基于纯态的量子通信系统模型*)

邢莉娟　李　卓　白宝明　王新梅

(西安电子科技大学综合业务网国家重点实验室　西安 710071)

摘　要　量子通信与量子计算已经引起人们极大的关注。对于量子态如何用于信息处理的问题，提出了量子通信的两种基本模型：量子直接通信模型与量子隐形传态通信模型。在量子直接通信模型中，用模块化的方法将量子通信全过程分为量子信源编译码，量子信道编译码，量子信道与量子噪声模块，并详细阐述了各个模块的功能与用途。在量子隐形传态通信模型中，利用量子隐形传态特性，通过将待传粒子与纠缠对的联合测量模块化为量子调制部分，给出了基于隐形传态的量子通信一般模型。量子通信在安全性及效率方面具有经典通信无法比拟的优势。

关键词　量子通信，通信系统，模块化，量子调制，隐形传态

Quantum Communication System Models Based on the Pure State

XING Li-juan　LI Zhuo　BAI Bao-ming　WANG Xin-mei

(State Key Lab of Integrated Service Networks, Xidian University, Xi'an 710071, China)

Abstract　People pay more attention to quantum communication and quantum computation. On how to use quantum state in information processing, two basic quantum communication models are presented: quantum direct communication model and quantum communication model based on teleportation. In the direct quantum communication model, with the method of modularization, the whole process can be divided into several parts, including quantum source coding/decoding, quantum channel coding/decoding, quantum channel and quantum noise. The function and application of each part are given in detail. In the quantum communication model based on teleportation, joint measurement on the particle to be sent and the entangle pairs is modularized as Q-modulation. A general model of quantum communication based on teleportation is presented. Quantum communication has great advantages in security and efficiency over classical communication.

Keywords　Qantum communication, Communication system, Modularization, Quantum modulation, Tteleportation

量子力学的诞生极大地推动了20世纪人类社会的发展，当代经济的三分之一产值都来自于以量子力学为基础的高科技。量子信息科学是量子力学与信息科学相结合的产物。量子通信系统是面向未来的全新通信技术，在安全性、高效性上具有经典通信无法比拟的优势。并且，近年来光纤量子通道传输技术的出现将量子通信推向了实用化。

1　量子直接通信模型

实现量子信号在异地间传输的最简单模式是采用直接传输模式。直接传输模式是指量子消息产生后，经过信源压缩编码与信道纠错编码后，直接输入量子信道(光纤或大气)传输。由于传输中不可避免地受到噪声干扰，因此接收端对收到的信号首先进行纠错译码，然后信源解压缩，最后得到初始量子消息。这种方式与经典信息的传送方式相同。目前，直接传输模式是实现量子通信普遍采用的方式。量子直接通信系统的基本模型如图1所示。

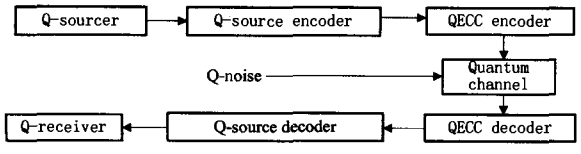

图1　量子直接通信系统的基本模型

1) 量子信源与编码

量子信号可以有几种形式，包括单光子量子信号、微弱激光脉冲量子信号、压缩光量子信号、量子光孤子信号以及调制的相干光量子信号等[1]。已知一组离散量子信源$|X_i\rangle_{i=1}^m$，其概率分布为λ_i，可以表示为

$$[|X\rangle]\sim\begin{pmatrix}|X_1\rangle & |X_2\rangle & \cdots & |X_m\rangle\\ \lambda_1 & \lambda_2 & \cdots & \lambda_m\end{pmatrix}$$

其密度算子$\rho=\sum_i\lambda_i\rho_i$，其中$\rho_i=|X_i\rangle\langle X_i|$。

其Von Neumann熵为$S(\rho)=-tr\rho\log_2\rho$

量子信源编码定理[2]：若量子信源以概率λ_i发送密度算子为ρ_i的量子态，ρ是信源的总的密度算子。如果所有ρ_i均限制为纯态，则Von Neumann熵确定了精确表示信源发送的信息所需的最小量子比特。

当量子态$|X_i\rangle$正交时，Von Neumann熵回到经典的Shannon信息熵情形，达到与经典相同的压缩情况；当不能完全区分每个量子态时，量子信源仍可进行压缩，这时以保真度来度量压缩前后的量子状态。这里假设经过信源编码后的量子状态为$|\varphi_i\rangle_{i=1}^q$，其概率分布为$q_i$。

2) 量子信道编码

在直接传输模式下，我们选择将量子态直接送入量子信道传输。为了对抗量子信道中的噪声，保证量子信息可靠而有效地传输，我们需要对量子态引入一定的冗余，使其能抵消噪声的影响，然后在想要恢复原来的状态时进行译码，即量子

*)基金项目：本文工作得到部委基金项目资助(编号：××060104)。**邢莉娟**　博士研究生，主要研究方向为量子信息学和量子编码。

纠错编码技术。

在量子信息理论中，由于一个量子比特对应一个复数域上的二维 Hilbert 空间，量子信息比特的基本错误类型有三种，一般的量子比特错误是这三种基本错误的线性组合。设单个量子比特对应的量子态为$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$，那么三种基本的错误类型为：

i) 比特翻转错误：

$|\varphi'\rangle=X|\varphi\rangle=\alpha|1\rangle+\beta|0\rangle$

ii) 相位翻转错误：

$|\varphi'\rangle=Z|\varphi\rangle=\alpha|0\rangle-\beta|1\rangle$

iii) 比特翻转错误＋相位翻转错误：

$|\varphi'\rangle=Y|\varphi\rangle=\alpha|1\rangle-\beta|0\rangle$

其中 X,Y,Z 分别为 pauli 算子

$$X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\qquad Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

$$Y=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}=XZ$$

根据上述的错误类型可以用量子纠错码来纠正发生的错误。目前已有的量子纠错码有很多，最初有可以纠正任意一量子比特错误[9,1]的 Shor 码[3]，后来又出现了 CSS 码[4,5]和稳定子码[6,7]，并且根据 CSS 码的构造方法，出现了基于经典线性码[8]的量子 RS 码[9]、量子 LDPC 码[10]等。这里假设经过量子信道编码后的量子信号状态为

$$[|\phi\rangle]\sim\begin{pmatrix}|\phi_1\rangle & |\phi_2\rangle & \cdots & |\phi_n\rangle\\ p_1 & p_2 & \cdots & p_n\end{pmatrix}$$

3) 量子噪声

量子信号在信道中传输时会受到环境的影响，导致量子信号与环境状态发生纠缠，出现量子信号的消相干现象，使得量子信号携带的量子信息或经典信息丢失。典型的量子噪声有以下三种(设发生错误的概率为 p)。

(a) 自发辐射衰变噪声：其 Kraus 算子和表示为

$$A_0=\begin{pmatrix}1 & 0\\ 0 & \sqrt{1-p}\end{pmatrix}\qquad A_1=\begin{pmatrix}0 & \sqrt{p}\\ 0 & 0\end{pmatrix}$$

(b) 退极化噪声：其 Kraus 算子和表示为

$$A_0=\sqrt{1-p}I,\qquad A_1=\sqrt{\frac{p}{3}}X$$

$$A_2=\sqrt{\frac{p}{3}}Y,\qquad A_3=\sqrt{\frac{p}{3}}Z$$

(c) 相位阻尼噪声：其 Kraus 算子和表示为：

$$A_0=\sqrt{1-p}I,\qquad A_1=\sqrt{p}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$$

$$A_2=\sqrt{p}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

4) 量子信道

直接传输模型通常使用两种传输介质：光纤和自由空间。目前采用直接传输方式，只能在几十 km 到 100km 左右的距离传输。为了在实际通信网络中实现量子通信，需要解决不受距离限制的量子信号传输问题。根据量子信号的特点，我们采用量子中继与量子信号放大技术来解决[11]。

纯态的量子信道容量[12]为

$$C=\max_{p}[H(\sum_i p_i\rho_i)-\sum_i p_i H(\rho_i)],\rho_i=|\phi_i\rangle\langle\phi_i|$$

5) 量子信道译码器

当量子态经过噪声信道到达接收端，接收者对收到的量子比特先进行纠错，然后再经过译码器，恢复被保护的量子信息。

6) 量子信源译码器

将恢复出的量子信息送入信源译码器，量子信息最终还原为消息。

2 量子隐形传态通信模型

与经典通信所不同的是，量子比特不但可以处于各种正交的叠加态上，还可以处于纠缠态。量子隐形传态传输的原理是利用两粒子最大纠缠态建立量子信道，然后利用量子操作实现消息的异地传送。隐形传态与直接通信方式的不同之处在于通信信道选用的不同。这里只介绍编码后的量子比特如何通过纠缠对进行传送。利用量子隐形传态实现间接传输的量子通信系统模型如图 2 所示。

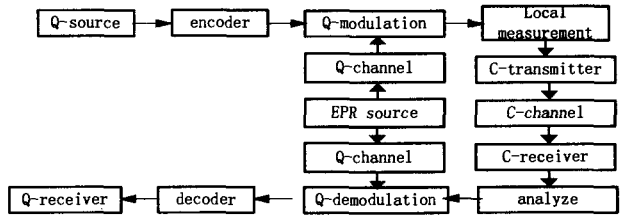

图 2 量子隐形传态通信系统基本模型

隐形传态的具体过程如图 3 所示[1]。发送端 Alice 需要把编码后的量子比特$|\phi_i\rangle$传给接收端的 Bob(这里仅以单量子比特为例，多量子比特情况请参考文献[13])。首先由 EPR 纠缠源产生一对 EPR(β_{23})，并通过量子信道将其中的一个粒子发送给 Alice，另一个粒子发送给接收端 Bob。其中$|\phi_i\rangle$与β_{23}分别表示为：

$|\phi_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle$

$(|\alpha_i|^2+|\beta_i|^2=1,i=1,2,\cdots,n)$

$$\beta_{23}=\frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

上述的$|\phi_i\rangle$与β_{23}可以联合表示为

$$|\phi_{i23}\rangle=|\phi_i\rangle|\beta_{23}\rangle=\frac{1}{\sqrt{2}}[\alpha_i|0\rangle(|01\rangle-|10\rangle)+\beta_i|1\rangle(|01\rangle-|10\rangle)]$$

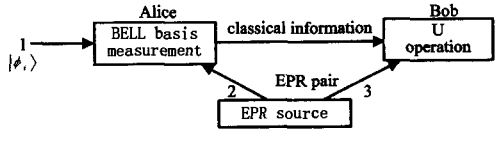

图 3 量子隐形传态过程

上式前两个量子比特属于 Alice，第三个量子比特属于 Bob。我们把 Alice 手中的待传比特$|\phi_i\rangle$与纠缠对中的粒子 2 相联合的过程称为量子调制。然后在本地测量模块中对这两个粒子进行 Bell 基测量。其具体过程如下：

$$|\Phi_{12}^+\rangle\langle\Phi_{12}^+|\phi_{i23}\rangle+|\Phi_{12}^-\rangle\langle\Phi_{12}^-|\phi_{i23}\rangle+$$
$$|\Psi_{12}^+\rangle\langle\Psi_{12}^+|\phi_{i23}\rangle+|\Psi_{12}^-\rangle\langle\Psi_{12}^-|\phi_{i23}\rangle=$$
$$\frac{1}{2}[|\Phi_{12}^+\rangle(-b|0_3\rangle+a|1_3\rangle)+[|\Phi_{12}^-\rangle(b|0_3\rangle+a|1_3\rangle)]+$$
$$|\Psi_{12}^+\rangle(-a|0_3\rangle+b|1_3\rangle)+|\Psi_{12}^-\rangle(-a|0_3\rangle-b|1_3\rangle)]$$

Alice 每次测量的结果将会是 Bell 基中的一个，同时 Bob 手中的粒子变成了下面相应的状态：

$|\Phi_{12}^+\rangle\rightarrow-b|0_3\rangle+a|1_3\rangle=-Y|\phi_i\rangle$

$|\Phi_{12}^-\rangle\rightarrow b|0_3\rangle+a|1_3\rangle=X|\phi_i\rangle$

$|\Psi_{12}^{+}\rangle \rightarrow -a|0_3\rangle + b|1_3\rangle = -Z|\phi_i\rangle$

$|\Psi_{12}^{-}\rangle \rightarrow -a|0_3\rangle - b|1_3\rangle = -I|\phi_i\rangle$

然后 Alice 将测量结果通过经典信道(例如打电话)告诉 Bob,Bob 根据得到的消息分析自己手中的粒子 3 处于哪个状态,最后根据相应的么正变换得到 $|\phi_i\rangle$。我们把根据已知消息进行相应么正变换的过程称为量子解调。这样,量子比特 $|\phi_i\rangle$ 就传给 Bob 了。Bob 再进行译码操作,最后还原为初始的量子信息。在整个隐形传态过程中,原来的量子状态 $|\phi_i\rangle$ 通过 Bell 基测量已经塌缩到 Bell 态中的一个,因此隐形传态并不违反未知量子态不可克隆原理。

结束语 本文提出了两种基本的量子通信系统模型:量子直接通信模型和量子隐形传态模型。在量子直接通信模型中,整个通信过程被划分成不同的模块,并描述了每个模块的功能与作用。在量子隐形传态通信模型中,描述了用纠缠对作为信息载体传送消息的过程。量子通信系统在安全性及效率方面具有经典系统无法比拟的优势,在不远的将来,量子通信系统必将走向实用化的道路。

参 考 文 献

[1] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Last modified. Cambridge: Cambridge University Press, 2000: 206-270

[2] 李承祖. 量子通信和量子计算. 第一版. 长沙:国防科技大学出版社, 2000: 73-143

[3] Shor P W. Scheme for reducing decoherence in quantum memory. Phys. Rev. A, 1995, 52(4): 2493-2496

[4] Calderbank A R, Shor P W. Good quantum error - correcting codes exist. Phys. Rev. A, 1996, 54(2): 1098-1105

[5] Steane A M. Multiple particle interference and quantum error correction// Proc. Roy. Soc. Lond. A, 1996, 452(1954): 2551-2577

[6] Gottesman D. Class of quantum error - correcting codes saturating the quantum Hamming bound. Phys. Rev. A, 1996, 54(3): 1862-1868

[7] Calderbank A R, Rains E M, Shor P W, et al. Quantum error correction and orthogonal geometry. Phys. Rev. Lett., 1997, 78(3): 405-408

[8] 王新梅,肖国镇. 纠错码——原理与方法. 修订版. 西安:西安电子科技大学出版社, 2001: 378-415

[9] Grassl M, Geiselmann W, Beth Th. Quantum Reed - Solomon Codes. AAECC-13. Honolulu, Hawaii, USA, 1999

[10] MacKay D J C, Mitchison G, McFadden P L. Sparse-graph codes for quantum error correction. IEEE Transactions on Information Theory, 2004, 50(10): 2315-2330

[11] van Loock P, Ladd T D, Sanaka K, et al. Hybrid Quantum Repeater Using Bright Coherent Light. Physical Review Letters, 2006, 96(24): 501-505

[12] Holevo A S. The capacity of the quantum channel with general signal states. IEEE Transactions on Information Theory, 1998, 44(1): 269-273

[13] Gordon G, Regolin G. Generalized Teleportation Protocol. Physical Review A, 2006, 73(4): 2309-2312

(上接第 90 页)

DHAFS 也能够提供很好的数据可用性,能够容忍服务器发生故障。以上的三组测试中使用的编码率为 3/4,在此基础之上测试一台服务器宕机的情况下,DHAFS 的纠错性能,结果如表 4 所示。从这个测试结果可以看到系统对大文件的读性能和传统网络文件系统已经很接近了,如果在稳定的网络环境中,当需要进行纠错处理时才发送纠错数据段,能够达到比传统网络文件系统更高的吞吐量。

表 4 DHAFS 的容错性能

	DHAFS 文件系统	
操作	延时(秒)	吞吐量(MB/s)
小文件读	1256	0.03
大文件读	312	7.03

结束语 随着磁盘容量的不断增大和价格的不断下降以及网络带宽的不断提高,通过低廉的磁盘设备和高速局域网组建高可靠、高性能的集群存储系统是网络存储领域的重要研究内容。现有的许多集群存储系统是集中控制的体系结构,根据元数据节点来进行数据的分布和请求调度决策。由于这种单一元数据节点的体系结构,系统不可避免地存在元数据节点的单点失效和单一元数据节点的性能瓶颈。

针对文件存储系统,本文提出了一种分散式体系结构的高可靠文件存储系统(DHAFS),系统中没有专用的元数据节点,各个存储节点通过高速局域网相互连接,每个存储节点的本地存储资源虚拟化为一个全局的存储空间,存储、缓存、数据/元数据的管理功能则分布在各个存储节点中,存储节点相互协作实现统一的文件名字空间,向客户端提供文件接口。相对于现有的集群存储系统而言,DHAFS 不仅弥补了单一元数据节点的单点失效,提高了存储系统的可用性,而且还能够支持客户端的并行访问数据,避免了元数据节点的性能瓶颈,提高了系统的动态可扩展性。

参 考 文 献

[1] Online Survey Results: 2001 Cost of Downtime. Eagle Rock Alliance Ltd., August 2001, accessed May 2003. http://contingencyplanningresearch.com/2001%20Survey.pdf

[2] Carns P H, Ligon W B. PVFS: A Parallel File System for Linux Cluster. Linux Journal, November 2000

[3] Matthew T, Keefe O. Shared File Systems and Fibre Channel// Proceeding of the 15th IEEE/6th NASA Goddard Conference on Mass Storage Systems and Technologies. College Park, Maryland, USA, March 1998: 1-16

[4] Rodeh O, TepermanA. zFS-A Scalable Distributed File System Using Object Disks// Proceedings of the 20th IEEE/11th NASA Goddard Conference on Mass Storage Systems and Technologies. San Diego, California, USA, April 2003: 207-218

[5] Xie Changsheng, Cai Bin. A Decentralized Storage Cluster with High Reliability and Flexibility// Proceedings of the 14th Euromicro International Conference on Parallel, Distributed and Network-based Processing. Montbeliard, Sochaux, France, February 2006

[6] Lampson B, Lomet D. A New Presumed Commit Optimization for Two Phase Commit// Proceedings of the 19th International Conference on Very Large Data Base. August 1993: 630-640

[7] Liu M L, Agrawal D, El Abbadi A. The Performance of Two Phase Commit Protocols in the Presence of Site Failures. Distributed and Parallel Databases, 1998, 6(2): 157-182

[8] Crovela E, Taqqu M S, Bestavros A. Heavy-tailed Probability Distributions in the World Wide Web. a Practical Guide to Heavy Tails. New York: Chapman & Hall, 1998: 3-26

[9] Douceur R, Bolosky W J. A Large-scale Study of File System Contents// Proceedings of the 1999 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems. Atlanta, Georgia, USA, May 1999: 59-70

[10] Kazar H M, Menees S, et al. Scale and Performance in a Distributed File System. ACM Transactions on Computer Systems, 1988, 6(1): 51-81