关于量子计算的认识

作者：赵月悦　　　　学号：1900011403　　　　专业：物理学院

【摘要】

随着集成电路技术逼近工艺极限，传统冯·诺依曼结构计算机面临着计算速度与储存空间难以突破等困难。而量子计算等新型计算技术很好地解决了这一问题。本文简要介绍量子计算机的工作原理，从数学角度描述相关的物理概念，并阐述量子计算的优势，对未来提出展望。

1 量子计算的工作原理

1982 年，Feynman 指出：按照量子力学原则建造的新型计算机对解决某些问题可能比常规计算机更有效。

常规计算机，即冯·诺依曼结构体系下的计算机，所依赖的储存系统所能储存的信息量随着储存单元的数量线性增长。因此即便未来集成电路的储存单元是单个原子，一些计算规模较大的问题也很难在现有算法下，于可接受的时间内得到结果。而且，即使能够达到以单个原子为储存单元的技术，又会出现电流难以稳定、计算受到量子效应影响等屏障，高密度的集成电路还有难以散热的问题，这些困难直接影响集成电路的储存规模。

根据量子力学的原理，一个处于 x 维态空间下的量子系统（记为 ϕ）最多拥有 x 个相互正交的分量，因而需要 x 个复数来描述它，而 n 个 ϕ 组成的新系统则需要 x^n 个复数来描述，这是因为新系统（记为 A）的态是 n 个 ϕ 的态的张量积。也就是说，A 的态的数量随着其子系统 ϕ 的个数呈指数型增加。

于是物理学家和计算机学家们自然地想到，以量子系统为计算机的储存结构，

储存规模会随储存单元的增加而呈指数型增长，从而解决上述传统计算技术面临的问题。

1.1 量子比特

一个量子态可通过希尔伯特空间中的一个复向量来描述，能够描述 n 个可区分量子态的希尔伯特空间的最小维度为 n，那么构造一个最简单的量子计算体系，其储存单元至少拥有两个分量[1]，称一个这样的单元为一个量子比特。在二进制下，引入 Dirac 括号，记|0>和|1>为二维希尔伯特空间的两个正交基，对应于经典比特中的 0 和 1。但不同于经典情况的是，一个经典比特非 0 则 1，但一个量子比特可以处于|0>和|1>的叠加状态，即

$$|\phi\rangle = p|0\rangle + q|1\rangle$$

其中 p、q 满足，

$$|p|^2+|q|^2=1$$

这样的结构可由现实中的二态量子力学系统实现，例如氢电子的基态和第 1 激发态、磁场中核子自旋的两个方向、圆偏振光的左旋和右旋等。

n 个量子比特组成的数据的态，是 n 个量子比特的张量积，拥有 2^n 个相互正交的分量，即

$$|A\rangle=|\varphi_1\rangle\otimes|\varphi_2\rangle\otimes\ldots\otimes|\varphi_n\rangle$$

写成分量形式，

$$|A\rangle=\sum_{00\ldots0}^{11\ldots1} q_i|i\rangle$$

其中 q_i 为概率振幅，$\{q_i \mid i$ 为 n 位二进制数$\}$满足概率归一化条件。

根据量子系统的特性，|A>是 2^n 个基态的叠加，因此这样的结构即能够储存 2^n 个数据。值得注意的是，在测量时|A>将会塌缩成一个状态，也就是说测量时只能读出一个数据，而在上述情况下，|A>可以写成 n 个量子比特的张量积的形式，因此读出数据的第 i 位由$|\varphi_i\rangle$独立决定。但是在某些情况下，多个量子比特组成的量子态无法写成量子比特的张量积形式，则称这多个量子比特处于“纠缠

状态”，最极端的例子如，

$$|A\rangle=q_0|00\ldots0\rangle+q_1|11\ldots1\rangle$$

只要测出数据的其中一位数，就能确定其他位数的数值[2]。不难猜想，满足类似情况的量子态可以用于数据加密传输等领域。

1.2 量子逻辑门

与经典计算相同，量子信息的计算也需要“门”来实现。而量子信息的计算是通过量子态在算法结构下经过幺正变换进行的，因此量子门是可逆的。

例如，量子非门的矩阵形式可表述为 $X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$。量子非门与经典非门相同，有且仅有一个输入端。考虑仅包含一个量子比特的输入，

$$X(\phi)=p\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}+q\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=p|1\rangle+q|0\rangle$$

$$X(X(\phi))=p\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}+q\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=p|0\rangle+q|1\rangle$$

其余量子门也可通过相同的过程证明。

量子计算与经典计算最大的区别在于其可逆性。经典计算机的不可逆性意味着分子的动能一部分会转化为势能和热能[3]，而后者导致集成电路对散热的要求，这种要求随着集成度升高而增大，从而影响经典计算机的计算速度和储存能力，同时不可逆性造成的能耗问题也是建设大型计算机面临的困难之一。而量子计算机通过幺正变换处理信息，既减少散热又降低能耗，为新一代超级计算机的出现奠定了基础。

2.量子计算的优势与发展

量子计算依赖于量子力学原理，与传统的冯·诺依曼结构体系有本质上的区别，一些传统计算机需要耗费大量资源才能完成的任务，量子计算机可以快速高效地完成，一些传统计算机不能解决的问题，量子计算机可以在可接受的时限内解决。下文主要阐述量子计算优势的表现形式

2.1 并行计算

相对于传统计算机，量子计算机最重要的优势是计算速度和储存能力，而这样的优势主要依赖量子计算机特有的并行计算能力。由于，一个包含 n 个量子比特的态 A 可同时储存 2^n 个数据，那么一个算符作用在 A 上时，相当于在计算一次计算所需的时间和储存空间里进行了经典计算机的 2^n 次计算，大大减少了计算所需的资源。

2.2 量子算法

量子计算机的并行计算能力为新算法的出现提供了机会，而新算法的核心在于用何种方式处理并行计算才能以较高的概率测量到观测者希望的结果[4]。

比较经典的量子算法有 Shor 提出的量子并行计算的大数因数分解算法和 Grover 提出的快速的基于无先验结构信息的量子搜索算法。但随着量子计算的进一步发展，量子计算与其他新兴算法的结合成为了热潮。例如量子遗传算法（QGA）引入了希尔伯特空间的复向量表示，比常规遗传算法取得了更好的效果[5]。

2.3 量子计算的未来

量子比特的纠缠态成为量子通信的基础之一，由量子力学原理决定的量子态本身的不可克隆性使由量子比特组成的密码有更高的安全性，可以说量子计算为计算机科学的发展开辟了一条崭新的道路。然而相关理论虽然已经有了基本完善的狂加，但是仍然面临着许多没有解决的困难。例如，以量子比特为单位的态虽然可以同时储存大量数据，但读取时却会引起态的塌缩，因此如何使多次测量称为可能是一个亟待解决的问题。再比如，消相干问题会影响量子比特储存的稳定性，如果不解决，也许会导致信息失真或丢失。总而言之，量子计算同时面临着光明的前景和坎坷的前路，或许未来能打开信息新时代。

参考文献

[1] 王帮海,龚洪波,量子计算与量子信息简介.现代计算机(专业版),2015(22):p.18-22.

[2] 夏培肃, 量子计算. 计算机研究与发展, 2001(10): p. 1153-1171.

[3] 乔佳韵, 浅析量子计算机的原理与应用. 数字通信世界, 2019(06): p. 192+186.

[4] 苏晓琴，郭光灿, 量子通信与量子计算. 量子电子学报, 2004(06): p. 706-718.

[5] 杨俊安 and 庄镇泉, 量子遗传算法研究现状. 计算机科学, 2003(11): p. 13-15+43.