学号：202121018094 **班级：**通信 2102 **姓名：**徐卉垚

2023-2024 学年第一学期 通信前沿技术讲座 报告

通信前沿技术讲座——量子计算

2023 年 11 月 2 日

一、课堂概述

1. 什么是量子计算
2. 量子计算的数学原理
3. 量子通信与量子隐形传态
4. 量子软件的功能和构成
5. 量子工业界现状

二、课堂内容

量子（quantum）是现代物理的重要概念。即一个物理量如果存在最小的不可分割的基本单位，则这个物理量是量子化的，并把最小单位称为量子。不但能量表现出这种不连续的分离化性质，其他物理量诸如**角动量、自旋、电荷、能级**等也都表现出这种不连续的量子化现象。

量子计算是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式。对照于传统的通用计算机，其理论模型是通用图灵机；通用的量子计算机，其理论模型是用量子力学规律重新诠释的通用图灵机。从可计算的问题来看，量子计算机只能解决传统计算机所能解决的问题，但是从计算的效率上，由于量子力学叠加性的存在，某些已知的量子算法在处理问题时速度要快于传统的通用计算机。

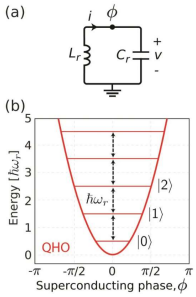
量子保密通信作为一种具有绝对安全性的通信技术，它不仅具备强大的信息的存储与携带能力，凭借量子计算机还可以解决各种复杂难度的计算，还具有进行高时速、高精准的并行计算的处理能力。量子保密通信是在原有的公钥体系进行创新改进，采取量子密钥分发和加密的量子保密通信方案，以应对原有量子计算体系内存在的安全威胁，并对现有加密体制进行升级，应用计算破解能力的后量子加密技术提高了被破解能力，避免信息泄露。

量子位是量子计算的理论基石。在常规计算机中，信息单元用二进制的 1 个位来表

2023-2024 学年第一学期 通信前沿技术讲座 报告

示，它不是处于“0”态就是处于“1”态。在二进制量子计算机中，信息单元称为量子位，它除了处于“0”态或“1”态外，还可处于叠加态。

如下图（a）所示，将电感和电容并联，这个模型称为 quantumharmonic oscillator（QHO）。图（b）给出了各个能级，其间距是相等的，我们可以人为地取基态和第一激发态（|0>和|1>）为量子比特的计算基态。



- 经典比特系统
  - 1 比特：0/1
  - 2 比特：00/01/10/11
  - ……
  - N 比特：2^n 种可能状态
- 量子比特系统与量子态
  - 1 比特：$|\Psi_0\rangle=\alpha_0|0\rangle+\alpha_1|1\rangle;|\Psi_1\rangle=\alpha_2|0\rangle+\alpha_3|1\rangle;$
  - 2 比特：

    $$|\Psi\rangle=|\Psi_0\rangle|\Psi_1\rangle=\alpha_0\alpha_2|00\rangle+\alpha_0\alpha_3|01\rangle+\alpha_1\alpha_2|10\rangle+\alpha_1\alpha_3|11\rangle;$$
  - ……
  - N 比特：$|\Psi\rangle=\sum_{i=0}^{2^n-1}\alpha_i|i\rangle;2^n$ 个连续振幅
- 用经典量子比特存储量子比特

1. 假设 α 只能取 0 或者 1，此时$|\Psi\rangle$只能为$|0\rangle$或者$|1\rangle$（计算基态），量子比特等于经典比特。
2. 假设 α 可以取任意值（量子态的叠加，$|\Psi\rangle=\sum_{i=0}^{2^n-1}\alpha_i|i\rangle$），存储 n 个量

学号：202121018094 **班级：**通信 2102 **姓名：**徐卉垚

2023-2024 学年第一学期 通信前沿技术讲座 报告

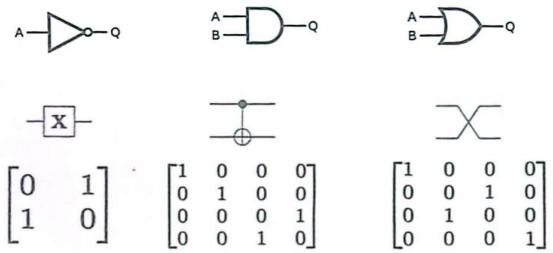
子比特=存储 2^n 个振幅（α）的数值，用 k 个经典比特存储一个振幅，存储 n 个量子比特需要 $k2^n$ 个经典比特。

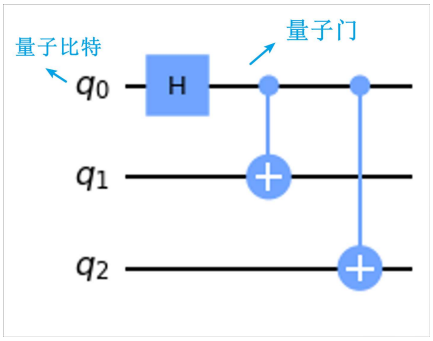
量子态的向量表示：

- 1 比特：$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix}$
- ……
- N 比特：$|\Psi\rangle = \sum_{i=0}^{2^n-1}\alpha_i|i\rangle = \begin{bmatrix}\alpha_0\\ \dots\\ \alpha_{2^n-1}\end{bmatrix}$

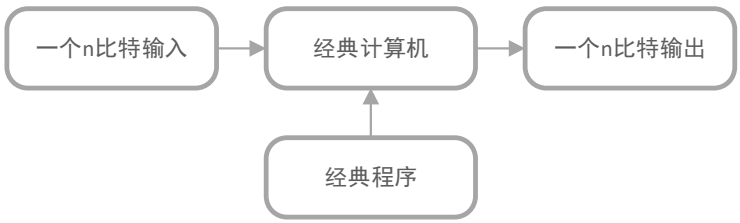
量子操作：可以用一个酉矩阵表示

$$U|\Psi\rangle = U\begin{bmatrix}\alpha_0\\ \dots\\ \alpha_{2^n-1}\end{bmatrix}$$





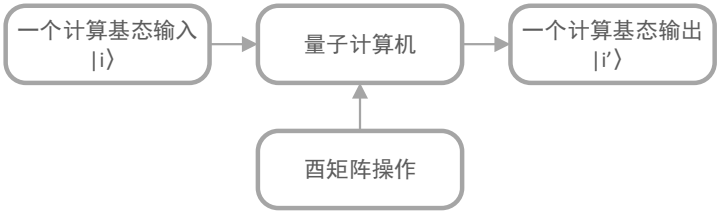
经典计算场景：



学号：202121018094 **班级：**通信 2102 **姓名：**徐卉垚

2023-2024 学年第一学期 通信前沿技术讲座 报告

量子计算场景：



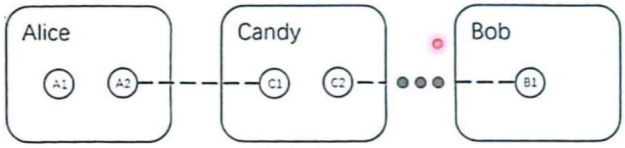
量子态的测量：测量操作的本质是量子态中的量子信息转化为经典信息；测量操作只能返回是否为$|0\rangle$和$|1\rangle$；测量操作可以精准判断$|0\rangle$和$|1\rangle$两种状态；$|\Psi\rangle=\alpha_0|0\rangle+\alpha_1|1\rangle$这种一般的量子态测量结果是概率性的。

量子通信和量子隐形传态：Alice 想要将她所拥有的量子态传输给 Bob

1. Alice 和 Bob 需要共享一对特殊的量子态（纠缠分发）。
2. Alice 在贝尔基上对她所拥有的两个量子态进行测量。得到的测量结果存储在两个经典比特中。
3. Alice 将两个存储测量结果的经典比特信息通过经典信道发送给 Bob。
4. Bob 根据其通过经典信道接收到的测量结果决定其后续执行的量子门操作，使得 Bob 所拥有的量子态等同于 Alice 想要传输的量子态。

量子通信网络：

- 多跳量子隐形传态链路



- 空天量子通信网络

量子计算机的非理想性：

1. 噪声
2. 消相干
3. 串扰
4. 量子操作的误差（门操作、测量操作）
5. 连通性

2023-2024 学年第一学期 通信前沿技术讲座 报告

6. 有限的基本门操作
7. …

算法设计层面解决：分布式算法等；

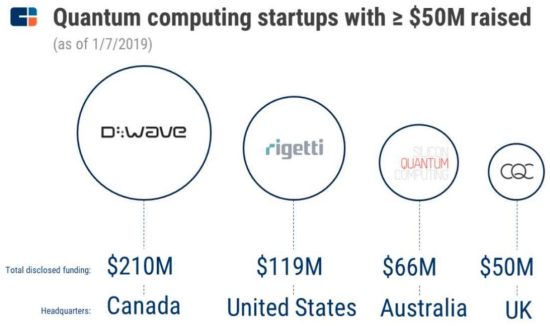
算法软件层面解决：编译、纠错算法等。

量子软件热点：AI for Quantum、量子组网（分布式）。

工业界量子软件平台：IBM、Google、intel、Microsoft、百度量子计算研究所、华为、腾讯、阿里巴巴

三、行业现状

业内只有少数公司能够筹集到至少 5000 万美元(筹集到 1 亿美元以上的公司则更少)，这表明，尽管存在大肆宣传，量子计算机在硬件和软件方面的商业应用目前还处于萌芽状态。



随着整个行业领域的利益增加，支持这些公司发展的整体生态系统也在增长。主流风险投资家和大公司已经开始在初创量子计算公司身上下注。谷歌风投(Google Ventures)和亚马逊等公司都投资了 IonQ，这家公司正在开发通用量子计算机，以应对广泛的应用。这个领域中著名的风投公司包括红杉资本，投资了量子计算硬件公司 Quantum Circuits。安德森·霍罗威茨公司(A16Z)已经投资了 Rigetti Computing；Draper Fisher Jurvetson 已经参与到了对 D-Wave 的多轮投资。2018 年 2 月，随着韩国移动电信运营商 SK Telecom 加入“游戏”，量子计算在通信安全方面的关注也得到了提升，几个月后，德国的 Deutsche Telekom 也加入了进来。这两家电信公司在 6500 万美元的投资中，购买 ID Quantique 的多数股权和少数股权。ID Quantique 提供基于量子技术的多协议网络加密，以确保通信安全。一些世界上最大的公司也在公司内部启动了量子计算项目。在谷歌量子人工智能实验室中，运行着一台 D-Wave 的量子计算机。这个实验室位于加利福尼亚州山景城的 NASA

2023-2024 学年第一学期 通信前沿技术讲座 报告

的 Ames 研究中心，由 NASA 和大学空间研究协会主持。2015 年 7 月，阿里巴巴的阿里云部门和中国科学院在上海建立了一个名为阿里巴巴量子计算实验室的研究机构。 这家实验室研究电子商务和数据中心的量子安全技术。2019 年 1 月，IBM 在 CES 上推出了第一台商用量子计算机。IBM 的 Q System One 使用 20 个量子比特，既有传统计算机的组件，也有量子计算机的组件。这家公司在声明中清楚地表明，商用量子计算机要打败今天的传统计算机还需要时间："IBM Q 系统旨在有朝一日解决目前被认为过于复杂和指数级的问题，而传统系统无法处理这些问题。"包括惠普、英特尔和微软在内的一系列其他科技公司也在部署量子计算。一些国防承包商和咨询公司也开始研究量子计算机，包括：Booz Allen Hamilton、Lockheed Martin、Raytheon 等等。除了公司投资，欧盟、美国、澳大利亚和中国也在支持旨在建造量子计算机的项目。2016 年，中国发射了世界上第一颗量子卫星，以寻求更安全的通信。

随着量子计算资源成本的下降，更多的行业参与者将会出现。随着越来越多的玩家深入到这个行业，量子计算将会在各个行业中有越来越多的应用，特别是那些传统计算机被证明效率低下的一些情况下。

医疗保健：量子计算机可以帮助加快比较不同药物对一系列疾病的相互作用和影响的过程，以确定最佳药物。此外，量子计算还可以带来真正的个性化医疗，利用基因组学的先进技术为每个病人量身定制治疗计划。基因组测序产生了大量的数据，一个人整个 DNA 链表达需要大量的计算能力和存储容量。一些公司正在迅速降低人类基因组测序所需的成本和资源。从理论上来说，量子计算机将使基因组测序更加高效，更容易在全球范围内扩展。量子计算机可以同时收集和整理所有可能的基因变异，并立即找到所有的核苷酸对，使整个基因组测序过程呈指数级缩短。快速量子基因组测序，可以让我们将全世界的 DNA 汇集到一个广泛的人口健康数据库中。利用量子计算机，我们还能够合成世界 DNA 数据中的模式，以便在更深层次上了解我们的基因组成，并有可能发现以前未知的疾病模式。

金融服务：金融分析师通常依赖由市场和投资组合表现的概率和假设组成的算法。量子计算可以帮助消除数据盲点，防止毫无根据的金融假设造成损失。具体来说，量子计算影响金融服务行业的方式是解决复杂的优化问题，如投资组合风险优化和欺诈检测。量子

2023-2024 学年第一学期 通信前沿技术讲座 报告

计算可以用来更好地确定有吸引力的投资组合，因为有成千上万的资产具有相互关联的依赖性，并且可以更有效地识别关键的欺诈模式。金融量子计算机带来的另一个变化，涉及运行业内通常称为蒙特卡洛模拟(Monte Carlo Simulation)的东西，这是一种概率模拟，用于了解风险和不确定性对金融预测模型的影响。传统计算机一次只能搜索一个文件或运行一个投资组合的蒙特卡罗模拟，量子计算机可以并行执行这些操作，并更有效地优化交易。

网络安全：量子计算机可以用来破解我们今天用来保护敏感数据和电子通信安全的密码。然而，量子计算机也可以用来保护数据免受量子黑客攻击，这需要一种被称为量子加密的技术。量子加密是一种将纠缠光子(entangled photons)通过量子密钥分配(QKD)进行远距离传输的想法，目的是保护敏感的通信。最重要的一点是，如果量子加密通信被人截获，加密方案将立即显示中断迹象，并显示通信不安全。这依赖于测量量子系统的行为会破坏系统的原理。这被称为“测量效应”。

农业：量子计算机可以帮助我们更有效地制造肥料。几乎所有有助于养活我们的肥料都是由氨制成的。更有效地生产氨(或替代物)的能力意味着更便宜、更低能耗的肥料。更容易获得更好的肥料将有利于环境，并有助于养活地球上不断增长的人口。但是，在改进制造或替代氨的工艺方面进展甚微，因为可能的催化剂组合数量是无限的。从本质上讲，如果没有 1900 年代被称为 Haber-Bosch Process 的工业技术，我们无法人工模拟这一过程。 这个过程需要极高的热量和压力将氮、氢和铁转化成氨。用今天的超级计算机进行数字化测试，找出合适的催化剂组合来制造氨需要几个世纪的时间。量子计算机将能够快速分析化学催化过程，并提出最佳的催化剂组合来产生氨。此外，我们知道植物根部的一种微小细菌，每天都用一种叫做固氮酶的特殊分子，以非常低的能量成本完成同样的过程。这种分子超出了我们最大的超级计算机的模拟能力，但是量子计算机可以做到。生产高能效肥料只是我们能够通过精确模拟分子行为来解决大问题的许多方法之一。

云计算：量子云计算正在成为行业中一个很有前景的领域。 量子云平台可以简化编程，并提供对量子计算机的低成本访问。QC Ware 公司是一家早期创业公司，正在开发基于云的量子计算平台。QC Ware 的投资者包括空中客车和高盛等公司。包括 IBM、谷歌和阿里巴巴在内的大公司也在部署量子云计算项目。