第 20 卷 第 4 期 物 理 学 进 展 Vol.20,No.4
2000 年 10 月 PROGRESS IN PHYSICS Oct.,2000

文章编号:1000-0542(2000)04-0407-25

量子信息研究进展

李传锋 郭光灿

(中国科学技术大学量子通信与量子计算开放实验室,合肥 230026)

摘 要: 量子信息论是经典信息论与量子力学相结合的新兴交叉学科。本文综述了量子信息领域的研究进展。即包括了为人们所熟知的量子通信与量子计算领域,也包括了刚刚兴起的但却有巨大潜力的量子对策论等领域。本文以介绍量子信息论的基本理论框架为主,同时也介绍了量子信息领域的实验研究进展。

关键词: 量子信息;量子通信;量子计算;量子对策论

中图分类号: O413 **文献标识码:** A

0 引 言

纵观绝大多数科学领域的发展,其过程类似盲人摸象,开始先是领域中的独立现象的研究,然后是各种现象之间的联系,再从千丝万缕的联系中找出这个领域的第一性原理,最后在第一性原理的指导下领域不断发展壮大,又与其它领域交叉产生新的分支。象相对论那样平地起高楼的毕竟少之又少。

量子信息论的奠基者们的本意是用量子力学来辅助完成一些经典信息过程,然而随着研究的深入,后来者们逐步把量子力学与经典信息论真正地结合起来。在此过程中,许多重大问题(如消相干等)得到解决,各种新的奇异现象被发现,这使得研究者们越来越坚定地相信量子信息论已成为一门独立的学科。这一点可以体现在量子信息领域的两位权威 Bennett 和 DiVincenzo 最近在《自然》杂志上对量子信息所做的总结性评价上[1]:从经典信息到量子信息的推广,就象从实数到复数的推广一样。

量子信息除了推广了经典信息中的信源与信道等概念外,还引入了其特有的量子纠缠。量子信息可以说是经典信息与量子纠缠的互补。经典信息可以被任意克隆,但只能从时空中的一点传到后面的一点。量子纠缠不可以被克隆,但可以把时空中的任意两点联系起来(非局域性)。

目前量子信息论中,量子通信与量子计算领域已经做了广泛深入的研究,新的领域如量子对策等也在兴起,而且其基础理论的研究也不断取得新的进展。相比较而言,实验进

收稿日期:2000-09-05
基金项目:国家自然科学基金资助(19874056,69878025)

展要小一些。

1 量子信息基础理论

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压可表示信息比特,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),它是两个逻辑态的叠加态

$$|\varphi\rangle = c_0|0\rangle + c_1|1\rangle, \quad |c_0|^2 + |c_1|^2 = 1 \tag{1}$$

经典比特可以看成量子比特的特例($c_0 = 0$ 或 $c_1 = 1$)。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,信息传输就是量子态在量子通道中的传送,信息处理(计算)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,其主要的有:

1) 量子纠缠:N(大于 1)的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。

2) 量子不可克隆:量子力学的线性特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质原理构成量子密码术的物理基础。

3) 量子叠加性和相干性: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,这就是所谓的量子相干性。

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,这就是消相干。消相干引起量子错误,量子编码的目的就是为了纠正或防止这些量子错误。

1.1 量子纠缠

量子纠缠是存在于多子系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的测量参数。虽然,近些年来,随着量子信息这一新兴领域的蓬勃发展,量子纠缠逐渐成为人们的热门话题,但它并不是什么新生事物,"纠缠"这一名词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,从它诞生之日起,围绕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[2]。在此文中爱因斯坦等人第一次提出纠缠态的想法,其目的意在说明在承认局域性和实在性的前提下,量子力学的描述是不完备的。玻尔虽然对此做出了相应的回答,但据玻尔的助手说,EPR 的文章对玻尔的影响是极为重大的。因为玻尔从中看到了,在考虑多粒子时量子理论会导致纯粹的量子效应。然而,

无论是玻尔还是爱因斯坦,都没有洞悉他们所讨论的纠缠态的全部含义,在经过了数十年的努力之后,这些含义才逐渐地被发掘出来[3]。

现在,量子纠缠态已被应用到量子信息的各个领域。对量子纠缠的深入研究无论是对于量子信息的基本理论还是对未来潜在的实际应用都将产生深远的影响。

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的形式,则,这个复合系统就是纠缠的。即:

$$\rho \neq \sum_i p_i \rho_i^{(1)} \otimes \rho_i^{(2)} \otimes \cdots \otimes \rho_i^{(N)} \tag{2}$$

这里 $p_1 \geqslant 0$,并且 $\sum_i p_i = 1$。

目前实验上制备的最完美的纠缠态是利用参量下转换的办法产生的纠缠光子对[4]。而最新进展则是在离子阱中制备出了四粒子纠缠态[5]。

1.1.1　Bell 态

两态的两粒子体系的纠缠态中有如下四个 Bell 基[6],它们构成特殊的表象,

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{3a}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{3b}$$

每个 Bell 基态都是双粒子体系最大纠缠态,它们是四维空间中的正交完备基,可用之对任意二粒子态 $|\Psi\rangle_{AB}$ 实施正交测量,称为 Bell 基测量。

每个 Bell 态携带非局域的两比特信息:Parity bit(宇称比特):$|\Phi\rangle$ 代表偶宇称,$|\Psi\rangle$ 代表奇宇称,Phase bit (相位比特) 分别由 +、– 来表征。

对单个两态粒子可实施如下的局域幺正变换(用 Pauli 矩阵表征):

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{4}$$

若对处于 Bell 基态的体系实施局域操作(如对粒子 A),则可实现 Bell 基之间的变换。σ_3 的作用是使 $|0\rangle_A$ 和 $|1\rangle_A$ 相对相位倒转,导致存储于纠缠态的相位比特倒转

$$|\Phi^+\rangle \leftrightarrow |\Phi^-\rangle, |\Psi^+\rangle \leftrightarrow |\Psi^-\rangle$$

σ_1 的作用是使自旋倒转($|0\rangle_A \leftrightarrow |1\rangle_A$),从而导致宇称比特倒转

$$|\Phi^+\rangle \leftrightarrow |\Psi^+\rangle, |\Phi^-\rangle \leftrightarrow |\Psi^-\rangle$$

σ_1 的作用等效于 $\sigma_1\sigma_3$ 功能,它使宇称比特和相位比特同时倒转

$$|\Phi^+\rangle \leftrightarrow |\Psi^-\rangle, |\Phi^-\rangle \leftrightarrow |\Psi^+\rangle$$

假定 Alice 和 Bob 分别持有处于 Bell 态的粒子 A 和 B,那么他们可使用局域幺正变换使某 Bell 基变换到任意 Bell 基,但这种局域变换无法改变粒子 A 和 B 的状态,它们的约化密度算符始终为 $\rho_A = \rho_B = \frac{1}{2}I$,换句话讲他们所操作的信息无法被局域地读出来。

若 Alice 和 Bob 对粒子 A 和 B 进行联合操作,就可以获得 Bell 态的宇称和相位比特的信息。

1.1.2 纠缠的度量

我们先来介绍由两子系构成的复合系统的纠缠定量化问题。目前,人们已广泛使用四个 Bell 态作为定量化两子系系统纠缠的标准,每个 Bell 态的纠缠度定义为 1,也称为一个 ebit(纠缠比特)。所谓纠缠度,就是指所研究的纠缠态携带纠缠的量的多少。纠缠度的提出,为不同的纠缠态之间建立了可比关系。

在给出具体的纠缠度定义之前,我们先介绍定量纠缠度所遵从的原则。最近荷兰科学家 Horodecki 父子将定义纠缠度的假定前提分成三组[7]。(一)明显假定:a)非负性,即 $E(\rho)\geqslant 0$;b)当 ρ 为非纠缠态,则 $E(\rho)=0$;c)四个 Bell 态的纠缠度为 1。(二)基本假定:a)局域操作下的单调性 如果仅对纠缠态 ρ 的各个子系实施局域的量子操作,以 p_i 的概率获得量子态 σ_i,则纠缠的期望值不能增长,即 $E(\rho)\geqslant\sum_i p_i E(\sigma_i)$,$\sum_i p_i=1$;b)凸性(信息抛除下的单调性):$E(\sum_i p_i\rho)\leqslant\sum_i p_i E(\rho_i)$,$\rho=\sum_i p_i\rho_i$。(三)渐进性假定:a)部分可加性:$E(\rho^{\otimes n})=nE(\rho)$;b)连续性 如果当 $n\to\infty$ 时 $<\Psi^{\otimes n}|\rho_n|\Psi^{\otimes n}>\to 1$,则 $\frac{1}{n}|E(\Psi^{\otimes n})-E(\rho_n)|\to 0$,这里 ρ_n 为 n 对的联合态。这三组假定是对目前所认识到的纠缠态规律的一个概括性的总结,带有相当普遍的意义。

目前,对两子系复合系统中纯态的纠缠定量化已经完成。它的纠缠度等于任一子系统约化密度矩阵的 von Neumann 熵[8]。由于两子系复合系统可以进行 Schmidt 分解[9],所以两子系统的纠缠度相等。对于混合态的纠缠度量则存在很大困难。Bennett 等人提出了生成纠缠和蒸馏纠缠的概念[10]。生成纠缠态 $E_F(\rho_{AB})$ 定义为:通过局域操作和经典通信过程,为制备纠缠态 ρ_{AB} 所消耗掉 Bell 态的最小数目,即如果制备 ρ_{AB} 的 n 份拷贝需要 k 个 Bell 态,则生成纠缠 $E_D(\rho_{AB})=\lim\limits_{n\to\infty}\frac{k'_{\min}}{n}$。类似地,蒸馏纠缠 $E_D(\rho_{AB})$ 定义为:通过局域操作和经典通信过程,可以从 ρ_{AB} 中提取出的 Bell 态的最大数目,即,有 n 份 ρ_{AB} 的拷贝,可从中提取 k' 个 Bell 态,则 $E_D(\rho_{AB})=\lim\limits_{n\to\infty}\frac{k'_{\max}}{n}$,生成纠缠和蒸馏纠缠的关系是 $E_F>E_D$。

除此之外,还有很多纠缠度的定义,这里不在赘述。迄今为止,人们仍未放弃寻找物理意义鲜明,同时又简单、易求解的纠缠度的定义。

多子系的纠缠态具有很多为两子系纠缠态所不具备的性质,定量化非常困难,目前对其研究尚处于起步阶段。现在,人们认为多子系纠缠态的纠缠度应由一组数来描述。Bennett 等人提出了最小可逆纠缠生成集的概念[11]。任何一个多子系纠缠态可由这组生成集以渐进可逆的方式实现,每个生成元都联系着一个纠缠度。但是,目前对这个生成集的构成尚不十分清楚。

1.1.3 纠缠态的判别及其分类

以上给出的纠缠态的定义非常形式化的。一般情况下,对一个具体的密度矩阵,人们

并不知道它是否具有子系密度矩阵的直积形式的分解,也就是说,不知道它是纠缠的还是非纠缠(可分)的。最先研究这个问题并取得重要进展的是 Peres,他给出了判别两子系系统的量子态为可分的必要条件[12]:两子系系统可分量子态 ρ_{AB} 的部分转置矩阵 σ_{AB} 为半正定。这里 ρ_{AB} 与 σ_{AB} 矩阵元的关系为:

$$\sigma_{m\mu,nv} = < m_A | < \mu_B | \sigma | n_A > | v_B > = < m_A | < v_B | \rho | n_A > | \mu_B > = \rho_{mv,n\mu} \quad (5)$$

此条件可以作为判别纠缠态的充分条件。即,如果我们发现一个密度矩阵的部分转置矩阵带有负的本征值,我们就可以判定这个量子态为纠缠态。人们将部分转置为负定的情形简记为 NPT,相反,部分转置为半正定则记为 PPT。Horodecki 等人随后证明了,PPT 是 2×2 和 2×3 系统可分态的充分必要条件[13],但若维度大于 2×3,PPT 仅为必要条件。

任何一个带有 PPT 特性的两子系复合系统的量子态,即使生成纠缠不为零,但蒸馏纠缠为零,即,我们无法通过局域操作和经典通信的手段从中提取出 Bell 态。Horodecki 将这种态称为“束缚纠缠态”[14]。这直接导致了纠缠态的分类,一般将束缚纠缠态以外的纠缠态通称为‘可蒸馏的纠缠态”。最新的研究成果表明,即使是 NPT 的纠缠态也存在束缚纠缠态的情况[15]。

由于无法从束缚纠缠态中蒸馏出 Bell 态,所以束缚纠缠态不能胜任 Bell 态在量子通信中的所扮演的角色。但束缚纠缠态的存在,提示了自然界更为深刻的一面,即信息的不可逆过程,这很类似于热力学中的熵增加现象。近来,关于束缚纠缠态的研究逐渐展开。人们发现在束缚纠缠态中存在一种‘纠缠激活’的有趣现象[16]。即当两地分享某种可蒸馏的纠缠态的同时也分享一定量的束缚纠缠态,在这种情况下,束缚纠缠态可以起到一定的‘泵浦’作用,使可蒸馏纠缠态具有更强的隐形传态能力。

1.2　量子不可克隆定理

1.2.1　量子不可克隆定理

1982 年,Wootters 和 Zurek 在《自然》杂志上发表了一篇短文中提出这样一个问题:是否存在一种物理过程,实现对一个未知量子态的精确复制,使得每个复制态与初始量子态完全相同?该文证明,量子力学的线性特性禁止这样的复制,这就是量子不可克隆定理的最初表述[17]。

量子不可克隆定理的证明很简单。以两态量子系统为例,其基矢选为 $|0>$ 和 $|1>$,设 $|s>$ 代表此二维空间任意量子态,量子克隆过程可以表示为

$$|s>|Q>_x \rightarrow |s>|s>|\tilde{Q}_s>_x \quad (6)$$

式中右端 $|s>|s>$ 表示初始模和复制均处于 $|s>$ 态,$|Q>_x$ 和 $|\tilde{Q}_s>_x$ 分别为装置在复制前后的量子态,复制后装置的量子态 $|\tilde{Q}_s>_x$ 可能依赖于输入态 $|s>$。假如存在(6)式的变换,那么对基矢 $|0>$ 和 $|1>$ 应该分别有

$$|0>|Q>_x \rightarrow |0>|0>|\tilde{Q}_0>_x \quad (7a)$$

$$|1>|Q>_x \rightarrow |1>|1>|\tilde{Q}_1>_x \quad (7b)$$

现假定 $|s>$ 是一个任意的叠加态,即

$$|s>=\alpha|0>+\beta|1>,\ |\alpha|^2+|\beta|^2=1 \tag{8}$$

由 7 式及量子操作的线性特征,不难得到在操作后,$|s>$ 将演变为 $|s>|Q>_x=(\alpha|0>+\beta|1>)|Q>_x\rightarrow\alpha|0>0>|\tilde{Q}_0>_x+\beta|1>1>|\tilde{Q}_1>_x)$ 如果复制机的态 $|\tilde{Q}_0>_x$ 与 $|\tilde{Q}_1>_x$ 不恒等,那么上式给出的初始模和复制模均于 $|0>$ 与 $|1>$ 的混合态;如果态 $|\tilde{Q}_0>_x$ 与 $|\tilde{Q}_1>_x$ 恒等,则初始模和复制模将处于纠缠态 $\alpha|0>0>+\beta|1>1>$。无论哪种情况,初始模和复制模都不可能处于直积态 $|s>|s>$。因此如果一个量子复制机能精确复制态 $|0>$ 和 $|1>$,则它不可能复制两态的叠加态 $|s>$,此即量子不可克隆定理的内容。

量子态不可克隆是量子力学的固有特性,它设置了一个不可逾越的界限。量子不可克隆定理是量子信息科学的重要理论基础之一。量子信息是以量子态为信息载体(信息单元)。量子态不可精确复制是量子密码术的重要前提,它确保了量子密码的安全性,使得窃听者不可能采取克隆技术来获得合法用户的信息。鉴于这个定理的重要性,近年来人们对它作了进一步的研究,揭示出更丰富的物理内涵。

在 W-Z 的证明中,假设了输入态是完全未知的。但在实际情况中,我们往往知道输入态属于一个确定的态集合。例如在基于非正交态的量子密码术中,输入态是两个非正交态的其中之一。W-Z 的证明基于量子叠加原理,该证明行之有效至少需要 3 种可能的输入态,如上面的 $|0>$,$|1>$ 及 $\alpha|0>+\beta|1>$,因此它没有排除克隆两个量子态的可能性。之后人们推广了量子不可克隆定理,使之适用于两态情况,指出如果克隆过程可以表示为一幺正演化,则幺正性要求两个态可以被相同的物理过程克隆,当且仅当它们相互正交,亦即非正交态不可以克隆[18]。该结果在量子密码术中有重要应用,我们知道,一个简单的量子密码方案就是随机地传送两个非正交的量子态,正因为非正交态不可克隆,所以窃听者无法窃取信息。

适用于两态的量子不可克隆定理后来被进一步推广到混合态情况,并证明了一个更强的定理,文献中称为量子不可播送定理[19]。设系统 A 处于两个可能的混合态 $\{\rho_0,\rho_1\}$ 中的一个,ρ_0,ρ_1 为密度算符,如果要将系统 A 的态克隆到系统 B 上,则演化后系统 AB 的态应为 $\rho_s\otimes\rho_s$,其中 $s=0,1$。但量子播送的要求更弱些,记演化后系统 AB 的态为 ρ_s,量子播送只要求

$$Tr_A(\rho_s)=\rho_s,\ Tr_B(\rho_s)=\rho_s \tag{9}$$

其中 Tr_A,Tr_B 分别表示对系统 A,B 求迹。因此量子播送只要求系统 AB 的约化态与演化前系统 A 的态一致。量子不可播送定理指出,两个混合态经过幺正演化可以被量子播送,当且仅当它们相互对易。该定理是量子不可克隆定理的强化,当 ρ_0,ρ_1 表示纯态时,显然量子不可播送定理回到两态的量子不可克隆定理。近来不可克隆定理又被推广到纠缠态情况[20]。Mor 甚至指出复合系统的正交态不可以被克隆[21],当然,这种正交态的不可克隆定理需要狭义相对论做基础。

量子不可克隆定理断言,非正交态不可以克隆,但它并没有排除非精确克隆即复制量子态的可能性。目前主要有两种克隆机:普适克隆机和概率克隆机。

1.2.2　普适量子克隆机

文献中常用态的保真度来表征量子克隆机的性能。设输入态为 $|\Psi_0>$,输入出态为 ρ,则保真度 F 定义为

$$F = <\Psi_0|\rho|\Psi_0> \tag{10}$$

普适量子克隆机(Buzek – Hillery 克隆机)对于任意的量子态都适用。其性能与输入态无关,两个输出态完全相同,但不等于输入态。这表明输入态在克隆过程中不可避免地遭到破坏,选择一组最佳参数可使得这种破坏达到最小程度。业已证明,对二维系统,输入、输出态之间的保真度最高可以达到 5/6[22]。

以上考虑的是一到二的克隆机。更一般的量子克隆机具有 N 个相同的输入态和 M 个($M > N$)相同的输出态。对于 N 到 M 的普适量子克隆机,其保真度最高可达到[23,24]

$$F_{N,M} = \frac{M(N+1)+N}{M(N+2)} \tag{11}$$

显然,当 $N=1$, $M=2$ 时,上式给出了单输入双输出的量子复制机的最佳保真度 5/6。

Buzek 等人给出了普适克隆机的逻辑网络[25],我们已经用光学的办法在实验上实现了普适量子克隆机[26]。

1.2.3　概率量子克隆机

概率量子克隆机(段 – 郭克隆机)[27,28]适用于线性无关的态集。它把幺正演化和测量过程相结合,以确定的大于零的概率产生输出,而且输出态一定是输入态的精确复制态。为构造概率量子克隆机,测量和合适的幺正演化都是不可缺的。如果只有幺正演化,显然非正交态不可以精确克隆;另一方面,如果只有测量,当输入态为非正交态时,机器不可能对其中任意一个输入态都以大于零的概率产生输出,且输出态还应是输入态的精确复制态。因此构造概率量子克隆机的关键是要设计出合适的幺正演化并要联系测量过程[29]。

概率克隆机成功产生输出的概率,定义为克隆效率,它决定了该机器的性能。显然,对于确定的输入态集合,我们希望设计一种机器,使得它具有最大效率,且该效率不依赖于具体的输入态,此时该机器称为最佳概率量子克隆机。业已证明,如要输入态属于集合 $\{|\Psi_0>, |\Psi_1>\}$,则概率量子克隆机的最高效率为

$$\eta_{\max} = \frac{1}{1+<\Psi_0|\Psi_1>} \tag{12}$$

显然只有对于正交输入态,该效率才能达到 1,这一点保证了基于传送两个非正交态的量子密钥体系的安全性。

1.3　消相干与量子编码

现在利用计算机进行复杂运算时,我们不再为结果的可靠性担心。但是在计算机概念刚提出时,曾经有人提出如下反驳:在计算机这样一个复杂系统中,噪声是不可避免的,只要噪声使得计算机中任一部件发生一次错误,最后的运算结果都会变得面目全非,因

此,利用计算机进行复杂运算是不可能的。这一困难后来是怎样克服呢?编码在这过程中起了关键性的作用。什么是编码?编码,更准确地说,信道编码,指的是,通过引入冗余信息,使得在一部分比特发生错误的情况下,仍有可能按照一定的规则纠正这些错误,以实现无失真地传送和处理信息。举一个最简的重复码为例,我们可以将信号 0 编码为 000,信号 1 编码为 111,这样如果最多只有一个比特发生错误,譬如,000 变成了 001,我们可以按照少数服从多数的原则,找出错误的比特(第三比特),并纠正该错误。

以上是经典编码的基本概念,为什么要引进量子编码呢?这与量子信息论特别是量子计算机的发展有关。量子信息论中,信息的载体为量子比特。量子比特可以处于 0,1 两个本征态的任意叠加态,而且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,这就是所谓的量子相干性,已经发现,在量子信息论的各个领域,量子相干性都起着本质性的作用,可以说,量子信息论的所有优越性均为自于量子相干性,但由于环境的影响,量子相干性将不可避免地随时间指数衰减,这就是困扰整个量子信息论的消相干问题[30]。消相干引起量子错误,量子编码的目的就是为了纠正或防止这些量子错误。虽然量子编码和经典编码的基本想法类似,即要以合适的方式引进信息冗余,以提高信息的抗干扰能力,但量子码可不是经典码的简单推广,在量子情况下,编码存在着一些基本困难,表现在如下 3 个方面。

1)经典编码中,为引入信息冗余,需要将单比特态复制到多比特上去,但在量子力学中,量子态不可克隆定理禁止态的复制。

2)经典编码在纠错时,需要进行测量,以确定错误图样,在量子情况下,测量会引起态坍缩,从而破坏量子相干性。

3)经典码中的错误只有一种,即 0,1 之间的跃迁。而量子错误的自由度要大得多。对于一个确定的输入态,其输出态可以是二维空间中的任意态。因此,量子错误的种类为连续统。

因为这些原因,量子纠错比经典纠错困难得多,事实上,直到 1995 年底至 1996 年,Shor[31]和 Steane[32]才独立地提出了最初的两个量子纠错编码方案,量子纠错码通过一些巧妙的措施,克服了上面的 3 个困难,具体为

1)为了不违背量子态不可克隆定理,量子编码时,单比特态不是被复制为多比特的直积态,而是编码为一较复杂的纠缠态。对于纯态而言,纠缠态即指不能表示为直积形式的态。通过编码为纠缠态,既引进了信息冗余,又没有违背量子力学的原理。

2)量子纠错在确定错误图样时,只进行部分测量,通过编码,可以使得不同的量子错误对应于不同的正交空间,部分的量子测量(即只对一些附加量子比特,而不是对全部比特进行测量)使得态投影到某一正交空间,在此正交空间,信息位之间的量子相干性仍被保持,同时测量的结果又给出量子错误图样。

3)量子错误的种类虽然为连续统,但人们发现,它可以表示为 3 种基本量子错误(对应于 3 个 Pauli 矩阵)的线性组合。只要纠正了这 3 种基本量子错,所有的量子错误都将得到纠正。

自从发现了最初的两个量子编码方案,各种更高效的量子码已被相继提出。下面我们介绍几种最重要的量子编码方案。

1.3.1　量子编码方案

(1)量子纠错码。Shor[31]的第一个纠错方案为量子重复码,它利用 9 比特编码 1 比特信息,可以纠正 1 位错,Shor 的方案简单,而且与经典重复码有较直接的类比,但它的效率不高。事实上,Steane[32]的编码方案对后来的量子纠错码影响更大,在该方案中,Steane 提出了互补基的概念,给出了量子纠错一些一般性的描述,并具体构造了一个利用 7 比特来编码 1 比特纠 1 位错的量子码。紧接着,Calderbank 和 Shor[33]以及 Steane[34]提出了一个从经典纠错码构造量子纠错码的方法,该方法建立在群论语言之上,纠 1 位错的最佳(效率最高)量子码也由两个小组独立地发现,该方案利用 5 比特来编码 1 比特,纠多位错的量子码情况更复杂,迄今为止,只发现一些简单的纠多位错的量子码。现有的各种量子纠错码,都可以被统一在群论框架之下,该描述已由 Gottesman[35]和 Calderbank 等[36]给出,但利用现有理论去构造新的量子纠错码,仍然是一件非常艰巨的工作,为了寻求更高效的量子码,人们往往需要逐步地摸索。

量子纠错码适用于独立消相干,其优点为适用范围广,缺点为效率不高。

(2)量子防错码。量子防错码[37,38]利用了量子 Zeno 效应(看门狗效应)。量子 Zeno 效应[39]是指 如果以很高的频率对一个系统进行测量,则系统不会发生演化。那么,如果以很高的频率来观察一个量子系统是否发生消相干,根据 Zeno 效应,系统将总是不发生消相干。量子防错码的效率高,但其缺点是测量的频率要求很高,而且噪声的增长不能太快。

(3)量子避错码。量子避错码基于消相干中的集体效应。Palma 等[40]和我们课题组[41]先后考察了量子比特消相干过程中的集体效应,发现集体消相干和独立消相干具有本质的不同,最突出的一点是,对于集体消相干,存在相干保持态。相干保持态是指一类能在噪声环境下保持稳定的态。量子避错码即是将一个任意输入态编码为一个较高维空间的相干保持态。对于实际中很重要的一类量子噪声,我们设计了一个用二比特编码一比特信息的量子避错码方案[42],意大利的量子信息小组将该方案推广到更普遍的噪声模型[43],但相应地要求用四比特来编码一比特量子信息。量子避错码的优点为效率很高,而且不需要进行测量和纠错操作,其缺点为只能适用于克服集体消相干。

关于量子编码的实验进展,目前已经在核磁共振中演示了纠相位错的三比特[44]和两比特[45]纠错码。

1.3.2　量子编码定理

量子编码定量研究的目标是要寻找经典 Shannon 定理的量子对应。Shannon 信源编码定理确定了任一信源给出的信息的最大压缩率,信道编码定理确定了信息在有噪信道中无失真地传输的最大速率,亦即信道容量,Shannon 定理奠定了整个经典信息论的基础。对于量子信息论,是否存在类似的定理?能否引进信道容量的概念?如何发展有效的算法去计算量子信道容量?这些问题显然都是量子信息论中的基本问题。

早在 1993 年,Schumacher 就证明了一个比较初步的量子信源编码定理[46],该证明后来经 Jozsa 和 Horevo 的工作得到进一步的简化和推广。量子信源以概率 p_i 发送密度算

符为 ρ_i 的量子态，$\rho=\sum_i^i p_i\rho_i$ 表示信源的总密度算符。量子信源编码定理要回答的是，对于这样的量子系统，其信息最少可以用多少量子比特表征出来？Schumacher 的定理表明，如果所有 ρ_i 均限制为纯态，以 2 为底的 Von-Neumann 熵 $S(\rho)=-tr(\rho\log_2\rho)$ 确定了所需的最小量子比特数。熵是量子力学中的重要概念。Schumacher 的定理揭示出，量子力学和信息论这两个看起来互不相关的学科，实际上却存在着内在的联系。Schumacher 的定理后来经 Holevo 推广到 ρ_i 为混合态的情况，此时相对 Von-Neumann 熵 $S(\rho)-\sum_i p_i S(\rho_i)$ 确定了所需的最小量子比特数。

在经典信息中，信道容量只需要一个量即可表征。但在量子信息中，根据不同的辅助资源和通信用途，量子信道有几种不同的容量[1]。包括：

1）经典容量，C，等于通过此量子信道可靠地传送经典比特的最大速率。

2）量子容量，Q，指通过信道完全可靠地传送量子比特的最大速率。

3）经典辅助量子容量，Q_2，定义为在通信双方无限制的经典通信辅助下，通过信道完全可靠地传送量子比特的最大速率。

4）纠缠辅助经典容量，C_E，定义为在通信双方拥有无限制的事先分享的量子纠缠的辅助下，通过此信道可靠地传送经典比特的最大速率。

对于所有已知的量子信道，这些容量之间满足关系 $Q\leqslant Q_2\leqslant C\leqslant C_E$，这些容量各自随着信道参数的变化而独立变化，但是计算起来比较困难。

2 量子通信

量子通信是量子信息中研究较早的领域，比较典型的通信方式有：量子密集编码[47]，用量子信道传送经典比特；量子隐形传态[48]，用经典辅助的办法传送量子态。量子通信中还有一个很重要的分支是量子密码，即信息的保密传送。

2.1 量子密集编码

假定 Alice 与 Bob 早已建立量子通道，他们共享 Bell 态 $|\Phi^+>_{AB}$，Alice 对她的纠缠粒子 A 可以施加四种可能的幺正变换 $\{I,\sigma_1,\sigma_2,\sigma_3\}$。她选择其中之一进行操作，其作用是编码进两个比特经典信息。这个操作实际上是将 A－B 量子通道 $|\Phi^+>_{AB}$ 变换成下列四种正交态中一个上：

$$|\Phi^+>_{AB},(\text{偶宇称，正相位}),(0,0)$$
$$|\Psi^+>_{AB},(\text{奇宇称，正相位}),(1,0)$$
$$|\Psi^->_{AB},(\text{奇宇称，负相位}),(1,1)$$
$$|\Phi^->_{AB},(\text{偶宇称，负相位}),(0,1)$$

现在 Alice 将她的粒子 A 发送给 Bob，Bob 对两个粒子实行 Bell 基测量（联合测量），测量结果可使 Bob 确认 Alice 所做的变换，于是他获得由 Alice 传送给他们两个比特的经典信息。因此，Alice 仅送给 Bob 一个粒子，便能成功地传送了两个比特的经典信息，这就是所谓的“密集编码”[45]。

量子密集编码有如下优点：

1)保密性强。所传的量子比特 $\rho_A = \frac{1}{2} I_A$,不携带任何信息,窃听者即使载获此量子比特,也无法破译。所有信息均编制在 A-B 之间关联上,局域测量无法提取。

2)量子通道可以在使用之前早就制备好,在紧急时使用,就可以更有效地传送信息。

量子密集编码已由 Innsbruck 小组完成[49],由于 Bell 基识别的困难,他们只实现了四种操作中的三种,即传送了 1.58 比特。

2.2　量子隐形传态

在量子密集编码中,量子纠缠可用来加速经典信息的传输。那么,我们可否使用经典信息来实现量子信息传输？

现假定 Alice 和 Bob 之间有 EPR 对 $|\Phi^+>_{AB}$,Alice 有一粒子 C 处于未知量子态 $|\Psi>C$。Alice 对 C 和她拥有的 EPR 粒子 A 实施 Bell 基测量,这个测量将随机地把 $A\otimes C$ 投影到四个态 $|\Phi^\pm>_{CA}$,$|\Psi^\pm>_{CA}$ 当中的一个。然后 Alice 将测量结果(两比特的经典信息)告诉 Bob,后者按照这个信息对他所拥有的粒子 B 施加相应的操作(四种 Pauli 操作之一),这个作用可以使 B 的粒子变换到 $|\Psi>_c$ 的精确复制态上,这便实现了量子隐形传态[44]。Alice 的测量结果与 Bob 应当实施的相应局域操作之间的对应关系如下：

$$|\Phi^+>_{CA}\rightarrow I_B,\ |\Psi^+>_{CA}\rightarrow\sigma_1^{(B)}$$
$$|\Psi^->_{CA}\rightarrow\sigma_2^{(B)},\ |\Phi^->_{CA}\rightarrow\sigma_3^{(B)} \tag{13}$$

量子隐形传态的特点是,量子态 $|\Psi>_C$ 被传送给 $|\Psi>_B$(从 $C\rightarrow B$),但粒子 C 本身不被传送。应特别指出

1)事先,粒子 C 与 B 不纠缠,Alice 测量之后,在 A 与 C 之间建立了关联。

2) Alice 的测量输出是完全随机,故这个测量无法获得任何关于 $\Psi>C$ 的信息。

3)从 Alice 传送给 Bob 的两比特经典信息,也给不出 $|\Psi>_C$ 信息。

4) A 与 B 共享的 EPR 粒子对也给不出 $|\Psi>_C$ 信息,它们早就存在了。

5)这过程不是克隆 $|\Psi>_C$,因为在 Alice 测量之后,$|\Psi>_C$ 已被破坏掉。

6) $|\Psi>_C$ 被分解为经典信息和量子信息两部分,只有两者共同组合才能重新构造出来。

下面用量子力学公式来描述上述的量子隐形传态过程。设

$$|\Psi>_C = a|0>+b|1>,\ |a|^2+|b|^2=1 \tag{14}$$

初始时,粒子 C 和 EPR 粒子对 A-B 构成的整个系统,其量子态为

$$|\Psi>_C\otimes|\Phi^+>_{AB} = \frac{1}{2}|\Phi^+>_{CA}|\Psi>_B+\frac{1}{2}|\Psi^+>_{CA}\sigma_1|\Psi>_B$$
$$+\frac{1}{2}|\Psi^->_{CA}(-i\sigma_2)|\Psi>_B+\frac{1}{2}|\Phi^->_{CA}\sigma_3|\Psi>_B, \tag{15}$$

式中为 $|\Phi^\pm>_{CA}$,$|\Psi^\pm>_{CA}$ 粒子 C 和 A 的 Bell 基态。

Alice 对粒子 C 和 A 的实施 Bell 基测量,会使 Bob 粒子 B 投影到相应的纯态上,这个纯态与 $|\Psi>_B$ 之间为幺正变换。Bob 可按照 Alice 经典通道传送来关于她测到那个 Bell

基态的信息,采用式(13)相应的幺正变换对粒子 B 实施操作,粒子 B 便处式(14)的量子态上。

目前已有四个小组完成了量子隐形传态实验。Innsbruck 小组用了与密集编码相同的装置实现了从一个光子的态传递到另一个光子上[50]。Rome 小组则采用了一个更为简单的办法,把量子态从纠缠光子对中的一个光子传递到另一个光子上[51]。最近 CIT 小组则根据 Vaidman 的方案[52]完成了连续变量的隐形传态[53]。还有一个实验是在 NMR(核磁共振)中实现的[54],但是传递的距离很短,把态从样品分子中的一个原子传递到另一个原子上。

2.3 量子密码术

现代保密通信的原理图如下:

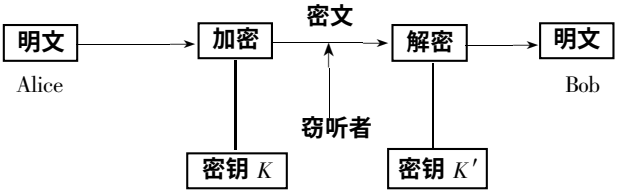

图 1 保密通信原理图

Alice 采用密钥 K(随机数)将她要发送给 Bob 的明文通过某种加密规则变换成密文,然后经由公开的经典信息通道传送给 Bob,后者采用密钥 K' 通过适当的解密规则将密文变换成为明文。这个过程如果能够有效地防止任何非法用户的窃听,那就是安全的保密通信。

按照密钥 K 和 K' 是否相同,密钥系统可分为对称密码($K = K'$)和非对称密码($K \neq K'$)。数学上证明存在有不可破译的对称密钥,即 Vernam 密码或一次性便笺式密码,它要求密钥应与明文一样长,而且仅能使用一次。这种体系需要用户双方拥有庞大的相同密码(随机数),因此密钥的传送、保管等都极不安全,不宜广泛使用。目前广泛用于网络、金融行业的是非对称密码,它是一种公开密钥,加密和解密法则、加密的密钥 K 均是公开的,只是解密的密钥 K' 不公开,只有接收者 Bob 本人知道。这种密钥的安全性基于大数因子分解这样一类不易计算的单向性函数。数学上虽没能严格证明这种密钥不可破译,但现有经典计算机几乎无法完成这种计算。

Shor 量子算法证明,采用量子计算机可以轻而易举地破译这种公开密钥体系。这就对现有保密通信提出了严峻挑战。解决这个问题的有效途径是量子密码术。它采用量子态作为信息载体,经由量子通道传送,在合法用户之间建立共享的密钥(经典随机数)。

量子密码的安全性由量子力学原理所保证。所谓绝对安全性是指窃听者智商极高,采用最高明的窃听策略,使用一切可能的先进仪器,在这些条件下,密钥仍然是安全的。窃听者的基本策略有两类:一是通过对携带着经典信息的量子态进行测量,从其测量的结果来获取所需的信息。但是量子力学的基本原理告诉我们,对量子态的测量会干扰量子态本身,因此,这种窃听方式必然会留下痕迹而被合法用户所发现。二是避开直接量子测

量而采用量子复制机来复制传送信息的量子态,窃听者将原量子态传送给 Bob,而留下复制的量子态进行测量以窃取信息,这样就不会留下任何会被发现的痕迹。但是量子不可克隆定理确保窃听者不会成功,任何物理上可行的量子复制机都不可能克隆出与输入量子态完全一样的量子态来。因此,量子密码术原则上可以提供不可破译、不可窃听的保密通信体系。

首先想到将量子力学用于密码术的是美国的 Wiesner,他在 1970 年提出用共轭编码制造不可伪造的‘银行支票’等。因为他的想法太新奇,论文被拒绝刊登,直到 1983 年才得以在会议录上发表[55]。

目前,量子密码的方案主要有四种:

1)基于两种共轭基的四态方案,其代表为 BB84 协议[56];

2)基于两个非正交态的两态方案,如 B92 协议[57];

3)基于 EPR 佯谬的 EPR 对方案,由 Ekert 于 1991 年提出,称为 EPR 协议或 E91 协议[58];

4)基于正交态的密钥分配方案[21,59,60],其基础为正交态的不可克隆定理[21]。

显然,这里所说的量子密码(量子密钥分配)实际上是量子辅助的经典密码。最近,我们建立了真正意义上的量子密码体系[61]。

量子密钥分配(QKD)的第一个演示性实验由 Bennett 等人完成[62]。目前的实验方向有二:光纤中的 QKD 和自由空间的 QKD。光纤中的 QKD 实验已经逐渐走向成熟[63~66],目前传输距离已经达到 48 公里[66]。自由空间中的 QKD 也不断取得突破[67~69],现在达到的传输距离为 1.5 公里[69],而且是在白天进行的实验。前面的实验都是基于 BB84 或 B92 协议,最近 E91 协议的 QKD 也已取得重大进展[70~72]。

关于量子保密通信,还有许多问题需要解决。其中最典型和最重要的是量子比特承诺问题。量子比特承诺是最基础的量子保密通信协议,如果比特承诺是可行的,则可利用它来实现各种各样的保密通信协议,如远程硬币投掷、保密量子计算等等。

问题本身很简单,比如 A 向 B 宣称自己有特异功能,如果 B 要投掷一枚硬币,A 能预测出硬币是‘正面’还是‘反面’朝上。两个人需要用比特承诺的办法来检验 A 是否说谎。一个很实际的办法是:A 把他的预测写在一张纸上,如果‘正面’朝上,则写 0;“反面”朝上,则写 1。然后把纸放到一个密码箱里。A 把密码箱给 B,但钥匙必须自己保留(否则 B 可以根据纸上的结果来投掷硬币)。等 B 掷完硬币后,A 再打开密码箱检验他是否预测成功。然而这个办法却是不安全的,因为 B 可以用透视等等办法看到纸上的内容。用量子力学的办法能否实现比特承诺呢?

开始时,许多量子比特承诺的方案被提出。但是后来 Mayers[73],Lo 和 Chau[74] 独立证明所有以前的比特承诺方案都是有漏洞的,即存在 EPR 攻击。A 可以利用量子纠缠的办法任意地改变 0 和 1(此结论被称为 Mayers-Lo-Chau 定理)。此后,量子信息界对量子比特承诺比较悲观。但是 Mayers-Lo-Chau 定理并没有表明任意的量子比特方案都是不安全的,现在关于量子比特承诺是否安全的争论仍在继续。

3 量子计算

量子比特可以制备在两个逻辑态 0 和 1 的相干叠加态,换句话讲,它可以同时存储 0 和 1。考虑一个 N 个物理比特的存储器,若它是经典存储器,则它只能存储 2^N 个可能的数当中的任一个,若它是量子存储器,则它可以同时存储 2^N 个数,而且随着 N 的增加,其存储量子信息的能力将指数上升,例如,一个 250 量子比特的存储器(由 250 个原子构成)可能存储的数目比现有已知的宇宙中的全部原子数目还要多。

由于数学操作可以同时对存储器中全部的数进行,因此,量子计算机在实施一次的计算中可以同时对 2^N 个输入数进行数学运算。其效果相当于经典计算机要重复实施 2^N 次操作,或者采用 2^N 个不同的处理器实行并行操作。可见,量子计算机可以节省大量的运算资源(如时间、记忆单元等)。

量子加速表现最明显的是大数因子分解问题,其量子算法(Shor 算法)[75,76]是经典算法的指数加速。另外存在指数加速的还有 D-J 算法[77]和多体量子体系模拟[78]等。相对而言,有大量的问题存在方根加速,即解决此类问题的量子算法所需时间正比于经典算法所需时间的平方根,其代表是搜索问题[79,80]。而对于其它问题则没有量子加速,这包括迭代问题[81]和宇称问题[82]等。

3.1 量子算法

我们主要介绍具有广泛影响的 Shor 算法和 Grover 算法。

3.1.1 大数因子分解算法(Shor 算法)

为开拓出量子计算机巨大的并行处理能力,必须寻找适用于这种量子计算的有效算法。Shor 于 1994 年发现的 Shor 算法[75]可以有效地用来进行大数因子分解。大数因子分解是现在广泛用于电子银行、网络等领域的公开密钥体系 RSA 安全性的依据。采用现有计算机对数 N(二进制长度为 $\log N$)做因子分解,其运算步骤(时间)随输入长度($\log N$)指数增长。

Shor 算法的主要思想为,首先利用数论中的一些定理,将大数因子分解转化为求一个函数的周期问题,而后者可以用量子快速傅立叶变换在多项式步骤内完成。设 N 为要分解的自然数,首先随机地选择一个与 N 互质的自然数 c,构造如下函数

$$f(x) = c^x (\mathrm{mod}\ N) \tag{16}$$

其中 mod N 表示 $f(x)$与 c^x 对 N 的余数相等,如 $1 = 4 (\mathrm{mod}\ 3)$。Shor 证明,只要求得 $f(x)$的周期,就能按一定程序得到 N 的一个因子。求 $f(x)$的周期,用的是量子 FFT 算法。输入态

$$| \Psi_i > = \sum_{x=00\ldots0}^{x=11\ldots1} f(x) | x > \tag{17}$$

的量子 FFT 由下式给出

$$|\Psi_f\rangle = \sum_{x=00\ldots0}^{x=11\ldots1} [2^{-k/2}\sum e^{2\pi i x x'}] f(x') |x\rangle \tag{18}$$

其中 k 为 x 在二进制表示下数据长度。可以看出,量子 FFT 实际上就是将态前面的叠加系数变为原叠加系数的离散傅里叶变换,可以证明,上述变换可以大约在 k^2 步骤内完成。对变换后的波函数进行位置的测量,就可以得出原叠加系数的周期,这非常类似于利用晶格的 X 光衍射来确定晶格周期,晶格周期就相当于这里 $f(x)$的周期。得到 $f(x)$的周期后,按照一定的概率算法,可以推导出 N 的一个因子,但因为是概率算法,所以不一定每次都成功。Shor 证明,成功的概率仅随着输入数 N 的二进制长度多项式递减。因此只要将上述过程重复多项式次,就可以以非常接近 1 的概率找到 N 的一个因子,而多项式算法的多项次重复,仍然是个多项式算法。这就证明,利用量子计算机,可以在多项式步骤内进行大数因子分解。

实验上,目前一个推广了的 Shor 算法已经在核磁共振中得到实现[83]。

3.1.2　量子搜索算法(Grove 算法)

1997 年 Grover 发现了另一种很有用的量子算法,即所谓的量子搜索算法[76],它适用于解决如下问题:从 N 个未分类的客体中寻找出某个特定的客体。经典算法只能是一个接一个搜寻,直到找到所要的客体为止,这种算法平均地讲要寻找 $N/2$ 次,找到几率为 1/2,而采用 Grover 的量子算法则只需要$\sqrt{N}$次。例如,要从有着 10^6 号码的电话本中找出某人的电话号码,该电话本是以号码排序的。经典方法是一个个找,平均要找 5×10^5 次,才能以 1/2 几率找到所要电话号码。Grover 的量子算法每查询一次可以同时检查所有 10^6 个号码。由于 10^6 量子比特处于纠缠态,量子干涉的效应会使前次的结果影响到下一次的量子操作,这种干涉生成的操作运算重复 1000(即$\sqrt{N}$)次后,获得正确答案的几率为 1/2。但若再多重复操作几次,那么找到所需电话号码的几率接近于 1。

Grover 算法的用途很广,可以寻找最大值、最小值、平均值等,也可以用于下棋。最有趣的是可有效地攻击密码体系,如 DES (the data encryption standard)体系,这个问题的实质是从 $2^{56}\approx7\times10^{16}$个可能的密钥中寻找一个正确的密钥。若以每秒 10^6 密钥的运算速率操作,经典计算需要 1000 年,而采用 Grover 算法的量子计算机则只需小于 4 分钟的时间。

目前,Grover 算法已经在核磁共振[84,85]和光学系统[86]得到实现。

3.2　量子模拟

除了进行上些超快速计算外,量子计算机另一方面的重要用途是用来模拟量子系统。早在 1982 年,Feymann 就猜想,量子计算机可以用来模拟一切局域量子系统,这一猜想,在 1996 年由 Lloyd 证明为正确的[87]。Lloyd 进一步指出,大约需要几百至几千个量子比特,即可精确地模拟一些具有连续变量的量子系统,例如格点规范理论和一些量子引力模拟。这些结果表明,模拟量子系统的演化,很可能成量子计算机的一个主要用途[78]。

一般地说,量子模拟可以按下列步骤来完成:① 根据所研究的量子体系的哈密顿量,设计出能够实现相应的幺正变换 U 的量子网络;②将 N-量子比特按照要求制备为特定

初态 $|\Psi_0>$；③操作计算机进行模拟运算。计算机的终态就是所需的量子态 $U|\Psi_0>$。因此，一旦人们有了量子模拟计算机，就无需求解薛定谔方程或者采用蒙特卡罗方法在经典计算机上做数值运算，便可精确地研究量子体系的特性。

有许多量子体系可以用这种方法来研究，例如：①高温高密度等离子体；②采用格点规范理论描述的体系，如量子色动力学；③晶体固态模型，包括诸如 Hubbard 模型的固体费米系统，其量子对称性使得它们难以采用蒙特卡罗技术来模拟；④固体模型，包括诸如高温超导体的长程关联；⑤ 分子行为的量子模型等等。

在核磁共振中，量子模拟的初步实验业已展开[88,89]，目前已经模拟了量子谐振子和反谐振子的动力学行为[88]以及三体碰撞哈密顿量的演化[89]。

3.3 量子逻辑网络

正如经典计算机建立在通用图灵机基础之上，量子计算机也可建立在量子图灵机基础上。量子图灵机可类比于经典计算机的概率运算。通用图灵机的操作是完全确定性的，用 q 代表当前读写头的状态，s 代表当前存储单元内容，d 取值为 L，R，N，分别代表读写头左移、右移和不动。在确定性算法中，当 q，s 给定时，下一步的状态 q'，s' 以及读写头的运动 d 完全确。我们也可以考虑概率算法，即当 q，s 给定时，图灵机以一定的概率 $\delta(q,s,q',s',d)$ 变换到状态 q'，s' 及实行运动 d。概率函数 $\delta(q,s,q',s',d)$ 为取值[0，1]的实数，它完全确定了概率图灵机的性质。

量子图灵机非常类似于上面描述的经典概率图灵机，现在 q，s，q'，s' 响应地变成了量子态，而概率函数则变成了取值为复数的概率振幅函数，量子图灵机的性质由概率振幅函数确定。正因为现在的运算结果不再按概率叠加，而是按概率振幅叠加，所以量子相干性再量子图灵机中起本质性的作用，这是实现量子并行计算的关键。

量子计算机可以等效为一个量子图灵机，但量子图灵机是一个抽象的代数模型，如何再物理上构造出量子计算机呢？理论上已证明[90]，量子图灵机可以等价为一个量子逻辑电路，因此可以通过一些量子逻辑门的组合来构成量子计算机。量子逻辑门按其输入比特的个数可分为单比特、二比特以及三比特逻辑门等。因为逻辑门是可逆的，所以其输入和输出比特数相等。量子逻辑门对输入比特进行一个确定的幺正变换，得到输出比特。Deutsch[91]最先发现，几乎所有的三比特量子逻辑门都是通用逻辑门。通用逻辑门的含义是指，通过该逻辑门的级联，可以以任意精度逼近任何一个幺正操作。后来不少人发展了 Deutsch 的结果，最终 Deutsch 和 Lloyd 独立地证明[92]，几乎所有的二比特量子逻辑门都是通用的，这里‘几乎’是指，两比特通用量子逻辑门的集合是所有两比特逻辑门的集合的一个稠密子集。

实验上通常用一些具体的量子逻辑门来构造计算机。Barenco 等人[93]证明，一个两比特的受控非和对一比特进行任意操作的门可构成一个通用量子门集。相对来说，单比特逻辑门在实验上比较容易实现，现在的不少实验方案都集中于制造量子受控非。量子受控非和经典异或门非常类似，它有两个输入比特：控制比特和受控比特。当控制比特处于 $|1>$ 态，即在上能级时，受控比特态发生反转。用记号 C_{12} 代表量子异或操作，其中 1，2 分别代表控制和受控比特，则有 $|n_1>_1|n_2>_2 \xrightarrow{c_{12}} |n_1>_1|n_1\oplus n_2>_2$，其中 n_1，n_2 取值

0 或 1,$\oplus$表示模 2 加。

量子逻辑网络另一个值得关注的方向是 Gottesman 和 Chuang 在《自然》杂志撰文提出的利用单比特逻辑门,Bell 基测量和多粒子纠缠实现任意的逻辑网络[94]。这种逻辑网络的构造思路,请参阅[95]。

3.4　量子容错计算

经典的容错计算是由 von Neumann 发现的,他指出只要经典门操作出错的几率小于一定的阈值,那么就可以用这些不可靠的逻辑门可靠地完成任意长度的经典计算。

量子容错计算[96]对量子计算机的发展至关重要,一种形象的说法是量子容错计算把量子计算机从垃圾堆里捡了回来。研究表明只要消相干出错和量子门操作出错的几率都小于一定的阈值(各种估计表明在 $10^{-6}\sim10^{-2}$之间),就可以进行任意复杂的量子计算。量子容错计算的基础是量子纠错编码。

4　量子对策论

对策论亦称博弈论,作为运筹学中的一个重要分支,就是研究具有对抗性或竞争性质的数学理论和方法。早在两千多年前的中国古代,就已经有了"田忌赛马"这样的对策研究的例子。不过,经典对策论直到本世纪初才成为数学的一个重要分支被系统地研究,其奠基之作就是 von Neumann 和 Morgenstern 合著的《博弈论和经济行为》。

物理学家受到量子信息其它领域的启发,很自然的要考虑:如果对策拓展到量子领域,即允许存在量子策略会得出什么结果?一个很自然的结论就是量子策略不会比经典策略差,因为经典策略集是量子策略集的子集。实际研究表明,由于量子力学的纠缠和叠加等特性,量子对策比经典对策要丰富多采得多。

量子对策论与量子信息论的其他领域如量子通信与量子计算有着深刻的联系。比如量子通信的各方与窃听者的对抗,对抗双方可以采用量子及经典策略。

量子对策论是一个新兴领域,具体的框架还不明朗。我们将通过详细介绍几个例子,包括 PQ 翻硬币问题[97]、量子博弈[98]和量子囚徒怪圈[99],来看一下量子对策的内容和方法及一些结果。

4.1　PQ 翻硬币问题

代号为 P 和 Q 的两个人进行这样一个游戏:P 把一枚正面朝上的硬币放进一个盒子里,然后他和 Q 二人按 Q,P,Q 的顺序去操作,即翻或不翻这枚硬币,但是不能看这枚硬币的状态(即朝上还是朝下);当最后打开盒子时,如果正面朝上,Q 赢,否则 P 赢。

这是一个二人零和游戏,可以用下面的支付矩阵来分析:

	NN	*NF*	*FN*	*FF*
N	– 1	1	– 1	1
F	1	– 1	1	– 1

表格的两行表示 P 的两种策略,四列表示 Q 的四种策略;F 表示翻,N 表示不翻;表格里的数字表示 P 的收益,1 表示 P 赢而 Q 输,– 1 表示 P 输 Q 赢。例如,第一行第二列,表示 Q 第一次不翻而第二次翻,P 不翻;这样硬币的状态就先后为:H,H,H,T,所以这一局 P 赢。

象这一个对策游戏没有一个确定性的策略解,任何一方使用一个确定策略(或称为单纯策略),另一方就可以使用相应策略使其必输无疑。但是,von Neumann 已经证明,任何一个有限策略的零和对策,总存在概率解,即混合策略。象这一游戏,其平衡解就是:P 分别以 1/2 的概率使用其两种策略 N,F;而 Q 分别以 1/4 的概率使用其四种策略 NN,NF,FN,FF 或者说每次都以 1/2 的概率使用 N,F 两种策略。在此情况下,双方的收益的期望值都为 0,并且在一方采取平衡解时,另一方无法通过改变其使用的概率来提高其期望值。

本游戏的主人公之一 P 用概率论分析得到以上结果后,发现这游戏还算公平,就答应与 Q 玩这一游戏,可是结果每次都输,原因何在?

其中奥妙就在于 Q 没有按上面的分析每次混合使用策略 N,F。在经典情况下,硬币状态集为 $\{H,T\}$,Q 可采取混合策略 $\frac{1}{2}\begin{bmatrix} & H & T \\ H & 1 & 1 \\ T & 1 & 1 \end{bmatrix}$,即无论硬币处于 H 还是 T 状态,都以 1/2 的概率翻或者不翻。Q 使用的是量子策略,是把这两种策略叠加起来,使用 $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ 策略,这样就把硬币从 $|H>$ 态变为 $\frac{1}{\sqrt{2}}(|H>+|T>)$ 态,无论 P 翻($|H>$ 变为 $|T>$,$|T>$ 变为 $|H>$)还是不翻,硬币还是保持这一状态不变。然后,Q 再使用一次 $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ 策略,硬币状态就变为 $|H>$,所以 Q 必赢无疑。

对于二人零和对策问题,类比于经典对策论,Meyer 提出并证明了三个定理:

定理一 在二人零和对策中的对弈者,使用最优量子策略的收益期望值不低于使用最优经典混合策略的收益期望值。(证明:因为经典混合策略都可以找到一个量子策略来表示。)

定理二 二人零和对策中并不一定存在双方都采用单纯量子策略的平衡点。

定理三 二人零和对策中总存在双方均采取混合(或单纯)量子策略的平衡点。

4.2 量子博弈

赌博中有这样一个常见的游戏:Alice 在一个盒子里随机朝上或朝下(几率相等)放一个硬币。当 Bob 打开这个盒子,如果硬币朝上,Bob 赢(简单起见,假设赢一个硬币),否则 Bob 输一个硬币。但是在经典情况下,Bob 不易检验 Alice 是否按几率 $\frac{1}{2}:\frac{1}{2}$ 往盒子里放

硬币,尤其在对弈次数。但是这一游戏量子化后可以做到这一点。

量子化后的这一游戏框架如下 :Alice 有两个盒子 A 和 B 用来放一个粒子。粒子在 A 盒子或 B 盒子的状态用 $|a>$ 及 $|b>$ 来表示。Alice 把粒子制备到某个态上,然后将盒子 B 发送给 Bob。在下列两种情况下 Bob 赢 :(1)如果他发现粒子在 B 盒子里,Alice 检查确信粒子不在 A 盒子里,付给 Bob 一个硬币。(2)Bob 要求 Alice 把 A 盒子发送过来,检验到 Alice 制备的态不是 :$|\Psi_0>=\frac{1}{\sqrt{2}}(|a>+|b>)$,那么 Alice 就要付给 Bob R 个硬币。其它情况下,Alice 赢,Bob 付给 Alice 一个硬币。

Alice 的策略就是将粒子制备到 $|\Psi_0>$ 态上,即粒子处在盒子 A,B 的均等叠加态上,测量后在两个盒子发现粒子的几率相等可以确保其收益期望值不低于 0。当然也可以将粒子制备在偏离 $|\Psi_0>$ 的态 :$|\Psi_1>=\alpha|a>+\beta|b>$ 上,这样就有可能被 Bob 发现从而受罚损失 R 个硬币。

Bob 的策略是收到 B 盒子后并不立即测量粒子是否在 B 盒子里,而是先做一个变换 :

$$|b>=\sqrt{1-\eta}\,|b>+\sqrt{\eta}\,|b'> \tag{19}$$

(这里 $|b>$,$|b'>$ 正交)就好象把把粒子在 B 盒子的态不破坏的分成两部分,在这里分裂参数依赖于惩罚参数 R。在完成态劈裂操作后,Bob 做态 $|b>$ 的投影测量,即查看盒子 B 里有没有 Alice 放置的粒子。如果 Bob 发现了粒子,Bob 赢了这一局。否则 Bob 向 Alice 索要 A 盒子用来检验 :他可以用 A 盒子和留下来的 $|b'>$ 来做联合测量,即看一下粒子是否处在 $|a>+\sqrt{\eta}\,|b>$ 态(忽略归一化因子)上,就可以以一定的概率判断出 Alice 是否作弊。

这一量子化结果在实验上如果用一般的粒子(如原子及离子)来实现是比较困难的事情。我们发现如果利用光子,在现有技术下完全能够实现。具体实验方案[100]是利用光子的经过分束器的路径来代表 A,B 两个盒子,利用光子的偏振来区别 $|b>$,$|b'>$。

4.3　量子“囚徒怪圈”

在经典“囚徒怪圈”中的两个局中人(假设为 Alice 和 Bob)面临着这样的局面 :Alice 与 Bob 两个囚徒被抓起来,如果双方合作都不提供对方犯罪证据,司法部门会因为证据较少各判他们三年有期徒刑,都提供对方犯罪证据,双方会都被判五年,一方提供一方不提供,提供方立功被判一年,另一方被判七年。这一对局可以用下表中的数值表示

		Bob	
		C	D
Alice	C	(3, 3)	(0, 5)
	D	(5, 0)	(1, 1)

在此策略-支付表格中,括号内前面的数值为 Alice 的收益而后者为 Bob 的收益。C 代表与对方合作,D 代表与对方对抗。从这张表格中可以看出,对任何参加者来说,无论对方采用什么策略,自己采用 D(对抗)策略要比 C (合作)策略要好,即主动提供对方犯

罪证据要比顽抗好。这样双方就找到了平衡点 $D:D$。但是我们从表中看出,如果双方能够合作,其结果要比双方对抗更为有利,但是双方都在独立的追求自己的最大利益的情况下,却得到比较差的结果 $D:D$,这就是所谓囚徒怪圈。

量子化后的模型如下图:

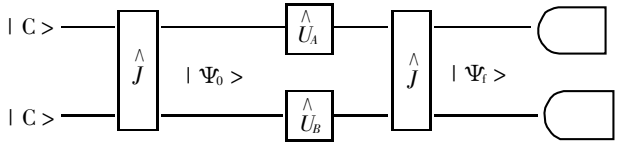

图 2 量子囚徒怪圈模型

对弈的初态为 $|\Psi_0\rangle = \hat{J}|CC\rangle$,这里 $\hat{J}$ 是一个幺正变换:$\hat{J} = \exp\{i\gamma D\otimes D/2\}$,且 $\gamma\in[0,\pi/2]$. 然后 Alice,Bob 分别对分给自己的那一部分态做幺正变换。最后系统再做一个反变换 $\hat{J}^+$,输出态即为 $|\Psi_f\rangle = \hat{J}^+(\hat{U}_A\otimes\hat{U}_B)\hat{J}|CC$。最后对末态做 $|C\rangle$,$|D\rangle$ 正交测量,支付取决于测量结果,例如,Alice 的收益期望值即为

$$\$_A = rP_{CC} + pP_{DD} + tP_{DC} + sP_{CD} \tag{20}$$

这里 $P_{\sigma\sigma'}$ 即测量得到 $\sigma\sigma'$ 的概率。作者分析了当 Alice,Bob 的幺正变换限制为这样的形式时[99]

$$\hat{U}(\theta,\phi) = \begin{bmatrix} e^{i\phi}\cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & e^{-i\phi}\cos\theta/2 \end{bmatrix} \tag{21}$$

双方存在平衡策略 $\hat{Q} = \hat{U}(0,\pi/2)$:双方均采取平衡策略时,收益为 3。对一般幺正变换[101],研究表明不存在单纯策略构成的平衡点,双方都要采用混合量子策略。在以上两种情况下,双方的收益期望值都优于经典对策平衡点处的收益(1,1)。

对策量子化的方法主要是引入量子力学中叠加性以及利用纠缠态。但是对于大部分实例,叠加策略在测量后又化为经典混合策略,并不出现新结果。本文前两个例子都是多步对策,利用了多步量子操作的优点:干涉,所以带来了新的结果。第三个例子则是引入了纠缠,即利用 $\hat{J}$ 变换把 Alice 和 Bob 所处的状态纠缠起来,这也是经典情况不能做到的,从而促使两位局中人采用非完全对抗策略。此外,我们发现量子测量也可以做为一种量子对策[102]。所举例子都是二人对策,最近已有人研究多人对策[103]。

5 量子信息过程的物理实现

在最近的一篇引言性质的文章中[104],DiVincenzo 总结了对量子计算(和量子通信)的物理实现的五(加二)个要求。

对量子计算的物理实现的五个要求为:

1)一个能表征量子比特并可扩展的物理系统。原则上讲,任何两能级体系都可以满

足这个要求。

2)把量子比特的初始态制备成基准态,如|000...>,的能力。这个要求来自于任何计算的输入态应当是已知的。

3)消相干时间长,要比量子门操作时间长得多的。

4)能构造量子门的一个“普适”序列。这是因为任何计算都可以由一些基本的量子门组合而完成。

5)对任意量子比特都能进行测量的能力。

以上五条对量子计算本身而言已经足够,但是如果考虑到量子通信等,则还需要两个附加条件:

6)静止比特和飞行比特相互转换的能力。静止比特,如原子,离子等,在空间上是不动的。飞行比特则在空间飞行,其典型例子是光子。

7)在空间中无失真地传送飞行比特的能力。这是很多量子通信过程的基本要求。

目前,学术界主要考虑的用做量子计算的物理系统有:原子物理(离子阱)[105],量子光学[106],核磁共振[107],电磁共振[108],超导[109],电子物理[110]以及量子点[111]。

6　结束语

尽管量子信息的基本框架已经成型,但是我们也应当看到目前量子信息领域还有许多问题亟待解决。例如在实验技术上,哪一种物理系统更适合构造量子计算机就不是短期内能解决的问题;理论上,在量子信息领域占有特殊地位的量子纠缠的很多特性,甚至包括度量问题,尚未研究清楚。然而这无损于量子信息的发展势头,反而吸引各方面的专家参加到量子信息的研究中来。我们有理由相信量子信息科学的明天会更加光明灿烂,人类从信息时代进入量子信息时代已不再是一种梦想。

参　考　文　献

[1] Bennett C H and DiVincenzo D P. Nature, 2000, 404:247~255.

[2] Einstein A, Podolsky B And Rosen N. Phys. Rev., 1935, 47:777.

[3] Milburn G J 著,郭光灿等译,费曼处理器,江西教育出版社,1999, 49~55.

[4] White A G, et al. Phys. Rev. Lett., 1999, 83:3103:3107.

[5] Sackett C A, et al. Nature (London), 2000, 404:256~259.

[6] 郭光灿等. 物理,1999, 28(2):120.

[7] Horodecki M, Horodecki P and Horodecki R. e-print quant-ph/9908065.

[8] Vedral V et al. Phys. Rev. Lett., 1997, 78:2275.

[9] Hughston L P, Jozsa R, Wootters W K. Phys. Lett. A, 1993, 183:14.

[10] Bennett C H, et al. Phys. Rev. A, 1996, 54:3824.

[11] Bennett C. H, et al. e-print quant-ph/9908073.

[12] Peres A. Phys. Rev. Lett., 1996, 77:1413.

[13] Horodecki M, Horodecki P and Horodecki R. Phys. Lett. A, 1996, 223:1.

[14] Horodecki M, Horodecki P and Horodecki R. Phys. Rev. Lett., 1998, 80:5239~5242.
[15] DiVincenzo D P, et al. e-print quant-ph/9910026.
[16] Horodecki M, Horodecki P and Horodecki R. Phys. Rev. Lett., 1999, 82:1056.
[17] Wootters W K and Zurek W H. Nature (London), 1982, 299:802.
[18] Yuen H P. Phys. Lett. A, 1986, 113:405; D'Ariano G M and Yuen H P. Phys. Rev. Lett., 1996, 76:2832.
[19] Barnum H. et al. Phys. Rev. Lett., 1996, 76:2818.
[20] Koashi M and Imoto N. Phys. Rev. Lett., 1998, 81:4264.
[21] Mor T. Phys. Rev. Lett., 1998, 80:3137.
[22] Buzek V and Hillery M. Phys. Rev. A, 1996, 54:1844.
[23] Gisin N and Massar S. Phys. Rev. Lett., 1997, 79:2153.
[24] Bruss D, Ekert A And Macchiavello C. Phys. Rev. Lett., 1998, 81:2598.
[25] Buzek V, Braunstein S L, Hillery M and Bruss D. Phys. Rev. A, 1997, 56:3446.
[26] Huang Y-F, Li W-L, Li C-F, et al. e-print quant-ph/0006032.
[27] Duan L-M and Guo G-C. Phys. Rev. Lett., 1998, 80:4999.
[28] Duan L-M and Guo G-C. Phys. Lett. A, 1998, 243:261.
[29] Zhang C-W Wang Z-Y, Li C-F, et al. Phys. Rev. A, 2000, 61:062310.
[30] DiVincenzo D P. Science, 1995, 270:255; Bennett C H. Phys. Today, 1995, 48:24.
[31] Shor P W. Phys. Rev. A, 1995, 52:R2493-2496.
[32] Steane A M. Phys. Rev. Lett., 1996, 77:793.
[33] Calderbank A R And Shor P W. Phys. Rev. A, 1996, 54:1098~1105.
[34] Steane A M. Proc. R. Soc. London A, 1996, 452:2551~2577.
[35] Gottesman D. Phys. Rev. A, 1996, 54:1844.
[36] Calderbank A R, et al. Phys. Rev. Lett., 1997, 78:405.
[37] Vaidman L, et al. Phys. Rev. A, 1996, 54:R1745.
[38] Duan L-M and Guo G-C. Phys. Rev. A, 1998, 57:2399~2402.
[39] Itano W M, et al. Phys. Rev. A, 1990, 41:2295; Knight P. Nature (London), 1990, 344:493.
[40] Palma G M, Suominen K A and Ekert A K. Proc. R. Soc. London A, 1996, 452:567.
[41] Duan L-M and Guo G-C. Phys. Rev. A, 1998, 57:737.
[42] Duan L-M and Guo G-C. Phys. Rev. Lett., 1997, 79:1953.
[43] Zanardi P and Rasetti R. Phys. Rev. Lett., 1997, 79:3306.
[44] Cory D G, et al. Phys. Rev. Lett., 1998, 81:2152~2155.
[45] Leung D, et al. Phys. Rev. A, 1999, 60:1924~1943.
[46] Schumacher B. Phys. Rev. A, 1995, 51:2738.
[47] Bennett C H, Wiesner S J. Phys. Rev. Lett., 1992, 69:2881~2884.
[48] Bennett C H, et al. Phys. Rev. Lett., 1993, 70:1895~1898.
[49] Mattle K, et al. Phys. Rev. Lett., 1996, 76:4656~4659.
[50] Bouwmeester D, et al. Nature (London), 1997, 390, 575~579.
[51] Boschi D, et al. Phys. Rev. Lett., 1998, 80:1121~1124.

[52] Vaidman L. Phys. Rev. A, 1994, 49:1473~1476.
[53] Furusawa A, et al. Science, 1998, 282:706~709.
[54] Nielsen M A, Knill E And Laflamme R. Nature, 1998, 396:52~55.
[55] Wiesner S J, SIGACT News, 1983, 15:78.
[56] Bennett C H and Brassard G. Proc. IEEE Internat. Conf. On Computers, Systems and Signal Processing, Bangalore, New York, IEEE, 1984, P175.
[57] Bennett. C H. Phys. Rev. Lett., 1992, 68:3121.
[58] Ekert A K. Phys. Rev. Lett., 1991, 67:661.
[59] Goldenberg L and Vaidman L. Phys. Rev. Lett., 1995, 75:1239.
[60] Masato and Imoto N. Phys. Rev. Lett., 1997, 79:2383.
[61] Li C-F, Y-S Zhang, Guo G-C, et al. unpublished.
[62] Bennett C H and Brassard G. SIGACT news, 1989, 20:78.
[63] Townsend P D. Nature (London), 1997,385:47.
[64] Muller A, et al. Europhys. Lett., 1993, 23:383.
[65] Franson J D and Ilives H. Appl. Optics, 1994, 33:2949.
[66] Hughes R J, et al. J. Mod. Opt., 2000, 47:533~547.
[67] Butter W T, et al. Phys. Rev. A, 1998, 57:2379~2382.
[68] Butter W T, et al. Phys. Rev. Lett., 1998, 81:3283~3286.
[69] Butter W T, et al. Phys. Rev. Lett., 2000, 84:5652~5655.
[70] Jennewein T, et al. Phys. Rev. Lett., 2000, 84:4729~4732.
[71] Naik D S, et al. Phys. Rev. Lett., 2000, 84:4733~4736.
[72] Tittel W, et al. Phys. Rev. Lett., 2000, 84:4737~4740.
[73] Mayers. Phys. Rev. Lett., 1997, 78:3414~3417.
[74] Lo H-K and Chau. Phys. Rev. Lett., 1997, 78:3410~3413.
[75] Shor P W. in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, (IEEE computer Society Press, Los Alamitos, CA, 1994) 124~133.
[76] Ekert A and Jozsa R. Rev. Mod. Phys., 1996, 68:733~753.
[77] Deutsch D And Jozsa R. Proc. R. Soc. London A, 1992, 439:553.
[78] Abrams D S and Lloyd S. Phys. Rev. Lett., 1997, 79:2586~2589.
[79] Grover L K. Phys. Rev. Lett., 1997, 79:325~328.
[80] Boyer M, et al. Fortschr. Phys., 1998, 46:493~506.
[81] Ozhigov Y. eprint quant-ph/9712051.
[82] Farhi E, et al. Phys. Rev. Lett., 1998, 81:5442~5444.
[83] Vandersypen L M K, et al. eprint quant-ph/0007017.
[84] Chuang I L, et al. Phys. Rev. Lett., 1998, 80:3408~3411.
[85] Jones J A, et al. Nature (London), 1998, 393:344~346.
[86] Kwiat P G, et al. J. Mod. Opt., 2000, 47:257~266.
[87] Lloyd S. Science, 1996, 273:1073.
[88] Somaroo S, et al. Phys. Rev. Lett., 1999, 82:5381~5384.

[89] Tseng C H, et al. eprint quant – ph/9908012.
[90] Yao A. in Proceedings of the 34th Annual Symposium of Foundation of Computer Science, (IEEE Computer Society, Los Alamitos, CA, 1993) P. 352.
[91] Deutsch D. Proc. R. Soc. London A, 1989, 425:73.
[92] Deutsch D. Proc. R. Soc. London A, 1995, 449:669; Lloyd S., Phys. Rev. Lett., 1995, 75:346.
[93] Barenco A, et. al. Phys. Rev. Lett., 1995, 74:4083.
[94] Gottesman D and Chuang I L. Nature (London), 1999, 402:390.
[95] Zhang C-W, Li C-F, Wang Z-Y and Guo G-C. Phys. Rev. A (2000), in press. (quant-ph/0001081).
[96] Preskill J. Proc. R. Soc. London A, 1998, 454:385 – 410; and reference therein.
[97] Meyer D A. Phys. Rev. Lett., 1999, 82:1052.
[98] Goldenberg L, Vaidman L, Weisner S. Phys. Rev. Lett., 1999, 82:3356.
[99] Eisert J, Wilkens M, Lewenstein M, Phys. Rev. Lett., 1999, 83:3077.
[100] Zhang Y-S, Li C-F, Guo G-C, et al. eprint quant-ph/0001008.
[101] Benjamin S C, Hayden P M. eprint quant-ph/0003036; Eisert J, Wilkens M. eprint quant-ph/0004076.
[102] Li C-F, Y-S Zhang, Y-F Huang, Guo G-C. e-print quant-ph/0007120.
[103] Benjamin S C and Hayden P M. eprint quant-ph/0007038.
[104] DiVincenzo D P. eprint quant-ph/0002077.
[105] Cirac J I and Zoller P. Phys. Rev. Lett., 1995, 74:4091; Pellizzari T, et al. Phys. Rev. Lett., 1995, 75:3788; Monroe C, et al. Phys. Rev. Lett., 1995, 75:4714; Sorensen A and Molmer K. Phys. Rev. Lett., 1999, 82:1971; Schneider S, James D F V and Milburn G J. eprint quant-ph/9808012.
[106] Turchette Q A, et al. Phys. Rev. Lett., 1995, 75:4710; Imamoglu A, et al. Phys. Rev. Lett., 1999, 83:4204.
[107] Gershenfeld N and Chuang I. Science, 1997, 275:350; Cory D, et al. Proc. Nat. Acad. Sci., 1997, 94 (5):1634; Jones J A, Vedral V, Ekert A, Castagnoli G. Nature (London), 2000, 403:869 ~ 871.
[108] Kane B. Nature, 1998, 393, 133; Vrijen R, et al. Phys. Rev. A, in press (quant-ph/9905096).
[109] Averin D. Solid State Commun., 1998, 105:659; Shnirman A, et al. Phys. Rev. Lett., 1997, 79:2371; Mooij J E, et al. Science, 1999, 285:1036.
[110] Platzman P M and Dykman M I. Science, 1999, 284, 1967; Bertoni A, et al. Phys. Rev. Lett., 2000, 84:5912 ~ 5915.
[111] Loss D And DiVincenzo D P. Phys. Rev. A, 1998, 57:120; Sherwin M, Imamoglu A and Montroy T. Phys. Rev. A, 1999, 60:3508; Tanamoto T. Phys. Rev. A, 2000, 61:022305.

PROGRESS IN QUANTUM INFORMATION RESEARCH

Li Chuanfeng and Guo Guangcan

(*Laboratory of Quantum Communication and Quantum Computation*, *University of Science and Technology of China*, *Hefei* 230026)

Abstract: Quantum information theory is the combination of classical information theory and quantum mechanics. In this paper, we review the recent research progress in quantum information theory, including the newly developed promising field of quantum game theory as well as the well-known fields such as quantum communication and quantum computation. We concentrate on the fundamental theoretical frame of the quantum information theory, and introduce the experiment research in the field at the same time.

Key words: Quantum Information, Quantum Communication, Quantum Computation, Quantum Game Theory