作用。

子纠缠和量子纠错技术来控制量子比特的相干性和纠缠状态，以及使用低温和高真空等环境条件来减少退相干的影响。

- **数学**：量子计算依赖于复杂数学理论，包括线性代数、概率论、离散数学等。研究量子算法需要深入了解这些数学领域。
- **材料科学与工程**：量子计算机的制造需要研究和开发新型量子材料以及相关技术。材料科学家和工程师在这方面发挥着重要作用。
- **电子工程**：量子计算机的硬件设计、微电子制造和量子比特控制等方面需要电子工程的专业知识。
- **化学**：量子化学是一个研究化学现象的理论框架，量子计算在量子化学模拟和分子结构预测方面具有潜在优势。
- **生物学**：量子计算在生物学中的应用包括基因组学数据处理、蛋白质折叠模拟以及药物设计等。
- **信息论与密码学**：量子计算机具有处理复杂数学问题的潜力，这使得它在信息论和密码学领域具有巨大价值。量子密码学已经成为信息安全领域的一个重要分支。

因此，虽然称量子计算涉及最广泛的大学学科可能夸大其词，但它的确是一个高度跨学科的领域，吸引了来自各种背景的研究人员。

1.1.1. 量子力学

量子力学是研究原子、分子、原子核以及基本粒子等微观粒子行为和相互作用的物理学分支。它是 20 世纪初诞生的一种革命性的理论，为我们理解和描述自然界微观现象提供了一个全新的框架。

与经典物理学相比，量子力学在描述原子尺度的微观粒子时具有明显的优势。在经典物理学中，物体的位置和动量可以被同时精确测量，物体遵循牛顿运动定律。然而，对于原子尺度的微观粒子，这种描述已经不再适用。量子力学揭示了在微观尺度下，物体的行为表现出波粒二象性，即它们既具有波动性，又具有粒子性。

量子力学的主要特点包括：

- **波函数**（Wave Function）：在量子力学中，波函数是描述量子系统的一种数学工具。

  它是一个复数函数，可以用来预测量子系统的物理性质和行为。波函数通常用希腊字母 ψ 表示，它的形式可以是一维、二维或三维的，具体取决于所描述的物理系统的性质和结构。

  波函数包含了关于量子系统的全部信息，包括位置、动量、自旋和能量等性质。在量子力学中，波函数的演化是由薛定谔方程来描述的，它可以预测波函数随时间的演化以及系统的能量本征态和本征值。

  波函数的模平方值代表了找到一个粒子在某一特定位置的概率。例如，对于一个单独的电子，它的波函数可以用来预测电子在空间中的分布，而它的模平方值则表示了在一个特定位置找到这个电子的概率。

  最后，波函数是描述量子系统的基本数学工具，在量子力学中发挥着至关重要的作用。通过使用波函数，可以预测量子系统的各种物理性质和行为，并且波函数的作用也在实验中得到了广泛的验证。
- **测量与坍缩**：总的来说，在测量之前，微观粒子处于一种概率性的状态（即量子叠加态）。在进行测量后，波函数会坍缩成一个确定的状态。

具体讲就是，在量子力学中，测量是指通过某种方式来获取一个量子系统的信息。测量的结果是一个经典的物理量，例如位置、动量或能量，它通常以一个确定的数值表示。然而，在量子力学中，测量并不总是产生确定的结果，而是具有一定的概率性。具体地说，测量的结果是由波函数的性质和测量过程中的随机性决定的。

在量子力学中，测量会导致波函数的坍缩，即波函数的一部分会消失，而其余部分会转化为一个确定的状态。例如，对于一个处于叠加态的量子比特，进行测量会导致它处于两个状态中的一个，而另一个状态将被消除。在这个过程中，波函数的坍缩是不可逆的，而且是由测量过程本身所决定的。

测量与波函数的坍缩是量子力学中的两个基本概念。它们是量子力学理论中的核心，也是解释量子世界的重要基础。它们的存在说明了量子世界与经典世界的巨大差异，而且在现代科技中也有广泛应用。

- **测不准原理**（Heisenberg's Uncertainty Principle）：由维尔纳 · 卡尔 · 海森堡[13]在 1927 年提出，表明某些物理量（如位置和动量）不能同时被精确测量。这一原理揭示了量子世界的根本不确定性，是量子力学中的一个基本原理，测不准原理揭示了在量子尺度下，某些物理量对的测量存在着根本性的限制。

  根据测不准原理，对于一个量子系统，例如一个微观粒子，我们不能同时精确测量某一对互补物理量，如位置（x）和动量（p）。换句话说，当我们试图更精确地测量一个物理量（如位置）时，与之相关的另一个物理量（如动量）的不确定性将增加。这种限制并非是由测量工具的不精确性导致的，而是量子系统本身固有的性质。

  数学上，测不准原理可以表示为：

$$\Delta x \cdot \Delta p \geq \frac{\overline{h}}{2} \tag{1.1}$$

  其中，Δx 表示位置的不确定性，Δp 表示动量的不确定性，$\overline{h}$ 表示约化普朗克常数（即普朗克常数除以 2π）。这个表达式说明了，位置和动量的不确定性乘积的最小值受到约化普朗克常数的限制。

  测不准原理对量子力学的发展产生了深远影响，强调了在微观世界中，概率和不确定性是根本性的特征。这与经典物理学中的决定性观念形成了鲜明对比。测不准原理的发现对量子力学的基础和应用产生了重大影响，如量子计算、量子通信和量子加密等领域。

- **量子纠缠** Quantum entanglement：两个或多个微观粒子的状态可以相互关联，即使它们相隔很远，对其中一个粒子的测量会立即影响另一个粒子的状态。这种现象被爱因斯坦称为“鬼

[13] **维尔纳 · 卡尔 · 海森堡**（Werner Karl Heisenberg，1901 年 12 月 5 日 – 1976 年 2 月 1 日）是一位德国理论物理学家，被认为是量子力学创立者之一。他在原子物理学、核物理学和粒子物理学等领域做出了重要贡献，尤其是他关于量子力学的不确定性原理，对现代物理学产生了深远影响。

海森堡 1925 年提出了一种矩阵力学的形式体系，这是量子力学发展的一个重要里程碑。矩阵力学为描述原子系统的动力学行为提供了一种新的数学框架，不同于经典力学的方法。矩阵力学与薛定谔的波动力学最终证明是等价的，两者共同构成了量子力学的基础。

海森堡在 1927 年提出了著名的海森堡不确定性原理，这是量子力学中最重要和最具挑战性的观念之一。不确定性原理表明，在相同时间内，粒子的位置和动量不能同时被精确测量。类似地，粒子的能量和时间也受到不确定性原理的限制。这一原理揭示了量子世界的根本性质，即在微观尺度上，物理现象具有概率性和不确定性。

海森堡在核物理学领域的工作也非常重要。他在 1932 年提出了一个描述原子核的力学模型，称为液滴模型。这一模型为后来的核物理研究提供了理论基础。此外，他还参与了德国在第二次世界大战期间的核研究项目，尽管这个项目最终未能实现核武器的研制。

海森堡在 1932 年获得了诺贝尔物理学奖，以表彰他在量子力学方面的杰出贡献。他的工作对现代物理学产生了深远影响，尤其是在量子力学、核物理学和粒子物理学等领域。

魅般的超距作用”。

量子纠缠是量子力学中一种特殊的现象，它描述了两个或多个量子系统之间的非常强的关联。当量子系统被纠缠时，一个系统的状态将会立即影响另一个系统的状态，即使它们之间的距离相当遥远。这种现象超越了经典物理学范畴，因为它看似违反了经典物理中的局部实效原理[14]。

量子纠缠起初是由爱因斯坦、波多尔斯基和罗森于 1935 年提出的，他们认为这种现象是量子力学理论的不完备之处，因为它违反了他们所认为的物理现实观念。后来，贝尔（Bell）提出了贝尔不等式，用以检验这种纠缠现象是否真实存在。随后的实验表明，贝尔不等式在某些情况下确实被违反了，这为量子纠缠提供了强有力的证据。

量子纠缠现象在量子信息学领域具有重要应用价值，例如量子通信、量子计算和量子密码学。

所以说量子力学不仅推翻了经典物理学的许多观念，而且为现代科学技术的发展提供了基础，如半导体、激光、核能、量子计算等领域。尽管量子力学的某些现象直观上难以理解，但它已经成为描述自然界微观现象的最成功和最完善的理论。

1.1.2. 量子信息理论

量子信息理论是一门研究量子系统中信息处理和传输的跨学科领域，它将量子力学的基本原理应用于信息科学和通信技术。量子信息理论的核心思想是利用量子力学的特性（如量子叠加和量子纠缠）来实现对信息的高效处理、安全传输和存储。

量子信息理论主要包括以下几个方面：

- **量子计算**：量子计算是量子信息理论中的一个关键概念，它利用量子力学的基本原理进行信息处理和计算。与经典计算机使用比特（0 或 1）作为基本信息单位不同，量子计算使用量子比特（qubit）作为基本信息单位。量子比特可以处于 0、1 或者它们的线性叠加态，即同时处于多个状态。这使得量子计算机在理论上可以进行高度并行的计算，从而在某些问题上比经典计算机更加高效。

  量子计算中的基本操作是量子门（Quantum Gates），类似于经典计算中的逻辑门。量子门在量子比特上执行特定的操作，例如保持不变、翻转或者实现两个量子比特之间的纠缠。这些操作都是可逆的，并且满足一定的幺正性质。通过组合这些基本量子门，可以构建复杂数学和逻辑运算的量子算法。

  量子计算的一个显著优势是在某些问题上可以显著超越经典计算机的性能。著名的量子算法包括 Shor 算法（用于整数分解和解决 RSA 加密问题）和 Grover 算法（用于无序数据库搜索）。这些算法在量子计算机上的运行速度比经典计算机快得多，为解决许多实际问题提供了全新的途径。

  然而，量子计算也面临着许多挑战，如实现可扩展的、可控的量子硬件以及解决与量子比特相互作用和保真度相关的问题。尽管如此，量子计算仍被认为是未来计算技术的一个重要方向。

[14] 局部实效原理（Local Realism）是指在经典物理学中，物体或系统之间的相互作用必须是局部的，即它们之间的作用是通过在空间和时间上相互接近的点之间传递信息或者因果关系来实现的。换句话说，在经典物理世界中，系统之间的相互作用不可能瞬间跨越很远的距离。

局部实效原理基于两个基本概念：

实效性（Realism）：这个概念表示物体的属性或状态在进行测量之前就已经确定，不依赖于观察者的知识或测量行为。局部性（Locality）：这个概念表示在空间上分离的物体之间的相互作用不能瞬时发生，而是受到光速的限制，即信息不能超过光速传播。

- **量子通信**：量子通信是量子信息理论中的一个重要领域，它利用量子力学的原理进行信息的传输和处理。与经典通信系统使用经典比特（0 或 1）作为信息载体不同，量子通信使用量子比特（qubit）作为信息载体，通常采用光子（光量子）来实现量子比特的传输。

  量子通信的主要优势在于它提供了一种具有更高安全性的通信方式。在量子通信中，信息的传输过程利用了量子纠缠和量子隐形传态等现象，使得在理论上可以实现无条件安全的通信。这是因为任何对量子信道的监听或窃取行为都会导致信道状态的改变，从而被通信双方察觉。这种安全性是经典通信系统无法实现的。

  量子通信的一个典型应用是量子密钥分发（Quantum Key Distribution, QKD）。量子密钥分发利用量子通信技术在通信双方之间分发密钥，以实现安全的加密通信。著名的量子密钥分发协议包括 BB84 协议[15]和 E91 协议[16]等。量子密钥分发系统已经在一些实际场景中得到了应用，如银行、政府和军事通信等领域。

  虽然量子通信具有显著的优势，但它仍然面临着许多技术挑战，如提高信道传输距离、降低误码率和实现大规模量子网络的构建等。研究人员正致力于克服这些挑战，以实现量子通信在更广泛领域的应用。

- **量子密码学**：量子密码学（Quantum Cryptography）是一个研究如何利用量子力学原理来实现信息安全的学科。量子密码学的主要目标是为通信双方提供无条件安全的通信方式，即使在面对拥有无限计算能力的攻击者时也能保证通信的安全性。

  量子密码学最著名的应用领域是量子密钥分发（Quantum Key Distribution, QKD）。量子密钥分发利用量子通信技术在通信双方之间安全地传输密钥，以实现安全的加密通信。在量子密钥分发过程中，由于量子测量的不可克隆性和不可逆性，任何试图窃听通信的行为都会引入错误，从而被通信双方察觉。这种安全性是经典密码学和通信系统无法实现的。

  量子密码学包括以下主要部分：

  - **量子密钥分发**：如前述，量子密钥分发是量子密码学的核心应用。著名的量子密钥分发协议包括 BB84 协议和 E91 协议等。
  - **量子隐形传态**：量子隐形传态是利用量子纠缠现象实现在远程的两个地点之间传输未知量子态的一种技术。在量子隐形传态中，通信双方需要共享一对纠缠的量子比特，并利用经典通信信道来传输关于测量结果的信息。
  - **量子隐写术**：量子隐写术是一种使用量子信道来隐藏信息的技术。通过量子隐写术，可以将信息“隐藏”在量子信道中，使窃听者无法察觉到信息的存在。
  - **量子签名**：量子签名是一种基于量子力学原理的数字签名技术。与经典数字签名相比，量子签名在理论上可以提供更强的安全性。

  尽管量子密码学在理论上具有无条件安全的优势，但在实际应用中，由于设备的缺陷、信道损耗等因素，量子密码学的安全性仍然需要通过严密的数学证明和实际测试来保障。量子密码学在政府、军事、金融等领域具有广泛的应用潜力。

[15] BB84 协议是量子密钥分发（Quantum Key Distribution, QKD）领域的一个著名协议，由查尔斯·贝内特（Charles H. Bennett）和吉列斯·布拉萨德（Gilles Brassard）于 1984 年提出，因此得名 BB84。该协议利用量子力学原理实现密钥在通信双方之间的安全分发，保障通信的安全性。

[16] E91 协议是一个量子密钥分发（Quantum Key Distribution, QKD）协议，由 Artur Ekert 于 1991 年提出，因此得名 E91。该协议利用量子纠缠的特性实现密钥在通信双方之间的安全分发，保障通信的安全性。E91 协议与之前提到的 BB84 协议有相似之处，但在原理上存在一些不同。

- **量子纠错**：量子纠错（Quantum Error Correction）是量子信息处理领域中的一个重要概念，它主要研究如何在量子计算和量子通信过程中纠正由于噪声和其他误差引入的错误。由于量子比特（qubit）非常敏感，容易受到外部环境和设备缺陷的影响，因此在量子计算和量子通信过程中保持量子态的稳定性是至关重要的。量子纠错技术正是为解决这一问题而发展起来的。

  量子纠错的基本原理与经典纠错编码有相似之处，都是通过冗余编码的方式来检测和纠正错误。然而，量子纠错面临着比经典纠错更为复杂的挑战。量子比特可以处于 0、1 或者它们的线性叠加态，这使得量子纠错编码需要考虑更多的情况。此外，由于量子力学的不确定性原理和测量的不可逆性，量子纠错过程中不能直接对量子态进行测量，否则会破坏量子态本身。

  量子纠错编码的一个重要概念是量子纠错码（Quantum Error-Correcting Code），它是一种将逻辑量子比特编码为多个物理量子比特的方法，从而在物理量子比特出现错误时，可以通过冗余信息检测和纠正错误。著名的量子纠错码包括 Shor 算法，如算法1[17]和 Steane 代码，如算法2[18]等。

  在量子纠错过程中，除了需要设计有效的纠错码之外，还需要开发一系列用于错误检测和纠正的量子算法和量子门。这些算法和量子门应当满足一定的幺正性质，以保证在纠错过程中不引入新的错误。

  量子纠错是实现大规模、可靠的量子计算和量子通信的关键技术之一。尽管目前的量子纠错技术仍然面临许多挑战，但随着量子信息技术的不断发展，量子纠错的应用前景十分广阔。

  Shor 代码的纠错过程包括以下几个步骤：

1. **对编码后的 9 个物理量子比特进行错误检测，这通常通过一系列受控非门（CNOT 门）和受控受控非门（Toffoli 门）来实现。在此过程中，需要注意的是不能直接对量子比特进行测量，以避免破坏量子态本身。**
2. 分析错误检测的结果，确定错误的类型和位置。
3. 应用适当的量子门（如 X 门或 Z 门）来纠正检测到的错误。
4. 对修复后的量子比特进行解码，恢复原始的逻辑量子比特。

  Steane 代码的纠错过程包括以下几个步骤：

1. **对编码后的 7 个物理量子比特进行错误检测。这通常通过一系列受控非门（CNOT 门）以及辅助量子比特来实现。在此过程中，同样需要注意不能直接对量子比特进行测量，以避免破坏量子态本身。**
2. 分析错误检测的结果，确定错误的类型和位置。
3. 应用适当的量子门（如 X 门或 Z 门）来纠正检测到的错误。
4. 对修复后的量子比特进行解码，恢复原始的逻辑量子比特。

[17] Shor 代码是一种量子纠错码，由 Peter Shor 于 1995 年首次提出。Shor 代码是一种能够纠正任意单个量子比特错误的纠错码。Shor 代码的提出标志着量子计算领域的一个重要突破，因为它证明了在量子计算过程中可以纠正错误，从而增强了实现大规模量子计算机的可行性。

[18] Steane 代码是一种量子纠错码，由 Andrew Steane 于 1996 年首次提出。Steane 代码是一种能够纠正任意单个量子比特错误的纠错码，与 Shor 代码一样，它可以同时检测和纠正单个量子比特的位翻转错误（X 错误）和相位翻转错误（Z 错误）。Steane 代码的提出进一步推动了量子纠错领域的发展。

Algorithm 1 Shor's Code Error Correction (量子纠错：Shor 代码)

procedure ShorErrorCorrection($|\psi\rangle$)
    准备辅助量子比特，状态为 $|0\rangle$
    使用 Shor 代码对 $|\psi\rangle$ 进行编码
    应用 CNOT 门进行错误检测
    测量辅助量子比特
    利用测量结果确定错误的类型和位置
    if 检测到位翻转错误 **then**
        应用 X 门进行纠正
    end if
    if 检测到相位翻转错误 **then**
        应用 Z 门进行纠正
    end if
    对纠正后的量子比特进行解码，恢复原始状态 $|\psi\rangle$
end procedure

Algorithm 2 Steane's Code Error Correction (量子纠错：Steane 代码)

procedure SteaneErrorCorrection($|\psi\rangle$)
    准备辅助量子比特，状态为 $|0\rangle$
    使用 Steane 代码对 $|\psi\rangle$ 进行编码
    应用 CNOT 门进行错误检测
    测量辅助量子比特
    利用测量结果确定错误的类型和位置
    if 检测到位翻转错误 **then**
        应用 X 门进行纠正
    end if
    if 检测到相位翻转错误 **then**
        应用 Z 门进行纠正
    end if
    对纠正后的量子比特进行解码，恢复原始状态 $|\psi\rangle$
end procedure

量子信息理论是一个充满挑战和潜力的领域，它为未来信息技术的发展提供了全新的可能。随着量子计算、量子通信和量子密码学等技术的不断发展，量子信息理论有望在许多领域产生深远的影响，如密码安全、高性能计算、人工智能等。

1.1.3. 计算机科学与量子计算

计算机科学与量子计算是两个相关的但有所区别的领域。计算机科学是研究计算机系统设计、软件开发和信息处理的理论和实践的学科。它包括各种子领域，如算法设计、数据结构、编程语言、操作系统、数据库管理、人工智能等。计算机科学的核心是经典计算理论，基于经典比特（bit）进行信息处理。

量子计算则是计算机科学的一个子领域，专注于开发和理解基于量子力学原理的新型计算模型。量子计算利用量子比特（qubit）作为信息单位，它可以同时处于多个状态（即量子叠加态），从而在某些问题上实现比经典计算更快的速度。量子计算涉及到量子算法设计、量子计算机硬件实现、量子纠错等方面的研究。

计算机科学与量子计算的关系可以总结为以下几点：

- 量子计算是计算机科学的一个子领域，但它采用了截然不同的计算模型。
- 量子计算基于量子力学原理，而计算机科学主要依赖于经典物理学。
- 计算机科学与量子计算之间存在一定的交叉与互动。例如，计算机科学中的算法设计和优化方法可以应用于量子算法，而量子计算的发展也可能对计算机科学中的问题提供新的解决方案。
- 量子计算的发展可能对计算机科学的未来产生深远影响。如果实现可扩展的量子计算机，它可能会在许多领域（如密码学、优化问题等）实现比经典计算更高效的解决方案，从而推动计算机科学的进步。
- 量子计算对计算机科学的教育和研究方法产生影响。随着量子计算的发展，计算机科学专业可能需要加入量子计算相关的课程，以便学生能够掌握这一领域的基本概念和技能。此外，研究人员需要开发新的模拟工具和编程语言来实现量子算法和量子计算机的设计。
- 计算机科学与量子计算在硬件设计方面有所区别。传统计算机硬件基于经典物理学原理，如晶体管和集成电路。而量子计算硬件则需要利用量子力学现象，如超导量子比特、离子阱、光子量子比特等。这些技术在原理和实现上与传统计算机硬件有很大差别。
- 计算机科学与量子计算在工业应用方面有所区别。传统计算机科学技术已经广泛应用于各个行业，如金融、医疗、通信等。而量子计算目前尚处于发展初期，尽管在某些特定问题上具有潜在优势，但其在工业应用方面的普及和实际价值仍需时间和技术突破。
- 计算机科学与量子计算在安全性和隐私保护方面有所区别。量子计算对现有的密码学体系产生挑战，如 Shor 算法可以在量子计算机上快速分解大整数，从而破解 RSA 等加密算法。这促使计算机科学研究人员开发新的抗量子加密技术，如基于格的密码学、基于哈希的签名算法等。

计算机科学与量子计算是两个相互关联但有所区别的领域。量子计算作为计算机科学的一个子领域，以量子力学原理为基础，具有潜在的并行性和高效性。量子计算的发展可能对计算机科学产生深远的影响，推动信息技术领域的进步。

对于我们的目的，我们将重点关注量子计算机与经典计算机的区别所在。

每台经典计算机（即非量子计算机）都可以用量子力学来描述，因为量子力学是物理宇宙的基础。然而，经典计算机没有利用量子力学所提供的特定属性和状态来进行计算。

为了深入研究我们在量子计算机中使用的特定属性，让我们先讨论量子力学的一些关键概念：

- 如何表示量子系统中的叠加态?
- 什么是纠缠?
- 可逆性、计算和物理系统之间的联系是什么?

1.2. 量子力学基础

在本课程中，我们广泛使用狄拉克符号、线性代数和其他工具；读者被鼓励在需要时参考本文后面的数学章节进行复习。

1.2.1. 狄拉克符号

狄拉克符号（Dirac notation），又称为 bra-ket 表示法，是一种用于描述量子力学中的态和算符的简洁符号体系。这种表示法由著名物理学家保罗·狄拉克（Paul Dirac）[19]引入，以便更方便地处理量子力学中的数学计算。

在狄拉克符号中，量子态用一个被称为 ket 的符号表示，如：$|\psi\rangle$。这表示一个量子态，可以是一个量子比特（qubit）或多个量子比特组成的系统。另一方面，bra 符号表示一个复共轭[20]的态，如：$|\psi\rangle$。通过 bra 和 ket 的组合，可以计算内积、外积以及算符作用等操作。

狄拉克符号在量子计算中具有重要意义，因为它为处理量子比特（qubit）和量子门等核心概念提供了一种简洁有效的表示方法。量子计算中的基本单位是量子比特，其状态可以用狄拉克符

[19] **保罗·狄拉克**（Paul Dirac、1902 年 8 月 8 日 – 1984 年 10 月 20 日）是一位英国理论物理学家，被认为是 20 世纪最重要的物理学家之一。他在量子力学和量子场论方面的开创性工作为现代物理学的发展奠定了基础。狄拉克的研究涉及许多领域，包括电动力学、粒子物理、引力理论以及数学物理。

狄拉克最著名的贡献之一是狄拉克方程，这是一个描述相对论性电子行为的方程。狄拉克方程成功地将量子力学与狭义相对论结合起来，为电子和其他基本粒子的性质提供了深刻的理解。狄拉克方程的一个重要结果是预言了电子的反粒子——正电子的存在，这在后来的实验中得到了证实。

狄拉克还对量子力学的数学表示和形式体系做出了重要贡献。他引入了一种称为狄拉克符号（bra-ket 表示法）的表示方法，用以简化量子力学的数学计算。这种表示法在现代物理学和量子计算中被广泛应用。

狄拉克还对粒子物理学的发展产生了重要影响。他提出了狄拉克海这一概念，即所有负能量电子状态的集合。这一理论为量子场论的发展奠定了基础，并为物质和反物质之间的对称性提供了理论支持。

狄拉克在 1933 年与奥地利物理学家埃尔温·薛定谔共同获得了诺贝尔物理学奖，以表彰他们在原子理论和量子力学方面的杰出贡献。狄拉克对现代物理学的影响是深远的，他的工作为量子力学、相对论性粒子物理学以及量子信息科学等领域的发展奠定了基础。

[20] **复共轭**（complex conjugate）是一种与给定复数相关的另一个复数，它的实部与原复数相同，但虚部的符号相反。复共轭的概念主要用于复数运算，尤其是在复平面上表示和操作复数时非常有用。

给定一个复数 z，表示为：

$$z = a + bi$$

其中 a 和 b 是实数，i 是虚数单位，满足 $i^2 = -1$。那么 z 的复共轭表示为：

$$z* = a - bi$$

可以看到，实部相同，而虚部的符号相反。

复共轭在复数运算中有许多重要性质。例如：

- 两个复数的乘积与它们的复共轭的乘积相等：$(z_1 z_1)^* = z_1^* z_2^*$；
- 一个复数与其复共轭的乘积等于该复数的模的平方：$|z|^2 = zz^*$；
- 如果一个复数的实部或虚部为零，则该复数等于其复共轭；
- 两个复数的和的复共轭等于它们各自复共轭的和：$(z_1 + z_1)^* = z_1^* + z_2^*$。

在量子力学和量子计算中，复共轭在表示和处理复数概率振幅时起到重要作用。例如，在狄拉克符号中，bra 表示一个量子态的复共轭，用于计算量子态的内积和概率分布。

号表示为：

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.2}$$

其中，α 和 β 是复数，它们的模平方之和等于 1（即 $|\alpha|^2 + |\beta|^2 = 1$）。$|0\rangle$ 和 $|1\rangle$ 分别表示量子比特的基本态，类似于经典计算中的 0 和 1。

在量子计算中，狄拉克符号还可以用于表示量子门（quantum gate）。量子门是量子计算中的基本操作，可以理解为量子比特状态的变换。例如，Pauli-X 门可以表示为：

$$\mathrm{X} = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{1.3}$$

在这里，X 是一个 2x2 的矩阵，可以作用于一个量子比特的状态，从而实现状态的变换。

狄拉克符号在量子计算中起到了关键作用，它为表示和处理量子态、量子门等核心概念提供了一种简洁有效的方法。这使得量子计算的理论研究和实际实现更加清晰和直观。

1.2.2. 量子计算基础

根据量子力学的原理，只有在进行测量时，系统才被设置为一个确定的状态。在测量之前，系统处于不确定的状态；在我们测量它们之后，它们就处于一个确定的状态。如果我们有一个系统，当进行测量时可以采取两种离散状态之一，我们可以用狄拉克符号表示这两种状态，如 $|0\rangle$ 和 $|1\rangle$。然后，我们可以将状态的叠加表示为这些状态的线性组合，例如公式1.2, 其中，α 和 β 是复数，且满足

$$\alpha^2 + \beta^2 = 1 \tag{1.4}$$

，以确保总概率为 1。

公式1.2是量子计算中的一个基本概念，表示一个量子比特（qubit）的量子态。在量子计算中，量子比特是基本的信息单位，与经典计算中的比特（bit）类似。然而，与经典比特不同的是，量子比特可以同时处于 0 和 1 的状态，这种现象被称为**量子叠加**。

在这个公式中，$|0\rangle$ 和 $|1\rangle$ 分别表示量子比特的基本态，即类似于经典比特中的 0 和 1。而 $|\psi\rangle$ 是一个一般的量子态，可以通过基本态的线性组合表示。α 和 β 是复数系数，它们的模平方之和等于 1，这个条件确保了量子态的概率解释是合理的。α 和 β 的值决定了量子态 $|\psi\rangle$ 的具体形式。当我们测量这个量子态时，它会坍缩为 $|0\rangle$ 或 $|1\rangle$，并以 $|\alpha|^2$ 的概率得到 $|0\rangle$，以 $|\beta|^2$ 的概率得到 $|1\rangle$，即一个量子比特可以同时处于多个状态的线性组合。这种特性使得量子计算具有潜在的并行性和高效性，可以在某些问题上实现比经典计算更快的速度。

在量子系统中，我们可以将多个粒子纠缠在一起，这意味着它们之间存在一种关联性，无论它们之间有多远的距离。例如，如果两个粒子是纠缠的，当我们改变其中一个粒子的状态时，另一个粒子的状态也会相应地改变，即使它们之间相隔数千万英里。

量子计算机的关键优势在于它们能够在计算中利用这种纠缠现象和叠加态。另外，量子计算机中的运算通常是可逆的，这意味着可以通过相反的运算将计算结果。

当我们将一个量子系统测量时，它会坍缩到一个确定的状态。但在测量之前，它处于叠加态，可以表示为一组基矢量的线性组合：

$$|\psi\rangle = \sum_i c_i |i\rangle \tag{1.5}$$

其中 c_i 是一组复数系数，$|i\rangle$ 是一组基矢量。在测量之前，我们无法知道系统处于哪个基矢量上，只能计算出处于每个基矢量的概率为 $|c_i|^2$。在测量之后，系统会坍缩到一个确定的基矢量上，概率等于 $|c_i|^2$。

在量子计算机中，我们利用叠加态和量子纠缠来加速计算。量子计算机的计算方式与经典计算机不同，可以利用叠加态和纠缠来处理信息，从而在某些情况下比经典计算机更高效。

1.2.3. 叠加原理

举例来说，让我们考虑光的一个性质，它展示了状态的叠加。光具有一种固有属性，称为偏振，我们可以用它来展示状态的叠加。在几乎所有日常生活中看到的光线（例如来自太阳的光），没有偏振的优先方向。偏振状态可以通过偏振滤波器来选择，这是一种带有轴的薄膜，只允许与该轴平行的偏振光通过。叠加态是指一个量子系统处于多个基态的线性组合。叠加态是量子计算中的核心概念，它体现了量子系统在某种程度上可以同时存在于多个状态，这与经典计算中的二进制位（0 或 1）有很大的不同。

使用单个偏振滤波器，我们可以选择光的一个偏振，例如垂直偏振，我们可以表示为 $|\uparrow\rangle$. 水平偏振，我们可以表示为 $|\rightarrow\rangle$，是垂直偏振的正交状态。这些状态一起形成了任何偏振光的基础。也就是说，任何偏振状态 $|\psi\rangle$ 都可以被写成这些状态的线性组合。我们使用希腊字母来表示系统的状态

$$|\psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\rightarrow\rangle \tag{1.6}$$

公式1.6中系数 α 和 β 是称为振幅的复数。系数 α 与垂直偏振相关，系数 β 与水平偏振相关。它们在量子力学中有重要的解释。在选择垂直偏振的偏振滤波器之后，我们可以引入第二个偏振滤波器。假设我们将第二个滤波器的轴与第一个垂直。那么第二个滤波器会透过多少光？如果你对这个问题的答案是否定的，那么你是正确的。水平状态 $|\rightarrow\rangle$ 是第一个状态的正交，因此第一个垂直滤波器后没有任何水平偏振。

现在假设我们将第二个偏振滤波器的轴朝着第一个的对角线（即垂直 $\uparrow$ 和水平 $\rightarrow$ 之间的对角线）方向旋转 45°。现在我们问同样的问题——第二个滤波器会透过多少光？如果你对这个问题的答案是否定的，你可能会惊讶地发现答案是肯定的。实际上，我们会看到一些光透过第二个滤波器。如果所有经过第一个滤波器的光都是垂直偏振，那么这是如何发生的？原因在于我们可以将垂直偏振表示为对角线分量的叠加。也就是说，让 $|\nearrow\rangle$ 表示 45° 偏振，让 $|\nwarrow\rangle$ 表示 -45° 偏振，我们可以写成：

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}\,|\nearrow\rangle + \frac{1}{\sqrt{2}}\,|\nwarrow\rangle \tag{1.7}$$

从几何直觉上预期，垂直状态包含相等部分的 $|\nearrow\rangle$ 和 $|\nwarrow\rangle$。

正是因为这个原因，我们会看到一些光透过第二个滤波器。也就是说，垂直偏振可以被写成状态的叠加，其中一个状态恰好是我们允许通过第二个滤波器的 45° 对角线状态 $|\nearrow\rangle$。由于 $|\nearrow\rangle$ 只是叠加中的一个术语，因此并不是所有的光都通过滤波器，但是一些光确实通过了。在这种情况下，传输的量恰好是 $1/2$。（更正式地说，传输光的强度是入射光的 $1/2$。）这个值是由 Born 法则确定的，我们现在来讨论。

马克斯·玻恩（Max Born）[21]在他 1926 年的论文中证明，状态振幅的模平方是测量后该状态

[21] **马克斯·玻恩**（Max Born，1882 年 - 1970 年）是一位德国籍的英国理论物理学家和数学家，因在量子力学领域的开创性贡献而获得广泛认可。他在量子力学的建立和发展过程中扮演了关键角色，并因此荣获了 1954 年的诺贝尔物理学奖。

玻恩出生于德国汉诺威，曾在哥廷根大学、柏林洪堡大学和爱丁堡大学等学府学习和工作。他的研究生导师是著名数学家大卫·希尔伯特（David Hilbert），这使得玻恩在数学和理论物理方面接受到了良好的教育。

出现的概率 [38]。在这种情况下，由于振幅是 $1/\sqrt{2}$，因此测量到该状态的概率为 $1/2$。注意，我们选择了振幅为 $1/\sqrt{2}$，以使状态归一化，这样振幅的模平方之和将等于一。这使我们能够使用玻恩法则将振幅连接到测量的概率上。

1.3. 玻恩规则

在一个量子态的叠加中，一个态的振幅模平方是测量得到该态的概率。此外，叠加中所有可能态的振幅模平方之和等于 1。所以，对于态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$，我们有：

$$|\alpha|^2 + |\beta|^2 = 1$$

虽然在上面的偏振示例中，两个态各有 50% 的概率，但如果我们观察其他物理系统，可能会有 75% 的概率分布或其他概率分布。经典力学和量子力学之间的一个关键区别是振幅（而非概率）可以是复数。

换句话说，出现在玻恩规则陈述中的系数 α 和 β 可以是复数，例如 $i = \sqrt{-1}$ 或 $(1+i)\sqrt{-1}$。只有在我们取这些振幅的模平方时，我们才得到实数，即实际的概率。请参阅第 11 章以复习复数及如何确定复数模平方。

量子叠加本身就足够奇特，量子力学描述了一种特殊类型的叠加，这进一步挑战了我们的想象力：纠缠。

1935 年，当爱因斯坦与波多尔斯基和罗森共同发表了关于量子纠缠的论文 [19] 时，他们的目标是攻击量子力学的基石（这篇论文现在被称为 EPR 论文）。尽管爱因斯坦因 1905 年关于光电效应的量子性质的工作获得了诺贝尔奖，但他直到晚年仍在抨击量子力学的含义。

爱因斯坦在 1952 年写道，量子力学对他来说似乎是

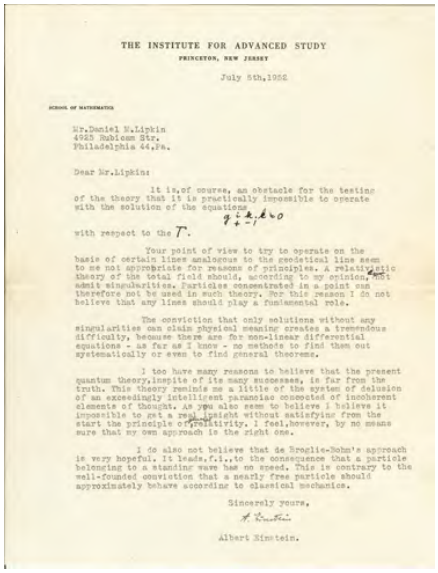
“a system of delusion of an exceedingly intelligent paranoiac concocted of incoherent elements of thought（一个极度聪明的妄想狂用不连贯的思想元素捏造的幻觉体系）”

如图1.5。他希望 EPR 论文能证明他认为的量子力学的不足之处。

在 20 世纪初，玻恩开始了他在量子力学领域的研究。他与其他科学家，如沃纳 · 海森堡（Werner Heisenberg）和尼尔斯 · 玻尔（Niels Bohr）等，一起发展了这一革命性的理论体系。在 1920 年代，玻恩对波恩概率解释的提出和数学公式的精确描述，成为量子力学的核心组成部分。玻恩概率解释说明了波函数的平方与粒子存在的概率密度之间的关系。

除了量子力学领域的贡献外，马克斯 · 玻恩还在晶体学、固态物理学和光学等领域取得了成果。在第二次世界大战期间，由于他的犹太血统，他逃离了德国，并在英国继续了他的学术生涯。1954 年，玻恩因在量子力学领域的贡献获得了诺贝尔物理学奖。

马克斯 · 玻恩是一位在物理学领域产生深远影响的科学家，他的研究对量子力学的发展起到了关键性作用。



THE INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY

July 5th,1952

SCHOOL OF MATHEMATICS

Mr.Daniel M.Lipkin
4925 Hublcom Str.
Philadelphia 44,Pa.

Dear Mr.Lipkin:

It is,of course, an obstacle for the testing of the theory that it is practically impossible to operate with the solution of the equations

$$g_{\mu\nu,\alpha\beta}=0$$

with respect to the T.

Your point of view to try to operate on the basis of certain lines analogous to the geodetical line seem to me not appropriate for reasons of principles. A relativistic theory of the total field should, according to my opinion, not admit singularities. Particles concentrated in a point can therefore not be used in such theory. For this reason I do not believe that any lines should play a fundamental role.

The conviction that only solutions without any singularities can claim physical meaning creates a tremendous difficulty, because there are for non-linear differential equations - as far as I know - no methods to find them out systematically or even to find general theorems.

I too have many reasons to believe that the present quantum theory,inspite of its many successes, is far from the truth. This theory reminds me a little of the system of delusion of an exceedingly intelligent paranoiac conceited of incoherent elements of thought. As you also seem to believe i believe it impossible to get a real insight without satisfying from the start the principle of relativity. I feel,however, by no means sure that my own approach is the right one.

I do also not believe that de Broglie-Bohm's approach is very hopeful. It leads,f.i.,to the consequence that a particle belonging to a standing wave has no speed. This is contrary to the well-founded conviction that a nearly free particle should approximately behave according to classical mechanics.

Sincerely yours,

Albert Einstein.

图 1.5: 爱因斯坦给丹尼尔 · M · 利普金的签名信，普林斯顿，1952 年 7 月 5 日。图片来自于 christieshttps://www.christies.com/en/lot/lot-6210437

ERP 论文 [19] 表明，如果你拿两个相互纠缠的粒子，然后测量其中一个，这将自动触发第二个粒子的相关状态，即使两者相距很远；这是 EPR 希望用来证明量子力学本身存在缺陷的看似不合逻辑的结果。讽刺的是，我们现在认为纠缠是量子力学的基石。纠缠发生在不可分离的态的叠加中。

这种“鬼魅般的距离作用”似乎与我们的直觉和先前的物理学相悖。据报道，合著者中年龄最小的波多尔斯基将论文泄露给《纽约时报》，以便向公众突显这对量子力学大厦的攻击。1935 年 5 月 4 日，《纽约时报》以“爱因斯坦攻击量子理论”为标题，在头版刊登了这篇报道。

如今，纠缠不仅被接受为标准量子力学的一部分，我们还将在后面的章节中看到，我们可以利用纠缠来进行新颖类型的计算和通信。从信息论的角度来看，纠缠是一种不同的信息编码方式。如果我们有两个纠缠在一起的粒子，关于它们的信息不是局部地编码在每个粒子中，而是编码在两者之间的关联中。

约翰 · 普雷斯基尔喜欢用两种书的比喻来解释纠缠和非纠缠 [20] [22]：在普通的、非纠缠的书中，我们可以像平常一样阅读每一页的信息。然而，在纠缠的书中，每一页都包含看似胡言乱语的内容。信息被编码在页面之间的关联中，而不是每一页单独的内容。这正是薛定谔在创造“纠缠”这个术语时所表达的：

[22] 这篇论文的主要内容是关于”NISQ（Noisy Intermediate-Scale Quantum）” 时代及其之后量子计算的研究，作者 John Preskill 提出了许多观点和建议。
论文的主要观点如下：
NISQ 时代的量子计算机具有一定的规模和噪声，因此其能力相对有限，但仍然有潜力在某些领域取得突破。
发展量子纠缠和量子误差校正等技术，可以提高量子计算机的可靠性和性能。
发展量子模拟和量子优化等领域的算法，可以在实际问题中展现量子计算机的优势。
在 NISQ 时代中，需要进一步发展量子硬件和量子软件，同时也需要建立一些实际问题的测试平台，以便在实际应用中测试量子计算机的性能。
在未来，量子计算机可能会推动量子物理、量子信息和量子工程等领域的发展，从而引领新的科技革命。
论文的主要实验手段是理论分析和综述，对已有的研究成果进行了总结和归纳。作者提出的观点和建议，对于当前和未来的量子计算机研究具有重要的指导作用。
该论文的主要贡献是提出了 NISQ 时代及其之后量子计算的研究方向和目标，对量子计算机的发展和应用具有指导作用。

另一种表达这种奇特情况的方式是：”对整体的最佳可能了解并不一定包括对所有部分的最佳可能了解。”[21]

薛定谔[23]进一步指出，在他看来，纠缠不仅仅是量子力学描述的现象之一，“而是量子力学的特征，使其完全脱离了经典思维模式。”[21]。

1.4. 纠缠

如果两个系统的测量结果以比经典世界更强的方式与另一个系统的状态相关，那么这两个系统处于被称为纠缠的量子力学叠加态的特殊情况。换句话说，这两个系统的状态是不可分的。

现在我们已经介绍了量子力学的两个核心思想——叠加和纠缠，让我们转向另一个不太常被涉及的基本概念——**信息的物质性**。当**罗尔夫·兰道尔**[24]提出以下问题时，他开启了一条新的探索方向：寻求更快、更紧凑的计算电路，直接引发了这样一个问题：

“这方面的进展在物理上有什么终极限制？... 我们可以证明，或者至少强烈暗示，信息处理过程中不可避免地伴随着一定程度的热量产生。[22]”

换句话说，计算基本单位过程中能量损耗的下限是多少？由于兰道尔和其他人的研究，我们现在相信确实存在这样一个限制；这被称为兰道尔界限（LB）。更具体地说，擦除 n 位比特的能量成本是 $nkT\ln 2$，其中 k 是玻尔兹曼常数，T 是以开尔文表示的计算设备周围热汇的温度，$\ln 2$ 当然是 2 的自然对数（约 0.69315）。这个限制是不可逆计算的最小能量损耗。

兰道尔承认，这个最小值不一定是系统能量消耗的限制因素。

当然，很明显，热噪声和能量耗散的要求在目前计算机组件中的比例是完全可以忽略的。然而，计算出的耗散是一个绝对最小值。[22]

兰道尔将逻辑不可逆定义为“设备的输出不能唯一确定输入”的条件。然后他声称，“逻辑不可逆性... 反过来意味着物理不可逆性，而后者伴随着耗散效应。”这是由热力学第二定律推导出的，该定律指出，一个系统的总熵不能减少，而且更具体地说，在不可逆过程中必须增加。关于可逆性、热力学和计算的更多背景知识，请参阅费曼的《计算讲义》[84]

在经典计算中，我们使用不可逆计算。例如，布尔”或”（表示为 ∨）门具有以下真值表，其中 0 表示“假”，1 表示“真”：

注意，输出值 1 不能唯一地追溯到一组输入。我们可以通过输入组合得到该输出；一旦转到输出，输入状态就丢失了。这并没有违反信息守恒，因为信息已经转化为耗散热量。

亦或门也是不可逆的，同样适用于经典计算中的通用 NAND 门。NAND 表示“非与”，是布尔与运算符的逆。通过检查它的真值表来验证 NAND 是不可逆的：

[23] **薛定谔**（Erwin Schrödinger，1887 年 8 月 12 日 – 1961 年 1 月 4 日），是一位奥地利物理学家，曾获得 1933 年的诺贝尔物理学奖。他被誉为现代量子力学的奠基人之一，对于波动力学方程的建立做出了重要贡献。

薛定谔在 1918 年提出了著名的薛定谔方程，用以描述量子体系的运动和行为。他也因此被誉为“波动力学之父”，并成为了量子力学的重要代表人物之一。他还提出了著名的“薛定谔的猫”思想实验，用来探讨量子力学中的测量问题和量子态的纠缠问题。

薛定谔在物理学领域的贡献不仅限于量子力学，他还在许多其他领域做出了重要的贡献，如在物态方程、热力学、色散理论、宇宙学等领域。

薛定谔的学术成就对于现代物理学的发展有着深远的影响。他不仅在理论物理学方面取得了杰出的成就，而且还对科学哲学、科学教育和科学传播做出了重要的贡献。

[24] **罗尔夫·兰道尔**，Rolf Landauer (1927–1999) 是一位德国裔美国物理学家，他在信息理论和统计物理学方面作出了重大贡献。他在 IBM 托马斯·J·沃森研究中心工作了大部分的职业生涯。

罗尔夫最为人所知的贡献是他在 1961 年提出的罗尔夫原理，该原理阐述了在某些条件下，计算机操作的物理限制。他的理论指出，信息的擦除在物理上必然伴随着能量的耗散，这与当时的普遍观点相反。这一原理在纳米尺度科学和量子计算机领域具有重要意义。

他的另一个重要贡献是关于电子在固体中输运的理论，这对理解和设计微电子设备非常重要。Landauer 的工作对现代信息和计算理论产生了深远影响。

X	Y	X ∨ Y
0	0	0
0	1	1
1	0	1
1	1	1

X	Y	X	Y
0	0	1	
0	1	1	
1	0	1	
1	1	0	

“在量子计算中，我们将自己限制在可逆逻辑运算上”[23] 这句话的意思是，在量子计算中，我们确实经常将自己限制在可逆逻辑运算上。这是由于量子机械的基本动力学是可逆的，也就是说，如果你知道一个系统的当前状态，你就可以准确地推算出它的过去和未来状态。因此，量子计算的基本操作——量子门，也必须是可逆的。

在经典计算中，许多逻辑运算都是不可逆的。例如，如果你看到一个 AND 门的输出是 0，你无法确定输入是什么。然而，在量子计算中，所有的操作都必须是可逆的。这意味着，如果你知道输出，你就可以准确地推算出输入。例如，量子计算中的 CNOT 门（受控非门）就是一种可逆逻辑门。

这种限制在可逆逻辑运算的原因还有另一个层面，那就是罗尔夫 · 兰道尔提出的兰道尔原理，该原理表明，每个不可逆的运算都会导致能量的耗散。因此，基于量子力学的可逆性和能源效率的考虑，量子计算通常都限制在可逆逻辑运算上。稍后在本书中，我们将考虑哪些量子算子组合是通用的。现在，让我们专注于量子计算中的要求，将我们的算子集限制为可逆门。

这个要求源于不可逆操作的性质：如果我们执行不可逆操作，我们就丢失了信息，因此测量结果。此时我们的计算周期将结束，我们将无法继续执行程序。相反，通过将所有门限制为可逆算子，只要我们能保持系统的相干性，我们就可以继续将算子应用于我们的量子比特集。当我们说可逆时，我们指的是理论上无噪声的量子计算机。在一个有噪声的量子计算机中，我们当然无法反转操作。

1.5. 量子计算的可逆性

除测量外，量子计算中使用的所有算子都必须是可逆的。

量子计算的可逆性是指在量子计算过程中，每个量子操作（通常由量子门实现）都是可逆的。这意味着每个量子门操作都具有一个逆操作，该逆操作可以完全恢复输入量子态。在量子力学中，这个特性体现在量子操作（量子门）是幺正的。幺正操作具有以下性质：其逆操作就是其共轭转置（在量子力学中，共轭转置通常表示为酉矩阵）。

可逆性是量子计算与经典计算的一个重要区别。在经典计算中，有些操作是不可逆的，例如逻辑与门（AND gate）和逻辑或门（OR gate）。在这些操作中，输出信息会丢失输入信息的一部分，因此无法通过输出状态唯一地确定输入状态。然而，在量子计算中，这种信息丢失是不允许的，因

为它会破坏量子态的相干性。

可逆性在量子计算中具有重要意义，因为它保留了量子系统的相干性，并允许量子算法在量子计算过程中探索可能的解空间[25]。这使得量子计算在某些问题上具有优越性，例如大整数因式分解（Shor 算法）和无序数据库搜索（Grover 算法）。这些量子算法利用量子计算的特性，比经典计算方法更高效地解决了相应的问题。

1.5.1. 计算表达

可逆性在量子计算中的表示主要体现在量子门的性质上。在量子计算中，量子门是对量子比特进行操作的基本单元。为了满足可逆性，量子门必须是幺正的。幺正矩阵是一个满足以下性质的矩阵：它的共轭转置（酉矩阵）等于它的逆矩阵。用数学表示，设 U 是一个量子门，那么有：

$$U^\dagger U = UU^\dagger = I \tag{1.8}$$

其中，U 是一个正矩阵，$U^\dagger$ 表示 U 的共轭转置（酉矩阵），I 表示单位矩阵。这意味着 U 的逆操作就是 $U^\dagger$。

在量子计算中，常见的量子门如 X、Y、Z 门，以及 Hadamard 门、CNOT 门、Toffoli 门等都是幺正的。这些量子门都可以通过它们的共轭转置来实现逆操作，从而实现可逆性。

可逆性在量子计算中具有重要意义，因为它保证了量子态在操作过程中的相干性。由于量子门是幺正的，量子态在经过量子门操作后仍然保持在同一希尔伯特空间（量子态所在的线性空间）内。这使得量子计算能够在一定程度上利用量子叠加和量子纠缠等现象，实现对于某些问题的优越性能。

1.6. 总结

在本章中，我们研究了量子力学系统的四个基本原则：叠加、玻恩规则、纠缠和可逆计算。这四个原则对于理解经典计算与量子计算之间的差异至关重要，我们将在本书后面进一步学习。

[25] 在数学和计算机科学中，解空间是指包含了一个给定问题所有可能解的集合。解空间可以被用来描述一系列的可能情况，或者是一个问题的所有可能答案。

例如，考虑一个简单的线性代数问题，比如线性方程组。这个方程组的解空间是由所有满足该方程组的解组成的向量空间。

在优化或搜索问题中，解空间可能包含了所有可能的候选解，而求解的过程就是在这个解空间中寻找最优解或满足特定条件的解。

解空间的大小和结构取决于具体问题的性质和约束条件。有的问题解空间可能非常大，甚至是无限的，而有的问题解空间可能就只有有限的几个解。