大研报告：关于量子态的远程控制

Pan Zan
panzan@mail.ustc.edu.cn
University of Science and Technology of China

【摘要】 所谓量子态的远程控制，就是以纠缠比特为资源，通过局域操作和经典通信来传递未知的操作，这是建立量子网络比不可少的一步。本文从量子隐形传态开始，对相关的一些进展进行了调研，主要内容包括 HPV 协议及其在多比特情形下的推广，利用 GHZ 态的两种实现：联合 RIO 协议和控制 RIO 协议。此外，我们还简单介绍了纠缠梳理的思想，但未能充分展开。对于专业名词的翻译，请参照索引。

目录

1 课题简介

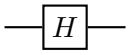
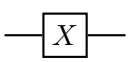
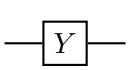
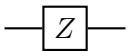
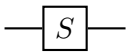
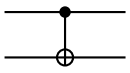
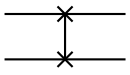
量子隐形传态是利用纠缠将未知态从局域系统发送到遥远的另一方。类似地，我们可以通过纠缠来传递未知的量子操作，以达到远程控制的目的。从实际应用的角度来看，仅当它比通常的途径消耗更少的资源时，对它的研究才更有意义。如果接受方的量子态和发送方的量子操作都是完全未知的，文献[1]已经证明其所需的资源达到最大。但是，当那些要远程实现的量子操作部分已知时，我们能够利用较少的资源来完成。这对于量子信息的处理和通信有着重要的意义。本文就是基于这个出发点来展开研究的。

在第2节，我们将回顾一下量子信息中的基本知识，并着重介绍量子隐形传态；在第3节，我们详细讨论 HPV 协议，并将其推广到 N-qubit 系统(即第4节)；在第5节，我们研究利用 GHZ 态的实现。最后，在第6节我们简要介绍一下纠缠梳理这个有趣的课题。

2 基础回顾

2.1 常用量子门

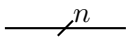
在这一部分，我们要给出一些最基本的量子逻辑门，采用的记号遵从教材[3]。

Hadamrad 门		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X 门 (σ_1)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y 门 (σ_2)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z 门 (σ_3)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
相位门		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
受控非门		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
交换门		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

这些量子门在文献和后面的讨论中频繁出现，熟悉相应的性质对于今后的推导是必须的。

2.2 量子线路

量子线路很类似于经典线路，但量子线路不允许出现回路，也没有所谓的扇入，这是由量子门的酉性决定的。当然，量子力学禁止比特的复制，即不可克隆定理，对一般量子态的扇出操作更是不可能的。下面是量子线路中的符号约定：

测量运算		投影到 $\|0\rangle$ 和 $\|1\rangle$ 上
量子比特		承载单量子比特的线
经典比特		承载单经典比特的线
n 量子比特		承载 n 量子比特的线

2.3 Bell 基和 GHZ 态

Bell 态，也称为 EPR 态或 EPR 对，是有着最大纠缠度的双比特量子态，其纠缠度为 1，定义为 1 e-bit。纠缠是一种资源，是量子密码、量子隐形传态、量子路由器和量子超密编码等应用的关键。在局域操作和经典通信下，纠缠不能增加。

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

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{1b}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{1c}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1d}$$

GHZ 态是有着最大纠缠度的三比特量子态，共有八个，使用最多的一个是：

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{2}$$

2.4 量子隐形传态

充分理解量子隐形传态的过程及其意义将十分有助于讨论我们的研究课题。第一，量子隐形传态是量子远程控制的基础，后者无论是在思想上还是在实现过程上都与前者具有很大的传承性；第二，隐形传态所体现的处理量子态的优雅技巧将同样应用于关于量子远程控制的一些推导之中。

我们假定要传送的量子态为

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \tag{3}$$

其中 a 和 b 是未知的。输入线路的状态是

$$|\psi_0\rangle = |\psi\rangle\,|\Phi^+\rangle = \frac{1}{\sqrt{2}}\big[a\,|0\rangle\,(|00\rangle + |11\rangle) + b\,|1\rangle\,(|00\rangle + |11\rangle)\big], \tag{4}$$

并约定前两个量子比特属于 Alice，第三个量子比特属于 Bob。根据测量基的不同，可以有两种实现方式：

■ 参照图1，Alice 先把她的量子比特送到一个受控非门，得到

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\big[a\,|0\rangle\,(|00\rangle + |11\rangle) + b\,|1\rangle\,(|10\rangle + |01\rangle)\big], \tag{5}$$

接着她让第一量子比特通过一个 Hadamard 门，得到

$$|\psi_2\rangle = \frac{1}{2}\big[a(|0\rangle+|1\rangle)(|00\rangle+|11\rangle)+b(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)\big] \tag{6}$$

经过重新组项，这个状态可以写为

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{\sqrt{2}}\big[\,|00\rangle\,(a\,|0\rangle+b\,|1\rangle)+|01\rangle\,(a\,|1\rangle+b\,|0\rangle)+|10\rangle\,(a\,|0\rangle-b\,|1\rangle)\,|11\rangle\,(a\,|1\rangle-b\,|0\rangle)\big]\\ &= \frac{1}{\sqrt{2}}\big[\,|00\rangle\,|\psi\rangle+|01\rangle\,\sigma_1\,|\psi\rangle+|10\rangle\,\sigma_3\,|\psi\rangle\,|11\rangle\,(-i\sigma_2)\,|\psi\rangle\,\big]\end{aligned} \tag{7}$$

然后 Alice 以 $|0\rangle\langle 0|$ 和 $|1\rangle\langle 1|$ 为基，分别测量她拥有的两个量子比特，得到四个可能结果 00，01，10 和 11 中的一个；她把这个信息发给 Bob，据此 Bob 对他拥有的那一半 EPR 对进行四个操作中的一种，从而恢复原始的 $|\psi\rangle$：测量结果为 00 时，Bob 不需要做什么；如果是 01，Bob 可以用 Pauli-X 门来恢复；如果是 10，Bob 可以用 Pauli-Z 门；如果是 11，Bob 可以先用 Pauli-X 再用 Pauli-Z 门。总之，Bob 只需要应用变换 $Z^{M_1}X^{M_2}$ 到他的量子比特上就能恢复 Alice 传送的状态 $|\psi\rangle$。

■ Alice 只需对她的两个比特做联合 Bell 基测量，并将结果通知给 Bob；Bob 根据测量结果做 4 种可能的变换之一，即可得到 $|\psi\rangle$。

$$\begin{aligned}|\psi_0\rangle &= \frac{a}{\sqrt{2}}\,|000\rangle+\frac{a}{\sqrt{2}}\,|011\rangle+\frac{b}{\sqrt{2}}\,|100\rangle+\frac{b}{\sqrt{2}}\,|111\rangle\\ &= \frac{1}{2\sqrt{2}}\big[(|00\rangle+|11\rangle)(a\,|0\rangle+b\,|1\rangle)+(|01\rangle+|10\rangle)(a\,|1\rangle+b\,|0\rangle)\\ &\quad +(|00\rangle-|11\rangle)(a\,|0\rangle-b\,|1\rangle)+(|01\rangle-|10\rangle)(a\,|1\rangle-b\,|0\rangle)\big]\\ &= \frac{1}{2}\big[\,|\Phi^+\rangle\,|\psi\rangle+|\Psi^+\rangle\,\sigma_1\,|\psi\rangle+|\Phi^-\rangle\,\sigma_3\,|\psi\rangle+|\Psi^-\rangle\,(-i\sigma_2)\,|\psi\rangle\,\big]\end{aligned} \tag{8}$$

量子隐形传态强调量子力学不同资源之间的互换性，揭示出一个共享的 EPR 对加上两个经典比特的通信构成一个至少等于单量子比特通信的资源。需要注意的是，量子隐形传态并没有带来超光速通信，因为 Alice 必须通过经典信道把她的测量结果传给 Bob，否则，隐形传态根本不传送任何信息。事实上，在 Alice 测量完成后而 Bob 得到测量结果前，Bob 系统的状态，即约化密度矩阵是 $I/2$，这不依赖于 $|\psi\rangle$，故阻止了 Alice 用隐形传态以超光速向 Bob 传送信息。

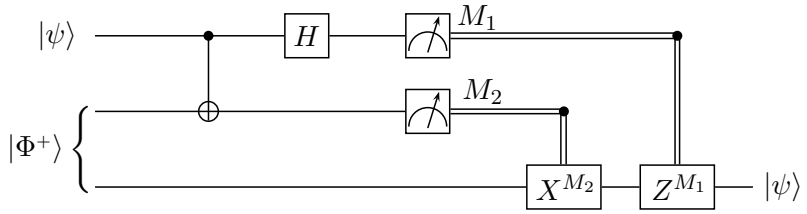


图 1. 单量子比特的隐形传态线路，上方两根线表示 Alice 的系统，下方的线是 Bob 的系统。本文所有的插图都是由LaTeX 的宏包PSTricks生成。

3 HPV 协议

某些特定量子操作的远程实现最早是由 Huelga，Plenio 和 Vaccaro 提出的，参见文献[5]。在 HPV 协议中，Alice 是发送方，Bob 是接受方，联合系统的初态为

$$|\Theta_1\rangle = |\Phi^+\rangle_{AB}\otimes|\xi\rangle_Y \tag{9}$$

其中 $|\Phi^+\rangle_{AB}$ 是 Alice 和 Bob 共享的一个 Bell 纠缠态，见(1a)。未知的量子态为

$$|\xi\rangle_Y = y_0 |0\rangle + y_1 |1\rangle_Y \tag{10}$$

由 Bob 拥有。要被远程实现的量子操作属于以下对角与反对角的两种特定类型：

$$U(0) = \begin{pmatrix} u_{00} & 0 \\ 0 & u_{11} \end{pmatrix}, \quad U(1) = \begin{pmatrix} 0 & u_{01} \\ u_{10} & 0 \end{pmatrix}. \tag{11}$$

下面我们将讨论简化的 HPV 协议，其量子线路见图2。为叙述的简便，我们不妨假定 Bob 拥有的第一个比特，即与 Alice 纠缠的那个，为

$$|\phi\rangle_B = x_0 |0\rangle_B + x_1 |1\rangle_B . \tag{12}$$

按照文献[7]，HPV 协议的全过程可分为五步：

一. Bob 进行一个受控非门操作，他用自己拥有的第二个比特，即(9) 中的第三比特，作为控制量子比特；然后以 $|b\rangle\langle b|$, $b = 0, 1$ 为基测量他的第一个比特。

$$\begin{aligned} |\phi\rangle_B \otimes |\xi\rangle_Y &\xrightarrow{\text{CNOT}} (x_0 |0\rangle_B + x_1 |1\rangle_B) \otimes y_0 |0\rangle_Y + (x_0 |1\rangle_B + x_1 |0\rangle_B) \otimes y_1 |1\rangle_Y \\ &= \sigma_0^B |\phi\rangle_B \otimes y_0 |0\rangle_Y + \sigma_1^B |\phi\rangle_B \otimes y_1 |1\rangle_Y \\ &= \left(\sigma_0^B \otimes |0\rangle_Y\langle 0| + \sigma_1^B \otimes |1\rangle_Y\langle 1|\right) |\phi\rangle_B \otimes |\xi\rangle_Y \\ &\xrightarrow{\text{Measure}} \left(|b\rangle_B\langle b| \otimes \sigma_0^Y\right) \left(\sigma_0^B \otimes |0\rangle_Y\langle 0| + \sigma_1^B \otimes |1\rangle_Y\langle 1|\right) |\phi\rangle_B \otimes |\xi\rangle_Y \end{aligned} \tag{13}$$

经过这两步操作，Bob 实现了下面这个量子算符：

$$\mathcal{P}_B(b) = \left(|b\rangle_B\langle b| \otimes \sigma_0^Y\right) \left(\sigma_0^B \otimes |0\rangle_Y\langle 0| + \sigma_1^B \otimes |1\rangle_Y\langle 1|\right) \tag{14}$$

二. 完成测量后，Bob 通过经典信道向 Alice 发送测量结果 b。据此，Alice 决定她的下一步操作：如果 $b = 0$，Alice 不必做任何操作 ($\sigma_0 = I$)；如果 $b = 1$，Alice 需要做一个 σ_1 变换。倘若 Bob 固定他的测量基，并事先告诉了 Alice，那么这将节省传递一经典比特所需的资源。

三. Alice 接收到 Bob 发来的经典比特 b 后，依次做一个 σ_b 操作、$U(d)$ 操作和 Hadamard 变换，然后以 $|a\rangle_A\langle a|$ ($a = 0, 1$) 为基测量她的量子比特，即

$$\mathcal{S}_A(a, b; d) = \left(|a\rangle_A\langle a|\right)\left[H^A U(d) \sigma_b^A\right], \tag{15}$$

其中 $U(d)$ 由(11)定义。

四. Alice 发送经典比特 d 和 a 给 Bob。

五. Bob 通过以下操作即可得到量子态 $U(d)|\xi\rangle$：

$$\mathcal{R}_B(a; d) = \sigma_0^B \otimes \left\{\left[(1-a)\sigma_0^Y + a\sigma_3^Y\right]\sigma_d^Y\right\} \tag{16}$$

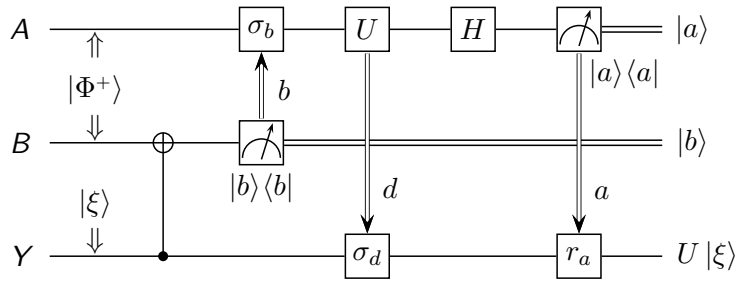


图2. 简化的 HPV 协议量子线路，其中 $U(d)$ 是要远程实现的部分已知的量子操作，H 是 Hadamard 门，σ_b, σ_d 是单位阵或非门，$r(a) = (1-a)\sigma_0 + a\sigma_3$, 两次测量分别是以 $|a\rangle\langle a|$ 和 $|b\rangle\langle b|$ 为基。

下面我们给出一个完整的证明，比文献[5]中的更易懂，不需要用到什么特殊的技巧。

■ 直接通过代入演算，可以得到

$$\begin{aligned}
\mathcal{S}_A\mathcal{P}_B|\Theta_1\rangle &= \big[\,|a\rangle_A\langle a|\,H^A U(d)\sigma_b^A\big]\otimes(|b\rangle_B\langle b|\otimes\sigma_0^Y)(\sigma_0^B\otimes|0\rangle_Y\langle 0| \\
&\quad + \sigma_1^B\otimes|1\rangle_Y\langle 1|)\,\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}(y_0|0\rangle+y_1|1\rangle)_Y \\
&= (|a\rangle_A\langle a|\,H^A U(d)\sigma_b^A\otimes|b\rangle_B\langle b|)\,\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}\otimes y_0|0\rangle_Y \\
&\quad + (|a\rangle_A\langle a|\,H^A U(d)\sigma_b^A\otimes|b\rangle_B\langle b|)\,\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB}\otimes y_1|1\rangle_Y \\
&= |a\rangle_A\langle a|\,H^A U(d)|0\rangle\otimes|b\rangle\otimes y_0|0\rangle + |a\rangle_A\langle a|\,H^A U(d)|1\rangle\otimes|b\rangle\otimes y_1|1\rangle \\
&= \frac{1}{\sqrt{2}}|a\rangle_A\langle a|\,[|0\rangle+(-1)^d|1\rangle]\otimes|b\rangle\otimes u_{d0}y_0|0\rangle \\
&\quad + \frac{1}{\sqrt{2}}|a\rangle_A\langle a|\,[|0\rangle-(-1)^d|1\rangle]\otimes|b\rangle\otimes u_{1-d,1}y_1|1\rangle \\
&= |a\rangle\otimes|b\rangle\otimes\big[(1-a)+(-1)^d a\big]\big[u_{d0}y_0|0\rangle+(-1)^a u_{1-d,1}y_1|1\rangle\big]
\end{aligned} \tag{17}$$

$$\begin{aligned}
\mathcal{R}_B\mathcal{S}_A\mathcal{P}_B|\Theta_1\rangle &= |a\rangle\otimes|b\rangle\otimes\big[(1-a)\sigma_0+a\sigma_3\big]\big[(1-d)\sigma_0+d\sigma_1\big]\big[(1-a) \\
&\quad + (-1)^d a\big]\big[u_{d0}y_0|0\rangle+(-1)^a u_{1-d,1}y_1|1\rangle\big] \\
&= |a\rangle\otimes|b\rangle\otimes\big[(1-a)+(-1)^d a\big]\big\{u_{d0}y_0\big[(1-d)|0\rangle+(1-2a)d|1\rangle\big] \\
&\quad + (-1)^a u_{1-d,1}y_1\big[d|0\rangle+(1-2a)(1-d)|1\rangle\big]\big\}
\end{aligned} \tag{18}$$

当 $d=0$ 时，$U(0)|\xi\rangle = u_{00}y_0|0\rangle + u_{11}y_1|1\rangle$，我们有

$$\begin{aligned}
\mathcal{R}_B\mathcal{S}_A\mathcal{P}_B|\Theta_1\rangle &= |a\rangle\otimes|b\rangle\otimes\big[u_{00}y_0|0\rangle+(-1)^a(1-2a)u_{11}y_1|1\rangle\big] \\
&= |a\rangle\otimes|b\rangle\otimes U(0)|\xi\rangle
\end{aligned} \tag{19}$$

当 $d=1$ 时，$U(1)|\xi\rangle = u_{01}y_1|0\rangle + u_{10}y_0|1\rangle$，我们有

$$\begin{aligned}
\mathcal{R}_B\mathcal{S}_A\mathcal{P}_B|\Theta_1\rangle &= |a\rangle\otimes|b\rangle\otimes(1-2a)\big[(-1)^a u_{01}y_1|0\rangle+(1-2a)u_{10}y_0|1\rangle\big] \\
&= |a\rangle\otimes|b\rangle\otimes U(1)|\xi\rangle
\end{aligned} \tag{20}$$

文献[1]指出，若要通过局域协议来远程传递任意的单比特量子操作(即 $SU(2)$ 的元素)，用少于 2 e-bits 和 4 c-bits 的资源是不行的，这等价于双向量子隐形传态所消耗的资源。而在简化的 HPV 协议中，由于要实现的量子操作部分已知，仅需要 1 e-bit 和 3 c-bits 即可完成。

4 多比特的远程控制

4.1 特定的集合

文献[7]将 HPV 协议中的两类操作扩展到了多量子比特情形。对于 N-qubit 系统，其量子操作的矩阵中每行和每列都只能有一个非零元素，即总共有 $2^N!$ 种不同的类型。我们用 t_m 来表示第 m 行的非零元素，那么这些特定的量子操作可写为

$$T_N^r(x,t)=\sum_{m=1}^{2^N} t_m \left|m,D\right\rangle \left\langle p_m(x),D\right| \tag{21}$$

其中 $x=1,2,\ldots,2^N!$，$|m,D\rangle$ 为二进制下 m 所对应的基底，并且

$$p(x)=\big(p_1(x),p_2(x),\ldots,p_{2^N}(x)\big) \tag{22}$$

是 $\{1,2,\ldots,2^N\}$ 的全排列集合中的元素。(21)代表的所有量子操作的集合我们用 $\mathbb{T}_N^r$ 来表示。由于

$$T_N^r(x,t)[T_N^r(x,t)]^\dagger=\sum_{m=1}^{2^N} t_m t_m^* \left|m,D\right\rangle\left\langle m,D\right| \tag{23}$$

$$[T_N^r(x,t)]^\dagger T_N^r(x,t)=\sum_{m=1}^{2^N} t_m^* t_m \left|p_m(x),D\right\rangle\left\langle p_m(x),D\right| \tag{24}$$

当且仅当 $t_m=e^{i\phi_m}$，ϕ_m 为实数时，$T_N^r(x,t)$ 满足酉矩阵的要求。应该指出，这里的多比特量子操作集合不可以约化到单比特操作的直积。因此，对它们的讨论是非平凡的。

以双量子比特为例，$\{1,2,3,4\}$ 的全排列为

$$\begin{aligned}\mathbb{P}_4=\{&(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2),\\&(2,1,3,4),(2,1,4,3),(2,3,1,4),(2,3,4,1),(2,4,1,3),(2,4,3,1),\\&(3,1,2,4),(3,1,4,2),(3,2,1,4),(3,2,4,1),(3,4,1,2),(3,4,2,1),\\&(4,1,2,3),(4,1,3,2),(4,2,1,3),(4,2,3,1),(4,3,1,2),(4,3,2,1)\}\end{aligned} \tag{25}$$

并且 $|1,D\rangle=|00\rangle$，$|2,D\rangle=|01\rangle$，$|3,D\rangle=|10\rangle$，$|4,D\rangle=|11\rangle$。容易看到，在量子信息处理中起重要作用的受控操作都属于这些特定的集合

$$U_C(1)=T_2^r(2,t)|_{t_1=t_2=1}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}0&t_3\\t_4&0\end{pmatrix} \tag{26a}$$

$$U_C(2)=T_2^r(6,t)|_{t_1=t_3=1}=\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}0&t_2\\t_4&0\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix} \tag{26b}$$

$$U_C(3)=T_2^r(7,t)|_{t_1=t_2=1}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\otimes\begin{pmatrix}0&t_3\\t_4&0\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{26c}$$

$$U_C(4)=T_2^r(15,t)|_{t_2=t_4=1}=\begin{pmatrix}0&t_1\\t_3&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix} \tag{26d}$$

如果取(21)中所有的非零元素为 1, 那么就得到了 Bob 在该协议中的恢复操作

$$R_N(x)=\sum_{m=1}^{2^N}\left|m,D\right\rangle\left\langle p_m(x),D\right| \tag{27}$$

在建立协议时，我们需要两个映射表：一个是从 $T_N^r(x,t)\in\mathbb{T}_N^r$ 到经典信息 x 的映射，要提供给 Alice；另一个是从经典信息 x 到 $R_N(x)$ 的映射，要提供给 Bob。

4.2 swapping 变换

为以后的讨论做铺垫，我们需要研究一般情形 N-qubit 下的 swapping 变换，主要参考[7]。由第2.1小节可知，双量子比特的 swapping 变换为

$$S_W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{28}$$

满足 $S_W |\alpha_X \beta_Y\rangle = |\beta_Y \alpha_X\rangle$。易证 S_W 具有以下性质，

$$S_W (M^X \otimes M^Y) S_W = M^Y \otimes M^X \tag{29}$$

即 S_W 把空间 $H_X \otimes H_Y$ 变成 $H_Y \otimes H_X$。

对于 N-qubit 系统，交换第 i 比特和第 $(i+1)$ 比特的变换为

$$S_N(i, i+1) = \sigma_0^{\otimes(i-1)} \otimes S_W \otimes \sigma_0^{\otimes(N_i-1)}, \tag{30}$$

其中 $\sigma_0^{\otimes(i-1)}$ 表示对前 $(i-1)$ 个比特做恒等操作，$\sigma_0^{\otimes(N_i-1)}$ 表示对后 $(N-i-1)$ 个比特做恒等操作。同时，我们还要定义下面两类变换：

$$F_N(i,j) = \prod_{\alpha=1\leftarrow}^{j-i} S_N(j-\alpha, j+1-\alpha) \tag{31}$$

$$P_N(j,k) = \prod_{\beta=j\leftarrow}^{k-1} S_N(\beta, \beta+1) \tag{32}$$

其中 $F_N(i,j)$ 变换将自旋态 j 移到 $i (i<j)$ 之前，而 $P_N(j,k)$ 将 j 移到 $k (k>j)$ 之后。注意，“$\leftarrow$”表示相乘的各因子是从右到左排列。进一步定义

$$\Lambda(2,N) = \prod_{i=1\leftarrow}^{N-1} P_{2N}\big(2(N-i), 2N-i\big) \quad (N \geqslant 2) \tag{33}$$

$$\Omega(2,N) = \prod_{i=1\leftarrow}^{N} P_{2N}(1, 2N) \quad (N \geqslant 2) \tag{34}$$

于是，我们有

$$\Lambda(2,N)\Big(\otimes_{i=1}^N |a_i b_i\rangle \Big) = \Big(\otimes_{i=1}^N |a_i\rangle \Big) \otimes \Big(\otimes_{j=1}^N |b_j\rangle \Big) \tag{35}$$

$$\Lambda(2,N)\Big[\otimes_{i=1}^N \Big(M_{\alpha_i}^{A_i} \otimes M_{\beta_i}^{B_i} \Big) \Big] \Lambda^{-1}(2,N) = \Big(\otimes_{i=1}^N M_{\alpha_i}^{A_i} \Big) \otimes \Big(\otimes_{j=1}^N M_{\beta_j}^{B_j} \Big) \tag{36}$$

$$\Omega(2,N)\Big[\Big(\otimes_{i=1}^N |a_i\rangle \Big) \otimes \Big(\otimes_{j=1}^N |b_j\rangle \Big) \Big] = \Big(\otimes_{i=1}^N |b_i\rangle \Big) \otimes \Big(\otimes_{j=1}^N |a_j\rangle \Big) \tag{37}$$

$$\Omega(2,N)\Big[\Big(\otimes_{i=1}^N M_{\alpha_i}^{A_i} \Big) \otimes \Big(\otimes_{j=1}^N M_{\beta_j}^{B_j} \Big) \Big] \Omega^{-1}(2,N) = \Big(\otimes_{i=1}^N M_{\beta_i}^{B_i} \Big) \otimes \Big(\otimes_{j=1}^N M_{\alpha_j}^{A_j} \Big) \tag{38}$$

上述四个等式，我们只给出 $N=2$ 的证明，推广到 $N>2$ 应该很容易。对于(35)，我们有

$$\Lambda(2,2)\big(|a_1 b_1\rangle \otimes |a_2 b_2\rangle \big) = P_4(2,3) |a_1 b_1 a_2 b_2\rangle = |a_1 a_2 b_1 b_2\rangle = \big(\otimes_{i=1}^2 |a_i\rangle \big) \otimes \big(\otimes_{j=1}^2 |b_j\rangle \big) \tag{39}$$

对于(36)，根据 $\Lambda(2,2)=P_4(2,3)=S_4(2,3)=P_4^{-1}(2,3)$，我们可以得到

$$\begin{aligned}
&\Lambda(2,2)\Big[\Big(M_{\alpha_1}^{A_1}\otimes M_{\beta_1}^{B_1}\Big)\otimes\Big(M_{\alpha_2}^{A_2}\otimes M_{\beta_2}^{B_2}\Big)\Big]\Lambda^{-1}(2,2)\,|\alpha_1\beta_1\alpha_2\beta_2\rangle\\
=&S_4(2,3)\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}\Big)S_4(2,3)\,|\alpha_1\beta_1\alpha_2\beta_2\rangle\\
=&S_4(2,3)\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}\Big)\,|\alpha_1\alpha_2\beta_1\beta_2\rangle\\
=&P_4(2,3)\Big(M_{\alpha_1}^{A_1}\,|\alpha_1\rangle\otimes M_{\beta_1}^{B_1}\,|\alpha_2\rangle\otimes M_{\alpha_2}^{A_2}\,|\alpha_2\rangle\otimes M_{\beta_2}^{B_2}\,|\beta_2\rangle\Big)\\
=&M_{\alpha_1}^{A_1}\,|\alpha_1\rangle\otimes M_{\alpha_2}^{A_2}\,|\alpha_2\rangle\otimes M_{\beta_1}^{B_1}\,|\alpha_2\rangle\otimes M_{\beta_2}^{B_2}\,|\beta_2\rangle\\
=&\Big(\otimes_{i=1}^{2}M_{\alpha_i}^{A_i}\Big)\otimes\Big(\otimes_{j=1}^{2}M_{\beta_j}^{B_j}\Big)\,|\alpha_1\beta_1\alpha_2\beta_2\rangle
\end{aligned}\tag{40}$$

对于(37)，我们有

$$\begin{aligned}
&\Omega(2,2)\big(\,|a_1a_2\rangle\otimes|b_1b_2\rangle\,\big)=P_4(1,4)P_4(1,4)\,|a_1a_2b_1b_2\rangle\\
=&P_4(1,2)\,|a_2b_1b_2a_1\rangle=|b_1b_2a_1a_2\rangle=\big(\otimes_{i=1}^{2}|b_i\rangle\,\big)\otimes\big(\otimes_{j=1}^{2}|a_j\rangle\,\big)
\end{aligned}\tag{41}$$

对于(38)，由 $\Omega^{-1}(2,2)=P_4^{-2}(1,4)=F_4^2(1,4)$，我们可以得到

$$\begin{aligned}
&\Omega(2,2)\Big[\Big(M_{\alpha_1}^{A_1}\otimes M_{\alpha_2}^{A_2}\Big)\otimes\Big(M_{\beta_1}^{B_1}\otimes M_{\beta_2}^{B_2}\Big)\Big]\Omega^{-1}(2,2)\,|\alpha_1\beta_1\alpha_2\beta_2\rangle\\
=&P_4(1,4)P_4(1,4)\Big(M_{\alpha_1}^{A_1}M_{\alpha_2}^{A_2}M_{\beta_1}^{B_1}M_{\beta_2}^{B_2}\Big)F_4(1,4)F_4(1,4)\,|\alpha_1\beta_1\alpha_2\beta_2\rangle\\
=&P_4(1,4)P_4(1,4)\Big(M_{\alpha_1}^{A_1}M_{\alpha_2}^{A_2}M_{\beta_1}^{B_1}M_{\beta_2}^{B_2}\Big)F_4(1,4)\,|\beta_2\alpha_1\beta_1\alpha_2\rangle\\
=&P_4(1,4)P_4(1,4)\Big(M_{\alpha_1}^{A_1}M_{\alpha_2}^{A_2}M_{\beta_1}^{B_1}M_{\beta_2}^{B_2}\Big)\,|\alpha_2\beta_2\alpha_1\beta_1\rangle\\
=&P_4(1,4)P_4(1,4)\Big(M_{\alpha_1}^{A_1}\,|\alpha_2\rangle\otimes M_{\alpha_2}^{A_2}\,|\beta_2\rangle\otimes M_{\beta_1}^{B_1}\,|\alpha_1\rangle\otimes M_{\beta_2}^{B_2}\,|\beta_1\rangle\Big)\\
=&P_4(1,4)\Big(M_{\alpha_2}^{A_2}\,|\beta_2\rangle\otimes M_{\beta_1}^{B_1}\,|\alpha_1\rangle\otimes M_{\beta_2}^{B_2}\,|\beta_1\rangle\otimes M_{\alpha_1}^{A_1}\,|\alpha_2\rangle\Big)\\
=&M_{\beta_1}^{B_1}\,|\alpha_1\rangle\otimes M_{\beta_2}^{B_2}\,|\beta_1\rangle\otimes M_{\alpha_1}^{A_1}\,|\alpha_2\rangle\otimes M_{\alpha_2}^{A_2}\,|\beta_2\rangle\\
=&\Big(\otimes_{i=1}^{2}M_{\beta_i}^{B_i}\Big)\otimes\Big(\otimes_{j=1}^{2}M_{\alpha_j}^{A_j}\Big)\,|\alpha_1\beta_1\alpha_2\beta_2\rangle
\end{aligned}\tag{42}$$

同样，我们引入

$$\Upsilon(3,N)=\prod_{i=1\leftarrow}^{N-1}F_{3N}(3i,2N+i)\quad(N\geqslant 2)\tag{43}$$

$$\Gamma(3,N)=\big[I_{2^N}\otimes\Omega(2,N)\big]\big[\Lambda(2,N)\otimes I_{2^N}\big]\tag{44}$$

它们具有如下性质：

$$\Upsilon(3,N)\Big(\otimes_{i=1}^{N}|a_ib_i\rangle\,\Big)\otimes\Big(\otimes_{j=1}^{N}|y_j\rangle\,\Big)=\otimes_{i=1}^{N}|a_ib_iy_i\rangle\tag{45}$$

$$\Upsilon(3,N)\Big[\otimes_{i=1}^{N}\Big(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\Big)\Big]\Big(\otimes_{j=1}^{N}M_{\gamma_j}^{Y_j}\Big)\Upsilon^{-1}(3,N)=\otimes_{i=1}^{N}\Big(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\otimes M_{\gamma_i}^{Y_i}\Big)\tag{46}$$

$$\Gamma(3,N)\Big(\otimes_{i=1}^{N}|a_ib_i\rangle\,\Big)\otimes\Big(\otimes_{j=1}^{N}|y_j\rangle\,\Big)=\Big(\otimes_{i=1}^{N}|a_i\rangle\,\Big)\otimes\Big(\otimes_{j=1}^{N}|y_j\rangle\,\Big)\otimes\Big(\otimes_{k=1}^{N}|b_k\rangle\,\Big)\tag{47}$$

$$\begin{aligned}
&\Gamma(3,N)\Big[\otimes_{i=1}^{N}\Big(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\Big)\Big]\Big(\otimes_{j=1}^{N}M_{\gamma_j}^{Y_j}\Big)\Gamma^{-1}(3,N)\\
&\qquad=\Big(\otimes_{i=1}^{N}M_{\alpha_i}^{A_i}\Big)\otimes\Big(\otimes_{j=1}^{N}M_{\gamma_j}^{Y_j}\Big)\otimes\Big(\otimes_{k=1}^{N}M_{\beta_k}^{B_k}\Big)
\end{aligned}\tag{48}$$

我们也只对 $N=2$ 的情形给出证明。对于(45)，我们有

$$\Upsilon(3,2)\Big(\,|a_1b_1\rangle\otimes|a_2b_2\rangle\,\Big)\otimes\Big(\,|y_1\rangle\otimes|y_2\rangle\,\Big)=F_6(3,5)\,|a_1b_1a_2b_2y_1y_2\rangle=|a_1b_1y_1a_2b_2y_2\rangle\tag{49}$$

对于(46)，根据 $\Upsilon^{-1}(3,2)=F_6^{-1}(3,5)=P_6(3,5)$，我们可以得到

$$\begin{aligned}
&\Upsilon(3,2)\Big[\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}\Big)\otimes\Big(M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}\Big)\Big]\Big(M_{\gamma_1}^{Y_1}\otimes M_{\gamma_2}^{Y_2}\Big)\Upsilon^{-1}(3,2)\,|\alpha_1\beta_1\alpha_2\beta_2\gamma_1\gamma_2\rangle\\
=&F_6(3,5)\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}M_{\gamma_1}^{Y_1}M_{\gamma_2}^{Y_2}\Big)P_6(3,5)\,|\alpha_1\beta_1\alpha_2\beta_2\gamma_1\gamma_2\rangle\\
=&F_6(3,5)\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}M_{\gamma_1}^{Y_1}M_{\gamma_2}^{Y_2}\Big)\,|\alpha_1\beta_1\beta_2\gamma_1\alpha_2\gamma_2\rangle\\
=&F_6(3,5)\Big(M_{\alpha_1}^{A_1}|\alpha_1\rangle\otimes M_{\beta_1}^{B_1}|\beta_1\rangle\otimes M_{\alpha_2}^{A_2}|\beta_2\rangle\otimes M_{\beta_2}^{B_2}|\gamma_1\rangle\otimes M_{\gamma_1}^{Y_1}|\alpha_2\rangle\otimes M_{\gamma_2}^{Y_2}|\gamma_2\rangle\Big)\\
=&M_{\alpha_1}^{A_1}|\alpha_1\rangle\otimes M_{\beta_1}^{B_1}|\beta_1\rangle\otimes M_{\gamma_1}^{Y_1}|\alpha_2\rangle\otimes M_{\alpha_2}^{A_2}|\beta_2\rangle\otimes M_{\beta_2}^{B_2}|\gamma_1\rangle\otimes M_{\gamma_2}^{Y_2}|\gamma_2\rangle\\
=&\otimes_{i=1}^{2}\Big(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\otimes M_{\gamma_i}^{Y_i}\Big)\,|\alpha_1\beta_1\alpha_2\beta_2\gamma_1\gamma_2\rangle
\end{aligned}\tag{50}$$

对于(47)，我们有

$$\begin{aligned}
&\Gamma(3,2)\big(\,|a_1b_1\rangle\otimes|a_2b_2\rangle\,\big)\otimes|y_1y_2\rangle=\big[I_4\otimes P_4^2(1,4)\big]\big[P_4(2,3)\otimes I_4\big]\,|a_1b_1a_2b_2y_1y_2\rangle\\
=&\big[I_4\otimes P_4(1,4)P_4(1,4)\big]\,|a_1a_2b_1b_2y_1y_2\rangle=\big[I_4\otimes P_4(1,4)\big]\,|a_1a_2b_2y_1y_2b_1\rangle\\
=&|a_1a_2y_1y_2b_1b_2\rangle=\big(\otimes_{i=1}^{2}|a_i\rangle\big)\otimes\big(\otimes_{j=1}^{2}|y_j\rangle\big)\otimes\big(\otimes_{k=1}^{2}|b_k\rangle\big)
\end{aligned}\tag{51}$$

对于(48)，由 $\Gamma^{-1}(3,2)=\big[P_4(2,3)\otimes I_4\big]\big[I_4\otimes F_4^2(1,4)\big]$，我们可以得到

$$\begin{aligned}
&\Gamma(3,2)\Big[\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}\Big)\otimes\Big(M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}\Big)\Big]\Big(M_{\gamma_1}^{Y_1}\otimes M_{\gamma_2}^{Y_2}\Big)\Gamma^{-1}(3,2)\,|\alpha_1\beta_1\alpha_2\beta_2\gamma_1\gamma_2\rangle\\
=&\Gamma(3,2)\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}M_{\gamma_1}^{Y_1}M_{\gamma_2}^{Y_2}\Big)\big[P_4(2,3)\otimes I_4\big]\big[I_4\otimes F_4^2(1,4)\big]\,|\alpha_1\beta_1\alpha_2\beta_2\gamma_1\gamma_2\rangle\\
=&\Gamma(3,2)\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}M_{\gamma_1}^{Y_1}M_{\gamma_2}^{Y_2}\Big)\big[P_4(2,3)\otimes I_4\big]\,|\alpha_1\beta_1\gamma_1\gamma_2\alpha_2\beta_2\rangle\\
=&\big[I_4\otimes P_4^2(1,4)\big]\big[P_4(2,3)\otimes I_4\big]\Big(M_{\alpha_1}^{A_1}M_{\beta_1}^{B_1}M_{\alpha_2}^{A_2}M_{\beta_2}^{B_2}M_{\gamma_1}^{Y_1}M_{\gamma_2}^{Y_2}\Big)\,|\alpha_1\gamma_1\beta_1\gamma_2\alpha_2\beta_2\rangle\\
=&\big[I_4\otimes P_4^2(1,4)\big]M_{\alpha_1}^{A_1}|\alpha_1\rangle\otimes M_{\alpha_2}^{A_2}|\beta_1\rangle\otimes M_{\beta_1}^{B_1}|\gamma_1\rangle\otimes M_{\beta_2}^{B_2}|\gamma_2\rangle\otimes M_{\gamma_1}^{Y_1}|\alpha_2\rangle\otimes M_{\gamma_2}^{Y_2}|\beta_2\rangle\\
=&M_{\alpha_1}^{A_1}|\alpha_1\rangle\otimes M_{\alpha_2}^{A_2}|\beta_1\rangle\otimes M_{\gamma_1}^{Y_1}|\alpha_2\rangle\otimes M_{\gamma_2}^{Y_2}|\beta_2\rangle\otimes M_{\beta_1}^{B_1}|\gamma_1\rangle\otimes M_{\beta_2}^{B_2}|\gamma_2\rangle\\
=&\Big(\otimes_{i=1}^{2}M_{\alpha_i}^{A_i}\Big)\otimes\Big(\otimes_{j=1}^{2}M_{\gamma_j}^{Y_j}\Big)\otimes\Big(\otimes_{k=1}^{2}M_{\beta_k}^{B_k}\Big)\,|\alpha_1\beta_1\alpha_2\beta_2\gamma_1\gamma_2\rangle
\end{aligned}\tag{52}$$

4.3 两比特协议

和第3节类似，我们假定联合系统的初始态为

$$\big|\Theta_2^{\mathrm{ini}}\big\rangle=|\Phi^+\rangle_{A_1B_1}\otimes|\Phi^+\rangle_{A_2B_2}\otimes|\xi\rangle_{Y_1Y_2}\tag{53}$$

未知的量子态为

$$|\xi\rangle_{Y_1Y_2}=\sum_{j_1,j_2=0}^{1}y_{j_1j_2}\,|j_1j_2\rangle_{Y_1Y_2}\,,\tag{54}$$

其中 A_1, A_2 属于 Alice，B_1, B_2, Y_1, Y_2 属于 Bob。Alice 和 Bob 共享两个 Bell 纠缠态。在(53)中，系统的 Hilbert 空间为

$$H=H_{A_1}\otimes H_{B_1}\otimes H_{A_2}\otimes H_{B_2}\otimes H_{Y_1}\otimes H_{Y_2}.\tag{55}$$

为了将局域子空间的操作写得更简洁和便于推广到 N-qubit 系统，我们将采用在上一小节引入的 swapping 变换，仅在分析具体过程时才详细地给出不用该变换的表达式。容易得到：

$$\Upsilon^{-1}(3,2)\left|a_1b_1y_1\right\rangle\otimes\left|a_2b_2y_2\right\rangle = P_6(3,5)\left|a_1b_1y_1a_2b_2y_2\right\rangle = \left|a_1b_1a_2b_2y_1y_2\right\rangle \tag{56}$$

$$[\Lambda^{-1}(2,2)\otimes I_4]\left|a_1a_2\right\rangle\otimes\left|b_1b_2\right\rangle\otimes\left|y_1y_2\right\rangle = P_4(2,3)\otimes I_4\left|a_1a_2b_1b_2y_1y_2\right\rangle = \left|a_1b_1a_2b_2y_1y_2\right\rangle \tag{57}$$

$$\begin{aligned}\Gamma^{-1}(3,2)\left|a_1a_2\right\rangle\otimes\left|y_1y_2\right\rangle\otimes\left|b_1b_2\right\rangle &= [P_4(2,3)\otimes I_4][I_4\otimes F_4^2(1,4)]\left|a_1a_2y_1y_2b_1b_2\right\rangle\\ &= P_4(2,3)\otimes I_4\left|a_1a_2b_1b_2y_1y_2\right\rangle = \left|a_1b_1a_2b_2y_1y_2\right\rangle\end{aligned} \tag{58}$$

和简化的 HPV 协议一样，两比特的协议仍然分为五步:

一. Bob 执行两个受控非门操作，他用自己拥有的 Y_1, Y_2 作为控制量子比特，B_1, B_2 作为目标比特；然后以 $\left|b_1\right\rangle_{B_1}\!\langle b_1|\otimes\left|b_2\right\rangle_{B_2}\!\langle b_2|$ $(b_1,b_2=0,1)$ 为基测量 B_1, B_2。经过这两步操作，Bob 实现了下面这个量子算符：

$$\mathcal{P}_B(b_1,b_2) = \Upsilon^{-1}(3,2)\big\{\otimes_{m=1}^{2}\sigma_0^{A_m}\otimes\big[(\left|b_m\right\rangle_{B_m}\!\langle b_m|\otimes\sigma_0^{Y_m})C^{\mathrm{not}}(0,1)\big]\big\}\Upsilon(3,2) \tag{59}$$

如果不用 swapping 变换，那么这个操作可写为

$$\begin{aligned}\mathcal{P}_B(b_1,b_2) = &\big(\sigma_0^{A_1}\otimes\left|b_1\right\rangle_{B_1}\!\langle b_1|\otimes\sigma_0^{A_2}\otimes\left|b_2\right\rangle_{B_2}\!\langle b_2|\otimes\sigma_0^{Y_1}\otimes\sigma_0^{Y_2}\big)\\ &\big[\sigma_0^{A_1}C_2^{\mathrm{not}}(0,1)\otimes\sigma_0^{Y_2}\big]\big[\sigma_0^{A_1}\otimes\sigma_0^{B_1}\otimes\sigma_0^{A_2}\otimes C_1^{\mathrm{not}}(0,1)\big]\end{aligned} \tag{60}$$

其中，C_M^{not} 的定义见(61)，当 $M=0$ 时即为通常的 C-NOT 门，$(0,1)$ 表示最后一个比特为控制比特而第一个比特为目标比特，在控制比特为 $\left|1\right\rangle$ 时翻转。

$$C_M^{\mathrm{not}}(0,1) = \sigma_0\otimes\big(\otimes_{m=1}^{M}\sigma_0\big)\otimes\big(\left|0\right\rangle\!\langle 0|\big)+\sigma_1\otimes\big(\otimes_{m=1}^{M}\sigma_0\big)\otimes\big(\left|1\right\rangle\!\langle 1|\big) \tag{61}$$

二. 测量完成后，Bob 通过经典信道向 Alice 发送信息 b_1, b_2。

三. Alice 对她所拥有的两个比特 A_1, A_2 依次执行以下量子操作：$\sigma_{b_1}^{A_1}\otimes\sigma_{b_2}^{A_2}$、$T_2^r(x,t)$ 和两个 Hadamard 变换 $H^{A_1}\otimes H^{A_2}$ 。然后，Alice 以 $\left|a_1\right\rangle_{A_1}\!\langle a_1|\otimes\left|a_2\right\rangle_{A_2}\!\langle a_2|$ $(a_1,a_2=0,1)$ 为基测量她的量子比特。整个过程中，Alice 完成的操作为

$$\begin{aligned}\mathcal{S}_A(a_1,b_1,a_2,b_2;x,t) = &\big[\Lambda^{-1}(2,2)\otimes I_4\big]\big\{\big[\big(\left|a_1a_2\right\rangle_{A_1A_2}\!\langle a_1a_2|\big)\big(H^{A_1}\otimes H^{A_2}\big)\\ &T_2^r(x,t)\big(\sigma_{b_1}^{A_1}\otimes\sigma_{b_2}^{A_2}\big)\big]\otimes I_{16}\big\}\big[\Lambda(2,2)\otimes I_4\big]\end{aligned} \tag{62}$$

四. Alice 完成测量后，将两个经典比特 a_1, a_2 发送给 Bob。此外，Alice 仍需要把 x 告诉 Bob，使他知道被传递的量子操作是属于哪种类型。对于 2-qubit 系统，这需要 5 个经典比特 $(2^5>24)$。

五. Bob 通过以下操作来得到 Alice 远程实现的量子运算：

$$\mathcal{R}_B(a_1,a_2;x) = I_{16}\otimes\big\{\big[r^{Y_1}(a_1)\otimes r^{Y_2}(a_2)\big]R_2(x)\big\}, \tag{63}$$

其中 $R_2(x)$ 是通过映射表根据经典信息 x 得到的，$r(y)$ 定义为

$$r(y) = (1-y)\sigma_0+y\sigma_3. \tag{64}$$

在该协议中，Bob 和 Alice 所执行的全部量子操作可以写为

$$\mathcal{I}_R(a_1,b_1,a_2,b_2;x,t) = \mathcal{R}_B(a_1,a_2;x)\mathcal{S}_A(a_1,b_1,a_2,b_2;x,t)\mathcal{P}_B(b_1,b_2) \tag{65}$$

系统最终的量子态为

$$\left|\Theta_2^{\mathrm{fin}}\right\rangle = \mathcal{I}_R(a_1,b_1,a_2,b_2;x)\left|\Theta_2^{\mathrm{ini}}\right\rangle = \frac{1}{4}\left|a_1b_1a_2b_2\right\rangle_{A_1B_1A_2B_2}\otimes T_2^r(x,t)\left|\xi\right\rangle_{Y_1Y_2} \tag{66}$$

这个协议的证明，我们留到下一小节，它只不过是 $N=2$ 时的特例罢了。

4.4 多比特协议

我们要将上面的讨论推广到 N-qubit 情形。初态设为

$$\left|\Theta_N^{\rm ini}\right\rangle = \left(\otimes_{m=1}^N \left|\Phi^+\right\rangle_{A_mB_m}\right)\otimes\left|\xi\right\rangle_{Y_1Y_2\cdots Y_N}, \tag{67}$$

其中 $\left|\xi\right\rangle_{Y_1Y_2\cdots Y_N}$ 为任意未知的纯态，即

$$\left|\xi\right\rangle_{Y_1Y_2\cdots Y_N} = \sum_{k_1,k_2,\ldots,k_N=0}^{1} y_{k_1k_2\cdots k_N}\left|k_1k_2\cdots k_N\right\rangle \tag{68}$$

Alice 的量子态为 $\left|a_1a_2\cdots a_N\right\rangle$，Bob 的量子态为 $\left|b_1b_2\cdots b_Ny_1y_2\cdots y_N\right\rangle$。和前面的一样，协议仍分为五步，在很多情形下只需要将对应的 2-qubit 换成 N-qubit 即可，具体不再重复，我们这里只写出对应于(59, 62, 63, 65, 66)的式子。

$$\mathcal{P}_B(b) = \Upsilon^{-1}(3,N)\otimes_{m=1}^N\left\{\sigma_0^{A_m}\otimes\left[\left(\left|b_m\right\rangle\left\langle b_m\right|\otimes\sigma_0\right)C^{\rm not}(0,1)\right]\right\}\Upsilon_N(3,N) \tag{69}$$

$$\begin{aligned}\mathcal{S}_A(a,b;x,t) = {}& \left[\Lambda^{-1}(2,N)\otimes I_{2^N}\right]\left[\left(\otimes_{m=1}^N\left|a_m\right\rangle_{A_m}\left\langle a_m\right|\right)\right.\\ & \left.\left(\otimes_{m=1}^N H^{A_m}\right)T_N^r(x,t)\left(\otimes_{m=1}^N\sigma_{b_m}^{A_m}\right)\otimes I_{4^N}\right]\left[\Lambda(2,N)\otimes I_{2^N}\right]\end{aligned} \tag{70}$$

$$\mathcal{R}_B(a;x) = I_{4^N}\otimes\left\{\left[\otimes_{m=1}^N r(a_m)\right]R_N(x)\right\} \tag{71}$$

$$\mathcal{I}_R(a,b;x,t) = \mathcal{R}_B(a;x)\mathcal{S}_A(a,b;x,t)\mathcal{P}_B(b) \tag{72}$$

$$\left|\Theta_N^{\rm fin}\right\rangle = \mathcal{I}_R(a,b;x,t)\left|\Theta_N^{\rm ini}\right\rangle = \frac{1}{2^N}\left(\otimes_{m=1}^N\left|a_ib_i\right\rangle_{A_iB_i}\right)\otimes T_N^r(x,t)\left|\xi\right\rangle_Y \tag{73}$$

在以上各式中，我们采用了简写记法：a 代表 $a_1,a_2,\ldots,a_N$，b 代表 $b_1,b_2,\ldots,b_N$，Y 代表 $Y_1Y_2\cdots Y_N$。(71)中的 $r(a_m)$ 为

$$r(a_m) = \sum_{l_m=0}^{1}(-1)^{a_ml_m}\left|l_m\right\rangle\left\langle l_m\right| \tag{74}$$

下面我们要给出该协议的简要证明，具体参见文献[7]。

■ 利用 swapping 变换 Υ，我们可把系统初态(67)改写成

$$\left|\Theta_N^{\rm ini}\right\rangle = \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(3,N)\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\otimes_{m=1}^N\left(\left|00k_m\right\rangle+\left|11k_m\right\rangle\right) \tag{75}$$

结合 $N=2$ 的情形(56)，容易看出

$$\begin{aligned}&\frac{1}{\sqrt{2^N}}\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\Upsilon^{-1}(3,N)\otimes_{m=1}^N\left[\left(\left|00\right\rangle+\left|11\right\rangle\right)\left|k_m\right\rangle\right]\\ ={}&\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\left(\otimes_{m=1}^N\left|\Phi^+\right\rangle\right)\left(\otimes_{m=1}^N\left|k_m\right\rangle\right) = \left(\otimes_{m=1}^N\left|\Phi^+\right\rangle_{A_mB_m}\right)\otimes\left|\xi\right\rangle_{Y_1Y_2\cdots Y_N}\end{aligned} \tag{76}$$

在协议的第一步，Bob 执行了量子操作 $\mathcal{P}_B$，即

$$\left|\Theta_N^P\right\rangle = \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(3,N)\sum_{k_1,\cdots,k_N=0}^{1} y_{k_1\cdots k_N}\otimes_{m=1}^N\left\{\sigma_0\otimes\left[\left(\left|b_m\right\rangle\left\langle b_m\right|\right)C^{\rm not}(0,1)\right]\right\}\left(\left|00k_m\right\rangle+\left|11k_m\right\rangle\right) \tag{77}$$

其中 $C^{\text{not}}(0,1)$ 的定义见(61), 取 $M=1$。进一步，由 $\sigma_b\left|b\right\rangle=\left|0\right\rangle$ 和 $\sigma_b\left|1-b\right\rangle=\left|1\right\rangle$ $(b=0,1)$，可以推出以下的化简

$$\begin{aligned}
&\{\sigma_0\otimes[(\left|b\right\rangle\left\langle b\right|)C^{\text{not}}(0,1)]\}(\left|00k\right\rangle+\left|11k\right\rangle)\\
=&[\sigma_0\otimes(\left|b\right\rangle\left\langle b\right|)\otimes\sigma_0][(\left|000\right\rangle+\left|110\right\rangle)\delta_{k0}+(\left|101\right\rangle+\left|011\right\rangle)\delta_{k1}]\\
=&(\left|0b0\right\rangle\delta_{b0}+\left|1b0\right\rangle\delta_{b1})\delta_{k0}+(\left|1b1\right\rangle\delta_{b0}+\left|0b1\right\rangle\delta_{b1})\delta_{k1}\\
=&\left|bb0\right\rangle(\delta_{b0}+\delta_{b1})\delta_{k0}+\left|(1-b)b1\right\rangle(\delta_{b0}+\delta_{b1})\delta_{k1}\\
=&\left|bb0\right\rangle\delta_{k0}+\left|(1-b)b1\right\rangle\delta_{k1}\\
=&(\sigma_b\otimes I_4)(\delta_{k0}\left|0b0\right\rangle+\delta_{k1}\left|1b1\right\rangle)\\
=&(\sigma_b\otimes I_4)(\delta_{k0}+\delta_{k1})\left|kbk\right\rangle\\
=&(\sigma_b\otimes I_4)\left|kbk\right\rangle
\end{aligned}\tag{78}$$

和(44)，可得

$$\begin{aligned}
\left|\Theta_N^P\right\rangle=&\frac{1}{\sqrt{2^N}}\Upsilon^{-1}(3,N)\sum_{k_1,\cdots,k_N=0}^{1}y_{k_1\cdots k_N}\otimes_{m=1}^{N}(\sigma_{b_m}\sigma_0\otimes\sigma_0)\left|k_mb_mk_m\right\rangle\\
=&\frac{1}{\sqrt{2^N}}\left[\otimes_{m=1}^{N}(\sigma_{b_m}\otimes\sigma_0)\otimes I^{2^N}\right]\sum_{k_1,\cdots,k_N=0}^{1}y_{k_1\cdots k_N}(\otimes_{m=1}^{N}\left|k_mb_mk_m\right\rangle)\otimes(\otimes_{m=1}^{N}\left|k_m\right\rangle)\\
=&\frac{1}{\sqrt{2^N}}\left[\otimes_{m=1}^{N}(\sigma_{b_m}\otimes\sigma_0)\otimes I^{2^N}\right]\Gamma_N^{-1}\sum_{k_1,\cdots,k_N=0}^{1}y_{k_1\cdots k_N}(\otimes_{m=1}^{N}\left|k_m\right\rangle)\\
&\otimes(\otimes_{m=1}^{N}\left|k_m\right\rangle)\otimes(\otimes_{m=1}^{N}\left|b_m\right\rangle)
\end{aligned}\tag{79}$$

在 Alice 发送经典信息和 Bob 完成恢复操作之后，系统最终的状态为

$$\begin{aligned}
\left|\Theta_N^{\text{fin}}\right\rangle=&\frac{1}{\sqrt{2^N}}\Gamma_N^{-1}\sum_{k_1,\ldots,k_N=0}^{1}y_{k_1\cdots k_N}\left(\otimes_{m=1}^{N}\left|a_m\right\rangle_{A_m}\right)\left[\left(\otimes_{m=1}^{N}\left\langle a_m\right|\right)\left(\otimes_{m=1}^{N}H^{A_m}\right)T_N^r(x,t)\right.\\
&\left.\left(\otimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\otimes\left[\left(\otimes_{m=1}^{N}r(a_m)\right)R_N(x)\left(\otimes_{m=1}^{N}\left|k_m\right\rangle_{Y_m}\right)\right]\otimes\left(\otimes_{m=1}^{N}\left|b_m\right\rangle_{B_m}\right)\\
=&\frac{1}{\sqrt{2^N}}\Gamma_N^{-1}\otimes_{m=1}^{N}\left|a_m\right\rangle_{A_m}\otimes\left\{\sum_{k_1,\ldots,k_N=0}^{1}y_{k_1\cdots k_N}\left[\left(\otimes_{m=1}^{N}\left\langle a_m\right|\right)\left(\otimes_{m=1}^{N}H^{A_m}\right)T_N^r(x,t)\right.\right.\\
&\left.\left.\left(\otimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\otimes\left[\left(\otimes_{m=1}^{N}r(a_m)\right)R_N(x)\left(\otimes_{m=1}^{N}\left|k_m\right\rangle_{Y_m}\right)\right]\right\}\otimes\left(\otimes_{m=1}^{N}\left|b_m\right\rangle_{B_m}\right)
\end{aligned}\tag{80}$$

由定义(21)和(27)，容易得到以下关系式

$$\begin{aligned}
T_N^r(x,t)=&\sum_{m=1}^{2^N}t_m\left|m,D\right\rangle\left\langle p_m(x),D\right|=\sum_{m=1}^{2^N}t_m\left|m,D\right\rangle\left\langle m,D\right|\sum_{n=1}^{2^N}\left|n,D\right\rangle\left\langle p_n(x),D\right|\\
=&\left(\sum_{j_1,j_2,\ldots,j_N=0}^{1}t_{j_1j_2\cdots j_N}\left|j_1j_2\cdots j_N\right\rangle\left\langle j_1j_2\cdots j_N\right|\right)R_N(x)
\end{aligned}\tag{81}$$

其中十进制系统下的 t_m 被改写成二进制下的 $t_{j_1 j_2 \cdots j_N}$。将(81) 和(74)代入(80)，即得

$$\begin{aligned}\left|\Theta_N^{\text{fin}}\right\rangle = \frac{1}{\sqrt{2^N}}\Gamma_N^{-1} \otimes_{m=1}^N |a_m\rangle_{A_m} \otimes \Bigg\{ \sum_{j_1,\cdots,j_N=0}^{1} \sum_{k_1,\ldots k_N=0}^{1} \sum_{l_1,\ldots,l_N} t_{j_1\cdots j_N} y_{k_1\cdots k_N} \\ \Big(\prod_{m=1}^N \langle a_m| H |j_m\rangle\Big)\big[\big(\otimes_{m=1}^N \langle j_m|\big) R_N(x) \big(\otimes_{n=1}^N |k_n\rangle\big)\big]\big[\big(\otimes_{m=1}^N \langle l_m|\big) R_N(x) \\ \big(\otimes_{n=1}^N |k_n\rangle\big)\big]\Big(\prod_{m=1}^N (-1)^{a_m l_m}\Big)\big(\otimes_{m=1}^N |l_m\rangle_{Y_m}\big)\Bigg\} \otimes \big(\otimes_{m=1}^N |b_m\rangle_{B_m}\big)\end{aligned} \tag{82}$$

由于 $R_N(x)$ 的每行每列都仅有一个非零元素，于是，我们有

$$\begin{aligned}&\big[\big(\otimes_{m=1}^N \langle j_m|\big) R_N(x) \big(\otimes_{m=1}^N |k_m\rangle\big)\big]\big[\big(\otimes_{m=1}^N \langle l_m|\big) R_N(x) \big(\otimes_{m=1}^N |k_m\rangle\big)\big] \\ =&\Big(\prod_{m=1}^N \delta_{j_m l_m}\Big)\big[\big(\otimes_{m=1}^N \langle j_m|\big) R_N(x) \big(\otimes_{m=1}^N |k_m\rangle\big)\big]\end{aligned} \tag{83}$$

将 $T_N^r(x,t)$ 作用于未知态上，我们会得到

$$T_N^r(x,t)\,|\xi\rangle = \sum_{j_1,\ldots,j_N=0}^{1} \sum_{k_1,\ldots,k_N=0}^{1} t_{j_1\cdots j_N} y_{k_1\cdots k_N} \langle j_1 j_2 \cdots j_N|\, R(x)\, |k_1 k_2 \cdots k_n\rangle\, |j_1 j_2 \cdots j_N\rangle \tag{84}$$

再由于

$$\langle a_m| H |j_m\rangle (-1)^{a_m j_m} = \frac{1}{\sqrt{2}} \tag{85}$$

最终，我们得到

$$\left|\Theta_N^{\text{fin}}\right\rangle = \frac{1}{\sqrt{2^N}} \otimes_{m=1}^N |a_m b_m\rangle_{A_m B_m} \otimes \big(T_N^r(x,t)\,|\xi\rangle_{Y_1\cdots Y_N}\big) \tag{86}$$

即完成了证明。

5 基于 GHZ 态的实现

5.1 联合 RIO 协议

设 N-qubit 的量子操作 $\mathcal{U} = \mathcal{U}_2\mathcal{U}_1$，其中 $\mathcal{U}_1$, $\mathcal{U}_2$ 都属于4.1小节所讨论的那些特定类型，分别用 $T_N^r(x_1,v_1)$ 和 $T_N^r(x_2,v_2)$ 来表示。如果按照以前的协议，通过远程传递 $\mathcal{U}_1$ 和 $\mathcal{U}_2$ 来实现，那么总共需要 $2N$ 个 Bell 对。我们将看到，若有两个发送者采用 GHZ 态来完成，将只需要 N 个 GHZ 态。这里，我们只研究 $N=1$ 的情形，此处的讨论参考[8]。

不失一般性，对于三粒子系统，我们假定初态为

$$\left|\Theta^{\text{ini}}\right\rangle = |\text{GHZ}\rangle_{ABC}\,|\chi\rangle_X\,|\xi\rangle_Y\,|\zeta\rangle_Z\,, \tag{87}$$

其中 GHZ 态的定义见(2)，由 Alice，Bob 和 Charlie 共享，$|\chi\rangle_X$，$|\xi\rangle_Y$ 和 $|\zeta\rangle_Z$ 都是未知的单比特量子态。在这六个比特中，A 和 X 属于 Alice，B 和 Y 属于 Bob，C 和 Z 属于 Charlie。据此，可以把全系统的 Hilbert 空间写成以下形式：

$$H = H_A \otimes H_B \otimes H_C \otimes H_X \otimes H_Y \otimes H_Z \tag{88}$$

很显然，三人在初态(87)中的角色是完全对称的，可以任意指定两个作发送方，而另一个为接受方。于是，可进一步将上式写成

$$H_{\text{Sender 1}} \otimes H_{\text{Sender 2}} \otimes H_{\text{Receiver}} \otimes H_{\text{Unknown State}} \tag{89}$$

我们不妨选 Alice 和 Bob 为发送方，Charlie 为接受方，$\mathcal{U}_1$ 和 $\mathcal{U}_2$ 属于(11)所定义的类型, 分别记为 $U(d_1, u)$ 和 $U(d_2, v)$。我们将初态(87)写为

$$\left|\Theta^{\text{ini}}\right\rangle = \left|\text{GHZ}\right\rangle_{ABC} \left|\zeta\right\rangle_Z , \tag{90}$$

其中，未知态为

$$\left|\zeta\right\rangle = z_0 \left|0\right\rangle_Z + z_1 \left|1\right\rangle_Z \tag{91}$$

联合 RIO 协议的量子线路见图3，全过程可分为七步：

一. Charlie 执行一个受控非门操作，他用自己拥有的那个未知态作为控制量子比特，而第一比特即联合 GHZ 态中的第三部分作为目标比特；然后以 $|c\rangle\langle c|$ $(c = 0, 1)$ 为基测量他的第一个比特，即

$$\mathcal{P}_C(c) = I_4 \otimes \left\{ \left[(|c\rangle_C\langle c|) \otimes \sigma_0^Z \right] \left[\sigma_0^C \otimes C^{\text{NOT}}(2,1) \right] \right\}, \tag{92}$$

其中 C^{NOT} 定义为

$$C^{\text{NOT}}(2,1) = \sigma_0 \otimes (|0\rangle\langle 0|) + \sigma_1 \otimes (|1\rangle\langle 1|) \tag{93}$$

二. Charlie 发送经典信息 c 给 Alice 和 Bob。

三. Alice 依次执行四个操作：σ_c，$U(d_1, u)$，Hadamard 变换和测量 $|a\rangle_A\langle a|$ $(a = 0, 1)$，即

$$\mathcal{S}_A(a, c; d_1, u) = \left[(|a\rangle_A\langle a|) H^A U(d_1, u) \sigma_c^A \right] \otimes I_8 \tag{94}$$

四. Alice 发送 d_1 给 Bob，发送 a, d_1 给 Charlie。

五. Bob 依次执行四个操作：$\sigma_{d_1}\sigma_c$，$U(d_2, v)$，Hadamard 变换和测量 $|b\rangle_B\langle b|$ $(b = 0, 1)$，即

$$\mathcal{S}_B(b, c; d_1, d_2, v) = \sigma_0 \otimes \left[(|b\rangle_B\langle b|) H^B U(d_2, v) (\sigma_{d_1}^B \sigma_c^B) \right] \otimes I_4 \tag{95}$$

六. Bob 发送经典信息 b, d_2 给 Charlie。

七. Charlie 通过以下操作来得到状态 $U_2(d_2, v)U_1(d_1, u)\left|\zeta\right\rangle_Z$：

$$\mathcal{R}_C(a, b; d_1, d_2) = I_4 \otimes \sigma_0^C \otimes [r(b)\sigma_{d_2} r(a)\sigma_{d_1}], \tag{96}$$

其中 $r(z)$ 定义为

$$r(z) = (1 - z)\sigma_0 + z\sigma_3 \tag{97}$$

在该协议中，Alice，Bob 和 Charlie 所执行的全部量子操作可以写为

$$\begin{aligned} \mathcal{I}_R(a, b, c; d_1, d_2, u, v) = & \left[\left|a\right\rangle_A\!\left\langle a\right| H^A U(d_1, u) \sigma_c^A \right] \otimes \left[\left|b\right\rangle_B\!\left\langle b\right| H^B U(d_2, v) \sigma_{d_1} \sigma_c^A \right] \\ & \otimes \left\{ \left[\left|c\right\rangle\!\left\langle c\right| \otimes r(b)\sigma_{d_2} r(a)\sigma_{d_1} \right] C^{\text{NOT}}(2,1) \right\} \end{aligned} \tag{98}$$

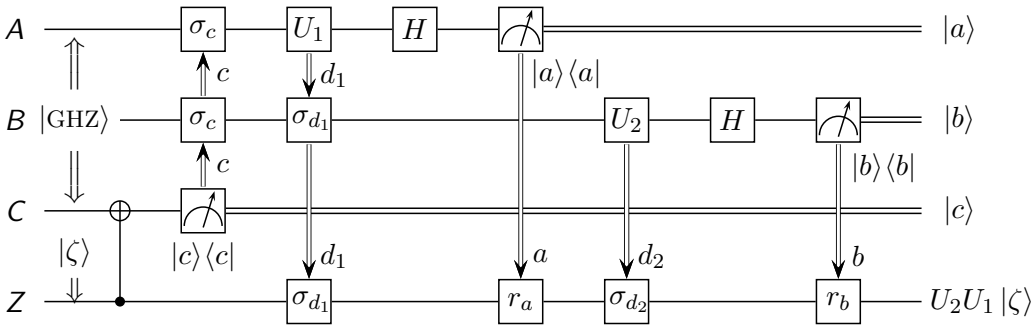


图 3. 联合 RIO 协议的量子线路，Alice 和 Bob 为发送方，Charlie 为接收方，要远程实现的操作为 $U(d_1,d_2)=U_2(d_2)U_1(d_1)$。

系统最终的量子态为

$$\left|\Theta^{\text{fin}}\right\rangle=\mathcal{I}_R(a,b,c;d_1,d_2,u,v)\left|\Theta^{\text{ini}}\right\rangle=\frac{1}{2\sqrt{2}}\left|abc\right\rangle_{ABC}\otimes U(d_2,v)U(d_1,u)\left|\zeta\right\rangle_Z \tag{99}$$

下面我们要给简要证明，具体参见文献[8]。

■ 由(91)和(78)易知，在第一步操作完成后，给出

$$\begin{aligned}\left|\Theta^P\right\rangle&=\mathcal{P}_C(c)\left|\Theta^{\text{ini}}\right\rangle\\&=I_4\otimes\left\{\left[(\left|c\right\rangle_C\!\left\langle c\right|)\otimes\sigma_0^Z\right]\left[\sigma_0^C\otimes C^{\text{NOT}}(2,1)\right]\right\}\left|\text{GHZ}\right\rangle_{ABC}\left|\zeta\right\rangle_Z\\&=\frac{1}{\sqrt{2}}(\sigma_c\otimes\sigma_c\otimes I_4)\sum_{k=0}^{1}z_k\left|kkck\right\rangle_{ABCZ}\end{aligned} \tag{100}$$

下面一步是 Alice 完成的：

$$\begin{aligned}\left|\Theta_1^S\right\rangle&=\mathcal{S}_A(a,c,d_1,u)\left|\Theta^P\right\rangle\\&=\left\{\left[(\left|a\right\rangle_A\!\left\langle a\right|)H^AU(d_1,u)\sigma_c^A\right]\otimes I_8\right\}\left\{\frac{1}{\sqrt{2}}(\sigma_c\otimes\sigma_c\otimes I_4)\sum_{k=0}^{1}z_k\left|kkck\right\rangle_{ABCZ}\right\}\\&=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}z_k\left[\left|a\right\rangle_A\!\left\langle a\right|HU(d_1,u)\left|k\right\rangle_A\right](\sigma_c\left|k\right\rangle_B)\left|ck\right\rangle_{CZ}\end{aligned} \tag{101}$$

下面一步是 Bob 完成的：

$$\begin{aligned}\left|\Theta_2^S\right\rangle&=\mathcal{S}_B(b,c,d_2,v)\left|\Theta_1^S\right\rangle=\left\{\sigma_0\otimes\left[(\left|b\right\rangle_B\!\left\langle b\right|)H^BU(d_2,v)(\sigma_{d_1}^B\sigma_c^B)\right]\otimes I_4\right\}\left|\Theta_1^S\right\rangle\\&=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}z_k\left[\left\langle a\right|HU(d_1,u)\left|k\right\rangle_A\left\langle b\right|HU(d_2,v)\sigma_{d_1}\left|k\right\rangle_B\right]\left|abck\right\rangle_{ABCZ}\end{aligned} \tag{102}$$

结合(11)和(97)，我们有

$$\begin{aligned}\left|\Theta^{\text{fin}}\right\rangle&=\mathcal{R}_C(a,b;d_1,d_2)\left|\Theta_2^S\right\rangle=\left\{I_4\otimes\sigma_0^C\otimes[r(b)\sigma_{d_2}r(a)\sigma_{d_1}]\right\}\left|\Theta_2^S\right\rangle\\&=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}z_k\left[\left\langle a\right|HU(d_1,u)\left|k\right\rangle\left\langle b\right|HU(d_2,v)\sigma_{d_1}\left|k\right\rangle\right]\left|abc\right\rangle_{ABC}\left[r(b)\sigma_{d_2}r(a)\sigma_{d_1}\left|k\right\rangle_Z\right]\\&=\frac{1}{\sqrt{2}}\sum_{j=0}^{1}\sum_{k=0}^{1}\sum_{l=0}^{1}u_jy_k\left[\left\langle a\right|H\left|j\right\rangle\!\left\langle j\right|\sigma_{d_1}\left|k\right\rangle\left\langle b\right|HU(d_2,v)\sigma_{d_1}\left|k\right\rangle\right]\\&\quad\left|abc\right\rangle_{ABC}\left[r(b)\sigma_{d_2}(-1)^{al}\left|l\right\rangle_Z\!\left\langle l\right|\sigma_{d_1}\left|k\right\rangle\right]\end{aligned} \tag{103}$$

再由于以下两个关系式

$$\langle j|\,\sigma_d\,|k\rangle\,\langle l|\,\sigma_d\,|k\rangle = \langle j|\,\sigma_d\,|k\rangle\,\delta_{jl},\quad \langle a|\,H\,|j\rangle\,(-1)^{aj} = \frac{1}{\sqrt{2}} \tag{104}$$

最终，我们可以得到

$$\begin{aligned}\left|\Theta^{\text{fin}}\right\rangle &= \frac{1}{2}\,|abc\rangle_{ABC}\left[\sum_{j=0}^{1}\sum_{k=0}^{1} u_j y_k\,\langle b|\,HU(d_2,v)\sigma_{d_1}\,|k\rangle\,\langle j|\,\sigma_{d_1}\,|k\rangle\right] r(b)\sigma_{d_2}\,|j\rangle_Y \\ &= \frac{1}{\sqrt{2}}\,|abc\rangle_{ABC}\left[\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1} v_i u_j y_k\,\langle i|\,\sigma_{d_2}\,|j\rangle\langle j|\,\sigma_{d_1}\,|k\rangle\right]|i\rangle_Y \\ &= \frac{1}{\sqrt{2}}\,|abc\rangle_{ABC}\left[U(d_2,v)U(d_1,u)\,|\xi\rangle_Y\right]\end{aligned} \tag{105}$$

5.2 控制 RIO 协议

由于 GHZ 态比 Bell 态的纠缠度更高，那么使用 GHZ 态来实现远程操作应该能够体现出更多的优越性。事实上正是如此，在控制 RIO 协议中，控制者可以同时扮演启动和认证两种角色。这对于量子信息的处理和通信具有十分重要的意义，具体的讨论仍参见[8]。我们仍只限于研究 $N=1$ 的情形。

当选定控制者之后，系统的状态空间可以改写为

$$H_{\text{Controller}}\otimes H_{\text{Sender}}\otimes H_{\text{Receiver}}\otimes H_{\text{Unknown State}} \tag{106}$$

我们不妨设 Alice 为发送方，Bob 为接收方，Charlie 为控制方，初态简化为

$$\left|\Theta^{\text{ini}}\right\rangle = F_4^{-1}(1,3)\,|\text{GHZ}\rangle_{CAB}\,|\xi\rangle_Y \tag{107}$$

对应的控制 RIO 协议的量子线路见图4，全过程可分为七步：

一. 控制者 Charlie 实施以下操作

$$\mathcal{C}(\gamma) = (|\gamma\rangle\langle\gamma|\,H)\otimes I_8 \tag{108}$$

二. Charlie 传递一个经典比特 γ 给发送方 Alice 或接受方 Bob，分别用 $C_{\text{cs}}(\gamma)$ 和 $C_{\text{cr}}(\gamma)$ 来表示。

三. 这一步由 Bob 来完成，要分两种情况：

①如果 Bob 没有收到 Charlie 的经典比特，那么他将执行以下操作

$$\mathcal{P}(\beta) = I_4\otimes\left[(|\beta\rangle\langle\beta|)\otimes\sigma_0\right]C^{\text{NOT}}(2,1) \tag{109}$$

②如果 Bob 收到了经典比特 γ，根据收到的时间又要分三种不同情况来处理：

(a)当 Bob 在完成该步操作前得到 γ 时，需要在(109)之前追加下面的操作

$$\mathcal{P}^{\text{pre}}(\gamma) = I_4\otimes r(\gamma)\otimes\sigma_0 \tag{110}$$

(b)当 γ 发送给 Bob 是在(109)之后而在第七步的恢复操作(115)之前，Bob 要改做下面的这个操作

$$\mathcal{P}^{\text{aft}}(\gamma) = I_4\otimes r(\gamma)\otimes r(\gamma) \tag{111}$$

(c)当 γ 是在(115)完成之后才发给 Bob 的，那么他需要做以下操作

$$\mathcal{R}^{\text{aft}}(\gamma) = (-1)^{\gamma d} I_4\otimes r(\gamma)\otimes r(\gamma) \tag{112}$$

四. Bob 发送经典信息 β 给 Alice，记为 $C_{\mathrm{rs}}(\beta)$。

五. 这一步由 Alice 来完成，要分两种情况：
①如果 Alice 没有收到 Charlie 的经典比特，那么他将执行以下操作

$$\mathcal{S}(\alpha,\beta;d,u)=\left[\sigma_0\otimes(|\alpha\rangle\langle\alpha|)HU(d,u)\sigma_\beta\otimes I_4\right. \tag{113}$$

②如果 Bob 收到了 γ，需要在(113)之前追加下面的操作

$$\mathcal{S}^{\mathrm{add}}(\gamma)=\sigma_0\otimes r(\gamma)\otimes I_4 \tag{114}$$

六. Alice 发送两个经典比特 α 和 d 给 Bob，记为 $C_{\mathrm{sr}}(\alpha;d)$。

七. Bob 通过以下操作来完成最后一步

$$\mathcal{R}(\alpha;d)=I_8\otimes[r(\alpha)\sigma_d] \tag{115}$$

在该协议中，Alice，Bob 和 Charlie 所执行的全部量子操作可以写为

$$\mathcal{I}_R(a,b,c;d)=F_4^{-1}(1,3)\left[(|c\rangle_C\langle c|)H^C\otimes|a\rangle_A\langle a|\,H^AU(d,u)\sigma_b^Ar(c)\otimes\sigma_0\otimes r(a)C^{\mathrm{NOT}}\right]F_4(1,3) \tag{116}$$

系统最终的量子态为

$$\left|\Theta^{\mathrm{fin}}\right\rangle=\mathcal{I}_R(a,b,c;d)\left|\Theta^{\mathrm{ini}}\right\rangle=\frac{1}{2\sqrt{2}}\left|abc\right\rangle_{ABC}\otimes U(d,u)\left|\xi\right\rangle_Y \tag{117}$$

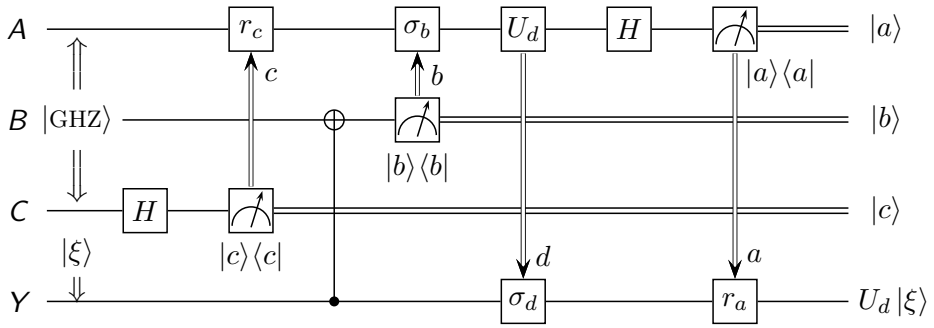


图 4. 控制 RIO 协议的量子线路，Alice 为发送方，Bob 为接收方，Charlie 为控制方，要远程实现的操作为 $U(d)$。

下面我们给出简要证明，具体参见文献[8]。

■ 当 Charlie 完成第一步操作后，给出

$$\begin{aligned}\left|\Theta^C\right\rangle&=F_4^{-1}(1,3)\mathcal{C}(c)F_4(1,3)\left|\Theta^{\mathrm{ini}}\right\rangle\\&=\frac{1}{2}F_4^{-1}(1,3)\left[\sigma_0\otimes r(c)\otimes I_4\right]\left[\,|c\rangle_C\otimes(|00\rangle+|11\rangle)_{AB}\otimes|\xi\rangle_Y\right.\\&=\frac{1}{2}F_4^{-1}(1,3)\left[I_4\otimes r(c)\otimes\sigma_0\right]\left[\,|c\rangle_C\otimes(|00\rangle+|11\rangle)_{AB}\otimes|\xi\rangle_Y\,\right]\end{aligned} \tag{118}$$

对第一种情况，Charlie 把她的经典比特 c 传给 Alice，则有

$$\begin{aligned}\left|\Theta^P\right\rangle&=F_4^{-1}(1,3)\mathcal{P}(b)F_4(1,3)\left|\Theta^C\right\rangle\\&=\frac{1}{2}\left\{F_4^{-1}(2,4)\left[r(c)\sigma_b\otimes I_8\right]\right\}\left[(y_0\,|00\rangle+y_1\,|11\rangle)_{AY}\otimes|bc\rangle_{BC}\,\right]\end{aligned} \tag{119}$$

$$
\begin{aligned}
\left|\Theta^{S}\right\rangle &= F_4^{-1}(1,3)\mathcal{S}^{\mathrm{all}}(a,b,c,d)\mathcal{S}^{\mathrm{add}}(c)F_4(1,3)\left|\Theta^{P}\right\rangle \\
&= \frac{1}{2}F_4^{-1}(2,4)\Big[\Big(\sum_{k}^{1} y_k \left\langle a\right| HU(d,u)\left|k\right\rangle \left|a\right\rangle_A \left|k\right\rangle_Y\Big)\otimes \left|bc\right\rangle_{BC}\Big]
\end{aligned}
\tag{120}
$$

对第二种情况，Charlie 把 c 传给 Bob，仍给出与(120)相同的结果。在 Bob 的恢复操作(115)完成后，我们有

$$
\begin{aligned}
\left|\Theta^{\mathrm{fin}}\right\rangle &= F_4^{-1}(1,3)\mathcal{R}(a,d)F_4(1,3)\left|\Theta^{S}\right\rangle \\
&= \frac{1}{2\sqrt{2}}\left|a\right\rangle_A \otimes F_3^{-1}(1,3)\Big[\Big(\sum_{j=0}^{1}\sum_{k=0}^{1} u_j y_k \left\langle j\right|\sigma_d\left|k\right\rangle \left|j\right\rangle_Y\Big)\otimes \left|bc\right\rangle_{BC}\Big] \\
&= \frac{1}{2\sqrt{2}}\left|abc\right\rangle_{ABC}\otimes U(d,u)\left|\xi\right\rangle_Y
\end{aligned}
\tag{121}
$$

6 梳理纠缠

下面，我们介绍有关多向纠缠操作的内容，主要讨论梳理纠缠。这是关于纠缠变换的新思路，相关评论可以参考[2]。可以预见，这项技术对于量子态的远程控制乃至量子网络的建立也有着重要意义。

所谓“梳理”，就是将多粒子之间存在的混乱纠缠转变成 ebits。在 Yang 和 Eisert 的论文[9] 中，协议是在特殊的一方 Alice 和多个 Bob 之间进行的。初态设为 $\left|\phi\right\rangle_{A,B_1,\ldots,B_m}$，这可以是一个具有很复杂纠缠结构的纯态。通过梳理(即局域操作和经典通信)，末态最终变为 $\left|\phi_1\right\rangle_{A_1,B_1}\otimes\cdots\otimes\left|\phi_m\right\rangle_{A_m,B_m}$，见图5所示。纠缠梳理的基础，是两个关于纠缠变换的最新进展：量子态合并[4] 和辅助纠缠[6]。

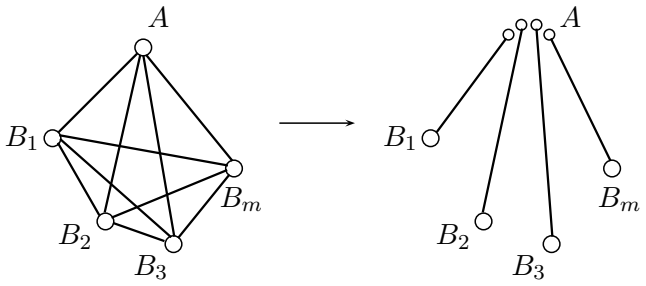


图 5. 在 LOCC 操作下，很混乱的多粒子纠缠被梳理成 ebits。

需要着重指出，这种梳理是在渐近意义下实现的。首先，我们引入记号: 如果存在一个序列 $\{i_n\}$, 使得我们在 LOCC 下能得到 $\lim_{n\to\infty}\|\left|\phi\right\rangle^{\otimes i_n}-\left|\phi_n\right\rangle\|=0$，并且 $\limsup_{n\to\infty} i_n/n = r/s$，那么我们就记为 $\left|\phi\right\rangle^{\otimes s}\to\left|\phi\right\rangle^{\otimes r}$。于是，纠缠梳理的过程应该严格表叙为：存在一种协议，使得 $\left|\phi\right\rangle_{A,B_1,\ldots,B_m}\to\left|\phi_1\right\rangle_{A_1,B_1}\otimes\cdots\otimes\left|\phi_m\right\rangle_{A_m,B_m}$，并且保持 A 和 $B_1,\ldots,B_m$ 之间的纠缠度不变，即 $\sum_k E_k=\sum_k S(\rho_{A_k})=S(A)$。具体的论证参见[9]，由于作者尚未完全理解，在此略去。

参考文献

[1] A. Chefles et. al., *Quantum remote control: teleportation of unitary operations*, Phys. Rev. A **63** (2001), 042303. arXiv: quant–ph/0005061v3.

[2] M. Christandl, *Straightening messy correlations with a quantum comb*, Physics **2** (2009), 99.

[3] I. L. Chuang and M. A. Nielsen, *Quantum computation and quantum information*, Cambridge University Press, 2000.

[4] M. Horodecki, J. Oppenheim, and A. Winter, *Quantum information can be negative*, Nature **436** (2005), 673.

[5] S. F. Huelga, M. B. Plenio, and J. A. Vaccaro, *Remote control of restricted sets of operations: teleportation of angles*, Phys. Rev. A **65** (2002), 042316. arXiv: quant–ph/0107110v1.

[6] J. A. Smolin, F. Verstraete, and A. Winter, *Entanglement of assistance and multipartite state distillation*, Phys. Rev. A **72** (2005), 052317.

[7] A. M. Wang, *Remote implementations of partially unknown quantum operations of multiqubits*, Phys. Rev. A **74** (2006), 0323171.

[8] A. M. Wang, *Combined and controlled remote implementations of partially unknown quantum operations of multiqubits using Greenberger-Horne-Zeilinger states*, Phys. Rev. A **75** (2007), 062323.

[9] D. Yang and J. Eisert, *Entanglement combing*, Phys. Rev. Lett. **103** (2009), 220501.

索引