

文章编号: 1007-5321(2007)02-0042-04

概率隐形传态中客户透明特性的分析

杜建忠^{1,2}, 陈秀波¹, 温巧燕¹, 朱甫臣³

(1. 北京邮电大学 理学院, 北京 100876; 2. 西安电子科技大学 综合业务网国家重点实验室, 西安 710071;

3. 现代通信国家重点实验室, 成都 610041)

摘要: 给出了基于客户/服务模式概率隐形传态的一个双边协议, 它达到成功隐形传态的最大概率. 证明了

Schmidt 分解为 $\sum_{j=1}^d \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$ 的部分纠缠共享量子信道对客户端是透明的; 对于一般化部分纠缠量子信道, 客户必需知道一个局域幺正算子, 将量子信道变换为客户端透明的量子信道, 才能执行概率隐形传态.

关键词: 隐形传态; 量子通信; 量子测量

中图分类号: TN918.1 **文献标识码:** A

Clients Transparency Properties in Probabilistic Teleportation

DU Jian-zhong^{1,2}, CHEN Xiu-bo¹, WEN Qiao-yan¹, ZHU Fu-chen³

(1. School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;

2. State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China;

3. National Laboratory for Modern Communications, Chengdu 610041, China)

Abstract: A bidirectional protocol of probabilistic teleportation on the clients/server model is proposed, leading to the maximal probability of successful teleportation. It is proved that the partially entangled

quantum channel $\sum_{j=1}^d \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$ by the Schmidt decomposition is transparent to the clients. To perform probabilistic teleportation via the generally entangled quantum channel, the clients must know a unitary operator that transforms the quantum channel into the clients' transparent quantum channel.

Key words: teleportation; quantum communication; quantum measurement

1993年, 文献[1]考虑了量子隐形传态: 用局域操作和传输 2 个经典比特, 发送者(Alice)可以通过 1 个共享的最大纠缠对(任一 Bell 态), 将 1 个未知态 $\alpha|0\rangle_1 + \beta|1\rangle_1$ 决定性地传给接收者(Bob).

以后, 替代最大纠缠信道, 考虑了部分纠缠信道, 提出了概率隐形传态协议. Alice 和 Bob 之间共

享的部分纠缠信道用 Schmidt 分解^[2]可以表示为

$|\psi\rangle_{2,3} = \sum_{j=1}^n \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$, 这里 d 是 Schmidt

数. $|\psi\rangle_{2,3}$ 还可表示为矩阵形式 UBV , 其中 U 和 V 是幺正矩阵, B 是对角矩阵. 假如 Alice 局域执行 U^+ 于粒子 2 上, Bob 局域执行 V^+ 于粒子 3 上, 则

收稿日期: 2006-03-28

基金项目: 国家“863 计划”项目(2006AA01Z419); 国家自然科学基金重大研究计划项目(90604023); 高等学校博士学科点专项科研基金项目(20040013007); 现代通信国家重点实验室基金项目(9140C1101010601); ISN 开放基金项目; 国家自然科学基金项目(60373059)

作者简介: 杜建忠(1970—), 男, 博士生, E-mail: ddddjjjjzzzz@tom.com.

$|\psi\rangle_{2,3}$ 变为 $|\psi_s\rangle_{2,3} = \sum_{i=1}^d b_i |i\rangle |i\rangle$.

部分纠缠态 $|\psi_s\rangle_{2,3}$ 可作为量子信道执行概率隐形传态^[3-6]. 文献[4]证明成功隐形传态的最大概率是 $d \min\{b_i^2 | i=1, 2, \dots, d\}$, 对应于纠缠熵^[7] E .

没有 Alice 的局域操作 U^+ , Bob 和 Alice 不能利用局域操作和经典通信将 $|\psi\rangle_{2,3}$ 变换为 $|\psi_s\rangle_{2,3}$, 因而不能利用已有的概率隐形传态协议.

本文中, 在 Alice 不知道 U^+ 条件下, 证明在 1 个 d 态概率隐形传态中, Alice 可以对共享量子信道

$|\psi_t\rangle_{2,3} = \sum_{j=1}^d \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$ 完全未知, 或者仅需要知道 1 个局域么正算子, 使得一般化量子信道 $|\psi\rangle_{2,3}$ 变换为 $|\psi_t\rangle_{2,3}$.

现实中, 顾客/服务模型是一种最常见的通信模型. 服务者知道信道的全部信息, 愿意承担更多的工作. 顾客总是希望信道是透明的. 假如信道不能透明, 顾客愿意知道最少的信道信息. 下面给出一个基于客户/服务模式的概率隐形传态的双边协议.

1 信道对发送者透明的概率隐形传态

一个 d 维空间 H_d 的量子态 $|\Phi\rangle_1 = \sum_{a=1}^d c_a |a\rangle$ 被隐形传态至远方, 信道是 $n \times n$ 维 Hilbert 空间 $H_n \times H_n$ 上 Schmidt 数为 d 的部分纠缠态 $|\psi_t\rangle_{2,3}$. Alice 对这种共享信道是完全未知的. 给出这种概率隐形传态协议的步骤.

1) 在粒子 1 和 2 上, Alice 执行联合投影测量^[1] $|\rho_{ef}\rangle_{12} \langle \rho_{ef}|$, $e, f = 1, 2, \dots, d$, 这里 $|\rho_{ef}\rangle = 1/\sqrt{d} \sum_{h=1}^d e^{2\pi i h e/d} |h\rangle \otimes |[(h+f-2) \bmod d] + 1\rangle$. Alice 将测量结果 ef 通过经典信道传给 Bob. 系统态变换到

$$|\Theta_0^{ef}\rangle_{123} = (|\rho_{ef}\rangle_{12} \langle \rho_{ef}| \otimes \mathbf{I}_3) (|\Phi\rangle_1 \otimes |\psi_t\rangle_{2,3}) = |\rho_{ef}\rangle_{12} \otimes \frac{1}{\sqrt{d}} \sum_{h=1}^d \sum_{i=1}^d \sum_{k=1}^n e^{-2\pi i h e/d} c_h \cdot u_{[(h+f-2) \bmod d] + 1, i} b_i v_{ik} |k\rangle_3$$

系统态为非正规形式, 下同.

一般测量等价于在被测粒子关联的辅助粒子上执行投影测量^[3-6].

2) Bob 收到用经典比特表示的测量结果 ef 后, 在粒子 3 上执行么正变换 V^+ . 系统态变换到

$$|\Theta_1^{ef}\rangle_{123} = (\mathbf{I}_1 \otimes \mathbf{I}_2 \otimes V^+) |\Theta_0^{ef}\rangle_{123} = |\rho_{ef}\rangle_{12} \otimes$$

$$\frac{1}{\sqrt{d}} \sum_{h=1}^d \sum_{i=1}^d e^{-2\pi i h e/d} c_h u_{[(h+f-2) \bmod d] + 1, i} b_i |i\rangle_3$$

3) Bob 在粒子 3 上执行测量^[5] $\{\mathbf{M}_1, \mathbf{M}_2\}$, 其中 $\mathbf{M}_1 = \text{diag}(b_{\min}/b_1, b_{\min}/b_2, \dots, b_{\min}/b_d)$, $\mathbf{M}_2 = \text{diag}(1 - b_{\min}/b_1, 1 - b_{\min}/b_2, \dots, 1 - b_{\min}/b_d)$, 这里 $b_{\min} = \min\{b_1, b_2, \dots, b_d\}$.

假如测量结果是 2, 系统态变换到

$$|\Theta_2^{ef}\rangle_{123} = (\mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \mathbf{M}_2) |\Theta_1^{ef}\rangle_{123} = |\rho_{ef}\rangle_{12} \otimes \frac{1}{\sqrt{d}} \sum_{h=1}^d \sum_{i=1}^d e^{-2\pi i h e/d} c_h u_{[(h+f-2) \bmod d] + 1, i} \cdot (1 - b_{\min}/b_i) b_i |i\rangle_3$$

因为基态 $|\min\rangle$ 的概率幅是 0, 隐形传态失败.

假如测量结果是 1, 系统态变换到

$$|\Theta_3^{ef}\rangle_{123} = (\mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \mathbf{M}_1) |\Theta_1^{ef}\rangle_{123} = |\rho_{ef}\rangle_{12} \otimes \frac{1}{\sqrt{d}} \sum_{h=1}^d \sum_{i=1}^d e^{-2\pi i h e/d} c_h u_{[(h+f-2) \bmod d] + 1, i} b_{\min} |i\rangle_3$$

4) Bob 在粒子 3 上执行么正变换 U^+ , 然后执行么正变换 w_{ef} ^[1], 这里

$$w_{ef} = \sum_{m=1}^d e^{2\pi i h e/d} |m\rangle \langle [(m+f-2) \bmod d] + 1|$$

系统态变换到

$$|\Theta_4^{ef}\rangle_{123} = (\mathbf{I}_1 \otimes \mathbf{I}_2 \otimes w_{ef} U^+) |\Theta_3^{ef}\rangle_{123} = |\rho_{ef}\rangle_{12} \otimes (1/\sqrt{d}) b_{\min} \sum_{m=1}^d c_m |m\rangle_3$$

粒子 1 上的未知态被隐形传态至粒子 3.

该协议中, 成功隐形传态的概率就是步骤 3) 中结果 1 出现的概率, 即 $d \times b_{\min}^2$, 对应纠缠熵 E ^[7].

2 一般信道的概率隐形传态中发送者必需的信道信息

假如 Alice 知道一个么正变换 Q , 使 $U = \sum_{j=1}^n \sum_{i=1}^d u_{ji} |j\rangle \langle i|$ 变换到 $U' = \sum_{j=1}^n \sum_{i=1}^d u'_{ji} |j\rangle \langle i|$, 在此条件下, 上面的协议可以被简单修改, 以适应一般量子信道 $|\psi\rangle_{2,3} = \sum_{j=1}^n \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$, 即在步骤 1) 中, $|\rho_{ef}\rangle_{12}$ 替换为 $(1/\sqrt{d}) \sum_{h=1}^d e^{2\pi i h e/d} |h\rangle \otimes Q^+ |[(h+f-2) \bmod d] + 1\rangle$; 在步骤 4), 替换 U^+ , Bob 在粒子 3 上执行变换 U'' .

问题是, 上面么正变换 Q 是否必要.

定理 1 在量子信道为一般形式 $|\psi\rangle_{2,3} = \sum_{j=1}^n \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$ 的 d -态概率隐形传态中,

发送者必需知道一个么正变换 Q , 使得

$$Q \sum_{j=1}^n \sum_{i=1}^d u_{ji} |j\rangle \langle i| = \sum_{j=1}^d \sum_{i=1}^d u'_{ji} |j\rangle \langle i|$$

证明 令 ef 表示 Alice 的测量结果, 对应的测

量算子是 $M_{ef} = \sum_{a=1}^d \sum_{j=1}^n \sum_{p=1}^{d \times n} w_{p,a \otimes j} |p\rangle \langle a| \langle j|$. 对

应地, 令算子 X_{ef} 表示 Bob 作用在粒子 3 上的由测

量操作和么正操作组成的合成操作, 即 $X_{ef} =$

$\left(\sum_{k=1}^n \sum_{q=1}^n x_{k,q} |q\rangle \langle k| \right) \text{diag}(b_{\min}/b_1, b_{\min}/b_2, \dots,$

$b_{\min}/b_d, 1, \dots, 1) V^+$, 这里 $\sum_{k=1}^n \sum_{q=1}^n x_{k,q} |q\rangle \langle k|$ 是么

正矩阵.

Alice 和 Bob 完成局域操作后, 整个系统态为

$$(M_{ef} \otimes I_3)(I_1 \otimes I_2 \otimes X_{ef})(|\Phi\rangle_{1,2} \otimes |\psi\rangle_{2,3}) =$$

$$b_{\min} \sum_{a=1}^d \sum_{j=1}^n \sum_{p=1}^{d \times n} \sum_{i=1}^d \sum_{q=1}^n c_a w_{p,a \otimes j} u_{ji} x_{iq} |p\rangle |q| \quad (1)$$

完成一个成功的隐形传态后, 整个系统最终态可以表示为

$$|R_E\rangle_{12b_1} |\Phi\rangle_{b_2} = \sum_{r=1}^n \sum_{s=1}^n \sum_{t=1}^{\lfloor n/d \rfloor} R_{rst} |rst\rangle \sum_{z=1}^d c_z |z\rangle \quad (2)$$

式中, b_2 是 Bob 的粒子 3 上隐形传态过来的态; b_1 是 Bob 方与 b_2 分离的态; $\lfloor n/d \rfloor$ 表示不超过 n/d 的最大整数, 不失一般性, 用 n/d 标记 $\lfloor n/d \rfloor$.

比较式(1)和式(2), 获得

$$y \sum_{a=1}^d \sum_{j=1}^n \sum_{i=1}^d c_a w_{r \otimes s, a \otimes j} u_{ji} x_{i,t \otimes z} = c_z R_{rst}$$

$$z = 1, 2, \dots, d; r, s = 1, 2, \dots, n; t = 1, 2, \dots, n/d$$

这里 y 是一个正规化系数. 因为每个 $w_{r \otimes s, a \otimes j}$, u_{ji} 及每个 $x_{i,t \otimes z}$ 与所有的 c_a, c_z 无关, 得到

$$y \sum_{j=1}^n \sum_{i=1}^d w_{r \otimes s, a \otimes j} u_{ji} x_{i,t \otimes z} = \delta_{a,z} R_{rst}$$

$$a, z = 1, 2, \dots, d; r, s = 1, 2, \dots, n; t = 1, 2, \dots, n/d \quad (3)$$

式中 $\delta_{a,z}$ 是 Kronecker 函数.

态函数要求至少一个 $R_{rst} \neq 0$, 标记 $R_{r's't'} \neq 0$.

因为 $\sum_{k=1}^n \sum_{q=1}^n x_{k,q} |q\rangle \langle k|$ 是么正矩阵, 从式(3)可以

写出 d^2 个关于未知数 $x_{i,t \otimes z}$ 的线性方程组

$$y \sum_{a=1}^d x_{i,t' \otimes a} w_{r' \otimes s', a \otimes j} = R_{r's't'} u_{ij}^* \\ j = 1, 2, \dots, n; i = 1, 2, \dots, d$$

令 $W = \sum_{a=1}^d \sum_{j=1}^n w_{r' \otimes s', a \otimes j} |a\rangle \langle j|$. 在一个成功的

隐形传态中, $\{x_{i,t' \otimes a} | i, a = 1, 2, \dots, d\}$ 应该有解,

由线性方程组有解时系数矩阵和增广矩阵应该满足

的关系知, 任意一个么正矩阵 Q 使得 $WQ^+ = W'$,

当且仅当 $U^+ Q^+ = U'^+$. 其中, $W' = \sum_{a=1}^d \sum_{j=1}^d$

$w'_{r' \otimes s', a \otimes j} |a\rangle \langle j|$, $U' = \sum_{j=1}^d \sum_{i=1}^d u'_{ji} |j\rangle \langle i|$,

$Q = \sum_{i=1}^d \sum_{j=1}^n q_{ji} |j\rangle \langle i|$, W, Q 是 $d \times n$ 矩阵, U 是

$n \times d$ 矩阵.

换句话说, Alice 的测量操作 M_{ef} 必需蕴含一个么正矩阵 Q , 满足 $QU = U'$, 才有可能成功隐形传态. 因此发送者必需知道这样的一个么正矩阵 Q .

3 基于客户/服务模型的双边概率隐形传态协议

尽管理想的量子信道是最大纠缠态, 可以简化通信者双方的操作, 并且导致决定性的隐形传态, 但获得这种信道是困难的. 因为混合态的量子信道不能精确地提供隐形传态^[8], 所以, 在实际中, 量子信道最可能是部分纠缠态信道.

在隐形传态之前, 共享的量子信道应该是已知的. 为了实验地决定量子信道 $|\psi\rangle_{2,3}$, 应用态层析技术 (state tomography technology)^[9], 需要重复测量态 $|\psi\rangle_{2,3}$ 的许多副本. 服务者独自完成这项耗时的的工作. 最初, 服务者知道关于量子信道的全部信息, 客户一无所知.

在确保通信的前提下, 服务者告诉客户有关信道的最少信息. 在关于 $|\psi\rangle_{2,3}$ 的 Schmidt 分解

$\sum_{j=1}^n \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$ 中, 假如 $j > d$ 时 $u_{ji} = 0$.

则服务者不需要告诉客户有关信道的任何信息. 特别地, 对于一个 n -态量子信道, 当 Schmidt 数为 n ,

条件“ $j > d$ 时 $u_{ji} = 0$ ”被平凡满足. 假如 $j > d$ 时

$u_{ji} \neq 0$, 服务者选择一个么正矩阵 $Q = (q_{pj})_{d \times n}$ 使

$QU = U'$, 这里 $j > d$ 时 $u'_{ji} = 0$, 然后将 Q 告诉客户.

此时 $|\psi\rangle_{2,3} = \sum_{p=1}^d \sum_{j=1}^n \sum_{i=1}^d \sum_{k=1}^n q_{jp}^* u'_{pi} b_i v_{ik} |j\rangle |k\rangle$. 么

正矩阵 Q 的选择应使客户容易执行隐形传态操作.

假如, 在量子信道更新前后, 相同的么正矩阵 Q 能将不同的么正矩阵 U 都变换到满足条件的不同的 U' , 量子信道的更新对客户是透明的.

当服务者是接收者, 客户是发送者, 可以利用上面给出的协议. 当服务者是发送者, 客户是接收者, 概率隐形传态可以看作纠缠浓缩 (entanglement concentration)^[10-11] 和决定性隐形传态^[1]. 概率隐形传态协议如下所述.

1) 服务者在粒子 3 上执行幺正变换 V^+ , 在粒子 3 上执行测量 $\{M_1, M_2\}$, 假如测量结果是 2, 概率隐形传态失败; 否则, 系统态变换为

$$|\Omega_1\rangle_{123} = (I_1 \otimes I_2 \otimes M_1)(|\phi\rangle_1 \otimes |\psi\rangle_{2,3}) = |\Phi\rangle_1 \otimes b_{\min} \sum_{p=1}^d \sum_{j=1}^n \sum_{i=1}^d q_{jp}^* u'_{pi} |j\rangle |i\rangle$$

2) 服务者在粒子 3 上执行 U'^+ , 系统态变换为

$$|\Omega_2\rangle_{123} = (I_1 \otimes I_2 \otimes U'^+) |\Omega_1\rangle_{123} = |\Phi\rangle_1 \otimes b_{\min} \sum_{p=1}^d \sum_{j=1}^n q_{jp}^* |j\rangle |p\rangle$$

3) 在粒子 1 和 3 上, 服务者执行联合投影测量^[1] $\{|\rho_{ef}\rangle_{13} \langle \rho_{ef}| | e, f = 1, 2, \dots, d\}$. 服务者将测量结果 ef 通过经典信道传给客户. 系统态变换到

$$|\Omega_3^{ef}\rangle_{123} = (|\rho_{ef}\rangle_{13} \langle \rho_{ef}| \otimes I_2) |\Omega_2\rangle_{123} = b_{\min} |\rho_{ef}\rangle_{13} \otimes \frac{1}{\sqrt{d}}$$

$$\sum_{h=1}^d \sum_{j=1}^n e^{-2\pi i h e / d} c_{h q_j}^* |[(h+f-2) \bmod d] + 1\rangle |j\rangle_2$$

4) 客户在粒子 2 上执行幺正变换 Q , 然后执行幺正变换 w_{ef} ^[1], 系统态变换到

$$|\Omega_4^{ef}\rangle_{123} = (I_1 \otimes I_3 \otimes w_{ef} Q) |\Omega_3^{ef}\rangle_{123} = |\rho_{ef}\rangle_{12} \otimes (1/\sqrt{d}) b_{\min} \sum_{m=1}^d c_m |m\rangle_2$$

粒子 1 上的未知态被隐形传态至粒子 2.

4 结 论

本文构造的基于客户/服务模型的双边概率隐形传态协议, 达到了最大的成功概率. 在概率隐形传态中, 对于客户透明的共享量子信道是

$$\sum_{j=1}^d \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle. \text{ 对于一般化的共享量子}$$

信道 $\sum_{j=1}^n \sum_{i=1}^d \sum_{k=1}^n u_{ji} b_i v_{ik} |j\rangle |k\rangle$, 客户必需知道一个局域幺正算子 Q , 将共享量子信道变换为

$$\sum_{j=1}^d \sum_{i=1}^d \sum_{k=1}^n u'_{ji} b_i v_{ik} |j\rangle |k\rangle, \text{ 因此, 客户的最小信道信}$$

息量对应某一特定的幺正矩阵 Q .

在部分纠缠信道上, 本文的基于客户/服务模式的概率隐形传态可用于实施一些纠缠交换方案^[12].

参考文献:

- [1] Bennett C H, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Phys Rev Lett, 1993, 70(13): 1895-1899.
- [2] Peres A. Quantum theory: concepts and methods[M]. Dordrecht: Kluwer Academic, 1993: 131-138.
- [3] Li W L, Li C F, Guo G C. Probabilistic teleportation and entanglement matching [J]. Phys Rev A, 2000, 61(3): 034301.
- [4] Son W, Lee J, Kim M S, et al. Conclusive teleportation of a d -dimensional unknown state [J]. Phys Rev A, 2001, 64(6): 064304.
- [5] Hsu L Y. Optimal information extraction in probabilistic teleportation [J]. Phys Rev A, 2002, 66(1): 012308.
- [6] Fang Jianxing, Lin Yinsheng, Zhu Shiqun, et al. Probabilistic teleportation of a three-particle state via three pairs of entangled particles [J]. Phys Rev A, 2003, 67(1): 014305.
- [7] Bennett C H, Bernstein H J, Popescu S, et al. Concentrating partial entanglement by local operations [J]. Phys Rev A, 1996, 53(4): 2046-2052.
- [8] Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy-channels [J]. Phys Rev Lett, 1996, 76(5): 722-725.
- [9] Vogel K, Risken H. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase [J]. Phys Rev A, 1989, 40(5): 2847-2849.
- [10] Gisin N. Hidden quantum nonlocality revealed by local filters[J]. Phys Lett A, 1996, 210(3): 151-156.
- [11] Horodecki M, Horodecki P, Horodecki R. Inseparable two spin-1/2 density matrices can be distilled to a singlet form [J]. Phys Rev Lett, 1997, 78(4): 574-577.
- [12] 秦素娟, 温巧燕, 朱甫臣. 利用 Bell 态纠缠交换的环式量子秘密共享协议[J]. 北京邮电大学学报, 2006, 29(2): 34-37.
Qin Sujuan, Wen Qiaoyan, Zhu Fuchen. A ring quantum secret sharing protocol based on entanglement swapping of Bell states[J]. Journal of Beijing University of Posts and Telecommunications, 2006, 29(2): 34-37.