通向通用量子计算机之路*

薛 飞† 杜江峰 周先意 韩荣典

(中国科学技术大学近代物理系 合肥 230026)

摘 要 量子计算机对信息的处理和计算与经典计算机相比有很大的优越性. 可编程量子计算器件是建造通用量子计算机的一个重要部分. 文章介绍了可编程量子计算中的一些主要结果,其中包括:建造通用可编程量子计算器件的困难;两类解决方案(概率的和精确的可编程量子计算器件,确定的和近似的可编程量子计算器件);通过量子软件控制的量子测量方案. 最后简要介绍了量子计算机物理实现的几个主要方向和未来的展望.

关键词 通用量子计算机,可编程逻辑门,量子中央处理器

Toward a general purpose quantum computer

XUE Fei† DU Jiang-Feng ZHOU Xian-Yi HAN Rong-Dian

(*Department of Modern Physics, University of Science and Technology of China, Hefei* 230026, *China*)

Abstract Quantum information processing has great advantages in information processing and computation. The design of a programmable quantum computation apparatus is an important step toward building a general purpose quantum computer (QC). We review recent progress in this field, including the impossibility of building an arbitrarily programmable QC, as well as the design of QCs with probabilistic and precise programming, determinate and approximate programming, and a quantum measuring apparatus controlled by software. Finally, a simple introduction to thephysical realization of QCs and future prospects is presented.

Key words programmable, quantum CPU, computation

1 引言

量子力学和信息学这两个看似相隔遥远的学科,其结合却产生了一个可能在根本上影响人类未来发展的交叉学科——量子信息学. 20 世纪后半叶,人类进入信息时代,计算机的发展日新月异,然而随着计算机芯片的集成度越来越高,元件越做越小,集成电路技术现在正逼近其极限,而且尽管计算机的运行速度与日俱增,但是有一些难题是现有计算机根本无法解决的,例如大数的因式分解. 几十年前,该领域的一些先驱者,如美国 IBM 公司的 Charles H. Bennett 等人就开始研究信息处理电路未来的去向问题,他们指出,当计算机元件的尺寸变得非常之小时,我们不得不面对一个严峻的事实:现有经典的描述不再适用,必须用量子力学来对它们进行描述. 进入 20 世纪 90 年代,实验技术和理论模型的进步为量子计算机的实现提供了可能. 尤其值得一提的是,1994 年美国贝尔实验室的 Peter W. Shor 证明运用量子计算机竟然能有效地进行大数的质因式分解. 这意味着以大数质因式分解算法为依据的电子银行、网络等领域的 RSA 公开密钥密码体系将在量子计算机面前不堪一击,几年后 Grover 提出的"量子搜寻算法",可以破译 DES 密码体系. 于是各国政府纷纷投入大量的资金和科研力量进行量子计算机的研究,如今这一领域已经形成一门新的

* 国家自然科学基金(批准号:10075041, 10075044)、国家重点基础研究发展计划(批准号:2001CB309300)资助项目

2003 - 11 - 05 收到初稿,2004 - 02 - 13 修回

† 通讯联系人. E-mail:Feixue@ustc.edu

学科——量子信息学.

量子力学在通信方面的应用产生了量子保密通信,在计算方面的应用则产生了量子计算机. 迄今为止,世界上还没有真正意义上的量子计算机. 但是,世界各地的许多实验室正在以巨大的热情追寻着这个梦想. 本文主要介绍实现可编程的量子计算机的各种设计方案,最后简单介绍了量子计算机物理实现的几个主要方向.

2 经典信息和量子信息

2.1 经典信息和量子信息

经典信息以比特(bit)作为信息基本单元,1 个比特代表具有两个可识别状态的抽象实体,例如是或非,真或假,0 或 1. 一般采用二进制数据位,每一个二进制数据位表示一比特信息. 从物理的角度讲,1 个比特是物理上能实现的系统或装置,例如电容器极板间的电压可以表示一比特信息:电容器有荷电时表示 1,而无电荷时表示 0. 比特这个术语有双重涵义:第一作为信息测量的基本单位,给出一个"是或非"问题的答案;第二表示存贮、传送信息的基本物理体系.

量子信息采用量子比特(qubit)或量子位作为信息基本单元,是比特的量子推广. 量子比特在物理上可以用两态量子系统来实现,例如两种偏振态的光子(水平和垂直偏振)、磁场中自旋为 1/2 的粒子(自旋向上和向下)、两能级的原子或离子(基态和激发态)以及量子系统的空间模式(例如光子)等等. 1 个量子比特可以处于两个逻辑态 0 和 1 的任意叠加,即

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \leftrightarrow \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \qquad (1)$$

式中 α,β 为任意复数,满足归一化条件 $|\alpha|^2 + |\beta|^2 = 1$. $|0\rangle$和$|1\rangle$为正交基,通常称为计算基态(基矢). 以这两个独立量子态作为基矢,张起 1 个二维复矢量空间,称为二维希尔伯特(Hilbert)空间,则 1 个量子比特就是这个二维希尔伯特空间的单位矢量. 因此,也可以用 1 个单位球面上的点(见图 1)表示 1 个量子比特的纯态,由欧拉(Euler)角 θ 和 φ 决定(整体的相因子通常可以忽略),这个球被称为布洛赫(Bloch)球. 经典比特可看成量子比特的特例(令 $\alpha=0$ 或 $\beta=0$),对应于布洛赫球上的两个极点,1 量子比特信息包含了 1 比特 的信息,同时连续变化,可以覆盖整个球面,所以 1 量子比特可以运载更多的信息量. 与比特类似,量子比特这个术语有双重涵义:第一,作为量子信息测量的基本单位;第二,表示存贮、传送量子信息的基本物理体系,在下文中有时为了明确区分,有时会用寄存器表示存储量子信息的体系,而使用量子位表示量子信息测量的基本单位.

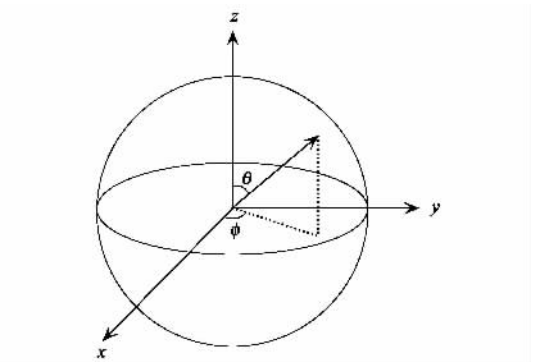

图 1 布洛赫(Bloch)球

2.2 经典逻辑门与量子逻辑门

在经典计算机中,信息的处理是通过逻辑门进行的. 已经证明,任意复杂的逻辑运算都能分解为一些"通用逻辑门组"的组合,"通用逻辑门组"的例子有:"AND"和"NOT"门,"OR"和"NOT"门,"XOR"和"AND"门. 一系列的逻辑门按照一定的顺序连接起来形成电路,可以完成各种各样不同的计算,这就是计算的电路模型,后面我们会经常用电路模型来描述量子计算器件. 对于一个逻辑门组成的电路,主要通过考察两种资源的消耗来衡量它的复杂性:使用逻辑门的数目和需要的比特数目.

量子计算中也有通用量子逻辑门,通过通用量子逻辑门的组合能够完成任意复杂的量子运算. 例如两量子位控制非门(CNOT 门)和对单量子位进行任意操作的量子逻辑门可以构成一个通用量子逻辑门组;几乎所有的两量子位逻辑门或 n 位量子逻辑门($n\geqslant 2$)都可以构成通用量子逻辑门组. CNOT 门的电路符号如图 2 所示. 在这里介绍两个量子逻辑门:单量子位旋转门[$R_i(\varphi)$]及两量子位控制非门(CNOT 门). 单量子位旋转门完成一个非常简单的量子操作,其量子逻辑功能是使该量子位绕 i 轴旋转 φ 角,即 $|\psi_0\rangle \xrightarrow{R_i(\varphi)} e^{i\frac{\varphi}{2}\sigma_i}|\psi_0\rangle$,($i = x, y$ 或 z). 两量子位的 CNOT 门完成这样的量子逻辑功能:根据控制位的值对目标位进行操作,具体地说,就是仅当控制位处在$|1\rangle$态时,才对目标位进行 NOT 操作,否则不变化. 例如,第一个量子比特为控制位,第二

个量子比特为目标位的 CNOT 门的逻辑功能为

$$|00\rangle \xrightarrow{\text{CNOT 12}} |00\rangle,$$
$$|01\rangle \xrightarrow{\text{CNOT 12}} |01\rangle,$$
$$|10\rangle \xrightarrow{\text{CNOT 12}} |11\rangle,$$
$$|11\rangle \xrightarrow{\text{CNOT 12}} |10\rangle. \quad (2)$$

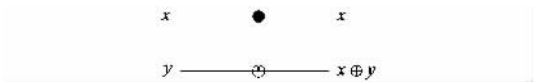

图 2　CNOT 12 门的电路符号

2.3　量子信息与经典信息相比的重要特点

(1)量子叠加性. 量子力学系统的状态可以由希尔伯特空间的矢量完全描述,能处在所有对应经典逻辑态的任意线性叠加态上,量子叠加性是量子并行计算的重要物理基础. 叠加原理中的叠加是几率幅的相干叠加,依靠几率幅之间的相对相位关系,叠加振幅可以相互干涉,出现彼此相长或相消,此即量子相干性.

(2)量子态随时间演化的幺正性. 孤立量子系统的态矢量$|\psi\rangle$随时间的演化遵从薛定谔方程

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = \hat{H}|\psi\rangle, \quad (3)$$

其中 $\hat{H}$ 为系统的哈密顿量. 孤立量子系统态矢的演化可以引入幺正演化算子 $U(t,t_0)$ 描写. $U(t,t_0)$ 定义为

$$|\psi(t)\rangle = U(t,t_0)\,|\psi(t_0)\rangle. \quad (4)$$

(3)量子态不可克隆性. 量子力学的线性特性禁止对一个未知的量子态进行精确的复制(克隆).

(4)量子测量公设. 观测任意量子态$|\psi\rangle$中的力学量 F,相应于将被测态$|\psi\rangle$按对应的厄米算符 $\hat{F}$ 的本征态族展开,即 $|\psi\rangle = \sum c_n |\psi_n\rangle$,测量所得的数值是不确定的,按 $|c_n|^2$ 的几率得到 $\hat{F}$ 的本征值之一 F_n,而整个量子态将坍缩到相应的本征态$|\psi_n\rangle$. 这种测量坍缩过程是随机的、不可逆的、斩断相干的和非定域性的. 由于测量量子计算结果输出的不惟一性,因此在计算过程中,只有充分利用几率幅的相长或相消干涉,尽可能增大需要结果出现的概率,同时减小不需要结果出现的概率,使对计算末态的测量以最大的概率得到需要的结果,完成量子计算的过程.

3　通用量子计算机

通用量子计算机就像我们现在使用的个人计算机一样,具有固定的硬件设置,通过不同的量子软件来完成不同的量子计算. 量子软件是一些经过特别设计的量子态,可以输入到量子计算机中,使量子计算机执行特定的任务. 通用量子计算机的设计是建造实用量子计算机的一个重要部分. 通用量子计算机设计中的一个重要部分是实现可编程的量子计算器件,用操作 G 表示,作用在任意的输入态上,输入态由程序态$|P_U\rangle$和数据态$|D\rangle$组成,操作 G 可以完成这样的操作,把程序态$|P_U\rangle$描述的幺正操作 U 作用在数据态$|D\rangle$上,即

$$G(|P_U\rangle \otimes |D\rangle) = |P_U'\rangle \otimes (U|D\rangle), \quad (5)$$

式中⊗表示直积. 可编程量子计算器件的电路如图 3 所示.

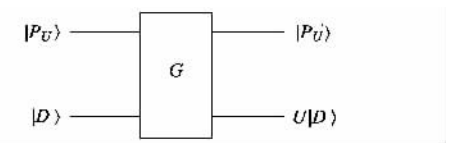

图 3　可编程量子计算器件的电路表示

3.1　不存在实现任意幺正操作的可编程量子计算器件

Nielsen 和 Chuang 说明了不存在确定性的和精确的实现任意幺正操作的可编程量子计算器件[1]. 他们假设$|P\rangle$和 $|Q\rangle$是两个程序态,分别实现不同的幺正操作 U_p 和 U_q,U_p 和 U_q 是不同的(即使忽略整体相位因子),对于任意的数据态$|D\rangle$,有

$$G(|P\rangle \otimes |D\rangle) = |P'\rangle \otimes (U_p|D\rangle), \quad (6)$$
$$G(|Q\rangle \otimes |D\rangle) = |Q'\rangle \otimes (U_q|D\rangle). \quad (7)$$

对上面两式做内积,得

$$\langle P|Q\rangle = \langle P'|Q'\rangle(\langle D|U_p^{\dagger}U_q|D\rangle). \quad (8)$$

假设$\langle P'|Q'\rangle \neq 0$,使其被上式两边同除,得

$$\frac{\langle P|Q\rangle}{\langle P'|Q'\rangle} = (\langle D|U_p^{\dagger}U_q|D\rangle). \quad (9)$$

上式左边与数据态$|D\rangle$无关,因此有 $U_p^{\dagger}U_q = \gamma I$,$\gamma$ 是复数,即,U_p 和 U_q 是相同的(忽略整体相位). 于是,要使$\langle P'|Q'\rangle \neq 0$,只能令 U_p 和 U_q 是相同的(忽略整体相位). 但我们已经假设 U_p 和 U_q 是不同的(忽略整体相位),故产生矛盾,因此有$\langle P'|Q'\rangle = 0$. 然后由(8)式得$\langle P|Q\rangle = 0$,这说明$|P\rangle$和

$|Q\rangle$是正交的,即对于任意不同的幺正操作,都必须使用正交态来编码. 然而即使是在单量子位上也有无穷多个不同的幺正操作,而一个量子比特只能编码两个正交态,这样一个量子位上的幺正操作就需要无穷多个量子比特来编码,因此可以得到这样的结论:确定性的和精确的实现任意幺正操作的可编程量子计算器件实际上是无法实现的.

3.2 概率的和精确的可编程量子计算器件

虽然 Nielsen 和 Chuang 说明了不存在确定性的和精确的可编程量子计算器件,可是我们仍然可以构造其他类型的可编程量子计算器件.

第一个概率的和精确的可编程量子计算器件的设计就是由 Neilsen 和 Chuang 给出的[1],如图 4 所示(所谓"概率的"是指该器件实现编程的操作不是一定会成功,有一定概率会成功地实现编程的操作,也有一定概率不能成功地实现编程的操作). 图中虚线框中的部分对应于可编程逻辑门阵列 G. 设 U 是要对数据态 $|d\rangle$进行的幺正操作,相应的程序态为

$$|P_U\rangle = (I \otimes U)|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle U|0\rangle + |1\rangle U|1\rangle),$$

其中 I 表示恒等操作,即不进行任何操作,$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 是一个 Bell 态. Bell 态的定义为:

$|\Phi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\Psi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$.

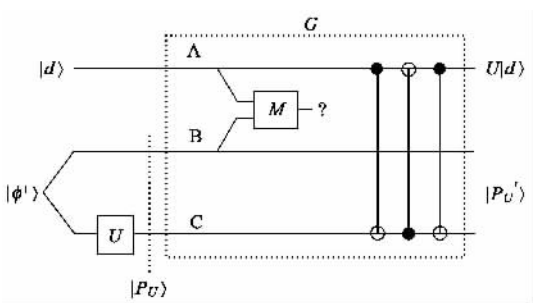

图 4 Neilsen 和 Chuang 的可编程量子计算器件设计

这类可编程量子计算器件是这样工作的:设有一个数据态 $|d\rangle = a|0\rangle + b|1\rangle$,其中 a,b 是复数,并满足归一化条件 $|a|^2 + |b|^2 = 1$,这时可编程量子计算器件 G 的输入态 $|d\rangle|P_U\rangle$ 为

$$(a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle U|0\rangle + |0\rangle U|0\rangle). \quad (10)$$

它可以表示成

$$\frac{1}{2}(|\Phi^+\rangle U|d\rangle + |\Phi^-\rangle U\sigma_z|d\rangle + |\Psi^+\rangle U\sigma_x|d\rangle + i|\Psi^-\rangle U\sigma_y|d\rangle), \quad (11)$$

式中 σ_x,σ_y,σ_z 为泡利矩阵,可以看到当测量(M)得到$|\Psi^+\rangle$的本征值时,储存程序态的第二个量子比特 C 的状态为 $U|d\rangle$,用 3 个 CNOT 门把它交换到数据寄存器上后,就可成功地实现对数据态 $|d\rangle$的幺正操作 U.

本方案有如下特点:

(1)针对单量子比特操作;

(2)需要事先准备纠缠态;

(3)需要进行测量才能确定操作是否完成;

(4)测量后通过测量结果可以知道操作是否成功;

(5)可编程量子计算器件 G 成功完成对数据态 $|d\rangle$的幺正操作 U 的概率为 1/4;

(6)本方案成功时,所实现的幺正操作 U 是精确的.

3.3 另一种概率的和精确的可编程量子计算器件

2001 年,Vidal 和 Kim 等人提出了一个不需要事先准备纠缠态的概率的和精确的可编程量子计算器件设计[2,3]. 为了叙述方便,我们不妨假设要执行的幺正操作具有如下形式:

$$U_\theta \equiv \exp(i\theta\frac{\sigma_z}{2}), \quad (12)$$

其中 $\theta \in [0,2\pi)$,幺正操作 U_θ 的作用可以理解为:使自旋 1/2 粒子沿 z 轴旋转 θ 角度.

假设我们只用一个量子比特来储存 U_θ(见图 5,图中虚线框中的部分对应于可编程逻辑门阵列 G). 这时可用下面的量子态来编码幺正操作 U_θ,

$$|\theta\rangle \equiv \frac{1}{\sqrt{2}}(e^{i\theta/2}|0\rangle + e^{-i\theta/2}|1\rangle), \quad (13)$$

即令程序态 $|P_U\rangle = |\theta\rangle$.

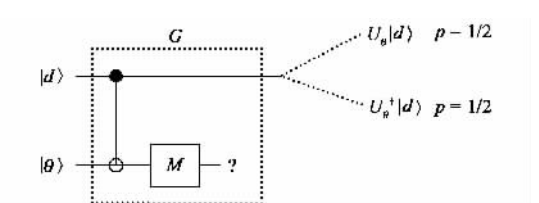

图 5 不需要事先准备纠缠态的概率的和精确的可编程量子计算器件设计方案 1

这类可编程量子计算器件是这样工作的:输入态 $|d\rangle|P_U\rangle = \frac{1}{\sqrt{2}}(e^{i\theta/2}|d\rangle|0\rangle + e^{-i\theta/2}|d\rangle|1\rangle)$,经过 CNOT 门后得到

$$\frac{1}{\sqrt{2}}(U_\theta|d\rangle|0\rangle + U_\theta^\dagger|d\rangle|1\rangle). \quad (14)$$

由(14)式可以看到,当对程序态测量得到 $|0\rangle$ 态的本征值时,数据寄存器的状态为 $U_\theta|d\rangle$,就可成功地实现对数据态 $|d\rangle$ 的幺正操作 U_θ.

如果可以使用多个量子比特编码幺正操作 U_θ(见图 6,图中虚线框中的部分对应于可编程逻辑门阵列 G),就可以提高成功完成 U_θ 的几率. 图 6 中的量子电路计算表明,只有当所有的程序态 $|\theta\rangle$, $|2\theta\rangle$,…, $|2^{N-2}\theta\rangle$, $|2^{N-1}\theta\rangle$ 测量都得到 $|1\rangle$ 态的本征值时,才会失败,不能完成预期的幺正操作,其中 N 为用来编码幺正操作 U_θ 的量子比特的数目,Λ_N(not)门是 CNOT 门和 Toffoli 门的推广,当 $N=1$ 时就是 CNOT 门,$N=2$ 时就是 Toffoli 门. Λ_N(not)门的电路如图 7 所示.

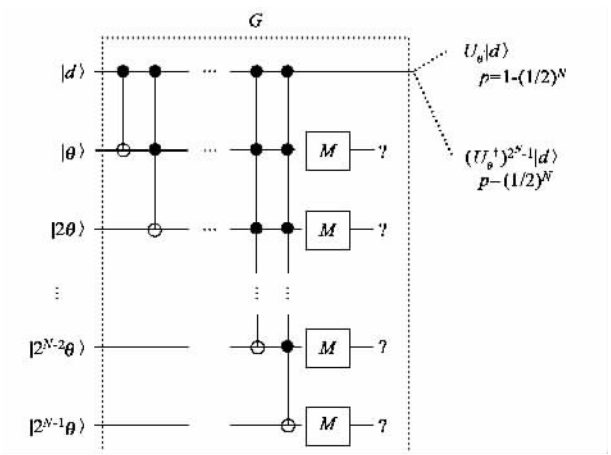

图 6 不需要事先准备纠缠态的概率的和精确的可编程量子计算器件设计方案 2

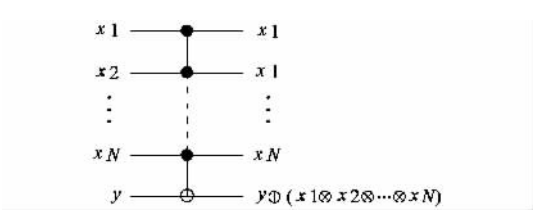

图 7 Λ_N(not)门的电路表示

实现任意单量子位幺正操作的方法如下:在一般情况下,利用图 8 中的电路设计,我们可以实现幺正操作:

$$U_\theta(L) \equiv \exp(i\theta\frac{\sigma_L}{2}), \quad (15)$$

其中 $\sigma_L \in \{\sigma_x,\sigma_y,\sigma_z\}$, $\sigma_x,\sigma_y,\sigma_z$ 为泡利矩阵. $\theta\in[0,2\pi)$, $U_\theta(L)$ 的作用可以这样理解:对自旋为 1/2 的粒子沿 $L(L\in\{x,y,z\})$ 轴旋转 θ 角度. 利用这样一个事实:如果有两个旋转轴是不平行的,任意的单量子位幺正操作都可以通过三个旋转操作来完成,将若干个图 8 中的电路串联起来,我们就可以实现任意单量子位幺正操作.

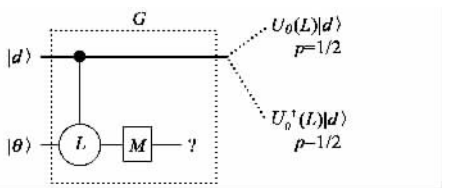

图 8 实现一般幺正操作 U 的设计

本方案有如下特点:

(1)针对单量子比特操作;

(2)不需要事先准备纠缠态;

(3)需要进行测量才能确定操作是否完成;

(4)测量后通过测量结果可以知道操作是否成功;

(5)可编程量子计算器件 G 成功完成对数据态 $|d\rangle$ 的幺正操作 U 的概率为 $1-(\frac{1}{2})^N$,其中 N 为用来编码幺正操作 U_θ 的量子比特的个数;

(6)当成功时,所实现的幺正操作 U 是精确的.

3.4 确定的和近似的可编程量子计算器件——量子中央处理器

上面两种方案成功完成对数据态 $|d\rangle$ 的幺正操作 U 的概率都小于 1,因此当一个量子计算需要串联很多个可编程量子计算器件时,整个计算被成功完成的概率会趋于 0. 为了克服这个困难,我们从另一个角度考虑,提出了量子中央处理器的设计[4]. 图 9 是一个量子中央处理器的电路图,它的数据寄存器的输入包含 n 个量子比特,程序寄存器的输入包含 $(m+2n-1)$ 个量子比特. 图中 R_i $(i=1,2,3\cdots m)$ 表示相应的旋转操作,C 表示相应的控制非门操作. 程序寄存器的一个输入

$$|b_n\rangle|p_n\rangle\cdots|b_3\rangle|p_3\rangle|b_2\rangle|p_2\rangle|a_m\rangle\cdots|a_2\rangle|a_1\rangle|r\rangle \quad (16)$$

称为一个指令序列(instructor sequence, IS).

量子中央处理器如何工作?由于量子信息的特

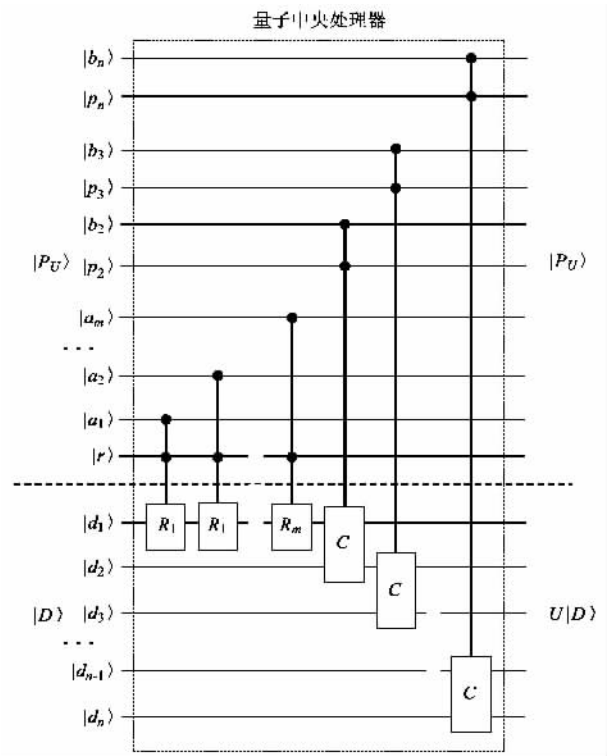

图9　量子中央处理器的电路表示

点，无法对量子寄存器中的量子态进行复制，也不能重置未知量子态[5,6]. 下面我们描述两种量子中央处理器的工作模式.

(1)把指令序列在空间上展开(见图10). 根据指令序列的数量需要多个 QCPU 串联起来. 它的特点是可以使用未知的指令序列，例如利用量子远程传态得到指令序列.

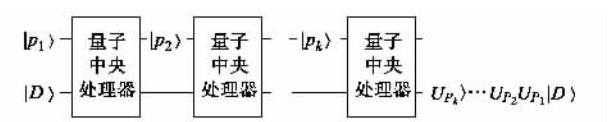

图10　指令序列在空间上展开，指令序列可以是未知的量子态

(2)把指令序列在时间上展开(见图11). 首先把数据寄存器和程序寄存器制备到已知的状态，例如$|00\cdots0\rangle$，然后利用设计好的程序(指令序列集 ISs)按照表1的步骤进行.

可以证明，对于在任意数目量子比特上的量子计算和任意要求的计算精度，量子中央处理器都可以被有效地构造. 所谓“有效地构造”是指它所需要的资源(量子比特的数目，其中逻辑门的数目)的数量随问题的规模(数据寄存器中包含的量子比特的数量)增长的关系是多项式的，而不是指数的.

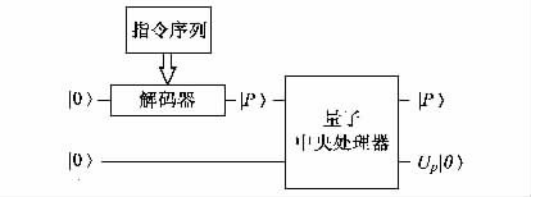

图11　指令序列在时间上展开，指令序列需要是已知的量子态

表1　指令序列在时间上展开的执行步骤

步骤	t_1	t_2	t_3	t_4	t_5	t_6	…
程序寄存器的状态	$\|0\rangle$	$\|P_0\rangle$	$\|P_0\rangle$	$\|P_1\rangle$	$\|P_1\rangle$	$\|P_2\rangle$	…
数据寄存器的状态	$\|0\rangle$	$\|0\rangle$	$U_{P_0}\|0\rangle$	$U_{P_0}\|0\rangle$	$U_{P_1}U_{P_0}\|0\rangle$	$U_{P_1}U_{P_0}\|0\rangle$	…
解码器的操作	无	U_{P_0}	无	$U_{P_1}U_{P_0}^{-1}$	无	$U_{P_2}U_{P_1}^{-1}$	…
QCPU 的操作	无	无	工作	无	工作	无	…

本方案有如下特点：

(1)可以完成多量子比特操作. 对于任意数目量子位和任意要求的计算精度，量子中央处理器总是可以被有效地构造；

(2)不需要事先准备纠缠态；

(3)不需要进行测量来确定操作是否完成；

(4)量子中央处理器对数据态$|D\rangle$执行的幺正操作不是概率性的，成功率是1；

(5)对实现任意的幺正操作 U 是近似的，所能达到的精度由程序寄存器中的量子比特的个数决定.

3.5　通过量子软件控制的量子测量器件[7,8]

通常我们对量子态进行测量，需要事先知道基态(基矢)，Fiurášek 和 Dušek 等人提出了一个通过量子软件(量子态)决定基态(基矢)的设计，可以完成在未知基态(基矢)上的‘测量’. 图12是一个简单的例子，设$|\Psi\rangle$为未知量子态，$|\Phi\rangle$和$|\Phi_\perp\rangle$为任意一组正交基. H 是 Hadamard 门，中间部分为 Fredkin 门，它的功能是，当量子寄存器 A 处于$|1\rangle$时，下面两个量子寄存器 B，C 状态交换，当控制比特处于$|0\rangle$时，下面两个量子寄存器状态保持不变.

由计算可知，在进行测量(M)前，系统的状态为

$$\frac{1}{2}|0\rangle(|\Phi\rangle|\Psi\rangle+|\Psi\rangle|\Phi\rangle)+\frac{1}{2}|1\rangle(|\Phi\rangle|\Psi\rangle-|\Psi\rangle|\Phi\rangle). \quad (17)$$

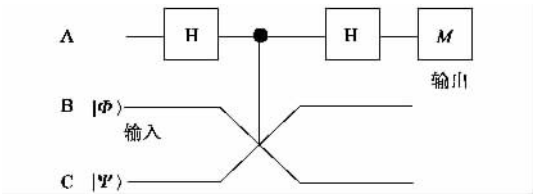

图 12　通过量子软件控制的量子测量器件的电路表示

测量量子寄存器 A，得到 $|0\rangle$ 本征值的概率为 $p_0 = (1 + |\langle\Phi|\Psi\rangle|^2)/2$，得到 $|1\rangle$ 本征值的概率为 $p_1 = (1 - |\langle\Phi|\Psi\rangle|^2)/2$；$|\Psi\rangle$ 在以 $|\Phi\rangle$ 和 $|\Phi_\perp\rangle$ 展开的正交基上测的 $|\Phi\rangle$ 的概率为 $p_\Phi(\Psi) = |\langle\Phi|\Psi\rangle|^2$，所以我们可以得到 $p_\Phi(\Psi) = 1 - 2p_1$，$p_{\Phi_\perp}(\Psi) = 2p_1$，或 $p_\Phi(\Psi) = 2p_0 - 1$，$p_{\Phi_\perp}(\Psi) = 2 - 2p_0$. 因此可以实现在未知基态（基矢）上的‘测量’.

本方案有如下特点：

（1）与一般的量子测量不同，关心的不是量子态的本征值；

（2）在量子信息处理中，人们关注的是不同量子态之间的关系，如量子态的区分；

（3）测量的基矢（量子态）由量子软件指定量子态决定，对操作者来说可以是未知的.

4　量子计算机物理实现的几个主要方向

实际建造量子计算机的困难在于：发现一个具有非线性相互作用的系统以便用来计算，并且可以有效地被外界控制，但又与环境很好的隔离，不致使系统很快消相干.

实现量子计算机的工作包含 5 个主要部分：

（1）制备初态（纯态，比如基态）；

（2）进行任意的单量子比特的操作；

（3）实现通用的两比特操作（例如，CNOT 门）；

（4）提供有效的测量手段来读出测量结果；

（5）可以操纵足够多的量子比特，即量子计算机具有足够的规模，能够用来解决实际问题.

所有操作都必须在系统的相干时间内完成. 下面简单介绍几种物理实现技术.

4.1　离子阱技术

离子阱是在特定形状的电极上加上静电场、交变电场和磁场的适当组合，将带电粒子稳定地囚禁于超高真空中的一种装置. 1995 年，Cirac 和 Zoller 首次提出可以用离子阱技术实现量子计算[9]. 把一串两能级离子囚禁在线形离子阱中，限制它们沿对称轴作一维运动，并利用边带冷却把它们冷却至运动态基态，利用离子的内态作为量子比特. 这些离子在阱的势场作用下做集体振荡，利用这种集体振荡可以实现不同离子之间的相互作用. 离子之间的距离大于光波的波长，通过激光束可以对不同离子分别进行控制操作或读出操作.

4.2　核自旋系统

利用原子核的核自旋作为量子比特，目前研究和使用最多的是液体核磁共振技术. 1997 年，Gershenfeld 和 Chuang 首次利用液体核磁共振技术实验实现了量子计算[10]. 液体核磁共振技术是利用溶于液体中分子中的自旋 1/2 的原子核的核自旋作为量子比特. 自旋向上（取外磁场 B_0 向下）$|\uparrow\rangle$ 表示 $|1\rangle$，自旋向下 $|\downarrow\rangle$ 表示 $|0\rangle$. 分子中不同原子的核自旋及其状态由于其磁共振频率不同可以被分别确认和区分，并且可以利用射频脉冲和核自旋之间的相互耦合对核自旋进行操纵和控制. 由于单个分子中原子的核自旋的信号十分微弱，目前的技术还不易检测，因此实验上利用大量分子的溶液（量级约为 0.1mmol，$\sim 10^{19}$ 个分子）进行量子计算. 所以核磁共振量子计算也称为集合自旋共振（bulk spin-resonance）量子计算. 原子核处于电子的包围之中，受到了很好的屏蔽，处于近独立的状态，几乎不受电子和分子热运动的干扰. 因此外部环境对它的影响较小，具有较长的消相干时间. 研究人员利用核磁共振技术进行了大量量子信息方面的实验研究，例如：量子逻辑门的实现、量子算法的实现、量子态的克隆、纠缠交换、几何量子计算等等. 我们实验室在核磁共振方面也作了一些工作，包括量子博弈[11]、量子随机游走[12]、量子态的相似度判断[13]、混态几何相[14]的研究等等. 原子核的核自旋是量子比特的一种很好的选择，除了液体核磁共振，还有一些方案也是利用核自旋作为量子比特的载体，如 Kane 的硅基核自旋方案[15]，光格子中的原子核[16].

4.3　光学技术

利用两种偏振态的光子（水平和垂直偏振）可以作为量子比特，也可以用特定位置光子的有无作为量子比特. 光学技术的难点在于光子之间很难找到非线性相互作用来构造多比特量子逻辑门. 这方面的一个重要进展是由 Knill 等人在 2001 年做出的，他们的研究小组提出了一个利用线性光学进行量子计算的方案[17]. 另一个重要进展是由 Sanaka 等人做出的，他们的研究小组在 2003 年实验实现了一个光子态的非线性的符号变化[18].

4.4 其他的一些技术

如原子和光腔相互作用[19],超导量子干涉[20],量子点操纵[21],电子自旋共振[22],液氦表面电子[23]等.

5 结束语

我们今天的技术条件已经使我们可以达到实现量子计算机5个主要部分的任何一个单独的要求.例如我们可以做到:

(1)通过原子冷却技术将一个原子制备到其基态.

(2)精确地控制一个核自旋.

(3)利用核自旋之间的相干完成两个核自旋间的通用两比特操作.

(4)对离子阱中的离子进行近乎理想的测量.

(5)利用半导体技术在一个芯片上集成成千上万个量子点.

然而同时满足这5个要求仍然是非常困难的,到目前为止我们实现的最大规模的量子计算仅包含7个量子比特[24],正如Bennett教授所说,"现在的量子计算机只是一个玩具,真正做到有实用价值的也许是5年,10年,甚至是50年以后".实现量子计算机的困难在于,量子系统既要有效地被外界控制,又要与环境很好的隔离.科学技术的发展过程充满了偶然和未知,就算是物理学泰斗爱因斯坦也决不会想到,为了批判量子力学而用他的聪明大脑假想出来的EPR态,在六十多年后不仅被证明是存在的,而且还被用在量子信息中.相信随着技术的进步和量子计算机结构设计上的进展,实用量子计算机会被建造出来,并象现在的经典计算机一样无处不在,给我们的生活带来巨大的影响.

参 考 文 献

[1] Nielsen M A, Chuang I L. Phys. Rev. Lett., 1997, 79: 321

[2] Vidal G, Masanes L, Cirac J I. Phys. Rev. Lett., 2002, 88: 047905

[3] Kim J, Cheong Y, Lee J S *et al*. Phys. Rev. A, 2002, 65: 012302

[4] Xue F, Chen Z B, Shi M J *et al*. Phys. Lett. A, 2003, 312: 301

[5] Zurek W H. Nature, 2000, 404: 130

[6] Pati A K, Braunstein S L. Nature, 2000, 404: 164

[7] Fiurášek Jaromír, Dušek Miloslav, Filip Radim. Phys. Rev. Lett., 2002, 89: 190401

[8] Dušek Miloslav, Buzěk Vladimír. Phys. Rev. A, 2002, 66: 022112

[9] Cirac J I, Zoller P. Phys. Rev. Lett., 1995, 74: 4091

[10] Gershenfeld N A, Chuang I L. Science, 1997, 275: 350

[11] Du J F, Li H, Xu X D *et al*. Phys. Rev. Lett., 2002, 88: 137902

[12] Du J F, Li H, Xu X D *et al*. Phys. Rev. A, 2003, 67: 042316

[13] XUE F, DU J F, ZHOU X Y *et al*. Chin. Phys. Lett., 2003, 20: 1669

[14] Du J F, Zou P, Shi M J *et al*. Phys. Rev. Lett., 2003, 91: 100403

[15] Kane B E. Nature, 1998, 393: 133

[16] Duan L M, Demler E, Lukin M D. Phys. Rev. Lett., 2003, 91: 090402

[17] Knill E, Laflamme R, Miburn G J. Nature, 2001, 409: 46

[18] Sanaka Kaoru, Jennewein Thomas, Pan J W *et al*. 2003, arXiv: quant-ph/0308134

[19] Maitre X, Hagley E, Nogues N *et al*. Phys. Rev. Lett., 1997, 79: 769

[20] Makhlin Yuriy, Scöhn Gerd, Shnirman Alexander. Nature, 1999, 398: 305

[21] Zanardi Paolo, Rossi Fausto. Phys. Rev. Lett., 1998, 81: 4752

[22] Troiani Filippo, Molinari Elisa. Phys. Rev. Lett., 2003, 90: 206802

[23] Dykman M I, Platzman P M, Seddighrad P. Phys. Rev. B, 2003, 67: 155402

[24] Vandersypen L M K, Steffen Matthias, Breyta Gregory *et al*. Nature, 2001, 414: 883

·读者和编者·

2004年第9期《物理》内容预告

评述

高迁移率二维电子系统中微波辐射引起的磁阻振荡和零电阻(雷啸霖);

颗粒物质(上)(陆坤权等).

前沿进展

α粒子对人体癌细胞损伤过程的Monte Carlo模拟及分析(江海燕等);

纳米光子学的最新进展(明海等);

金刚石紫外发光器件研究进展(郭江等);

金融市场中幂律分布的经验和理论研究进展——经济物理学研究的一个前沿(张宇等).

超短脉冲强激光在空气中的传输(郝作强).

物理学和高新技术

医学影像物理学科的现状和未来(张仕刚等).

庆贺黄祖洽院士80寿辰专栏