量子计算与量子计算机展望*

林 雄[1]，林 帅[2]
（1. 琼州大学 电子信息工程学院，海南 三亚 572022；
2. 四川大学 软件学院，四川 成都 610207）

摘 要：量子计算和量子计算机的研究是当代信息科学所面临的一个重大科学课题。阐述了量子计算、量子逻辑门的基本概念和 Shor 算法，指出了当前实现大规模量子计算所遇到的困难和可能的解决办法。

关键词：量子计算；量子逻辑门；Shor 算法；量子计算机
中图分类号：O413 **文献标识码**：A **文章编号**：1674-7720(2012)22-0004-03

Quantum computing and prospects of quantum computers

Lin Xiong[1], Lin Shuai[2]
(1. College of Electronic and Information Engineering, Qiongzhou University, Sanya 572022, China;
2. Software Engineering College, Sichuan University, Chengdu 610207, China)

Abstract: The study of quantum computing and quantum computers is a major scientific subject of contemporary information science research. This article gives an introduction to quantum computing, describes the basic concepts of quantum logic gates and Shor's algorithm, points out the difficulties encountered in the current large-scale quantum computing and possible solutions.

Key words: quantum computing; quantum logic gates; Shor's algorithm; quantum computers

1982 年，FEYNMAN R 首先提出量子计算的概念，但当时没有受到重视。1985 年，英国牛津大学的 DEUTSCH D 初步阐述了量子图灵机的概念[1]，并且指出量子图灵机可能比经典图灵机具有更强大的功能。1995 年，SHOR P 提出了大数因子分解的量子算法，并有其他人演示量子计算在冷却离子系统中实现的可能性。这时，大家才认识到量子计算机的超强计算能力，特别是破解编码的能力，之后就有很多研究学者加入这方面的研究。

1 量子计算

经典计算的输入态和输出态都是经典信号，用 0 和 1 作为信息的基本单位，在实际操作上则以电流在逻辑电路上的导通和截止或电压的高和低来完成各种逻辑运算。量子计算以量子力学为基础，其计算的基本单位是量子比特(qubit)，即经典比特状态的 0 和 1 必须由两个量子态|0>和|1>来替代。任意两态量子体系都可成为量子信息的载体，如二能级原子、分子或离子、光子偏振态或其他等效的自旋 1/2 的粒子。经典比特可以看作量子比特的特例(α=0 或 β=0)。典型的量子计算有 Shor 的大数因子分解和 Grover 的数据库量子搜索。

量子力学认为，所有的输入态和输出态都是某一力学量的本征态[2]。如输入二进制序列为 0110110，可用量子态|0110110>表示。与经典计算不同的是，经典计算认为所有的输入态皆相互正交。因此，对经典计算机不可能输入如下的叠加态：

$$|\psi>=\alpha|0>+\beta|1>,\quad |\alpha|^2+|\beta|^2=1 \tag{1}$$

即$|\psi>$处于态|0>的概率为$|\alpha|^2$，而处于态|1>的概率为$|\beta|^2$，除非检测到额外的信息才可知其值。

式(1)表明，原子可以同时处于|0>和|1>两个态，此时对应的是量子比特。如果以|0>和|1>这两个独立态为基矢，张开 1 个二维矢量空间，就可以说是 1 个二维的 Hilbert 空间。一般地，n 个 qubit 的态张起 1 个 2^n 维 Hilbert 空间，存在 2^n 个互相正交的态，通常取 2^n 个基底态为$|i>$，i 是一个 n 位二进制数。因此，n 个量子位的一般态可以表示为 2^n 个基底态的线性叠加，即：

* 基金项目：教育部科学技术研究重点项目(208110)；三亚市院地科技合作项目(2011YD18)

$$|\psi>=\sum_i C_i|i> \quad (2)$$

式中，i 分别取 0 和 1；C_i 为复系数，且满足 $\sum_i |C_i|^2=1$。

此外，由于量子的相干性，量子比特在测量过程中会表现出与经典情况完全不同的行为。在经典力学中，至少在理论上可以构造理想的测量，使得测量本身不会本质地改变被测体系的状态。而在量子力学中则不然，测量仪器与被测系统的相互作用会引起波包塌缩。

设|0>和|1>是力学量 A 的本征态，相应的本征值是 a_0 和 a_1。在|ψ>上对 A 进行测量，一旦单一的测量得到了值 a_0，波函数便塌缩到|0>上。这时|ψ>的相干性将被彻底破坏，即发生了所谓的量子退相干。正如在中子干涉问题中，一旦通过测量观测到中子到达屏的路径，干涉条纹将不复存在，这就是量子测量坍塌原理[3]。

对于两个比特的量子系统有 4（即 2^2）种不同的状态，即两个比特都在|0>上的状态|00>、两个比特都在|1>上的状态|11>、第一个比特在|0>上同时第二个比特在|1>上的状态|01> 以及第一个比特在|1>上同时第二个比特在|0>上的状态|10>。如：

$$|\psi>=\frac{1}{\sqrt{2}}(|01>+|10>) \quad (3)$$

|ψ>描述了处在自旋单态上的双电子体系，其中|1>代表电子自旋向上的状态，|0>代表电子自旋向下的状态。测量第一个电子的自旋，可以 50%几率得到向上的电子和 50%向下的电子；当第一个电子被发现向下，整个波函数被塌缩到态|01>上。这时，再测量第二个电子，必得到自旋向下的确定的结果。即使两个电子分开很远，这种关联仍然存在。

2 量子逻辑门

量子逻辑门是一个对特定的量子比特在一段时间间隔实现逻辑变换的量子逻辑线路，它是量子线路的基础。与传统逻辑门不同，量子逻辑门是可逆的。

量子逻辑门使用幺正（酉）矩阵表示。常见的量子逻辑门一般只针对一个或两个量子比特进行操作，这表明这些量子逻辑门可以用 2×2 或者 4×4 的幺正矩阵表示。操作 k 个量子比特的逻辑门可以用 $2^k\times 2^k$ 的幺正矩阵表示。一个逻辑门输入与输出的量子位数量必须相等。量子逻辑门的操作可以用代表量子逻辑门的矩阵与代表量子比特状态的向量作相乘来表示。

量子逻辑门是量子计算与量子计算机实现的基础，可用下列方法实现[4]：(1)量子点系统；(2)超导约瑟夫森(Josephson)结系统；(3)核磁共振量子系统；(4)离子阱系统；(5)腔量子电动力学系统等。

量子逻辑门按照其作用的量子位的数目可分为单比特门、二比特门和三比特门等。其中，常用的单比特门有哈达玛门 Hadamard(简记为 H)、Pauli-X 门、Pauli-Y 门等；常用的二比特门有可控非门(Controlled-NOT)、对换门(Swap)等；而常用的三比特门有三位非门(Toffoli)等。

3 Shor 算法

1994 年，贝尔实验室计算机科学家 SHOR P 发表了一种快速进行因数分解的方法，算法利用量子计算的并行性，对任意大的整数快速做因数分解，大大降低了当前普遍使用的 RSA(Rivest-Shamir-Adleman)公开密钥加密技术的破解时间。

Shor 算法包含两个部分：一个以传统的电脑运作的简化算法，将因子分解简化成搜寻目的问题，使用辗转相除法计算 $\gcd(a,N)$；一个量子算法，解决搜寻目的问题。

量子算法的核心是对处于叠加态|x>进行幺正变换 U_f，产生每个 x 对应的|f(x)>，即：

$$U_f:\sum_{x=0}^{2^n-1}|x,0>\rightarrow\sum_{x=0}^{2^n-1}|x,f(x)> \quad (4)$$

故量子计算的一次运算相当于经典的 2^n 次运算。量子态的这种特性称为量子并行性。

下面介绍量子算法的步骤[5]：

(1) 设待分解的数为 N，取 $N^2\leqslant q\leqslant 2N^2$，且 $q=2^L$。假设有两个量子寄存器，第一个有 L 个量子位，存放初始输入值 x，第二个用于存放函数值 $f_{a,N}(x)$。由于 $f_{a,N}(x)$ 不可能大于输入值 x，第二个寄存器存放最多 L 个量子位。对第一个寄存器用 H^L 变换制备出初始态：

$$|\psi_1>=\frac{1}{2^{L/2}}\sum_{x=0}^{2^L-1}|x>,\text{而 } H=\frac{1}{\sqrt{2}}\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix} \quad (5)$$

(2) 保持第二寄存器仍处在$|0>^L$态上，计算函数 $f_{a,N}(x)=a^x(\mathrm{mod}\ N)$，并把结果放到第二个寄存器中，得到两个寄存器的纠缠态：

$$U_f:|\psi_1>\rightarrow|\psi_2>=\frac{1}{2^{L/2}}\sum_{x=0}^{2^L-1}|x>|f(x)>=\frac{1}{2^{L/2}}\sum_{x=0}^{2^L-1}|x>|a^x(\mathrm{mod}\ N)> \quad (6)$$

如果 $x<2^L$，将 x 展开为二进制表示：

$$x=x_{L-1}2^{L-1}+x_{L-2}2^{L-2}+\cdots+x_0 \quad (7)$$

从而：

$$a^x(\mathrm{mod}\ N)=\left(a^{2^{L-1}}\right)^{x_{L-1}}\left(a^{2^{L-2}}\right)^{x_{L-2}}\cdots(a)^{x_0}(\mathrm{mod}\ N) \quad (8)$$

由于

$$a^{2^j}=\left(a^{2^{j-1}}\right)^2 \quad (9)$$

式(8)可以从 0~$L-1$，当 $x_j=1$ 时，就乘以 a^{2^j}，由此可见实现式(6)最多用 $L-1$ 个计算步骤完成。

(3) 对第二寄存器在计算机上进行测量。假定测量结果是 Z，其中 $Z\in\{a^x\ (\mathrm{mod}\ N)\}$，由于函数 $f_{a,N}(x)$ 的周期为 r，所以：

$$a^l(\mathrm{mod}\ N)=a^{jr+l}\ (\mathrm{mod}\ N) \quad (10)$$

式中，$l\leqslant r$；$j=0,1,\cdots,A$；A 是小于 $(2^L-l)/r$ 的最大整数；x 的取值为：

$$x=l,l+r,\cdots,l+Ar \quad (11)$$

当第二个寄存器坍塌时，第一个寄存器相应地坍塌为：

$$|\psi_1\rangle=\frac{1}{\sqrt{A+1}}\sum_{j=0}^{A}|l+jr\rangle \tag{12}$$

可以看出，第一寄存器是以 r 为周期的一组态的叠加，有关 r 的信息包含在第一寄存器中，由于 l 值未知，对 $|\psi_1\rangle$ 的测量不能给出 r 的精确值。如果 2^L 是 r 的整数倍，令 $A=q/r-1$，则：

$$|\psi_1\rangle=\sqrt{\frac{r}{q}}\sum_{j=0}^{q/r-1}|l+jr\rangle \tag{13}$$

对第一寄存器作量子傅里叶变换，$\mathrm{QFT}:|\psi_1\rangle\rightarrow\sum_c\tilde{f}(c)|c\rangle$，其中

$$\tilde{f}(c)=\frac{\sqrt{r}}{q}\sum_{j=0}^{q/r-1}\mathrm{e}^{2\pi\mathrm{i}(l+jr)c/q}=\frac{\sqrt{r}}{q}\mathrm{e}^{2\pi\mathrm{i}lc/q}\sum_{j=0}^{q/r-1}\mathrm{e}^{2\pi\mathrm{i}jrc/q} \tag{14}$$

因为：

$$\sum_{j=0}^{q/r-1}\mathrm{e}^{2\pi\mathrm{i}jrc/q}=\begin{cases}q/r, & \text{若 } c \text{ 为 } q/r \text{ 的整数倍}\\ 0, & \text{其他}\end{cases} \tag{15}$$

所以：

$$\tilde{f}(x)=\begin{cases}\frac{1}{\sqrt{r}}\mathrm{e}^{2\pi\mathrm{i}lc/q}, & \text{若 } c \text{ 为 } q/r \text{ 的整数倍}\\ 0, & \text{其他}\end{cases} \tag{16}$$

量子傅里叶变换使所需结果增强，并使不需要的结果为零。若 $c=kq/r$，则：

$$|\psi_1\rangle_{\mathrm{QFT}}=\frac{1}{\sqrt{r}}\sum_{j=0}^{q/r-1}\mathrm{e}^{2\pi\mathrm{i}lk/r}|kq/r\rangle \tag{17}$$

可见，量子傅里叶变换使第一寄存器的周期从 r 变为 q/r，l 已不复存在于第一寄存器的测量结果中。

(4) 测量第一寄存器得到 c'，由于 $c'=kq/r$，所以 $k/r=c'/q$。因为 c' 和 q 是已知的，如果 $\gcd(k,r)=1$，可求出 r，最大的 r 即是 $f(x)$ 的周期，至此算法结束。

4 量子计算机展望

量子计算机是实现量子计算的机器，它是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。量子计算机以处于量子状态的原子作为中央处理器和内存，应用的是量子比特，可以同时处于多个状态。

据称世界第一台通用编程量子计算机 2009 年在美国国家标准技术研究院诞生。然而，迄今为止，世界上还没有真正意义上的量子计算机。现在的实验只制备出单个的量子逻辑门，远未达到实现计算所需要的逻辑门网络。科学家也只能同时控制约 10 个量子比特，量子计算机至少需要几十个量子比特才能解决现实世界中的问题，进而成为一种可行的计算方式。目前已经提出利用原子和光腔相互作用、冷阱束缚离子、电子或核自旋共振、量子点操纵、超导量子干涉等实现量子计算方案。现在还很难说哪一种方案更有前景，只是量子点方案和超导约瑟夫森结方案更适合集成化和小型化。将来也许现有的方案都派不上用场，最后脱颖而出的是一种全新的设计，而这种新设计又是以某种新材料为基础。

实现量子计算的另一个困难是可集成性问题，可集成性最核心的问题不是将几个量子比特组装到一起，而是能相干地操控这些量子比特。作为量子计算机最终实现的要求，量子比特体系要有长的相干时间，基本的门操作的精度要能够达到容错量子计算的阈值之内。这是最核心的技术指标，只有这个目标实现了，才能实现真正意义上的多位量子计算机，从而物理体系的可集成性最终才能体现价值。

2007 年 12 月，中国科技大学的潘建伟领导小组[6]选择光子比特这样一种抗退相干能力强、单比特操纵精确的物理体系，系统地发展了一套国际领先的多光子相干操纵和纠缠态制备的实验技术。他们与牛津大学研究人员合作，在国际上首次用光子比特、也是首次用真正的纯态量子系统，实验演示了关键性的 Shor 算法，实现了 15=3×5 这一质因子分解，并且确认了量子计算中多体纯纠缠的存在，验证了量子加速的根本原因。

已经取得的研究表明，实现量子计算已经不存在原则性的困难。按照现在的发展速度，可以比较肯定地预计，在不久的将来，量子计算机一定会成为现实。到那时，量子计算将能够轻松地破解银行帐号、商业和电子商务数据使用的密码。而当今使用的基于 RSA 的加密算法公开密钥体系将不再有安全可讲。

参考文献

[1] DEUTSCH D. Quantum theory, the Church-Turing principle and the universal quantum computer[M]. Proceeding of the Royal Society of London A400, 1985:97-117.

[2] 维基百科.量子计算机[EB/OL].[2012-06-20].http://zh.wikipedia.org/wiki.

[3] 林帅,林雄.量子密码通信及其研究进展[J]. 电脑与信息技术, 2012,20(6):13-15.

[4] 周正威,徐涛,龚明,等. 量子计算的进展和展望[J].物理学进展,2009,29(2):127-165.

[5] 赵生妹,郑宝玉. 量子信息处理技术[M]. 北京:北京邮电大学出版社, 2010.

[6] 微尺度实验室.潘建伟等在国际上率先实现量子分解算法[EB/OL].(2007-12-19).中国科大报,第 595 期.http://news.ustc.edu.cn/kdb/200805/t20080519_62409.html.

(收稿日期:2012-08-19)

作者简介：

林雄，男，1962 年生，教授，主要研究方向：计算智能和软件开发。

林帅，男，1991 年生，本科在读，主要研究方向：信息安全。