量子通信协议设计

Design of Quantum Communication Protocols

彭家寅 / 著

科学出版社

量子通信协议设计

彭家寅 著

科学出版社
北京

内 容 简 介

量子信息学是物理、信息科学、数学和计算机科学等多学科交叉的新兴科学。本书主要介绍量子通信中量子态的多方间接传输协议的一些最新成果，涉及量子通信的基本原理、思想方法及相关技术。全书共分4章。第1章介绍预备知识；第2章讨论以多粒子最大纠缠态或非最大纠缠态为量子信息，多方参与的量子态分享方案；第3章介绍几类粒子量子态的多方远程联合制备协议；第4章研究几种量子信息集中方案，它们分别是通用量子克隆、辅助自由相位协变克隆和优化非对称量子克隆的逆过程。

本书可作为物理学、数学、计算机科学等学科的本科生和研究生的教材，也可供相关专业教师及科研人员参考。

图书在版编目(CIP)数据

量子通信协议设计 / 彭家寅著. — 北京：科学出版社, 2018.9

ISBN 978-7-03-058242-3

Ⅰ. ①量… Ⅱ. ①彭… Ⅲ. ①量子-通信协议 Ⅳ. ①TN915.04

中国版本图书馆 CIP 数据核字 (2018) 第 154265 号

责任编辑：冯 铂 / 责任校对：韩雨舟

封面设计：墨创文化 / 责任印制：罗 科

科学出版社出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

成都锦瑞印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2018年9月第 一 版 开本：787×1092 1/16

2018年9月第一次印刷 印张：11.75

字数：280千字

定价：89.00元

（如有印装质量问题，我社负责调换）

资助项目(基金):

四川省教育厅“量子态传输协议设计与量子程序验证”创新团队

教育部“本科教学工程”四川省地方属高校本科专业综合改革试点项目——内江师范学院数学与应用数学“专业综合改革试点”项目(ZG0464)

四川省高等教育“质量工程”(数学与应用数学专业综合改革)(01249)

四川省“西部卓越中学数学教师协同培养计划”项目

内江师范学院教材出版基金

前　言

在当今信息时代，信息科学对人们的生产、生活和社会文明产生着深刻而巨大的影响. 20 世纪微电子技术的高速发展，极大地提高了集成电路的集成度，为现代信息化社会奠定了物质基础. 依据“摩尔定律”，随着人类社会对信息需求日益增加，芯片上集成的晶体管越来越密，必然会使电路线宽不断变得狭窄，直到极限出现. 这时，电子的波动性将在电路中产生新的物理现象，即量子效应. 因此，信息科学的进一步发展势必把量子力学的原理和方法用于信息技术，一门新兴学科——量子信息学便应运而生，它是量子物理与信息科学相融合的新兴交叉学科，它以量子态载荷信息，按量子力学规则进行信息的传输和处理，以量子力学基本原理来保障通信安全和提供计算能力. 由于量子规律有别于经典规律，特别在量子多子系统中，量子态具有最奇妙、最不可思议的量子纠缠现象，使得量子信息具有能实现经典信息技术不可能实现的新功能.

量子通信作为量子信息学的重要分支，利用量子纠缠效应进行信息传输. 近年来，量子通信理论与实验研究不仅由于它重大的学术价值与科学意义引起了信息科学家和物理学家的兴趣，而且因它可预见的潜在应用价值引起了各国政府、科技领域、军工部门与信息产业界的密切关注，研究工作取得了巨大突破，不断爆出惊人的成果，发展出诸如量子隐形传态、量子密钥分配、量子远程态制备、远程量子信息集中，以及量子通信的复杂性等许多不同研究方向. 量子隐形传态、量子远程态制备和量子克隆是与量子信息分布密切相关的三个不同方面. 结合本书研究内容，我们就这三个方面及量子克隆的逆过程——远程信息集中进行简单的介绍.

1993 年，IBM 公司的 Bennett 等[1]提出了隐形传态(QT)模型，其大意是发送者将未知任意单量子态的信息分为经典信息和量子信息(发送者对原物进行某种测量来获得经典信息，量子信息便是测量中未提取的剩余信息)，分别通过经典信道和量子信道(EPR 对)传送给接收者. 此后，研究者们拓展了 Bennett 等[1]的 QT 思想，提出了如量子秘密分享[2]、受控隐形传态[3-4]、量子信息分裂[5-6]、经济(k，m)-门限受控隐形传态[7]等协议，引起人们高度的关注. 近十年来，基于许多不同量子资源的各种隐形传态方案被提出，如三能级未知两粒子态的概率隐形传态[8]、三粒子 W 态隐形传态[9]、任意四量子 GHZ 态分享[10]、离子肼系统中任意未知二离子态多方受控隐形传态[11]、基于腔 QED 中任意二原子态中任意二原子态分享[12]、连续变量隐形传态[13]等方案. 目前，有多个研究小组在实验上实现了隐形传态. Zeilinger 小组利用参量下换过程产生的纠缠光子实现了光子偏振态隐形传态[14]，并在多瑙河底光纤中实现了 600m 的量子隐形传态[15]；Rome 小组用了一个简单办法，把量子态从纠缠光子对中的一个传送到另一个光子上[16]；CIT 小组利用连续氩离子激光器实现了连续变量隐形传态[17]；Barrett 等用离子纠缠资源，以 0.78 的保真度实现了 30μm 原

子态隐形传态[18]；Marcikic 等实现了空间间隔为 55m 且光纤连接为 2km 的隐形传态[19]；中国合肥微尺度物资科学国家实验室与清华大学合作实现了保真度达到 0.89，传送距离为 16km 的单光子态隐形传态[20]；2012 年中国科学院与中国科技大学合作在青海湖以平均 0.8 的保真度，完成了近百公里量级的自由空间隐形传态[21].

一个信息处理过程类似于量子隐形传态的方案最初由 Lo[22]于 2000 年提出，称之为量子态远程制备(RSP)，它利用量子纠缠等牵连效应，制备者对自己粒子进行局域操作与测量，并通过经典通信将测量结果告知接收者，接收者施行适当的酉变换，将其粒子制备到某期望的量子态上. 由此可见，RSP 和 QT 都借助于量子纠缠资源和经典通信，把某个量子态从一处传送到遥远的另一处，因此它们都是量子态传输的物理实现方式，反映了量子力学中不同资源的相互交换. 但它们也有不同之处，具体来说，首先，在 RSP 中，发送者对要传送的态完全了解，而在 QT 中，发送者对要传送的态是未知的. 其次，在 QT 中，要传送态需荷载于具体粒子上，而 RSP 中要传送的态最初不荷载于任何粒子上. 最后，它们所需的经典资源耗费和量子操作复杂性不一样. Bennett 等[23]证明了隐形传态中经典信息耗费是远程态制备中所需经典信息的两倍，标准的隐形传态是决定的，而远程态制备为概率小于 1 的. Pati[24]指出关于 Block 球面的大极化圈上的态和赤道态的制备能是决定性的，所耗经典信息为 1 比特，而在 QT 中却需 2 比特. 这三位开拓者的工作引起了许多学者的研究兴趣，迄今为止，诸多优化的远程态制备[25]、高维的远程态制备[26]、忠信的远程态制备[27]、低纠缠度的远程态制备[28]、有(无)健忘的远程态制备[29-30]、推广的远程态制备[31]、连续变量的远程态制备[32]等大量协议被提出，同时，许多远程态制备方案被实验实现[33-37]. 2007 年，Xia 等[38]提出了联合远程态制备(JRSP)思想，它与量子远程态制备不同，在 JRSP 中，有多个发送者共同分享要制备态的信息，但任何单个或部分发送者都不能推断出制备态，接收者只能与全体发送者协作才能实现量子态的制备. 因 JRSP 中所有发送者都仅仅知道要制备态的独自部分信息，所以信息泄露的可能性很小，进而信息安全性在原理上较 RSP 更高. 不久，许多 JRSP 方案[39-44]被提出.

与 QT 和 RSP 一起被视为量子信息分布的另一信息处理技术是量子克隆. 1982 年，Wootters 和 Zurek[45]证明了对于一个未知的量子态不可能进行精确的克隆，并称之为量子不可克隆定理. 该定理刻画了量子力学的一个固有特征，并设置了一个不可逾越的界限，奠定了量子安全密钥分配的理论基础，使得窃听者不能利用克隆技术来获取用户的信息，确保了量子密码的安全性. 我们虽然不能精确克隆未知量子态，但是否可以近似地克隆未知量子态呢？1996 年，Bužek 和 Hillery[46]提出了近似克隆机的概念，引起了学者们研究量子克隆的兴趣. 目前主要有两大类量子克隆：普适量子克隆机[47-48]和概率量子克隆机[49-50]. 普适量子克隆机是以 1 的概率获得量子态的近似拷贝，适用于任何量子态，被克隆的量子态会遭到破坏；而概率量子克隆机是以小于 1 的概率得到量子态的精确拷贝，适用于线性无光的量子态集，被克隆的量子态不受影响. 量子克隆按输入态的不同可分为如下类型：若输入态的振幅和相位都是未知的，则称之为普适量子克隆[51-54]；若输入态的振幅已知而相位未知，则称之为相位协变克隆[55-58]；若输入态的振幅未知而相位已知，则称之为实数态克隆[59-61]. 最近，在实

验上实现了一些量子克隆，如 Cummins 等[62]通过核磁共振实验完成了 1→2 近似量子态克隆；Zou 等[63]用线性光学完成了 1→3 最优相位协变量子态克隆；Milman 等[64]用腔 QED 实验实现了普适量子克隆等. 随着量子克隆的深入研究，研究者发现概率量子克隆与量子态的确认和量子计算中编程具有内在的联系[65]，人们也在探究量子克隆机在量子密码窃听及量子态测量、估计和重构中可能的应用[66]. 作为远程量子克隆的逆过程——远程信息集中 RIC 的概念于 2001 年被 Murao 等[67]首次提出，其目的是借助事先分享的量子纠缠资源，将空间分离的粒子中的信息集中到一个量子态中. 继 Murao 之后，Augusiak 等[68]利用推广的 Smolin 态作为共享纠缠信道，提出量子比特系统中的 2→1 的信息集中方案，值得注意的是，Smolin 态不是最大纠缠态，且利用 Smolin 态的方案比 GHZ 态的方案通信安全性更高[69]. Hsu[70]给出利用 Bell 关联混合态的 M→1 的信息集中方案. 此外，一些采用最大纠缠态作为量子信道的 RIC 方案也被提出来[71-73]. 远程量子克隆和远程信息集中分别是一对多(或多对多)和多对一的信息传输过程，它们可分别看成远程信息的储存与提取，或者视为远程信息的编码与解码，因而在量子网络的信息处理及分布量子计算中都有潜在的应用.

由于量子信息学是一门新兴的学科，我国在这个领域的学术著作还不够丰富，尤其是量子通信领域资料匮乏，无法满足高校师生、广大科研工作者和工程技术人员的需求. 本书力争将作者近期一些关于量子通信研究的成果编写成为一本既着眼共性原理，又反映量子通信的一些新的思想方法，并直接面向高校师生、工程技术人员和科研工作者的参考书籍，为改善国内量子通信领域参考资料不足、普及量子通信科学做出自己的贡献.

本书主要介绍量子通信中量子态的多方间接传输协议的基本原理、思想与方法及相关技术. 本书共由 4 章内容组成. 第 1 章简要介绍量子通信领域的基本概念；第 2 章介绍量子态分享协议，主要给出以多粒子的最大或非最大纠缠量子态为信道的任意多方参与的量子态分享方案，并适时讨论方案的安全性问题；第 3 章讨论量子态的远程联合制备问题，给出任意二粒子、任意三粒子、四粒子 χ 态和五粒子 Brown 态的三方及任意多方制备，并讨论四维粒子态的远程联合制备问题，以望读者了解多维粒子态的远程联合制备思想；第 4 章讨论量子信息集中协议，主要给出基于通用量子克隆、辅助自由相位协变克隆、优化非对称量子克隆的信息集中的方案.

本书的特色主要体现在以下几个方面：一是从内容上展现了近几年研究的一些新成果；二是体现了当前量子通信协议设计的一些思想、方法和手段；三是通过前言或每章的引言让读者了解概况、建立起讨论问题的“逻辑起点”；四是内容陈述中去掉抽象的符号，尽量简明直白，可读性强.

本书主要内容是我攻读博士期间的主要工作情况，笔者得到了四川师范大学莫智文教授的精心指导，得到了柏明强博士、王进伟博士和章志华博士的帮助，西南交通大学罗明星博士也给予了很多指导和帮助，在此一并表示衷心的感谢. 由于笔者水平有限，不当之处在所难免，敬请广大读者批评指正.

彭家寅

2018 年 5 月

目　录

第 1 章　预备知识 …… 1
1.1　量子比特 …… 1
1.2　量子纠缠 …… 2
1.3　量子操作 …… 3
1.4　量子测量 …… 3
1.5　量子不可克隆定理 …… 4
第 2 章　量子态分享协议设计 …… 5
2.1　引言 …… 5
2.2　以最大纠缠态为信道，任意未知 n-粒子态的隐形传态 …… 6
2.2.1　以三粒子态为信道，任意未知 n-粒子态之完美隐形传态的两个方案 …… 6
2.2.2　以四粒子团簇态为量子信道，任意未知 n-粒子态的完美隐形传态 …… 8
2.2.3　以五粒子团簇态为量子信道，任意未知 n-粒子态的完美隐形传态 …… 10
2.2.4　以 GHZ 态组为量子信道，任意未知 n-粒子态的完美隐形传态 …… 13
2.3　以非最大纠缠态为信道，未知 $(n+m)$-粒子态的分享 …… 15
2.3.1　以两个非最大纠缠 GHZ 态为量子信道，分享未知 $(n+m)$-粒子态 …… 15
2.3.2　以非最大纠缠六粒子团簇态为量子信道，分享未知 $(n+m)$-粒子态 …… 20
2.4　通过 POVM 测量，分享未知 n-粒子态 …… 25
2.4.1　以非最大四粒子团簇态为信道，分享未知 n-粒子 GHZ 形态 …… 25
2.4.2　以非最大五粒子团簇态为信道，隐形传输任意 n-粒子态 …… 29
2.5　以最大纠缠态为信道，分层分享量子信息 …… 34
2.5.1　以非最大纠缠四粒子团簇态为信道，分层分享量子信息 …… 35
2.5.2　以非最大纠缠 $|x\rangle$ 为信道，分层分享量子信息 …… 40
第 3 章　联合远程量子态的制备协议设计 …… 47
3.1　引言 …… 47
3.2　联合远程任意二粒子态的制备 …… 48
3.2.1　三方远程制备任意二粒子态 …… 48
3.2.2　多方远程制备任意二粒子态 …… 51
3.2.3　用 POVM 测量的多方远程任意二粒子态制备 …… 54
3.3　联合远程任意三粒子态的制备 …… 59
3.3.1　以 EPR 对为信道，三方远程制备任意三粒子态 …… 59

3.3.2 以 GHZ 态为信道，三方远程制备任意三粒子态 …… 62
3.3.3 以 GHZ 型态为信道，多方远程制备任意三粒子态 …… 67
3.4 四粒子态和五粒子 Brown 态的联合远程制备 …… 71
3.4.1 四粒子态的三方远程制备 …… 71
3.4.2 四粒子 χ 态的多方联合远程制备 …… 77
3.4.3 Brown 的联合远程制备 …… 81
3.5 四维粒子态的联合远程制备 …… 85
3.5.1 实系数四维粒子态的联合远程制备 …… 85
3.5.2 复系数四维单粒子态的联合远程制备 …… 91
3.5.3 实系数四维二粒子态的联合远程制备 …… 94
3.5.4 复系数四维二粒子态的联合远程制备 …… 97
第 4 章 量子信息集中协议设计 …… 101
4.1 引言 …… 101
4.2 基于通用量子克隆的远程信息集中 …… 102
4.2.1 以最大纠缠态为信道且基于 $1\rightarrow 2$ 克隆的信息集中 …… 102
4.2.2 以非最大纠缠态为信道且基于 $1\rightarrow 2$ 克隆的信息集中 …… 106
4.2.3 基于 $1\rightarrow 3$ 通用量子克隆的远程信息集中 …… 110
4.3 基于辅助自由相位协变克隆的远程信息集中 …… 120
4.3.2 以最大纠缠 W 态为信道的远程信息集中 …… 120
4.3.2 以非最大纠缠 W 态为信道的远程信息集中 …… 124
4.3.3 采用 POVM 测量的远程信息集中 …… 128
4.4 基于优化非对称经济 $1\rightarrow 3$ 相位协变量子克隆的远程信道集中 …… 130
4.4.1 以纠缠 GHZ 态为信道的远程信息集中 …… 131
4.4.2 通过纠缠 W 态信道的远程信息集中 …… 133
4.4.3 以四粒子团簇态为信道的远程信息集中 …… 137
4.5 基于二粒子态优化通用非对称 $1\rightarrow 2$ 克隆的信息集中 …… 139
4.5.1 以最大纠缠八粒子态为信道，基于 GHZ 型态 OUAT 的信息集中 …… 141
4.5.2 以非最大纠缠八粒子态为信道，基于 GHZ 型 OUAT 的信息集中 …… 157
4.5.3 基于任意二粒子态 OUAT 的远程信息集中 …… 164
参考文献 …… 171

第1章 预 备 知 识

为了后续章节需要，本章简要回顾量子通信过程中涉及量子力学的基本概念和基础知识，主要包括量子比特、量子纠缠、量子酉操作、量子测量以及量子不可克隆定理等. 在量子力学中，Dirac 符号“$\langle|$”和“$|\rangle$”表示量子态，它们都是复数域上向量空间中的向量. 向量$|V\rangle$与向量$|W\rangle$的内积$\langle V|W\rangle$是一个复数.

1.1 量 子 比 特

现代物理把微观世界中诸如电子、原子、光子等所有的微观粒子统称为量子. 量子信息就是利用微观粒子状态表示的信息，而以量子力学基本原理、利用量子系统的若干相干特性，研究量子信息储存、提取、编码、传输和计算等的理论体系就称为量子信息学. 它遵循量子力学的法则，将信息储存在量子态中，依幺正演化处理信息，按量子测量提取信息.

在经典信息论中，信息的二进制存储基本单元是比特(bit). 从物理学上看，比特是由两个线性独立的状态构成的双态系统，它可以制备两个可识别状态中的一个. 一般来说，这两个状态之间有巨大的能量壁垒，使得它们不能进行自发的相互转换，人们通常用二进制数 0 和 1 来表示这两个经典状态.

在量子信息中，量子信息的存储单元是量子比特(qubit)，通常量子比特是一个用二维复希尔伯特空间(complex Hilbert space)可以描述的二能级量子体系，它的两个极化态$|0\rangle$和$|1\rangle$对应于经典状态的 0 和 1. 不同于经典比特，因微观世界中凸显出鲜明的量子效应，一个量子比特能够处于既不是$|0\rangle$也不是$|1\rangle$的状态上，它可以连续而随机地存在于状态$|0\rangle$和$|1\rangle$的任意一个复线性组合的所谓中间状态上，即处在$|0\rangle$和$|1\rangle$的叠加传态$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$上，其中$\alpha,\beta$为任意复数，且满足归一化条件$|\alpha|^2+|\beta|^2=1$. 也就是说，量子比特的状态是二维复向量空间中的单位向量. 特殊的$|0\rangle$和$|1\rangle$状态称为本征态或计算基态，它们构成此复向量空间的一组正交基. 借助于 Bloch 球，量子态$|\varphi\rangle$可表示为

$$|\varphi\rangle=\cos\frac{\theta}{2}|0\rangle+\mathrm{e}^{i\delta}\sin^{-1}\frac{\theta}{2}|1\rangle(-\pi\leqslant\theta\leqslant\pi,0\leqslant\delta\leqslant2\pi).$$

处于状态$|0\rangle$和$|1\rangle$叠加态的量子比特作为量子信息的基本存储单位，其信息容量非常大. 通过检查，可以确定经典比特是处在 0 或 1 的状态上，但却不能确定量子比特处于哪个量子态上. 人们只能说$|\varphi\rangle$为$|0\rangle$和$|1\rangle$的概率分别为$|\alpha|^2$和$|\beta|^2$.

众所周知，微观粒子具有“波粒二象性”. 粒子的波动性具有一个以上的信息状态可

累加在同一微观粒子上的“相干叠加性”现象，因此量子态具有可叠加的物理特征. 它被数学地刻画为如下量子叠加原理[74]：

如果$|\psi_1\rangle,|\psi_2\rangle,\cdots,|\psi_n\rangle$是一个量子系统的可能量子态，则这 n 个量子态的任意线性叠加$|\psi\rangle=\sum_{j=1}^{n}c_j|\psi_j\rangle$也是该系统的一个可能量子态，其中 c_j 是满足归一化条件$\sum_{j=1}^{n}|c_j|^2=1$的任意复数.

值得注意的是，微观系统中的量子叠加不同于经典的概率叠加，它是对量子态的函数叠加，叠加振幅可以相互干涉，出现相长相消的现象. 这种量子相干性在量子信息科学的各领域中都起着决定性作用，也是诸多不可思议量子信息特征的物理基础. 当然，因环境的影响及子系统的纠缠作用，子系统之间的干涉会遭到破坏，即引起子系统的退相干.

1.2 量子纠缠

存在于具有多个子系统的量子系统中且不同于经典物理的一个最奇妙、最不可思议的现象就是量子纠缠，它是两个或多个量子系统之间的非定域、非经典、超空间的关联，是量子系统内各子系统或各自由度之间的关联的力学属性[75]. 它表现为对量子系统中的某一子系统的测量结果是必然相关于对其他子系统的测量参数，量子的这种非局域性质是一种纯粹的量子效应. 从数学角度讲，在由 n 个子量子系统 $H_j(j=1,2,\cdots,n)$ 构成的联合系统 $H=\otimes_{j=1}^{n}H_j$ 中，对于$|\psi\rangle\in H$，若存在$|\psi\rangle\in H_j(j=1,2,\cdots,n)$，使得$|\psi\rangle=\otimes_{j=1}^{n}|\psi_j\rangle$，则称$|\psi\rangle$为非纠缠态，否则称之为纠缠态. n 体量子系统的量子纠缠表现为任一子系统的态均处于依赖于其他子系统态而各自都处于一种不确定的状态，从而对一个子系统测量必然使得其他子系统构成的系统产生关联的塌缩.

设$|\psi\rangle_{AB}$是由量子系统 A 和 B 构成的联合系统中的一个态，如果$|\psi\rangle_{AB}$可以表示为$|\psi\rangle=\sum_{ij}c_{ij}|i\rangle_A|j\rangle_B$，其中$\{|i\rangle\otimes|j\rangle\}$为此联合系统的一组正交完备基，则称它为纯态[76]. 若此联合系统的量子纯态$|\psi\rangle_{AB}$可表示为两个子系统的量子态$|\alpha\rangle_A$和$|\beta\rangle_B$的张量级，即$|\psi\rangle_{AB}=|\alpha\rangle_A\otimes|\beta\rangle_B$，则称此量子纯态为可分离态，否则称为纠缠纯态[76].

由不同的量子态矢$|\psi_j\rangle(j=1,2,\cdots,M)$表示的子系统构成的量子联合系统，若每个子系统在该联合系统中都以确定的概率出现，那么把这个联合系统叫作混合系统，并称联合混合系统的状态为混合态[77].

设 ρ_j 为第 j 个子系统的密度矩阵，$j=1,2,\cdots,M$，对应的 M 体混合态的密度矩阵 ρ 为经典关联态，如果$\rho=\sum_j\rho_j\rho_1\otimes\rho_2\otimes\cdots\otimes\rho_M$，其中$\rho_j>0$且$\sum_j\rho_j=1$，则称混合态为可分离态，否则叫作混合纠缠态[77]. 显然，可分离态的密度矩阵也可以写为

$$\rho=\sum_j\rho_j|\psi_1\rangle\langle\psi_1|\otimes|\psi_2\rangle\langle\psi_2|\otimes\cdots\otimes|\psi_M\rangle\langle\psi_M|$$

虽然处于纠缠的两个或多个量子系统之间没有实际物质上的联系，但不同的量子位却

会因纠缠而相互影响，使得一个量子的状态将同与之纠缠的另一量子的状态相关. 量子纠缠扮演的这种独一无二的角色将导致在测量塌缩中，子系统表现出一种超空间的、非定域的、没有经典对应的关联. 量子系统与环境发生很难避免的量子退相干，导致量子信息丢失. 量子纠缠是量子信息学中特有的信息资源，在量子隐形传态、量子密钥分配、量子远程态制备、量子密集编码、量子信息集中、量子纠错及量子计算加速等许多方面起着重要作用.

1.3　量 子 操 作

封闭量子系统随时间演化遵循 Schrödinger 方程[74]，且量子态演化具有量子力学的线性性和幺正性. 量子力学的线性性保证了未知量子态不可被复制和不可被识别，而幺正性保证了概率守恒[78]. 量子信息处理类似于经典信息处理，是对编码的量子态实施一系列的控制、操作及测量等行为，但不同于经典信息处理，量子信息处理中的一切操作都是遵循幺正演化规律的可逆变换，而且对于处在 $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$ 的量子比特施行的酉 $\boldsymbol{U}$ 操作，因量子态的线性关系 $\boldsymbol{U}|\varphi\rangle=\alpha\boldsymbol{U}|0\rangle+\beta\boldsymbol{U}|1\rangle$，可以达到同时操作 $|0\rangle$ 和 $|1\rangle$ 态的结果，即取得了并行操作的效果. 对量子比特施行的最基本的操作，就是所谓的量子门. 如何构造一些能实现量子逻辑运算的量子逻辑门是完成量子信息任务的关键. 根据量子信息论，任一多量子比特门都能由多个受控非门(CNOT)和一些单量子比特门复合而成，并且只要实现单比特量子门与两比特量子受控非门运算，就能构造出任一幺正操作.

在量子信息中，最常见的量子逻辑门是一位或两位量子门. 一位量子门主要包括 Pauli 门和 Hadamard 门等[76]：恒等操作 $\boldsymbol{I}:\boldsymbol{I}=|0\rangle\langle 0|+|1\rangle\langle 1|$; Pauli_$\boldsymbol{X}$ 门 $\sigma_x:\sigma_x=|0\rangle\langle 1|+|1\rangle\langle 0|$; Pauli_$\boldsymbol{Y}$ 门 $\sigma_y:\sigma_y=i\left(|0\rangle\langle 1|+|1\rangle\langle 0|\right)$; Pauli_$\boldsymbol{Z}$ 门 $\sigma_z:\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$；相位门 $\sigma_s:\sigma_s=|0\rangle\langle 0|+\mathrm{e}^{\mathrm{i}\theta}|1\rangle\langle 1|$; Hadamard门 $\boldsymbol{H}:\boldsymbol{H}=\frac{1}{\sqrt{2}}(\sigma_x+\sigma_z)$. 对二体量子系统，受控非门是很重要的两位量子门，该门的作用可数学表示为 $|A,B\rangle\to|A,B\oplus A\rangle$，其中 $\oplus$ 是模 2 加法. 此式的具体含义是：若控制量子比特置为 0，则目标量子比特将保持不变；若控制量子比特置为 1，则目标量子比特将翻转[76].

当然，在量子系统演化中，幺正的动力学映射可以刻画系统密度矩阵的变化：

$$\rho\to\boldsymbol{U}\rho\boldsymbol{U}^{+}(\boldsymbol{U}^{+}\boldsymbol{U}=\boldsymbol{I})$$

1.4　量 子 测 量

量子力学是一个数学框架或者构造物理学理论的规则，量子力学本身不能告诉我们物理系统服从什么定律，但它却通过基本假设把物理世界和量子力学的数学描述联系起来，提供了研究这些定律的数学和概念的框架[74]. 描述量子系统一般测量是通过如下假设给出的.

假设[74]量子测量由一组作用在被测系统状态空间上的测量算子 M_m 描述，其中测量算

子满足完备性方程 $\sum_m M_m^+ M_m = \boldsymbol{I}$，指标 m 表示实验中可能出现的测量结果. 若在测量前量子系统的最新状态是 $|\psi\rangle$，则结果 m 发生的概率为 $p(m)=\langle\psi|M_m^+ M_m|\psi\rangle$，且测量后系统的状态为 $M_m|\psi\rangle/\sqrt{\langle\psi|M_m^+ M_m|\psi\rangle}$.

众所周知，投影测量加上酉操作就完全等价于一般测量，而半正定算子值测量(POVM)可看成为研究一般测量的统计特性提供最简单的方法，而不需了解测量后状态的特殊测量[74]. 它们都是量子信息中两个重要的测量，也是本书主要用到的测量.

投影测量[74]由被观测状态空间上的一个可观测量 Hermite 算子 M 描述. 该可观测量具有谱分解 $M=\sum_m mP_m$，其中 P_m 是到特征值 m 的本征空间上 M 的投影. 测量的可能结果对应于测量算子的特征值 m. 测量状态 $|\psi\rangle$ 时，得到结果 m 的概率为 $p(m)=\langle\psi|p_m|\psi\rangle$. 给定的测量结果 m，测量后量子系统的状态即为 $P_m|\psi\rangle/\sqrt{p(m)}$.

例如，考虑一个单量子系统上的投影测量：可观测量 Pauli_$\boldsymbol{Z}$ 算子，它的特征值为 1 和 -1，对应的特征矢为 $|0\rangle$ 与 $|1\rangle$，即有谱分解 $\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$. 当测量状态 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle(|\alpha|^2+|\beta|^2=1)$ 时，得到结果 1 的概率为 $\langle\psi|0\rangle\langle 0|\psi\rangle=|\alpha|^2$，同样，得到-1 的概率为 $|\beta|^2$.

投影测量可看成一般测量的特例. 事实上，当一般测量中的测量算子 M_m 是 Hermite 的，且 $M_m M_n=\delta_{mn}M_m$，那么一般测量就退化为投影测量.

POVM 测量[74]设测量算子 M_m 在状态为 $|\psi\rangle$ 的量子系统上进行测量，得到结果 m 的概率为 $p(m)=\langle\psi|M_m^+ M_m|\psi\rangle$. 若令 $E_m=M_m^+ M_m$，则 E_m 为满足 E_m=$\boldsymbol{I}$ 和 $p(m)=\langle\psi|E_m|\psi\rangle$ 的半正定算子. 这样的 E_m 称为与测量相联系的 POVM 元，完整集合 $\{E_m\}$ 称为一个 POVM.

值得一提的是，投影测量只能用来区分正交态，测量后原量子态被毁坏. 而 POVM 测量可以用来区分非正交态，是一种非损坏性测量.

1.5 量子不可克隆定理

经典信息处理过程中常常需要对信息进行精确拷贝. 一个自然的问题是，能否在量子信息处理中精确地拷贝量子信息呢？1982 年，Wootters 和 Zurek[45]对此问题给出了否定性的答案，得到了一个重要结论：在量子力学中，不存在这样一个物理过程，它能实现对任意量子态的精确复制，使得每个复制态与初始态完全相同. 这就是著名的量子不可克隆定理. 该定理的证明很简单，其证明如下：设 $|\phi\rangle$ 和 $|\psi\rangle$ 同时被一幺正过程 $\boldsymbol{U}$ 所克隆，即

$$\boldsymbol{U}\left(|\phi\rangle|Q\rangle_x\right)=|\phi\rangle|\phi\rangle|Q_0\rangle_x,\boldsymbol{U}\left(|\psi\rangle|Q\rangle_x\right)=|\psi\rangle|\psi\rangle|Q_1\rangle_x$$

其中，$|Q\rangle_x,|Q_0\rangle_x,|Q_1\rangle_x$ 均为单位量子态，注意到 $\boldsymbol{U}$ 为幺正有

$$|\langle\phi|\psi\rangle|=|\langle\phi|\psi\rangle|^2\cdot|_x\langle Q_0|Q_1\rangle_x|\leqslant|\langle\phi|\psi\rangle|^2.$$

当且仅当 $|\phi\rangle$ 和 $|\psi\rangle$ 相互正交时，上式等号成立，即非正交态不可克隆. 量子不可克隆定理是安全量子通信的基础.

第 2 章　量子态分享协议设计

2.1　引　　言

当量子力学定律被调用于信息处理时，就会产生包括量子隐形传态[1]和超密编码[79]等一些新奇的超越现代科学技术手段或超自然力量的现象. 它使得作为量子力学与信息科学相结合的量子信息理论成为当今人们高度关注的主题.

1993 年，Bennett 等[1]首次提出两能级系统的量子隐形传态协议，该协议通过发送者和接受者事先共同分享的一个纠缠 EPR 粒子对作为量子信道，发送者传递一个未知量子纯态给接受者. 其要点是受量子力学不确定原理的限制，发送者必须将要传递的原物的量子态的信息划分为经典信息与量子信息，再分别通过经典信道和量子信道传送给接收者，接收者根据这两种信息构造出原量子态的完美复制品. 在隐形传态过程中，原物并没有被直接传送到接收者手中，只是原物的量子态被传递，而且此态在发送者提取经典信息和进行测量时已被毁坏，发送者可能不知道这个量子态的任何信息，接收者通过酉运算把别的物质的粒子变成处于与原物完全相同的量子态. 由于海森堡测不准原理、量子不可克隆定理及量子纠缠等特性，使得隐形传态具有可靠性与安全性高、速度快、应用潜力大等特点，引起人们的广泛关注[80-82]，近十年来，许多的隐形传态协议被提出来了[83-94]. 1999 年，Hillery 等[2]扩展了 Bennett 的隐形传态思想，率先提出了量子态秘密分享的概念. 其思想是将原始量子信息划分为多个部分，使得每个独立部分的信息持有者都不能获得完整的原始信息；只有各个部分的信息持有者共同合作，才能使得其中某个部分信息持有者获得完整的原始信息. 从那以后，量子态秘密分享在理论和实验研究上获得了大量成果[95-128]. 然而，先前大量的量子态分享(QSTS)协议聚焦在像 EPR 粒子对、GHZ 态及 W 态等这样的常见最大纠缠态作为首选的量子资源，分享如一粒子、二粒子等常见简单粒子的未知态秘密上，并且几乎协议考虑的情况是对称的，即协议中每个代理商有相同的权力获得发送者的秘密. 可是团簇态和一般多粒子态比 GHZ 态等具有更好的持久稳定性和较好抗退相干之鲁棒性；在真实通信环境中，不可避免地受环境影响，初始最大纠缠态容易演化为非最大纠缠态或混合态，且更一般的 QSTS 协议应包含非对称情况，即协议中不同代理商获得发送者秘密的权力不尽相同.

本章正是针对上述问题，并切实考虑通信物理实现的可能性等，提出一些新的 QSTS 协议，以期丰富量子秘密分享理论或应用.

2.2 以最大纠缠态为信道，任意未知 n-粒子态的隐形传态

假设有如下一个任意未知 n 粒子态

$$|\varphi\rangle_{12\cdots n}=\sum_{m_n=0}^{1}\cdots\sum_{m_2=0}^{1}\sum_{m_1=0}^{1}k_{m_1m_2\cdots m_n}|m_1\rangle_1|m_2\rangle_2\cdots|m_n\rangle_n \tag{2-1}$$

其中所有 $k_{m_1m_2\cdots m_n}$ 都是复数且 $\sum|k_{m_1m_2\cdots m_n}|^2=1$. 我们可以把它改写为

$$|\varphi\rangle_{12\cdots n}=\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_n+\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_n \tag{2-2}$$

满足 $\sum|a_{\{i\}}|^2=\sum|b_{\{i\}}|^2=1$，这里 $|\{i\}\rangle_{12\cdots(n-1)}(i\in\{0,1\})$ 为粒子 $1,2,\cdots,n-1$ 的计算基. 我们也可把态 $|\varphi\rangle_{12\cdots n}$ 表示成如下形式：

$$\begin{aligned}|\varphi\rangle_{12\cdots n}=&\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\right)|00\rangle_{(n-1)n}+\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\right)|01\rangle_{(n-1)n}\\&+\left(\sum c_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\right)|10\rangle_{(n-1)n}+\left(\sum d_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\right)|11\rangle_{(n-1)n}\end{aligned} \tag{2-3}$$

满足 $\sum|a_{\{i\}}|^2+\sum|b_{\{i\}}|^2+\sum|c_{\{i\}}|^2+\sum|d_{\{i\}}|^2=1$，其中 $|\{i\}\rangle_{12\cdots(n-2)}(i\in\{0,1\})$ 为关于粒子 $1,2,\cdots,n-2$ 的计算基. 态 $|\varphi\rangle_{12\cdots n}$ 还可以写成

$$\begin{aligned}|\varphi\rangle_{12\cdots n}=&\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|000\rangle_{(n-2)(n-1)n}+\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|001\rangle_{(n-2)(n-1)n}\\&+\left(\sum c_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|010\rangle_{(n-2)(n-1)n}+\left(\sum d_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|011\rangle_{(n-2)(n-1)n}\\&+\left(\sum e_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|100\rangle_{(n-2)(n-1)n}+\left(\sum f_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|101\rangle_{(n-2)(n-1)n}\\&+\left(\sum g_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|110\rangle_{(n-2)(n-1)n}+\left(\sum h_{\{i\}}|\{i\}\rangle_{12\cdots(n-3)}\right)|111\rangle_{(n-2)(n-1)n}\end{aligned} \tag{2-4}$$

这里 $\sum|a_{\{i\}}|^2+\sum|b_{\{i\}}|^2+\sum|c_{\{i\}}|^2+\sum|d_{\{i\}}|^2+\sum|e_{\{i\}}|^2+\sum|f_{\{i\}}|^2+\sum|g_{\{i\}}|^2+\sum|h_{\{i\}}|^2=1$，且 $|\{i\}\rangle_{12\cdots(n-3)}(i\in\{0,1\})$ 为关于粒子 $1,2,\cdots,n-3$ 的计算基. 我们将看到，将下列隐形传态方案作适当修改，便可得到量子态分享方案.

2.2.1 以三粒子态为信道，任意未知 n-粒子态之完美隐形传态的两个方案

现在，考虑 Alice 如何将多粒子态 $|\varphi\rangle_{12\cdots n}$ 传递给 Bob. 首先，假定 Alice 和 Bob 分享三粒子 W 态

$$|W\rangle_{BAA'}=\left(\alpha|001\rangle+\beta|010\rangle+\frac{\sqrt{2}}{2}|100\rangle\right)_{BAA'} \tag{2-5}$$

满足 $|\alpha|^2+|\beta|^2=\frac{1}{2}$，其中，$A$ 和 A' 属于发送者 Alice，而粒子 B 属于接收者 Bob. 整个系统的初始态为

$$\begin{aligned}|T\rangle_t &= |\varphi\rangle_{12\cdots n}\otimes|W\rangle_{BAA'}\\ &=\left[\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_n+\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)})1\rangle_n\right]\\ &\otimes\left(\alpha|001\rangle+\beta|010\rangle+\frac{\sqrt{2}}{2}|100\rangle)_{BAA'}\right)\end{aligned}\tag{2-6}$$

为了完成量子任务，Alice 利用$\left\{\left|\lambda_j^{\pm}\right>\middle|j=1,2\right\}$对粒子 n，A 和 A' 进行 von Neumann 测量，其中$\left|\lambda_1^{\pm}\right\rangle=\alpha|001\rangle+\beta|010\rangle\pm\frac{\sqrt{2}}{2}|100\rangle,\left|\lambda_2^{\pm}\right\rangle=\alpha|101\rangle+\beta|110\rangle\pm\frac{\sqrt{2}}{2}|000\rangle$. 粒子$1,2,\cdots,n-1$和 B 的态将塌陷为

$$_{nAA'}\left\langle\lambda_1^{\pm}|T\right\rangle_t=\frac{1}{2}\left[\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_B\pm\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_B\right]\tag{2-7}$$

$$_{nAA'}\left\langle\lambda_2^{\pm}|T\right\rangle_t=\frac{1}{2}\left[\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_B\pm\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_B\right]\tag{2-8}$$

其次，Alice 通过经典信道将测量结果通知 Bob. 根据 Alice 的不同测量结果，Bob 分别实施相应的酉运算I,σ_z,σ_x或$i\sigma_y$于粒子 B，略去全局因子，粒子$1,2,\cdots,n-1$和 B 的态变成$\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_B+\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_B$. 比较上态与$|\varphi\rangle_{12\cdots n}$的第一种表示，Alice 在初始纠缠系统中的粒子 n 现在被 Bob 的粒子 B 所替代. 因此仅仅通过一个粒子酉运算，未知多粒子态能被如实地传递且成功的概率和保真度都达到 1，所以本方案是完美的.

最后，我们考虑另一个方案：Alice 打算通过如下量子信息信道传递态$|\varphi\rangle_{12\cdots n}$给 Bob，$|\varphi'\rangle_{ABA'}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_{A'}$，这里的粒子 A 和 A' 属于 Alice，而粒子 B 被 Bob 拥有. 联合系统的初始状态可表示为

$$\begin{aligned}|T'\rangle_t &= |\varphi\rangle_{12\cdots n}\otimes|\varphi'\rangle_{ABA'}\\ &=\left[\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_n+\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_n\right]\\ &\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_{A'}\end{aligned}\tag{2-9}$$

Alice 先利用正交基$\{\phi^+,\phi^-,\psi^+,\psi^-\}$对粒子对$(n,A)$进行 Bell 态测量，其中$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$，然后用基$\{|0\rangle,|1\rangle\}$对其粒子 A' 实施单粒子测量，并将测量结果通过经典信道告诉 Bob. 剩余粒子态塌为下列态之一：

$$_{A'}\langle 0|_{nA}\left\langle\phi^{\pm}|T'\right\rangle_t=\frac{1}{2\sqrt{2}}\left[\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_B\pm\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_B\right]\tag{2-10}$$

$$_{A'}\langle 0|_{nA}\left\langle\psi^{\pm}|T'\right\rangle_t=\frac{1}{2\sqrt{2}}\left[\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_B\pm\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_B\right]\tag{2-11}$$

$$_{A'}\langle 1|_{nA}\left\langle\phi^{\pm}|T'\right\rangle_t=\frac{1}{2\sqrt{2}}\left[\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_B\pm\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_B\right]\tag{2-12}$$

$$_{A'}\langle 1|_{nA}\left\langle\psi^{\pm}|T'\right\rangle_t=\frac{1}{2\sqrt{2}}\left[\left(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|1\rangle_B\pm\left(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-1)}\right)|0\rangle_B\right]\tag{2-13}$$

收到 Alice 的测量结果后，Bob 选用酉变换$\{I,\sigma_z,\sigma_x,i\sigma_y\}$中之一使态$|\varphi\rangle_{12\cdots n}$的第一种表达式中粒子 n 变成粒子 B. 这样，未知多粒子纠缠态$|\varphi\rangle_{12\cdots n}$也能被完美地传递，且我们方案的保真度和成功的概率也都达到 1.

注　在上述方案中，假定粒子 A、B 和 A' 分别属于 Alice、Bob 与 Charlie，且 Alice 和 Bob 也分别是发送者与接收者，而 Charlie 是控制者. Alice 对粒子对(n,A)进行 Bell 态测量，并把结果告知 Bob 与 Charlie. 然后 Charlie 用基$\{|0\rangle,|1\rangle\}$对粒子 A' 实施单粒子测量，并把结果告诉 Bob. 收到结果后，Bob 通过适当的酉变换能确切地获得量子秘密. 因此我们的方案可修改为未知多粒子的三方量子隐形传态方案.

2.2.2　以四粒子团簇态为量子信道，任意未知 n-粒子态的完美隐形传态

现在考虑情况：Alice 想要以四粒子团簇态为量子信道，将$|\varphi\rangle_{12\cdots n}$传递给 Bob，其中四粒子团簇态为

$$|\varphi\rangle_{ABA'B'}=\frac{1}{2}\left(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle\right)_{ABA'B'} \tag{2-14}$$

这里粒子对(A,A')和(B,B')分别属于 Alice 和 Bob. 由态$|\varphi\rangle_{12\cdots n}$的第二表达式得联合系统的初始态为

$$\begin{aligned}|\Phi\rangle_t&=|\varphi\rangle_{12\cdots n}\otimes|\varphi\rangle_{AA'BB'}\\&=\Big[\Big(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|00\rangle_{(n-1)n}+\Big(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|01\rangle_{(n-1)n}\\&\quad+\Big(\sum c_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|10\rangle_{(n-1)n}+\Big(\sum d_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|11\rangle_{(n-1)n}\Big]\\&\quad\otimes\frac{1}{2}\left(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle\right)_{ABA'B'}\end{aligned} \tag{2-15}$$

为了完成量子任务，Alice 对粒子对$(n-1,A)$和(n,A')分别实施 Bell 态测量，并把测量结果告知 Bob. 于是，整个系统的态塌陷为下列态之一：

$$\begin{aligned}{}_{nA'}\langle\phi^+|_{(n-1)A}\langle\phi^\pm|\Phi\rangle_t&=\frac{1}{4}\Big[\Big(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|00\rangle_{BB'}+\Big(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|01\rangle_{BB'}\\&\quad\pm\Big(\sum c_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|10\rangle_{BB'}\pm\Big(\sum d_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|11\rangle_{BB'}\Big]\end{aligned} \tag{2-16}$$

$$\begin{aligned}{}_{nA'}\langle\phi^-|_{(n-1)A}\langle\phi^\pm|\Phi\rangle_t&=\frac{1}{4}\Big[\Big(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|00\rangle_{BB'}-\Big(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|01\rangle_{BB'}\\&\quad\pm\Big(\sum c_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|10\rangle_{BB'}\mp\Big(\sum d_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|11\rangle_{BB'}\Big]\end{aligned} \tag{2-17}$$

$$\begin{aligned}{}_{nA'}\langle\psi^+|_{(n-1)A}\langle\phi^\pm|\Phi\rangle_t&=\frac{1}{4}\Big[\Big(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|01\rangle_{BB'}+\Big(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|00\rangle_{BB'}\\&\quad\pm\Big(\sum c_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|11\rangle_{BB'}\pm\Big(\sum d_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|10\rangle_{BB'}\Big]\end{aligned} \tag{2-18}$$

$$\begin{aligned}{}_{nA'}\langle\psi^-|_{(n-1)A}\langle\phi^\pm|\Phi\rangle_t&=\frac{1}{4}\Big[\Big(\sum a_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|01\rangle_{BB'}-\Big(\sum b_{\{i\}}|\{i\}\rangle_{12\cdots(n-2)}\Big)|00\rangle_{BB'}\end{aligned}$$