文章编号: 1007 －4627(2002)增刊 －0162 －04

量子计算机理论中的量子叠加和量子纠缠y

周奇年

(浙江工程学院, 浙江 杭州 310033)

摘 要: 讨论了量子计算、量子通讯与量子计算机中的核心问题: 量子叠加和量子纠缠. 从量子态表示量子信息为出发点, 指出有关量子信息的所有问题都可采用量子力学理论来处理. 其中信息的演变遵从薛定谔方程, 信息的传输就是量子态在量子通道中的传送, 信息处理就是量子态的幺正变换, 信息提取则是对量子系统实行量子测量.

关 键 词: 量子计算机; 量子态; 量子比特; 量子叠加; 量子纠缠

中图分类号: O413.1 文献标识码: A

1 引言

在人类刚刚跨入 21 世纪之际, 信息科学面临着新的挑战. 计算机是否存在极限的运算速度、集成化可以达到何种程度? 能否实现不可破译、不可窃听的保密通信? 诸如此类的问题一直是数学家和电子技术专家以及计算机科学家们关注的重要课题. 近年来, 物理学家也加入到这个研究行列, 他们成功地将量子理论和信息科学结合起来, 提出许多令人耳目一新的概念、原理和方法, 于是"量子信息"和"量子计算"作为新兴的学科分支便应运而生. 当前量子计算机、量子通信以至于量子密码技术等已经成为研究热点, 并取得重要进展. 20 世纪 80 年代初期, Benioff 首先提出了量子计算的思想[1－3], 他设计了一台可执行的、有经典类比的量子 Turing 机——量子计算机的雏形. 此后不久, Feynman 发展了 Benioff 的设想, 提出量子计算机可以模拟量子系统[4,5]; Deutsch 提出基于量子干涉的计算机模型以及"量子逻辑门"这一新概念, 并指出量子计算机可以通用化、量子计算错误的产生和纠正等问题[6,7], 并由 Zurek 作了深入的分析和研究. 1993 年, Lloyd 指出许多物理系统可用于研制量子计算机, 且在一定情况下能避免 Landauer 提出的问题. 1994 年计算机科学家 Peter Shor 给出了第一个大数因子分解的量子算法, 它能在几秒内破译常规计算机"无法破译"的密码. 这是一个革命性突破, 显示了量子计算的效率可以远远超过现代计算机. 从 1994 年起, 计算机科学和物理学间的跨学科研究突飞猛进, Science, Nature, Physics Review Letters 等著名科学期刊上发表了大量的量子计算和信息方面的理论与实验的研究工作. 此外, 关于量子逻辑门、量子电路等许多设计方案不断涌现, 使得量子计算的理论和实验研究蓬勃发展.

2 量子态及叠加

现有的经典信息以比特作为信息单元. 从物理角度讲, 比特是个两态系统, 它可以制备为两个可识别状态中的一个, 如是或非, 真或假, 0 或 1. 在数字计算机中电容器平板之间的电荷可表示信息比特, 有电荷代表 1, 无电荷代表 0. 量子信息的单元称为量子比特(qubit), 满足

$$|\psi\rangle = C_1|0\rangle + C_2|1\rangle,$$
$$|C_1|^2 + |C_2|^2 = 1. \qquad (1)$$

它是两个逻辑态的叠加态, 这就是量子系统与经典系统的一个最大区别, 即它可以处于多个不同态的叠加态. 假定一个原子只有两个可能的量子态$|0\rangle$和$|1\rangle$, 这个原子既可以只处于态$|0\rangle$或者态$|1\rangle$, 也可以处于态$|0\rangle$和态$|1\rangle$的叠加态, 后者的意义是原子可以同时处于态$|0\rangle$和态$|1\rangle$. 量子系统这种奇

y 收稿日期: 2002 - 02 - 27; 修改日期: 2002 - 05 - 31

* 基金项目: 浙江工程学院留学人员(01727-E); 引进基金资助项目

作者简介: 周奇年(1957–), 男(汉族), 甘肃山丹人, 副教授, 从事计算机科学及原子与分子物理领域的研究.

特性质正是量子信息与量子计算的基础. 经典比特可以看成是量子比特的特例(如 $C_1= 0$, $C_2= 1$ 或 $C_1= 1$, $C_2= 0$) . 用量子态来表示信息是量子信息的出发点, 有关信息的所有问题都必须采用量子力学理论来处理, 信息的演变遵从薛定谔方程, 信息的传输就是量子态在量子通道中的传送, 信息处理(计算) 就是量子态的幺正变换, 信息提取便是对量子系统实行量子测量. 在实验中任何两态的量子系统都可以用来制备成量子比特, 常见的有: 光子的正交偏振态、电子或原子核的自旋、原子或量子点的能级、任何量子系统的空间模式等.

信息一旦量子化, 量子力学的特性便成为量子信息的物理基础, 其主要内容有: 量子纠缠, 量子不可克隆, 量子叠加性和相干性, 消相干等. 量子不可克隆指量子力学的线性特性和量子测量的奇异性禁止对任意量子态实行精确的复制, 量子不可克隆定理和不确定性原理构成了量子密码术的物理基础; 量子比特可以处在两个本征态的叠加态, 在对量子比特的操作过程中, 两态的叠加振幅可以相互干涉, 这就是量子相干性; 量子相干性在各种量子信息过程中都起着至关重要的作用, 但是因为环境的影响, 量子相干性将不可避免地随时间指数衰减, 此即消相干. 消相干将引起量子错误, 量子编码的目的就是为了纠正或防止这些量子错误.

3　量子纠缠

量子纠缠是指: N(大于 1) 量子比特可以处于量子纠缠态, 子系统的局域状态不是相互独立的, 对一个子系统的测量会获取另外子系统的状态. 如:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2) . \quad (2)$$

量子纠缠是存在于多子系统的量子系统中的一种奇妙现象, 即对一个子系统的测量结果无法独立于对其它子系统的测量参数. 它的出现可以追溯到量子力学诞生之初. 因为量子力学描述的物理实在具有无法消除的随机性, 所以, 有关量子力学的争论就从未间断过. 其主要表现为以爱因斯坦为代表的经典物理学家和以玻尔为代表的哥本哈根学派之间的冲突. 其间最著名的事例是在 1935 年爱因斯坦同 Podolsky 和 Rosen 一起提出的 EPR 佯谬. 其目的是想说明在承认局域性和实在性的前提下, 量子力学描述是不完备的.

那么, 什么样的量子态才算是纠缠态呢? 对于一个由 N 个子系统构成的复合系统, 如果系统的密度矩阵不能写成各个子系统的密度矩阵的直积的线性叠加形式, 则这个复合系统就是纠缠的. 如: 考虑体系 A 和 B 组成的二体系, 设 A 的一组力学量完全集的共同本征态记为 $|n\rangle$, n 代表一组完备量子数, B 的一组力学量完全集的共同本征态记为 $|v\rangle$, v 代表另一组完备量子数, 则 $|n\rangle_A|v\rangle_B$(直积形式, 简记为 $|n\rangle_A|v\rangle_B$) 可以作为复合体系A+ B的一个完备基, 复合体系的任意量子态一般可以表示成它们的线性叠加:

$$|\Psi\rangle_{AB} = \sum_{nv} C_{nv}|n\rangle_A|v\rangle_B , \quad (3)$$

如 He 原子的两个电子可以形成自旋单态和自旋三态

$$\begin{cases} x_{00} = \dfrac{1}{\sqrt{2}}[|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B] , \\ x_{10} = \dfrac{1}{\sqrt{2}}[|\uparrow\rangle_A|\downarrow\rangle_B + |\downarrow\rangle_A|\uparrow\rangle_B] , \\ x_{11} = |\uparrow\rangle_A|\uparrow\rangle_B , \\ x_{1-1} = |\downarrow\rangle_A|\downarrow\rangle_B . \end{cases} \quad (4)$$

4 个 Bell 基

$$|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}\{|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\} , \quad (5)$$

$$|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}\{|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\} . \quad (6)$$

二体系不能表示成一个直积形式的态, 称为二体系的纠缠态, 而直积形式的量子态, 例如 $|n\rangle_A|v\rangle_B$态(n, v 任意) , 则称为非纠缠态. 量子纠缠的重要性在于: 第一, 在测量坍缩中它们表现出一种非定域的关联: 一种没有经典对应的、超空间的关联; 第二, 量子系统与环境发生的难以避免的量子纠缠正是量子消相干的根源, 即量子信息丧失的主要方式.

由此可将量子纠缠定义为: 一个两体量子纯态 $|\Psi\rangle_{AB}$的量子纠缠度 E_ϕ, 用其中任一粒子态的 von

Neumann 熵 S 来定义:

$$E_\psi = S(\rho_A) = S(\rho_B), \quad (7)$$

这里 $\rho_A = \mathrm{Tr}^B(|\psi\rangle_{AB}{}_{AB}\langle\psi|)$, $\rho_B = \mathrm{Tr}^A(|\psi\rangle_{AB}{}_{AB}\langle\psi|)$, 而 $S(\rho)$ 定义(例如对 ρ_A)为

$$S(\rho_A) = -\mathrm{Tr}(\rho_A \ln \rho_A), \quad (8)$$

求迹内的对数以 2 为底.

于是, 对任何可分离态

$$|\varphi\rangle_{AB} = |\alpha\rangle_A \otimes |\lambda\rangle_B, \quad E_\psi = 0, \quad (9)$$

对有最大纠缠度的 Bell 态, 其纠缠度 $E_\psi = 1$. 对多粒子纯态, 纠缠度的定义有待最后的定论, 对于两体混态和多体混态, 相应纠缠度的定义仍处在研讨之中.

4 量子信息及其处理

为了说明量子计算机与经典计算机的本质区别, 先来看看信息的基本单位——位. 从物理的观点看, 一个位就是一个两态系统. 考虑如下的三位组成的寄存器, 3 个位的经典寄存器可以编码出 8 个不同的数字(状态): 000, 001, 010, 011, 100, 101, 110, 111. 但每一个时刻只能存储其中的一个. 而三量子寄存器可以同时储存所有 8 个数字(状态). 如每个寄存器有二个状态$|0\rangle, |1\rangle$, 则

$$|\Psi\rangle = |\sigma_1\rangle \otimes |\sigma_2\rangle \otimes |\sigma_3\rangle, \quad (10)$$

即

$$\begin{aligned}|\Psi\rangle = \sum_i C_i |\sigma_1^i\rangle \otimes |\sigma_2^i\rangle |\sigma_3^i\rangle \\ = C_1|0\rangle \otimes |0\rangle \otimes |0\rangle + \\ C_2|0\rangle \otimes |0\rangle \otimes |1\rangle + \\ C_3|0\rangle \otimes |1\rangle \otimes |0\rangle + \\ C_4|0\rangle \otimes |1\rangle \otimes |1\rangle + \\ C_5|1\rangle \otimes |0\rangle \otimes |0\rangle + \\ C_6|1\rangle \otimes |0\rangle \otimes |0\rangle + \\ C_7|1\rangle \otimes |1\rangle \otimes |0\rangle + \\ C_8|1\rangle \otimes |1\rangle \otimes |1\rangle, \end{aligned} \quad (11)$$

$$\begin{aligned}|\boldsymbol{a}\rangle = |\boldsymbol{a}_{n-1}\rangle \otimes |\boldsymbol{a}_{n-2}\rangle \otimes \cdots \otimes |\boldsymbol{a}_0\rangle, \\ \boldsymbol{a} = 2^{n-1}\boldsymbol{a}_{n-1} + 2^{n-2}\boldsymbol{a}_{n-2} + \cdots + 2^0\boldsymbol{a}_0, \\ \boldsymbol{a}_i = \begin{vmatrix} 0 \\ 1 \end{vmatrix}, \end{aligned} \quad (12)$$

对于一个 n 位的寄存器共有 $2n$ 个状态, 64 位寄存器可以表示 $1.844\,7\times10^{19}$个数字, 而量子寄存器可以同时储存所有 $1.844\,7\times10^{19}$个数字.

由此得出结论: 一旦量子寄存器同时储存了 $2n$ 个位, 对其一次操作(测量), 就相当于经典的 $2n$ 次操作. 例如: 么正变换对 qubit 的操作把单量子态变为叠加态, 即

$$|\Psi_{\mathrm{final}}\rangle = \hat{U}\begin{vmatrix} 0 \\ 1 \end{vmatrix} = \frac{1}{\sqrt{2}}\left|\begin{vmatrix} 1 \\ 0 \end{vmatrix} + \begin{vmatrix} 0 \\ 1 \end{vmatrix}\right|, \quad (13)$$

其中,

$$\hat{U} = \frac{1}{2}\begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix}, \quad (14)$$

对于 L 个 qubit 组成的一个量子寄存器, 先置零

$$|\boldsymbol{a}\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \quad (15)$$

作 Hadamard 变换, 即进行门操作

$$\begin{aligned}|\Psi\rangle \overset{\hat{U}}{\Rightarrow} \frac{1}{2}(|0\rangle + |1\rangle) \otimes \\ \frac{1}{2}(|0\rangle + |1\rangle) \cdots \otimes \frac{1}{2}(|0\rangle + |1\rangle) \\ = \frac{1}{\sqrt{2^L}}\sum_i (|\sigma_1^i\rangle \otimes |\sigma_2^i\rangle \cdots \otimes |\sigma_3^i\rangle) \end{aligned} \quad (16)$$

是各种态的组合.

由此可见, 信息即量子态; 信息处理即对量子进行变换. 任意计算过程都是对一组 qubit 的多维么正变换.

参 考 文 献:

[1] Benioff P. The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines[J]. J Statist Phys, 1980, **22**: 563.

[2] Benioff P. Quantum Mechanical Hamiltonian Models of Turing Machines[J]. J Statist Phys, 1982, **29**: 515.

[3] Benioff P. Quantum Mechanical Hamiltonian Models of Turing Machines that Dissipate no Energy[J]. Phys Rev Lett, 1982, **48**: 1581.

[4] Feynman R. Simulating Physics with Computers[J]. Internat J Theoret Phys, 1982, **21**: 467.
[5] Feynman R. Quantum Mechanical Computers[J]. Found Phys, 1986, **16**: 507.
[6] Deutsch D. Quantum Theory, the Church-turing Principle and the Universal Quantum Computer[J]. Proc Roy Soc London Ser A, 1985, **400**: 96.
[7] Deutsch D, Barenco A, Ekert. Universality of Quantum Computation [J]. Proc Roy Soc London Ser A, 1995, **449**: 669.

Quantum Superposition and Entangled State in the Theories of Quantum Computer*

ZHOU Qi-nian

(Zhejiang Institute of Science and Technology, Hangzhou 310033, *China)*

Abstract: The important problems that is quantum superposition and entangled state in the quantum computation, quantum communication and quantum computer have been discussed. From these, it is pointed out that the problems which are concern with quantum information can be handled by the quantum mechanics theories: quantum computing and transformation of the quantum information follows the Schrödinger Equation and U transformation in quantum system, respectively.

Key words: quantum computer; quantum state; quantum bit; quantum superposition; entangled state

(上接第 155 页 continued from page 155)

Importance of Bound-bound State Interaction in Harmonic Generation**

CAI Qing-yu, QIAO Hao-xue, LI Bai-wen

(State Key Laboratory of Magnetic Resonance and atomic and Molecular Physics, Wuhan Institute of Physic and Mathematics, Chinese Academy of Sciences, Wuhan 430071, *China)*

Abstract: One dimension parabolic potential is used to research the effect of bound-bound states interaction in the high harmonic generation. Using different frequency photons, we have obtained a result with only bound-bound states interaction. There is neither plateau nor obviously cutoff in the high harmonic generation, which is reasonable and significance.

Key words: intense laser field; bound state; harmonic generation; parabolic potential

更正: 第 19 卷第 2 期(131 页)文章“类氢铀离子的辐射电子俘获角分布研究”(作者马新文等), 全文中字符 ħ 全部应改为 ħ, 公式 2(132 页)右端分母 v^5 应为 v^{12}.

* **Foundation item:** Science Research Foundation of Zhejiang Institute of Science (01727-E) and Technology for Study Abroad Personnel and Person with Ability Work in

** **Foundation item:** National Natural Science Foundation of China