量子计算和量子计算机简述*

李承祖 曾淳 黄明球

(国防科技大学应用物理系 长沙 410073)

摘 要 介绍了量子计算和量子计算机的历史和发展，说明了量子计算机在什么地方超出经典计算机，介绍了量子计算机的原理和网络模型以及量子计算机实现中的困难。

关键词 量子计算，算法复杂性，量子网络，量子位和量子门，关联和脱散

分类号 TP38

Brief Introduction of Quantum Computation and Quantum Computer

Li Chengzu Zeng Chun Huan Mingqu

(Department of Applied Physics, NUDT, Changsha, 410073)

Abstract In this paper, the history and development of quantum computation and quantum computer are reviewed. We explain that in what sense the quantum computer were shown to be more powerful than classical computer, introduce the network model and physics principle of the quantum computer and the difficulty in realization of the quantum computer.

Key words quantum computation, algorithm complexity, quantum network, qubit and quantum gates, entanglement and decoherence

1 量子计算机概念的产生和发展

以计算机科学为核心的信息论和相对论、量子论一起，被称为20世纪科学的三大发现。近20年来，信息论和量子论结合产生了量子信息理论。量子计算机作为量子信息处理的工具，就成为近几年来人们十分关注的问题。

量子计算和量子计算机的概念起源于著名物理学家 Feynman。1982年，Feynman[1] 在研究物理系统的计算机模拟时，论证了用经典计算机模拟量子力学系统，随输入（粒子数、自由度）增大，计算资源（时间和空间）消耗将指数增大，并由此启发了用量子力学性质工作的计算机（量子计算机）可能避免这一困难。1985年，Dentsch[2] 提出了第一个量子计算机的设计蓝图、量子计算机的网络模型，定义了量子 Turing 机，预言了量子计算机的潜在能力。在90年代初，Deutsch，Berthianme 等人就寻找量子计算机可以比经典计算机更有效求解问题的量子算法。1994年，Shor[3] 设计了一个具体的量子算法，可以在量子计算机上，以输入的多项式时间分解大数质因子。分解大数质因子在经典算法复杂性理论中认为是个“难解问题”，现在广泛使用的公开钥密码系统 RSA 就是这个问题的难解为基础的，Shor 算法的发现，使量子计算机研究有了实用背景，因此也获得了新的推动力。1994年以后，量子计算和量子计算机研究出现了迅猛发展的势头。从最初仅是学术上感兴趣的对象，变成了对计算机科学、密码学、通讯技术以及国家安全和商业应用都有潜在重大影响的领域。

2 量子计算机在什么地方超出经典计算机

为了回答量子计算机在什么地方超出经典计算机的问题，需要回顾一下经典计算机科学中的可计

* 1997年11月30日收稿
第一作者：李承祖，男，1944年生，教授

算性和算法复杂性理论。在经典计算机科学中，称一个特殊指定的指令序列为算法，算法的难易程度由算法复杂性衡量。算法复杂性取决于执行这个算法解决具体问题消耗的物理资源多少。一般地限制计算机能力的物理资源有两类：时间和空间。按经典算法复杂性理论，一个问题的大小可以用一个整数 n 表示，n 是指定这个问题需要输入的信息量的度量，如果一个问题的大小是 n，解这一问题的最好算法需要的时间（或计算步数）为 $T(n)$，如果当 n 增大时，$T(n)$ 的增加始终不比 n 的一个多项式函数增加更快，就称这一算法是容易的，在算法复杂性分类中就属于 P 类问题。如果 $T(n)$ 随 n 指数增大，就说算法是难的，属于 NP 类问题。比如分解大数质因子和做两个大数乘法所需计算时间随输入位数 L 的增加的渐近行为显著不同。分解一个 L 位数的质因子大约需要作 $\overline{N} = 10^{L/2}$ 除法。执行这一算法所需计算时间随 L 指数上升。假如使用每秒做 10^{10} 次（10 亿次）的超级计算机，分解一个 20 位数大约需要 1s，分解一个34位大约需要一年，而分解一个60位数所需时间已超出现在估计的宇宙年龄。而两个60位数相乘，用这样的计算机也只是瞬间的事。一个 NP 类问题通常说成是“不可解的”，这是指当具体问题增大时，所需的物理资源是如此之多，以至对任何实际计算设备都是难以承受的。上面的分类不依赖于具体计算设备，这一点由 Church 定理保证：任何一个物理计算装置都可以被经典 Turing 机以多项式资源耗费来模拟。

在经典计算理论中还阐明了某些问题是 NP 完备的概念。对于一个 NP 完备问题，如果能找到一个可以在多项式时间内解决它的算法，即把它转化为 P 类问题，则其它任何 NP 类问题都可转化为 P 类问题。虽然未加证明，经典计算机科学家相信，所有的 NP 类问题似乎都是 NP 完备的。

量子计算机具有超出经典计算机的能力，是通过它能以多项式时间解某些经典计算中非 P 类问题说明的。量子计算机是服从量子力学规律的机器，它可以支持新类型的量子算法。既然 Shor 已经找到了分解大数质因子的快速算法，可以在多项式时间内解决在经典计算机需要指数时间的问题。这就在量子计算机上把一个 NP 类问题转化为 P 类问题（虽然没有证明分解大数质因子是 NP 类问题，但一直没找到解这一问题经典机器多项式算法，很多人相信它是 NP 类的）。这样按照上述经典算法复杂性理论，就有可能把经典计算理论中的某些 NP 类问题在量子计算机上化成易解的 P 类问题。这样经典计算复杂性理论分类在量子计算机上将失去绝对性，原来的以经典 Turing 机为基础的计算复杂性理就需要重新考虑。但是直到最近，仍不能肯定这种推理是否正确，即是否所有的 NP 类问题都能在量子计算机上化成 P 类问题，因为 Shor 的分解大数质因子量子算法，毕竟只是解决了这类问题中一个的量子计算。

1996年，Grover 研制的未加整理的数据库搜索量子算法[4]，是量子计算机可以比经典计算机更有效执行计算任务的另一个例子。Grover 算法中，N 个经典信息串可以以 $1/\sqrt{N}$ 的几率幅的迭加形式存放在量子寄存器中，运行 $\sqrt{N}$ 量级步数的变换，可以使要寻找的信息串以几率幅1表示出来，而经典计算机执行相同的搜索则需要 N 量级的时间。这一算法虽未改变问题的复杂性类，但量子加速甚至比 Shor 分解因子算法还要快得多。由于验证一个问题解比寻找这个问题的解要容易得多，量子搜索算法可以作为解 NP 类问题的最后方法。

量子计算机更重要的实用价值很可能还在物理学本身，已经有人提出了量子多体问题的量子计算机有效模拟算法[5]。前面已经提到在经典计算机理论中，量子力学系统的模拟是个 NP 类问题，用量子计算机模拟量子力学系统可能比任何经典计算机有效得多，而许多量子力学问题的解决，对材料科学、化学以及其它技术科学都会有潜在的巨大价值和实用意义。

3 量子计算机的物理原理和模型结构

任何计算装置都是一个物理系统。量子计算机是根据物理系统的量子力学性质、规律执行计算任务的机器。这里信息以量子态迭加、干涉的形式存贮，计算过程就是对初始态的按照算法要求执行的一系列么正演化，最后测量末态输出计算结果。

已经提出的量子计算机模型之一是量子网络模型，其中要处理的信息载体是量子位，而信息处理则由量子门实现，量子网络则是由量子门通过“线路”连结构成。

在量子计算机中, 充当信息存储单元的物理介质是一个双态量子系统, 称为量子位 (qubit)。比如一个双能级系统或具有两个自旋态的电子、质子等。为了叙述方便, 通常把自旋 $\hbar/2$的电子作为量子位。量子位与经典位不同就在于它可以同时处在两个量子态的迭加态中, 比如

$$\varphi = C_0|0> + C_1|1> \tag{1}$$

C_0, C_1 是两个复常数, $|C_0|^2 + |C_1|^2 = 1$, 其中 $|0>$ 和 $|1>$ 分别表示自旋向下和自旋向上态。所以一个量子位可同时包含有态 $|0>$ 和 $|1>$ 的信息。

若干个量子位的有序集合构成一个量子寄存器。一个二位量子寄存器, 有 4 个独立的态矢 $|00>$, $|01>$, $|10>$, $|11>$, 张起四维矢量空间, 寄存器可以存在这 4 个态的迭加态中, 因此可以同时包含这 4 个态的信息。类似地, 三位量子寄存器的态矢张起 8 维矢量空间, 一个 L 位量子寄存器态矢张起 2^L 维矢量空间, 因而可以存贮 2^L 个不同的经典信息。

对量子位进行的最简单的么正操作称为基本量子门。任何复杂的么正操作, 都可通过量子门的 "通用集合 "组合实现。而一个量子门的 "通用集合 ", 可以由少数几个基本量子门组成。现在已经证明[6], 为了对量子寄存器态执行任意么正变换, 能够产生对单个量子位在 Hilbert 空间中的任意转动和一对量子位间的控制转动操作就足够了, 特别控制 NOT 和一个一位门就足以构成这样的集合。如果记一个量子位的两个基底态分别为 $|0> = \begin{pmatrix}1\\0\end{pmatrix}$ 和 $|1> = \begin{pmatrix}0\\1\end{pmatrix}$ (称为计算基), 量子 NOT 门执行的运算可以由下面的么正矩阵表示:

$$U_{\mathrm{NOT}} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

如果记两量子位基底态为

$$\begin{aligned} |00> &= (1\ 0\ 0\ 0)^{\mathrm{T}} \qquad |01> = (0\ 1\ 0\ 0)^{\mathrm{T}}\\ |10> &= (0\ 0\ 1\ 0)^{\mathrm{T}} \qquad |11> = (0\ 0\ 0\ 1)^{\mathrm{T}} \end{aligned} \tag{2}$$

控制 NOT 门的作用就可用下面的么正矩阵表示

$$U_{\mathrm{XOR}} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \tag{3}$$

在量子计算中有些门操作是没有经典对应的, 例如么正矩阵

$$U_A = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{4}$$

这个门分别演化态 $|0>$ 和 $|1>$ 为迭加态为:

$$\begin{aligned} U_A|0> &= \frac{1}{\sqrt{2}}\left(|0> + |1>\right)\\ U_A|1> &= \frac{1}{\sqrt{2}}\left(|0> - |1>\right) \end{aligned} \tag{5}$$

这个门作用到态为 $|00\cdots0>$ 的 L 位寄存器上, 结果是

$$\begin{aligned} |\varphi> &= U_A \otimes U_A \otimes \cdots U_A|00\cdots0>\\ &= \frac{1}{\sqrt{2}}(|0> + |1>) \otimes \frac{1}{\sqrt{2}}(|0> + |1>) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0> + |1>)\\ &= \frac{1}{\sqrt{2^L}}(|00\cdots0> + |00\cdots1> + \cdots|11\cdots1>)\\ &= \frac{1}{\sqrt{2^L}}\sum_{X=0}^{2^L-1}|X> \end{aligned} \tag{6}$$

在量子寄存器中制备了 2^L 个经典态的等权重迭加态。由于可以制备经典上不同态的迭加态, 量子计算

机对迭加态的演化，就是对其中各个迭加成分的演化，即同时沿着经典上互不相同的路径计算。这就是所谓“量子并行”，量子计算机具有超出经典计算机信息处理能力，就源于它的这种高度并行计算。

4 量子计算机的实现及困难

量子计算机的网络模型，把作用到多个量子位上复杂的么正操作，归结为最基本的么正操作，这些基本么正操作，可以由通用量子门组实现。量子计算机实现首先必须解决量子位和量子门组的物理实现问题。迄今已经提出的实现技术有“离子阱技术”、“核磁共振技术”、“高 Q 光学腔技术”等。已经发现用激光束操纵冷冻在其空阱中的离子串有希望实现少数量子位数百个逻辑门操作。这种技术的主要困难是离子串的冷却和由于噪声引起的“脱散”。

量子计算机实现中最主要的困难是量子计算机系统和环境的相互作用引起计算态的“脱散”问题。脱散使计算机量子态衰变为经典态，而丢失掉计算中的量子信息。一方面量子计算机依赖于量子位之间的关联态迭加而具大有规模并行计算能力，另一方面量子位和环境之间的关联又破坏了量子计算的进行。1996年，Shor，Steane 建立了量子纠错的理论和方法[7]，Shor，Kitaev 等人还提出了量子容错计算的思想，即只要量子位和运算操作中的出错率低于某一阈值，就可以实现任意精度的量子计算。这些理论和技术，使人看到了克服“脱散”困难，最后实现量子计算机的新希望。现在可以说制造量子计算机在原理上已经没有根本性的困难了。但是真正造出一个实际运行的称得上计算机的设备，还需要解决许多技术上的难题。

5 小 结

量子物理与信息论及计算机科学的结合，产生了量子计算。量子计算机系统态的迭加、干涉和关联等量子力学性质提供了计算的新的物理资源，这种资源的开发和应用正引起信息理论和计算机科学重要的变革。量子计算机实现已不存在原则性的困难，但是克服复杂的技术问题可能还需要走很长的路程。

参考文献

1Feynman R P. Simulation physics with computers, Int. J. Theor. Phys, 1982, 21: 467- 488

2Deutsch D. Quantum theory, the Church- Turing Principle and the universal quantum computer. Proc. Roy. Soc. Lond., 1985, A 425: 73- 90

3Shor P W. Polynomial- time algorithms for prime factorization and discrete logarithms on a quantum computer. in Proc, 35th Annual symp on Foundations of Computer Science, Santa Fe, IEEE Computer Society Press; 1994, revised version, 1995

4Grover L K. Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett, 1997, 79: 325- 328

5Abrams D S et al. Simulation of manybody Fermi systems on a universal quantum computer (preprint quant- ph/9703054)

6DiVincenzo D P. Two- bit gates are universal for quantum computation. Phys. Rev. 1995, A51: 1015- 1022

7Shor P W. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A. 1995, 52: R2493- 2496

8Kitaev A. Fault- tolerant quantum computation by anyone (Preprint quant- ph/9707021)