中国科学技术大学

博士学位论文

量子非局域性与多体纠缠

作者姓名： 石飞

学科专业： 网络空间安全

导师姓名： 张先得 特任教授

完成时间： 二〇二二年五月二十九日

University of Science and Technology of China

A dissertation for doctor's degree

Quantum nonlocality and multipartite entanglement

Author: Fei Shi

Speciality: Cyberspace Security

Supervisor: Prof. Xiande Zhang

Finished time: May 29, 2022

中国科学技术大学学位论文原创性声明

本人声明所呈交的学位论文，是本人在导师指导下进行研究工作所取得的成果。除已特别加以标注和致谢的地方外，论文中不包含任何他人已经发表或撰写过的研究成果。与我一同工作的同志对本研究所做的贡献均已在论文中作了明确的说明。

作者签名：_____ 签字日期：_____

中国科学技术大学学位论文授权使用声明

作为申请学位的条件之一，学位论文著作权拥有者授权中国科学技术大学拥有学位论文的部分使用权，即：学校有权按有关规定向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅，可以将学位论文编入《中国学位论文全文数据库》等有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。本人提交的电子文档的内容和纸质论文的内容相一致。

控阅的学位论文在解密后也遵守此规定。

☑ 公开 ☐ 控阅（____ 年）

作者签名：_____ 导师签名：_____

签字日期：_____ 签字日期：_____

摘　要

量子非局域性理论和量子纠缠理论是量子力学中非常重要的理论，也是量子保密通信的基础理论。量子非局域性可以用于量子数据隐藏和量子秘密共享，而多体纠缠在量子密钥分发、量子隐形传态和量子纠错码中扮演着核心的角色。因此关于量子非局域性和多体纠缠的理论研究不仅对量子力学的发展添砖加瓦，同时也促进量子保密通信的发展。本文具体研究与量子非局域性相关的不可扩充乘积基和强量子非局域性，以及与多体纠缠相关的 k-均匀态和量子信息掩盖，其具体研究内容和创新点可以归纳为以下三部分：

首先建立了多维超立方体与不可扩充乘积基之间的关系。不可扩充乘积基具有量子非局域性，而量子非局域性可以保证信息安全。虽然目前关于最小数目的不可扩充乘积基的研究较多，但具有较大数目的不可扩充乘积基的结果较少，且缺少具体的构造。本文中，我们给出了砖块结构与两体系统中的不可扩充乘积基之间的对应关系，利用这个对应关系，构造了一系列两体系统中具有较大数目的不可扩充乘积基。我们将这个结构推广到了多体系统中，建立了多维超立方体与多体系统中的不可扩充乘积基之间的关系，利用多维超立方体的分解，构造了三体和四体系统中具有较大数目的不可扩充乘积基。考虑到不可扩充乘积基是局部不可区分的，要区分它必须借助于纠缠资源，因此我们也研究了两体系统中的不可扩充乘积基的纠缠辅助区分。

其次建立了多维超立方体与强量子非局域性之间的关系。强量子非局域性可以进一步地提高信息的安全性，但目前只有少量三体和四体系统中的强非局域的正交乘积集。本文中，利用前面提到的多维超立方体的分解，我们构造了三体、四体和五体系统中强非局域的正交乘积集和三体系统中强非局域的正交纠缠集，并证明了前面构造的三体和四体系统中的不可扩充乘积基具有强量子非局域性。此外，利用循环置换群作用，我们构造了一般 N 体齐次系统中的强非局域的正交纠缠集，并当 $N=3,4$ 时，找到了强非局域的正交真实纠缠集。

最后建立了量子纠错码与量子信息掩盖之间的关系，给出了非齐次系统中 $2,3$-均匀态的具体构造。目前关于非齐次系统中的 k-均匀态的构造较少，而多体系统中的量子信息掩盖有着很大的安全漏洞。本文中，利用混合正交阵列，我们构造了一系列非齐次系统中的 $2,3$-均匀态，并给出了两种从 k-均匀态到 $(k-1)$-均匀态的构造方法。利用影子不等式，我们给出了一些非齐次系统中的绝对最大纠缠态的不存在性结果。此外，我们提出了 k-均匀量子信息掩盖的概念，它要求任意 k 个子系统都无法访问掩盖之前的信息。我们建立了非齐次系统中的量子纠错码与 k-均匀量子信息掩盖之间的关系，基于这个关系，证明了不可掩盖定理

本质上是量子纠错码的量子 Singleton 界的一个特例，并给出了一个更一般的不可掩盖定理。我们也给出了几种从已知的非齐次系统中的量子纠错码构造新的量子纠错码的方法，这些方法可以用来构造非齐次系统中的 k-均匀态。

关键词：不可扩充乘积基；强量子非局域性；超立方体分解；k-均匀态；混合正交阵列；量子信息掩盖；量子纠错码

ABSTRACT

Quantum nonlocality theory and quantum entanglement theory are very important in quantum mechanics, and they are also the basic theories of quantum secure communication. Quantum nonlocality can be used for quantum data hiding and quantum secret sharing, while multipartite entanglement plays a central role in quantum key distribution, quantum teleportation, and quantum error-correcting codes. Therefore, the theoretical research on quantum nonlocality and multipartite entanglement not only contributes to the development of quantum mechanics, but also promotes the development of quantum secure communication. This dissertation specifically studies unextendible product bases and strong quantum nonlocality related to quantum nonlocality, as well as k-uniform states and quantum information masking related to multipartite entanglement, and specific research content and innovation points can be summarized into the following three parts:

Firstly, we establish a relation between hypercubes and unextendible product bases. Unextendible product bases have quantum nonlocality, which can guarantee information security. There are many studies on the minimum size of unextendible product bases currently, but the results on the large sizes of unextendible product bases, and explicit constructions are few. In this dissertation, we give the correspondence between tile structures and unextendible product bases in bipartite systems. By using this correspondence, we construct unextendible product bases with large sizes in bipartite systems. We also extend tile structures to multipartite systems, and establish a relation between hypercubes and unextendible product bases in multipartite systems. Based on the decomposition of hypercubes, we construct unextendible product bases with large sizes in three-partite and four-partite systems. Since unextendible product bases are locally indistinguishable, entanglement resources are necessary to distinguish them. So we also study the entanglement-assisted discrimination for unextendible product bases in bipartite systems.

Secondly, we establish a relation between hypercubes and strong quantum nonlocality. Strong nonlocality can further improve information security, but there are only few strongly nonlocal orthogonal product sets in three- and four-partite systems currently. In this dissertation, by using the previously mentioned decomposition of hypercubes, we construct strongly nonlocal orthogonal product sets in three-, four- and five-partite systems and strongly nonlocal orthogonal entangled sets in three-partite systems,

and also prove that our unextendible product bases in three-partite and four-partite systems have strong quantum nonlocality. Furthermore, by using cyclic permutation group action, we construct strongly nonlocal orthogonal entangled sets in general N-partite homogeneous systems, and when $N = 3, 4$, we find strongly nonlocal orthogonal genuinely entangled sets.

Finally, we establish a relation between quantum error-correcting codes and quantum information masking, and give the explicit constructions of $2, 3$-uniform states in heterogeneous systems. At present, there are few constructions of k-uniform states in heterogeneous systems, and quantum information masking in multipartite systems has a large security hole. In this dissertation, by using mixed orthogonal arrays, we construct a series of $2, 3$-uniform states in heterogeneous systems, and give two methods of generating $(k-1)$-uniform states from k-uniform states. By using shadow inequalities, we give some results on the nonexistence of absolutely maximally entangled states in heterogeneous systems. Furthermore, we propose the concept of k-uniform quantum information masking, which requires that collusion between any k parties can not reveal the encoded information. We establish a relation between quantum error-correcting codes in heterogeneous systems and k-uniform quantum information masking. Based on this relation, we show that the no-masking theorem is a special case of the quantum Singleton bound for quantum error-correcting codes in heterogeneous systems essentially, and give a more general no-masking theorem. We also give some methods for constructing new quantum error-correcting codes from old quantum error-correcting codes in heterogeneous systems, and these methods can be used to construct k-uniform states in heterogeneous systems.

Key Words: Unextendible product bases; Strong quantum nonlocality; Hypercube decomposition; k-Uniform states; Mixed orthogonal arrays; Quantum information masking; Quantum error-correcting codes

目　录

插 图 清 单

表 格 清 单

第 1 章　绪　　论

随着量子科技的不断发展，“第二次量子革命”已经向我们走来，而量子信息理论是这里面重要的一环。量子非局域性理论和量子纠缠理论可用于量子数据隐藏、量子秘密共享、量子密钥分发、量子隐形传态和量子纠错码等量子信息领域中。因此对量子非局域性理论和量子纠缠理论的研究至关重要。

本章将介绍量子非局域性和多体纠缠的研究背景、研究现状及其相关应用。1.1 节介绍了量子非局域性和多体纠缠在信息安全中的应用。1.2 节具体介绍了不可扩充乘积基、强量子非局域性、k-均匀态和量子信息掩盖的研究现状。1.3 节强调了本文的研究内容与创新点。1.4 节介绍了本文的结构安排和主要结论。

1.1　研究背景与意义

本节将介绍量子非局域性和多体纠缠的研究背景与意义。

1.1.1　量子非局域性

量子非局域性（quantum nonlocality）是量子力学中最重要的性质之一。如果纠缠态违反 Bell 型不等式，那么它具有 Bell 型非局域性[1-2]。如果一组正交态在局域操作和经典通信（local operations and classical communication, LOCC）下是不能区分的，那么这组正交态被称为局部不可区分的（locally indistinguishable）。局部不可区分性也具有量子非局域性，而基于局部不可区分性的量子非局域性是本文主要研究的对象。这种非局域性与 Bell 型非局域性有很大不同，原因是 Bell 型非局域性只发生在纠缠态中，而基于局部不可区分性的非局域性不限于此。1999 年，Bennett 等人[3]首先在 $\mathbb{C}^3 \otimes \mathbb{C}^3$ 中构造了一组局部不可区分的正交乘积基（orthogonal product basis），这表明了无纠缠的量子非局域性现象。后来，局部不可区分的正交乘积集（orthogonal product set）和正交纠缠集（orthogonal entangled set）被广泛地研究[4-21]。

当信息被编码在多体系统中的一个局部不可区分的正交集中时，这个信息将不能通过 LOCC 的方式被完全访问。因此，量子非局域性可用于量子数据隐藏（quantum data hiding）[22-25] 和量子秘密共享（quantum secret sharing）[26-28]。如图1.1中的左图所示，一个公司里面有一个老板和他的 N 个员工，这 N 个员工处于不同的实验室，并且可以进行局部测量和打电话的方式交流经典信息。这位老板把信息编码在一组具有非局域性的 N 体正交态中，通过量子信道将信息传递给他的 N 个员工，每位员工都只能得到其中的一部分信息。由于这组 N 体正

交态具有非局域性，这 N 个员工在 LOCC 下无法访问所有的原始信息，部分信息被隐藏起来了。例如，由于 Bell 基是局部不可区分的，如果我们将两个经典比特的信息编码到这组 Bell 基中，那么在 LOCC 下只有一个比特的信息能被提取出来[22,29]。因此量子非局域性可以提高信息的安全性。

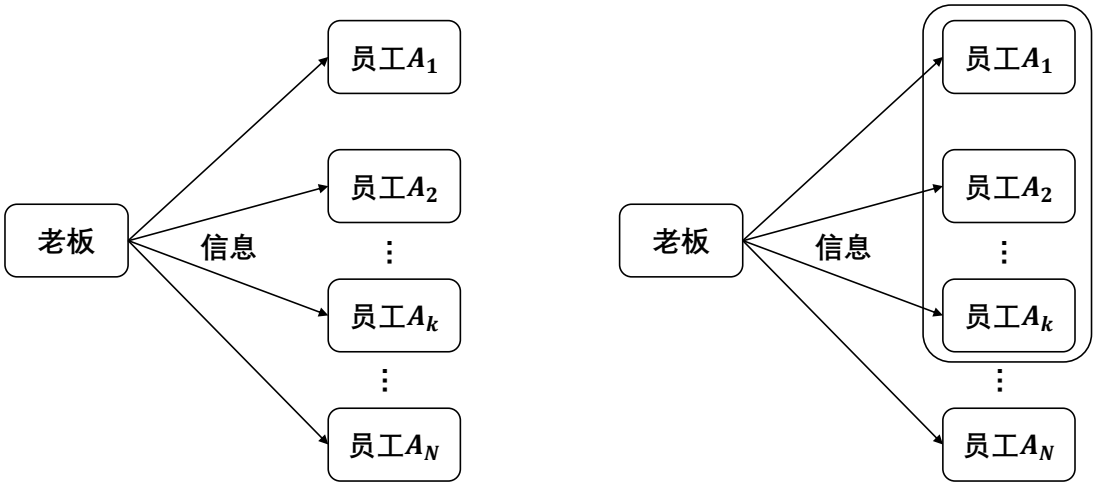

图 1.1　量子非局域性在信息安全中的应用。

不可扩充乘积基（unextendible product basis）[30] 是一类具有无纠缠的量子非局域性的结构。对于多体系统中的一个正交乘积集（非正交乘积基），如果它生成的子空间的正交补空间中没有乘积态，那么这个正交乘积集被称为不可扩充乘积基。不可扩充乘积基在量子信息中扮演着重要的角色，它可以构造束缚纠缠态[30]（bound entangled state），也与费米子系统和无量子违反的 Bell 不等式相关联[31-33]。目前，虽然在构造较小数目的不可扩充乘积基方面有了很多结果[30,34-38]，但在构造较大数目的不可扩充乘积基方面进展较少[4,39-40]，且缺少明确的构造。其次虽然不可扩充乘积基是局部不可区分的[4,30,41]，但是可以借助于纠缠辅助区分协议来区分不可扩充乘积基[42]。由于纠缠资源在量子信息中非常宝贵，如何利用较少的纠缠资源来完成区分过程是一个值得深究的问题。

2019 年, Halder 等人[43] 提出了一个更强版本的量子非局域性的概念: 强量子非局域性（strong quantum nonlocality）。如果通过正交保持的局部测量不能从一组多体正交态中消除一个或多个态，那么这组正交态被称为局部不可约的（locally irreducible）。一个局部不可约集一定是一个局部不可区分集，反之则不一定成立。此外，如果一组多体正交态在任意两体划分下都是局部不可约的，那么它被称为强非局域的（strongly nonlocal）。Halder 等人在 $\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3$ 和 $\mathbb{C}^4\otimes\mathbb{C}^4\otimes\mathbb{C}^4$ 中分别构造了强非局域的正交乘积基，这表明了无纠缠的强量子非局域性现象。

强量子非局域性也可以用于信息安全。在图1.1中的左图中，虽然老板利用量子非局域性可以一定程度上保证信息的安全性，但是如果其中有 k 个员工共谋（即这 k 个员工汇聚在其中一个员工的实验室内，它们知道彼此的信息，并可

以进行联合测量），那么原来的信息有可能被这 N 个员工完全访问，如图1.1中的右图所示。为了避免这种情况的发生，老板可以将原始的信息编码在一组具有强量子非局域性的 N 体正交态中，由于这组正交态在任意两体划分下是局部不可区分的，即使其中任意 k（$k < N$）个员工共谋，也不能访问所有的原始信息（有可能访问其中一部分信息）。此外，由于这组正交态在任意两体划分下是局部不可约的，如果这些员工只能进行正交保持的局部测量或联合测量，那么即使有员工共谋，原始的信息将完全无法访问。由此可见强量子非局域性进一步地提高了信息的安全性。

1.1.2　多体纠缠

多体纠缠在量子密钥分发[44-48]、量子隐形传态[49-50] 和量子纠错码[51]等领域中扮演着核心的角色。例如 2016 年，中国成功地发射了“墨子号”量子科学实验卫星，该卫星在国际上首次实现千公里级基于纠缠的量子密钥分发[47]，如图1.2所示。实验中，“墨子号”作为纠缠源，本身并不掌握密钥的任何信息，它只负责分发纠缠，即使卫星被别人控制了，密码也是安全的。所以该实验进一步提升了量子保密通信的现实安全性。2021 年中国科研团队成功实现了跨越 4600 公里的星地量子密钥分发，标志着中国已构建出天地一体化广域量子通信网雏形[48]。虽然纠缠在量子信息领域中发挥着至关重要的作用，但是刻画任意多体系统中的纠缠态仍具有挑战性[1]。最近一类特殊的纯态：k-均匀态（k-uniform state），吸引了很多研究者的关注[51-55]。

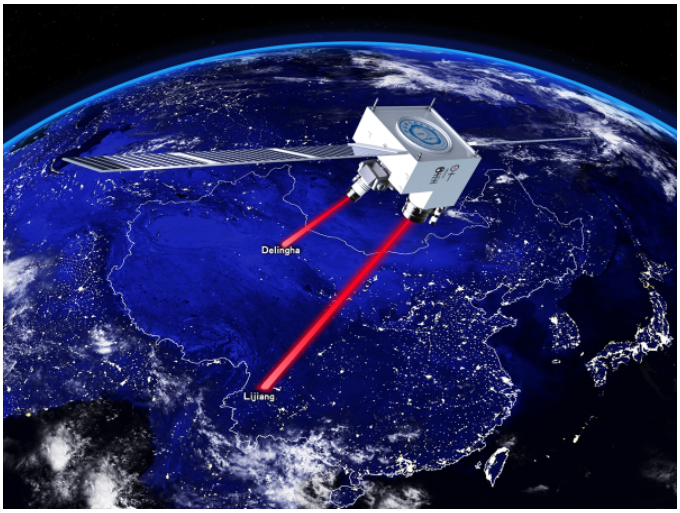

图 1.2　“墨子号”量子科学实验卫星在国际上首次实现千公里级基于纠缠的量子密钥分发[56]。

如果一个齐次系统 $(\mathbb{C}^d)^{\otimes N}$ 中的一个纯态在任意 k 体上的约化密度算子是最大混合的，那么它被称为 k-均匀态（k-uniform state）[51] 。$(\mathbb{C}^d)^{\otimes N}$ 中的 k-均匀态与参数为 $((N, 1, k+1))_d$ 的量子纠错码一一对应[51]，并且它可以通过正交阵

列[52]、拉丁方[57]、量子拉丁方[58]、对称矩阵和经典纠错码[53]来构造。根据施密特分解，$(\mathbb{C}^d)^{\otimes N}$ 中的 k-均匀态存在的必要条件是 $k \leqslant \lfloor \frac{N}{2} \rfloor$[59]。特别地，$\lfloor \frac{N}{2} \rfloor$-均匀态被称为绝对最大纠缠态（absolutely maximally entangled state），它在任意两体划分下都是最大纠缠态。绝对最大纠缠态可用于阈值量子秘密共享方案[60]、并行和开放目标的远程传输协议[60] 和全息量子纠错码[61]。局部维数 $d = 2$ 的绝对最大纠缠态仅存在于 $2, 3, 5, 6$ 体系统中[51,62-63]。当局部维数 $d \geqslant 3$ 时，有很多绝对最大纠缠态的存在性是未知的[64-65]。

在实验中，我们经常遇到更一般的系统：非齐次系统 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$。那么 k-均匀态和绝对最大纠缠态的概念也可以直接推广到非齐次系统中。类似地，$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的 k-均匀态与非齐次系统中参数为 $((N, 1, k+1))_{d_1, d_2, \cdots, d_N}$ 的量子纠错码一一对应[66]。最近有几个实验关注于构造非齐次系统中的多体纠缠态[67-69]，此外，一些三体非齐次系统中的绝对最大纠缠态在实验上被实现[70-72]，这使得非齐次系统中的 k-均匀态和绝对最大纠缠态的研究更有意义。

当量子信息通过带有噪声的信道时，错误是不可避免的[73-75]。量子纠错码（quantum error-correcting code）在量子信息处理中发挥着核心作用，它可以保护量子信息免受各种量子噪声的影响。齐次系统中的量子纠错码的研究较多[62,76-81]，但当编码后的态属于非齐次系统时，我们通常面临更复杂的情况，这使得研究非齐次系统中的量子纠错码更加复杂。齐次系统中的量子纠错码最重要的界：量子 Singleton 界（quantum Singleton bound）[77] 也可以推广到非齐次系统中的量子纠错码上[66]。量子 Singleton 界实际上起源于不可克隆定理[79,82]，我们可以期待它更多的性质。

不可克隆定理[83-85]、不可广播定理[86]、不可删除定理[87]和不可隐藏定理[88]等不可行定理（no-go theorem）都是量子力学的线性性和酉性的结果。最近 Modi 等人提出了量子信息掩盖（quantum information masking）的概念[89]，这是一个将量子信息编码到两体系统中的物理过程，使得信息对于每个单体子系统来说是完全未知的。值得注意的是，量子信息掩盖与前面提到的量子非局域性在信息安全中的应用所用的原理完全不同。这里的量子信息掩盖会使得掩盖后的所有态的单体约化密度算子都相等，从而达到掩盖量子信息的目的，而前面主要利用量子非局域性来隐藏信息。Modi 等人强调了另一个被称为不可掩盖定理的不可行定理，它指的是不能掩盖任意量子态。类似于强量子非局域性在信息安全中的应用，对于多体系统中的量子信息掩盖，一些子系统共谋也可能会揭露编码前的信息[89]，因此我们需要更强版本的量子信息掩盖。在本文中，我们将提出多体系统中的 k-均匀量子信息掩盖的概念，它要求任意 k 个子系统都无法访问原始信息。相比于之前的量子信息掩盖，k-均匀量子信息掩盖使得信息更加安全。

1.2　国内外研究现状

本节将给出不可扩充乘积基、强量子非局域性、k-均匀态和量子信息掩盖的研究现状。

1.2.1　不可扩充乘积基

1999 年，Bennett 等人[30]提出了不可扩充乘积基的概念，在 $\mathbb{C}^3\otimes\mathbb{C}^3$ 和 $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ 中分别给出了数目为 5 和 4 的不可扩充乘积基，他们利用不可扩充乘积基给出了束缚纠缠态的一个巧妙构造，并证明了不可扩充乘积基是局部不可区分的。对于 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的不可扩充乘积基的最小数目 $f(d_1,d_2,\cdots,d_N)$，Bennett 等人也证明了 $f(d_1,d_2,\cdots,d_N)\geqslant\sum_{i=1}^{N}(d_i-1)+1$。利用正交性图，Alon 等人[36]给出了 $f(d_1,d_2,\cdots,d_N)$ 达到下界的充分必要条件：除了 $N=2$ 且 $2\in\{d_1,d_2\}$，或 $\sum_{i=1}^{N}(d_i-1)+1$ 是奇数且至少有一个 d_i 是偶数之外，$f(d_1,d_2,\cdots,d_N)=\sum_{i=1}^{N}(d_i-1)+1$。利用 1-因子分解图，Feng[37]给出了一些 $f(d_1,d_2,\cdots,d_N)=\sum_{i=1}^{N}(d_i-1)+2$ 的例子。而对于 $d_1=d_2=\cdots=d_N=2$ 的情况，Johnston[34]完全确定了 $f(d_1,d_2,\cdots,d_N)$ 的数值：当 N 为奇数时，$f(d_1,d_2,\cdots,d_N)=N+1$；当 $N=4$ 或 $N=2\pmod 4$，$f(d_1,d_2,\cdots,d_N)=N+2$；当 $N=8$，$f(d_1,d_2,\cdots,d_N)=N+3$；其余情况下 $f(d_1,d_2,\cdots,d_N)=N+4$。当 $2\leqslant d_1\leqslant d_2\leqslant\cdots\leqslant d_N$，$d_N-1\geqslant\sum_{i=1}^{N-1}(d_i-1)$ 且 $f(d_1,d_2,\cdots,d_N)\geqslant\sum_{i=1}^{N}(d_i-1)+2$ 时，Chen 等人[31]利用代数几何的工具确定了 $f(d_1,d_2,\cdots,d_N)=\sum_{i=1}^{N}(d_i-1)+2$。最近 Zhang 等人[90]证明了 $f(2,2,4k-1)=4k+2$。

较大数目的不可扩充乘积基也有少量结果。对于 $n\geqslant 4$，利用砖块结构，DiVincenzo 等人[4]在 $\mathbb{C}^n\otimes\mathbb{C}^n$ 中给出了数目为 n^2-2n+1 的不可扩充乘积基，并对于 $3\leqslant m\leqslant n$，在 $\mathbb{C}^m\otimes\mathbb{C}^n$ 中给出了数目为 $mn-2m+1$ 的不可扩充乘积基。当 $m\geqslant 3$ 为奇数时，Halder 等人[39]也利用砖块结构在 $\mathbb{C}^m\otimes\mathbb{C}^m$ 中构造了数目为 $(m-1)^2+1$ 的不可扩充乘积基，并且 Zhang 等人[91]证明了这个不可扩充乘积基可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil}\otimes\mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分。对于 $d\geqslant 3$，利用三维立方体的分解，Agrawal 等人[92]给出了 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 中数目为 $d^3-8(\lfloor\frac{d-3}{2}\rfloor+1)$ 的不可扩充乘积基。

不可扩充乘积基有一些不存在性结果。Feng[37]证明了 $\mathbb{C}^2\otimes\mathbb{C}^n$ 中不存在非平凡的不可扩充乘积基。而 Chen 等人[93]证明了 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中数目为 $d_1d_2\cdots d_N-1$，$d_1d_2\cdots d_N-2$，$d_1d_2\cdots d_N-3$ 的不可扩充乘积基是不存在的。在另一篇文章中，Chen 等人[94]证明了 $(\mathbb{C}^2)^{\otimes N}$ 中不存在数目为 2^N-5 的不可扩充乘积基。当 k 为偶数时，Zhang 等人[90]则证明了 $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^k$ 中数目为 $k+3$ 的不可扩充乘积基是不存在的。当 N 为奇数时，Johnston[35]证明了 $(\mathbb{C}^2)^{\otimes N}$ 中不存在数目为 $N+2$ 的不可扩充乘积基。

关于不可扩充乘积基，文献[39]提出了以下公开问题。

问题 1： 当 $m \geqslant 3$ 为偶数时，是否可以将文献[39]中的不可扩充乘积的构造推广到 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中?

本文将在第三章回答问题 1。

1.2.2　强量子非局域性

2019 年, Halder 等人[43]提出了强量子非局域性的概念, 他们在 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 和 $\mathbb{C}^4 \otimes \mathbb{C}^4 \otimes \mathbb{C}^4$ 中分别构造了强非局域的正交乘积基。对于 $d \geqslant 3$, Yuan 等人[95]在 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ 和 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^{d+1}$ 中分别构造了数目为 $6(d-1)^2$ 和 $6d^2 - 8d + 4$ 的强非局域的正交乘积集，并在 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 和 $\mathbb{C}^4 \otimes \mathbb{C}^4 \otimes \mathbb{C}^4 \otimes \mathbb{C}^4$ 中分别构造了强非局域的正交乘积基[95]。当 $d \geqslant 3$ 为奇数（偶数）时，利用图的连通性，Li 等人[96]在 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ 中构造了数目为 $d^3 - (d-2)^2$（$d^3 - (d-2)^2 + 2$）的强非局域的正交真实纠缠集。

强量子非局域性的概念也被推广了。基于给定划分下的局部不可约性, Zhang 等人[97]给出了更一般的强量子非局域性, 并在 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 和 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 中给出了几个例子。Sumit 等人[98]提出了真实非局域性的概念，一组正交态如果在任意两体划分下都是局部不可区分的，那么它被称为真实非局域的，强非局域性一定能推出真实非局域性，反之则不然，他们对于真实非局域性也给出了具体的分类。在另外一篇文章[99]中，Sumit 等人给出了几例多体系统中的真实非局域的正交乘积集，并研究了他们的纠缠辅助区分。与此同时，对于 $N \geqslant 3$，$d_i \geqslant 3$ 和 $1 \leqslant i \leqslant N$，Li 等人[100]构造了 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中真实非局域的正交乘积集。至于纠缠集，对于 $N \geqslant 3$ 和 $d \geqslant 3$，Zhang 等人[101]在 $(\mathbb{C}^d)^{\otimes N}$ 中给出了真实非局域的正交纠缠集。

关于强量子非局域性，文献[43]提出了以下公开问题。

问题 2：

(i) 对于任何 $N \geqslant 4$，$d \geqslant 3$，如何构造 $(\mathbb{C}^d)^{\otimes N}$ 中强非局域的正交乘积集?

(ii) 是否存在强非局域的不可扩充乘积基?

(iii) 是否存在强非局域的正交纠缠集?

本文将在第四章回答问题 2。

1.2.3　k-均匀态

2004 年, Scott[51]提出了 k-均匀态的概念。Bell 态和 GHZ（Greenberger–Horne–Zeilinger）态均是 1-均匀态，由于任意 N 体齐次系统中的 GHZ 态都存在，对于 $d \geqslant 2$ 和 $N \geqslant 2$，$(\mathbb{C}^d)^{\otimes N}$ 中都存在 1-均匀态。Goyeneche 等人[52]建立了正交阵列与齐次系统中的 k-均匀态之间的关系，对于 $N \geqslant 6$，他们利用正交阵列构造了

$(\mathbb{C}^2)^{\otimes N}$ 中的 2-均匀态。当 $d \geqslant 2$ 为素数幂且 $N \geqslant 4$ 时，Li 等人[54]也利用正交阵列构造了 $(\mathbb{C}^d)^{\otimes N}$ 中的 2-均匀态；当 $N \geqslant 8$ 且 $N \neq 9$ 时，他们构造了 $(\mathbb{C}^2)^{\otimes N}$ 中的 3-均匀态。利用对称矩阵和经典纠错码，Feng 等人[53]构造了一系列齐次系统中的 k-均匀态。基于具有明确的最小汉明距离的正交阵列，Pang 等人[55]构造了几乎所有 $(\mathbb{C}^d)^{\otimes N}$ 中的 $2,3$-均匀态。在表1.1中，我们列出了 $(\mathbb{C}^d)^{\otimes N}$ 中 $1,2,3$-均匀态的存在情况。

表 1.1　齐次系统 $(\mathbb{C}^d)^{\otimes N}$ 中 $1,2,3$-均匀态的存在情况。

$(\mathbb{C}^d)^{\otimes N}$	存在性	不存在性	未知	参考文献
1-均匀态	$d \geqslant 2, N \geqslant 2$	无	无	[52]
2-均匀态	$d \geqslant 2, N \geqslant 4$ 除去 $d = 2, N = 4$	$d = 2,$ $N = 4$	无	[51-52,54-55,77,102-103]
3-均匀态	$d \geqslant 2, N \geqslant 6,$ 除去 $d = 2 \pmod 4,$ $N = 7$	$d = 2,$ $N = 7$	$d \geqslant 6,$ $d = 2 \pmod 4,$ $N = 7$	[54-55,63,77,104-105]

当 $k = \lfloor \frac{N}{2} \rfloor$ 时，$(\mathbb{C}^d)^{\otimes N}$ 中的 k-均匀态被称为绝对最大纠缠态，并记为 AME(N,d)。Scott[51]给出了 AME(N,d) 存在的一个必要条件：当 N 为偶数时，$N \leqslant 2(d^2-1)$；当 N 为奇数时，$N \leqslant 2d(d+1)-1$。利用影子不等式和量子纠错码，Rains[62]证明了如果 AME$(N,2)$ 存在，那么有 $N = 2,3,4,5,6,7$。当 $N = 2,3,5,6$ 时，AME$(N,2)$ 已被找到[52]；当 $N = 4$ 时，AME$(4,2)$ 被证明不存在[102]；当 $N = 7$ 时，Huber 等人[63]证明了 AME$(7,2)$ 不存在。所以 AME$(N,2)$ 存在当且仅当 $N = 2,3,5,6$。当 $d = 3,4,5$ 时，Huber 等人[106]利用影子不等式给出了一些 AME(N,d) 的不存在性结果。AME$(4,6)$ 的存在性已成为一个公开的问题[65]，它与正交量子拉丁方有关。最近 Rather 等人[103]解决了这一公开问题，找到了 AME$(4,6)$。Huber 等人[64]给出了一张关于 AME(N,d) 的存在性表格，根据这张表格，当 $d \geqslant 3$ 时，还有很多 AME(N,d) 的存在性是未知的。

k-均匀态和绝对最大纠缠态的概念也可以直接被推广到非齐次系统 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中[107-108]。Bryan 等人[109-110]借助于几何不变量理论给出了非齐次系统中存在 1-均匀态的充要条件，并构造了一些 1-均匀态。利用混合正交阵列，Goyeneche 等人[107]构造了一些 N 体非齐次系统中的 $1,2$-均匀态。Shen 等人[108]构造了一些 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3}$ 中的绝对最大纠缠态。

关于 k-均匀态，文献[107]提出了以下公开问题。

问题 3：非齐次系统中是否存在 3-均匀态?

本文将在第五章回答问题 3。

1.2.4　量子信息掩盖

2018 年，Modi 等人[89]提出了量子信息掩盖的概念。这是一个物理过程，它将 $\mathbb{C}^d$ 中的量子态通过等距线性算子映射到 $\mathbb{C}^d \otimes \mathbb{C}^{d_1}$ 中，使得映射后的态的单体约化密度算子都相等。Modi 等人给出了一个不可掩盖定理，即 $\mathbb{C}^d$ 中的所有态不能被掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^{d_1}$ 中。利用正交拉丁方，当 $d > 2$ 且 $d \neq 6$ 时，Li[111]等人证明了 $\mathbb{C}^d$ 中的所有态可以被掩盖到 $(\mathbb{C}^d)^{\otimes 3}$ 中。Han 等人[112]利用量子纠错码证明了 $\mathbb{C}^2$ 中的所有态不能被掩盖到 $(\mathbb{C}^2)^{\otimes 3}$ 中。Li 等人[113]表明了 $\mathbb{C}^d$ 中一组相互正交的态可以被掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^d$ 中，并证明了 $\mathbb{C}^d$ 中一组线性无关的态可以被概率性地掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^d$ 中。Liang 等人[114]研究了非零线性算子下的量子信息掩盖，主要是将 $\mathbb{C}^2$ 中的量子态通过非零线性算子映射到 $\mathbb{C}^2 \otimes \mathbb{C}^2$ 中，使得映射后的态的单体约化密度算子都相等，并且他们证明了 $\mathbb{C}^2$ 中具有非零测度的集合都不能在非零线性算子下进行掩盖。之后 Liang 等人[115]也证明了 $\mathbb{C}^d$ 中具有非零测度的集合都不能在等距线性算子下被掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^{d_1}$ 中，并说明了可掩盖的集合必须落在某些欧几里得空间中的球面上。Li 等人[116]研究了另一种概率性的量子信息掩盖，即在完全正定且迹下降（completely positive and trace-decreasing）的线性算子下的量子信息掩盖，并证明了 $\mathbb{C}^d$ 中的所有量子态不能被概率性地掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^{d_1}$ 中。Lv 等人[117]研究了非 Hermitian 系统中的量子信息掩盖，证明了 $\mathbb{C}^d$ 中任意一组相互正交的态都可以被掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^{d_1}$ 中，而 $\mathbb{C}^d$ 中的所有态不能被掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^{d_1}$ 中。最近，Liu 等人[118]给出了量子信息掩盖的光学实现。

关于量子信息掩盖，文献[111]提出了以下问题。

问题 4：

(i) 是否能将 $\mathbb{C}^d$ 中所有态掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ 中，使得掩盖后的态的单体约化密度算子不等于 $\frac{1}{d}\mathbb{I}_d$？

(ii) 是否能将 $\mathbb{C}^d$ 中所有态掩盖到 $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$ 中，使得 $n < d$？

本文将在第五章回答问题 4。

1.3　论文的研究内容与创新点

本文首先研究不可扩充乘积基的构造，并研究其纠缠辅助区分。其次本文研究强量子非局域性，并给出一些强非局域的正交集。最后本文研究非齐次系统中的 k-均匀态与 k-均匀量子信息掩盖。本文主要的工作与创新点有以下三个方面：

第一，建立了多维超立方体与不可扩充乘积基之间的关系。虽然目前在构造较小数目的不可扩充乘积基方面有了很多结果，但在构造较大数目的不可扩充乘积基方面进展较少，且缺少直观的结构。本文中，利用多维超立方体的分解，我们给出了具有较大数目的不可扩充乘积基的构造方法。针对两体系统中的不

可扩乘积基，虽然目前可以用砖块结构来构造，但是并不清楚砖块结构与不可扩乘积基的直接联系。本文中，我们给出了砖块结构对应两体系统中的不可扩充乘积基的一个充分必要条件，根据这个条件我们构造了一系列两体系统中具有较大数目的不可扩充乘积基。此外，我们给出了三维和四维超立方体的分解方案，并利用这个方案巧妙地构造了三体和四体系统中的不可扩充乘积基。由于我们的不可扩充乘积基具有直观的结构，也可以研究其它性质，如纠缠辅助区分和强量子非局域性。

第二，建立了多维超立方体与强量子非局域性之间的关系。目前关于强量子非局域性的研究主要集中于构造强非局域的正交集，而验证一个 N 体系统中的正交集具有强量子非局域性，需要验证作用在其任意 $N-1$ 体子系统上面的正交保持的局部测量是平凡的。这里有两个难点，当 N 较大时，这意味着我们需要验证 N 个 $N-1$ 体子系统具有这个性质；当态的个数较多时，我们很难验证正交保持的局部测量是平凡的。因此，目前只有少量的三体和四体系统中的强非局域的正交乘积集。本文中，为了克服第一个难点，我们利用前面提到的多维超立方体的分解来构造正交集，这个正交集在子系统的循环置换下有相同的结构，这样我们只用验证其中一个 $N-1$ 体子系统上面的正交保持的局部测量是平凡的。为了克服第二个难点，我们给出了两个工具来验证正交保持的局部测量是平凡的。基于多维超立方体的分解和这两个工具，我们给出了一系列多体系统中强非局域的正交乘积集、不可扩充乘积基和正交纠缠集。

第三，建立了量子纠错码与量子信息掩盖之间的关系，给出了非齐次系统中 $2,3$-均匀态的具体构造。目前齐次系统中的 k-均匀态和绝对最大纠缠态的结果有很多，但越来越多的实验开始着重实现非齐次系统中的纠缠态，这使得研究非齐次系统中的 k-均匀态和绝对最大纠缠态更有意义。非齐次系统比齐次系统更加复杂，需要引入更多的数学工具。本文中，我们利用混合正交阵列构造了一系列非齐次系统中的 $2,3$-均匀态，此外我们利用影子不等式，给出了一些非齐次系统中的绝对最大纠缠态的不存在性结果。目前的量子信息掩盖使得掩盖后任何单体子系统不能获取原来的信息，但是如果其中几个子系统共谋，那么可能会获取掩盖前的信息。为了提高信息的安全性，我们在本文中提出了 k-均匀量子信息掩盖的概念，在这种掩盖之下，即使其中任意 k 个子系统共谋，都无法获取掩盖前的信息。我们建立了 k-均匀量子信息掩盖与量子纠错码之间的关系，基于这个关系，我们证明了不可掩盖定理是量子纠错码的量子 Singleton 界的一个特例，并给出了一个更一般的不可掩盖定理。此外，我们还证明了齐次系统中的 k-均匀态可用于 k-均匀量子信息掩盖。

1.4　论文结构安排和主要结论

在图1.3中我们给出了本学位论文体系结构。本论文一共分为 6 章，各章的内容具体如下。

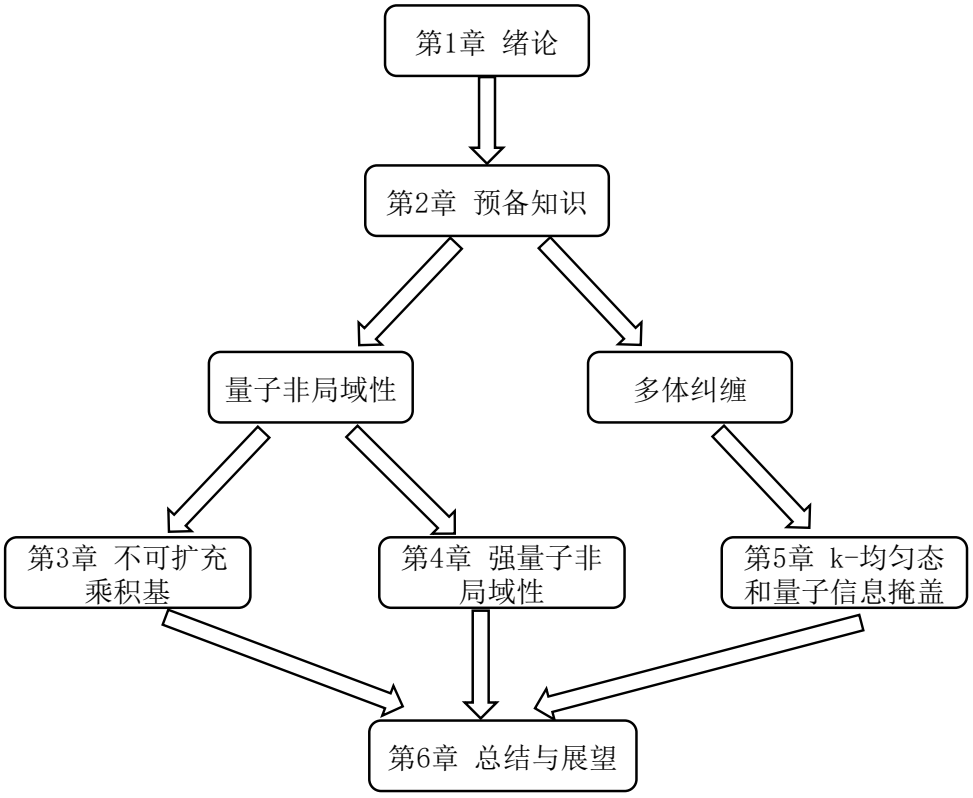

图 1.3　本学位论文体系结构。

第 1 章 绪论。我们介绍了研究背景，说明了量子非局域性与多体纠缠在信息安全中的应用，阐述了国内外研究现状、创新点和本学位论文体系结构。

第 2 章 预备知识。我们首先介绍了齐次系统和非齐次系统的概念，其次介绍了乘积态和纠缠态的概念，最后介绍了态的区分和局部区分的概念。这些概念将为后面的研究奠定基础。

第 3 章 不可扩充乘积基。

表 1.2　第 3 章中的不可扩充乘积基，其中 $3 \leqslant d_A \leqslant d_B \leqslant d_C \leqslant d_D$。

系统	条件	数目	定理
$\mathbb{C}^m \otimes \mathbb{C}^n$	$3 \leqslant m \leqslant n$	$mn - 4\lfloor\frac{m-1}{2}\rfloor$	引理3.2
	$4 \leqslant m \leqslant n, 4 \leqslant k \leqslant 2m-1$	$mn - k$	引理3.3
	$3 \leqslant m \leqslant n$	$mn - 4$	引理3.3
$\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_C}$	$0 \leqslant n \leqslant \lfloor\frac{d_A-3}{2}\rfloor$	$d_A d_B d_C - 8(n+1)$	定理3.5
$\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_C} \otimes \mathbb{C}^{d_D}$	$0 \leqslant n \leqslant \lfloor\frac{d_A-3}{2}\rfloor$	$d_A d_B d_C d_D - 16(n+1)$	定理3.7

首先我们建立了两体系统中的不可扩充乘积基与砖块结构之间的关系，利

用这个关系，我们构造了两体系统中一系列较大数目的不可扩充乘积基，由此回答了问题 1。其次我们将这种方法推广到了多体系统，即利用多维超立方体的分解来构造多体系统中的不可扩充乘积基，并成功地构造了三体和四体系统中的不可扩充乘积基。最后我们也研究了两体系统中的不可扩充乘积基的纠缠辅助区分。其主要结论见表1.2。

第 4 章 强量子非局域性。我们给出了证明强量子非局域性的有效方法，基于这种方法和多维超立方体的分解，我们构造出了一系列三、四、五体系统中强非局域的正交集。最后我们利用循环置换群作用，给出了 N 体齐次系统中强非局域的正交纠缠集。因此我们回答了问题 2。其主要结论见表1.3。

表 1.3　第 4 章中的强非局域的正交集，其中 $d_1, d_2, d_3, d_4, d_5 \geqslant 3$，$3 \leqslant d_A \leqslant d_B \leqslant d_C \leqslant d_D$，$0 \leqslant n \leqslant \lfloor \frac{d_A-3}{2} \rfloor$。

强非局域的正交集	系统	数目	定理
正交乘积集	$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3}$	$\prod_{i=1}^{3} d_i - \prod_{i=1}^{3}(d_i-2)$	定理4.4
	$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3} \otimes \mathbb{C}^{d_4}$	$\prod_{i=1}^{4} d_i - \prod_{i=1}^{4}(d_i-2)$	定理4.5
	$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3} \otimes \mathbb{C}^{d_4} \otimes \mathbb{C}^{d_5}$	$\prod_{i=1}^{5} d_i - \prod_{i=1}^{5}(d_i-2)$	定理4.6
不可扩充乘积基	$\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_C}$	$d_A d_B d_C - 8(n+1)$	定理4.8
	$\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_C} \otimes \mathbb{C}^{d_D}$	$d_A d_B d_C d_D - 16(n+1)$	定理4.10
正交纠缠集	$\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$，$d \geqslant 3$	$6(d-1)^2$	定理4.14
	$(\mathbb{C}^d)^{\otimes N}$，$d \geqslant 2$，$N \geqslant 3$	$d^N - (d-1)^N + 1$	定理4.16
正交真实纠缠集	$\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$，$d \geqslant 2$	$d^3 - (d-1)^3 + 1$	引理4.17
	$\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$，$d \geqslant 2$	$d^4 - (d-1)^4 + 1$	定理4.18

第 5 章 k-均匀态和量子信息掩盖。首先我们利用混合正交阵列，构造了一系列非齐次系统中的 2, 3-均匀态，并利用影子不等式给出了一些非齐次系统中的绝对最大纠缠态的不存在性结果。因此我们回答了问题 3。主要结论见表1.4。

表 1.4　非齐次系统 $(\mathbb{C}^d)^{\otimes N} \otimes (\mathbb{C}^2)^{\otimes t}$ 中 2, 3-均匀态的存在情况与非齐次系统中绝对最大纠缠态的不存在性情况。注意“-”表示是不清楚的。

$(\mathbb{C}^d)^{\otimes N} \otimes (\mathbb{C}^2)^{\otimes t}$	存在性	不存在性	定理
2-均匀态	$d \geqslant 2, t = 1, N \geqslant 5$	-	定理5.7
	$d \geqslant 2, t = 2, N \geqslant 7$	-	定理5.7和引理5.20(2)
3-均匀态	$d = 3, n \geqslant 1, 0 \leqslant N \leqslant 4^n$, $7 \times 36^n + 4 \leqslant t \leqslant 9 \times 36^n$	-	定理5.9
	$d = 5, n \geqslant 1, 0 \leqslant N \leqslant 6^n$, $5 \times 100^n + 4 \leqslant t \leqslant 6 \times 100^n$	-	定理5.9
绝对最大纠缠态	-	表5.2	引理5.12和计算机搜索

其次我们提出了 k-均匀量子信息掩盖的概念，建立了非齐次系统中的量子

纠错码与 k-均匀量子信息掩盖之间的关系。最后我们给出了几种从已知的非齐次系统中的量子纠错码构造新的量子纠错码的方法。主要结论为以下定理。

定理 1.1　如果 $\mathbb{C}^{d_0}$ 中所有态能够被 k-均匀地掩盖到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中，那么一定存在一个参数为 $((N,d_0,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码，反之亦然。此外，如果所有掩盖后的态都是 k-均匀态，那么这个量子纠错码是纯量子纠错码，反之亦然。

根据定理1.1，我们对问题 4 中的两个问题给予了否定回答。

第 6 章 总结与展望。我们总结前面所有的研究内容，并给出了之后的研究方向。

第 2 章　预 备 知 识

本章将介绍量子信息理论中的基本概念。2.1 节介绍了齐次系统与非齐次系统，并介绍了乘积态与纠缠态。2.2 节介绍了态的区分与局部区分。2.3 节为本章小结。

2.1　乘积态与纠缠态

首先，我们给出几个符号说明。我们记 $\mathbb{Z}_d := \{0, 1, \cdots, d-1\}$，$\mathbb{C}^d$ 为 d 维 Hilbert 空间，$w_n := e^{\frac{2\pi i}{n}}$，$\mathbb{I}$ 为单位算子，$\mathbb{Z}_d^N := \mathbb{Z}_d \times \mathbb{Z}_d \times \cdots \times \mathbb{Z}_d$，$(\mathbb{C}^d)^{\otimes N} := \mathbb{C}^d \otimes \mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d$，其中 $\mathbb{Z}_d$ 和 $\mathbb{C}^d$ 分别重复 N 次。

一个单体量子系统可以由一个 Hilbert 空间 $\mathcal{H}$ 来刻画，如果这个 $\mathcal{H}$ 的维数为 d，那么我们通常记 $\mathcal{H} := \mathbb{C}^d$。一个 N 体量子系统可以由 Hilbert 空间 $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_N}$ 来刻画，假设 $\mathcal{H}_{A_i}$ 的维数为 d_i，那么我们记 $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_N} := \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$。如果 $d_1, d_2, \cdots, d_N$ 不全相等，那么我们把 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 称为非齐次系统；如果 $d_1 = d_2 = \cdots = d_N = d$，那么我们记 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 为 $(\mathbb{C}^d)^{\otimes N}$，且称 $(\mathbb{C}^d)^{\otimes N}$ 为齐次系统，d 为局部维数。

$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个标准化的列向量被称为一个纯态，用符号 $|\psi\rangle$ 表示，有时候也用 $|\psi\rangle_{A_1 A_2 \cdots A_N}$ 表示。由于本文只考虑纯态，如果没有特殊说明，本文所有的态都指的是纯态。$\langle\psi|$ 表示 $|\psi\rangle$ 的转置共轭，而对于两个态 $|\psi\rangle$ 和 $|\phi\rangle$，$\langle\psi|\phi\rangle$ 表示 $|\psi\rangle$ 与 $|\phi\rangle$ 的内积。对于 $1 \leqslant i \leqslant N$，如果存在 $|\psi_i\rangle \in \mathbb{C}^{d_i}$，使得

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_N\rangle,$$

那么 $|\psi\rangle$ 被称为 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个乘积态。我们通常会省略 $|\psi\rangle$ 中的 “$\otimes$” 符号，即 $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle \cdots |\psi_N\rangle$。有时候为了表明 $|\psi_i\rangle \in \mathcal{H}_{A_i}$，我们也会将 $|\psi\rangle$ 表示为 $|\psi\rangle = |\psi_1\rangle_{A_1}|\psi_2\rangle_{A_2} \cdots |\psi_N\rangle_{A_N}$。如果 $|\psi\rangle$ 不是乘积态，那么 $|\psi\rangle$ 被称为 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个纠缠态。对于两个乘积态 $|\psi\rangle = |\psi_1\rangle_{A_1}|\psi_2\rangle_{A_2} \cdots |\psi_N\rangle_{A_N}$ 和 $|\phi\rangle = |\phi_1\rangle_{A_1}|\phi_2\rangle_{A_2} \cdots |\phi_N\rangle_{A_N}$，他们的内积有

$$\langle\psi|\phi\rangle = \prod_{i=1}^{N} \langle\psi_i|\phi_i\rangle_{A_i}.$$

如果 $\{|i\rangle\}_{i\in\mathbb{Z}_d}$ 是 $\mathbb{C}^d$ 中的一组标准正交基，那么我们把 $\{|i\rangle\}_{i\in\mathbb{Z}_d}$ 称为 $\mathbb{C}^d$ 的一组计算基。对于任何 $1 \leqslant s \leqslant N$，假设 $\{|i_s\rangle\}_{i_s\in\mathbb{Z}_{d_s}}$ 是 $\mathbb{C}^{d_s}$ 的一组计算基，则 $\{|i_1\rangle|i_2\rangle \cdots |i_N\rangle\}_{(i_1,i_2,\cdots,i_N)\in\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_N}}$ 是 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一组计算基，有时候我们也会将 $|i_1\rangle|i_2\rangle \cdots |i_N\rangle$ 记为 $|i_1 i_2 \cdots i_N\rangle$。对于任意的 $|\psi\rangle \in$

$\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$，$|\psi\rangle$ 可以表示为

$$|\psi\rangle=\sum_{\mathbf{u}\in\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_N}}a_{\mathbf{u}}|\mathbf{u}\rangle,\quad a_{\mathbf{u}}\in\mathbb{C}.$$

两体系统中的态有比较直接的方法来判断其是乘积态还是纠缠态。假设 $\{|i\rangle_A\}_{i\in\mathbb{Z}_m}$ 和 $\{|j\rangle_B\}_{j\in\mathbb{Z}_m}$ 分别是 $\mathbb{C}^m$ 和 $\mathbb{C}^n$ 中的一组计算基，则两体系统 $\mathbb{C}^m\otimes\mathbb{C}^n$ 中的任意一个态 $|\psi\rangle$ 都可以写成

$$|\psi\rangle=\sum_{i\in\mathbb{Z}_m,j\in\mathbb{Z}_n}m_{i,j}|i\rangle_A|j\rangle_B,\quad m_{i,j}\in\mathbb{C},$$

那么 $|\psi\rangle$ 与一个 $m\times n$ 的矩阵 $\boldsymbol{M}=(m_{i,j})_{i\in\mathbb{Z}_m,j\in\mathbb{Z}_n}$ 一一对应。我们记

$$\mathrm{rank}(|\psi\rangle):=\mathrm{rank}(\boldsymbol{M}),$$

其中 $\mathrm{rank}(|\psi\rangle)$ 也被称为 $|\psi\rangle$ 的施密特秩。如果 $\mathrm{rank}(|\psi\rangle)=1$，那么 $|\psi\rangle$ 是一个乘积态；如果 $\mathrm{rank}(|\psi\rangle)\geqslant 2$，那么 $|\psi\rangle$ 是一个纠缠态。如果 $m\leqslant n$，且 $\boldsymbol{M}$ 的奇异值为 $\left\{\frac{1}{\sqrt{m}},\frac{1}{\sqrt{m}},\cdots,\frac{1}{\sqrt{m}}\right\}$（$\frac{1}{\sqrt{m}}$ 出现 m 次），那么此时 $|\psi\rangle$ 被称为 $\mathbb{C}^m\otimes\mathbb{C}^n$ 中的一个最大纠缠态。例如，$\mathbb{C}^2\otimes\mathbb{C}^2$ 中的 Bell 态 $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)$ 对应于矩阵 $\boldsymbol{M}=\begin{pmatrix}\frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}}\end{pmatrix}$，那么 Bell 态是最大纠缠态。假设 $|\psi_i\rangle$ 对应一个矩阵 $\boldsymbol{M}_i$，其中 $i=1,2$，那么

$$\langle\psi_1|\psi_2\rangle=\mathrm{Tr}(\boldsymbol{M}_1^\dagger\boldsymbol{M}_2).$$

对于多体系统 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的态 $|\psi\rangle$，我们可以考虑态的两体划分。例如我们考虑两体划分 $A_1|A_2\cdots A_N$，这意味我们把 $N-1$ 体系统 $\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 看成一个单体系统 $\mathbb{C}^{d_2\cdots d_N}$，此时 $|\psi\rangle$ 就可以被看成两体系统 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2\cdots d_N}$ 中的一个态。对于多体系统 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的态 $|\psi\rangle$，如果它在任意两体划分下都是纠缠态，那么 $|\psi\rangle$ 被称为真实纠缠态。最著名的两个真实纠缠态分别是 GHZ 态和 W 态。一个局部维数为 d 的 N 体 GHZ 态可以表示为

$$|\,\mathrm{GHZ}\rangle_d^N=\sum_{i\in\mathbb{Z}_d}|i\rangle_{A_1}|i\rangle_{A_2}\cdots|i\rangle_{A_N}.$$

一个局部维数为 2 的 N 体 W 态可以表示为

$$|W\rangle_2^N=|1\rangle_{A_1}|0\rangle_{A_2}\cdots|0\rangle_{A_N}+|0\rangle_{A_1}|1\rangle_{A_2}\cdots|0\rangle_{A_N}+\cdots+|0\rangle_{A_1}|0\rangle_{A_2}\cdots|1\rangle_{A_N}.$$

对于 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个态集合 $\mathcal{S}:=\{|\psi_i\rangle\}$，如果其中任意两个态都相互正交，那么 $\mathcal{S}$ 被称为一个正交集。如果正交集 $\mathcal{S}$ 中每个态都是乘积态，那么 $\mathcal{S}$ 被称为一个正交乘积集；如果正交集 $\mathcal{S}$ 中每个态都是纠缠态，那么 $\mathcal{S}$ 被称为一个正交纠缠集；如果正交集 $\mathcal{S}$ 中每个态都是真实纠缠态，那么 $\mathcal{S}$ 被称为一个正交真实纠缠集。我们记 $|\mathcal{S}|$ 为 $\mathcal{S}$ 中态的数目。

2.2　态的局部区分

假设 Alice 被给予一个态集 $\mathcal{E}=\{|\psi_i\rangle\}_{i=1}^N$，她不知道里面每个态的身份，只知道整个集合 $\mathcal{E}$，她想通过测量来区分出每个态的身份，这个过程被称为态的区分。如果 Alice 能够区分出 $\mathcal{E}$ 中的每个态的身份，那么这个 $\mathcal{E}$ 是可区分的，反之则是不可区分的。$\mathcal{E}$ 可以区分当且仅当 $\mathcal{E}$ 是一个正交集[59]。

Hilbert 空间 $\mathcal{H}$ 上的正算子值测量（POVM）是一组半正定算子 $\{E_m=M_m^\dagger M_m\}$，且满足 $\sum_m E_m=\mathbb{I}_{\mathcal{H}}$，其中每个 E_m 被称为一个 POVM 元素，$\mathbb{I}_{\mathcal{H}}$ 是 $\mathcal{H}$ 上的单位算子。本文中的测量均指 POVM 。如果一个测量的所有 POVM 元素都与单位算子成比例，那么该测量是平凡的。否则，该测量是非平凡的。对集合 $\mathcal{E}$ 进行一个测量 $\{M_m^\dagger M_m\}$，对于其中一个 m，测量后的态变为

$$\left\{\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}\right\}.$$

有时候我们会忽略标准化向量，直接用 $\{M_m|\psi\rangle\}$ 表示测量后的态集合。对于任意的 m，如果测量后的态是相互正交的，那么这个测量被称为正交保持的测量。

对于正交集 $\mathcal{E}=\{|\psi_i\rangle\}_{i=1}^N$，Alice 可以进行测量 $E=\{|\psi_1\rangle\langle\psi_1|,|\psi_2\rangle\langle\psi_2|,\cdots,|\psi_N\rangle\langle\psi_N|,\mathbb{I}-\sum_{i=1}^N|\psi_i\rangle\langle\psi_i|\}$，此时注意 $|\psi_i\rangle\langle\psi_i|=(|\psi_i\rangle\langle\psi_i|)^\dagger|\psi_i\rangle\langle\psi_i|$，如果 Alice 点击测量算子 $|\psi_i\rangle\langle\psi_i|$，那么测量之后的态变为

$$|\psi_i\rangle\langle\psi_i|(|\psi_i\rangle)=|\psi_i\rangle;$$
$$|\psi_i\rangle\langle\psi_i|(|\psi_j\rangle)=0,\quad j\neq i,$$

那么 Alice 可以区分出 i。如果 Alice 点击其它测量算子（除 $\mathbb{I}-\sum_{i=1}^N|\psi_i\rangle\langle\psi_i|$ 之外），那么 Alice 会相应地区分出其它态。从而 $\mathcal{E}$ 是可区分的。

现在假设 Alice 和 Bob 分享同一个两体量子系统，他们被给予一组量子态 $\mathcal{F}=\{|\psi_i\rangle_{AB}\}_{i=1}^N$，且不知道每个态的具体身份，只知道整个集合 $\mathcal{F}$，Alice 和 Bob 只能进行局部测量和打电话的方式交流经典信息（LOCC）。他们通过 LOCC 来区分这组量子态的方式被称为态的局部区分。如果 $\mathcal{F}$ 在 LOCC 下是可以区分的，那么 $\mathcal{F}$ 是局部可区分的，反之则是局部不可区分的。

下面我们来看一个局部可区分的例子。假设 Alice 和 Bob 被给予 $\mathbb{C}^3\otimes\mathbb{C}^3$ 中的一个正交集 $\{|i\rangle_A|j\rangle_B\}_{i\in\mathbb{Z}_3,j\in\mathbb{Z}_3}$，那么区分过程如下：

步骤 1 Alice 进行一个测量 $\{|i\rangle_A\langle i|\}_{i\in\mathbb{Z}_3}$。如果 Alice 点击其中一个 $|s\rangle_A\langle s|$，那么测量后的态变为

$$\{|s\rangle_A\langle s|\otimes\mathbb{I}_B|i\rangle_A|j\rangle_B\}_{i\in\mathbb{Z}_3,j\in\mathbb{Z}_3}=\{|s\rangle_A|j\rangle_B\}_{j\in\mathbb{Z}_3},$$

然后 Alice 打电话给 Bob 并告诉他她的测量结果是 s（打电话的过程在后面具体区分过程中会省略）。

步骤 2 Bob 进行一个测量 $\{|j\rangle_B\langle j|\}_{j\in\mathbb{Z}_3}$。如果 Bob 点击其中一个 $|t\rangle_B\langle t|$，那么测量后的态变为

$$\{\mathbb{I}_A \otimes |t\rangle_B\langle t||s\rangle_A|j\rangle_B\}_{j\in\mathbb{Z}_3} = |s\rangle_A|t\rangle_B,$$

从而 Bob 能够区分出 $|s\rangle_A|t\rangle_B$。同样，如果 Alice 和 Bob 分别点击其余的测量算子，那么他们会相应地区分出其余 $\{|i\rangle_A|j\rangle_B\}_{i\in\mathbb{Z}_3,j\in\mathbb{Z}_3}$ 中的态。所以 $\{|i\rangle_A|j\rangle_B\}_{i\in\mathbb{Z}_3,j\in\mathbb{Z}_3}$ 是局部可区分的。

给定一个正交集 $\{|\psi\rangle_{AB}\}$，Alice 进行一个局部测量 $\{M_m^\dagger M_m\}$。对于其中任意一个 m，如果测量后的态 $\{M_m\otimes\mathbb{I}_B|\psi\rangle_{AB}\}$ 是相互正交的，那么 $\{M_m^\dagger M_m\}$ 被称为正交保持的局部测量。由于非正交集不能区分，那么在态的局部区分过程中，都是采用的正交保持的局部测量。

如果作用在 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 上的一个算子 $\boldsymbol{P}$ 可以写成

$$\boldsymbol{P} = P_1\otimes P_2\otimes\cdots\otimes P_N,$$

那么 $\boldsymbol{P}$ 被称为 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 上的一个乘积算子。取任意一个子集 $\boldsymbol{A} = \{A_{i_1}, A_{i_2}, \cdots, A_{i_k}\} \subset \{A_1, A_2, \cdots, A_N\}$，不失一般性，假设 $\boldsymbol{A} = \{A_1, A_2, \cdots, A_k\}$，那么 $\boldsymbol{P}$ 在 $\boldsymbol{A}$ 上取偏迹被定义为：

$$\begin{aligned}\mathrm{Tr}_{\boldsymbol{A}}\boldsymbol{P} &:= \mathrm{Tr}(P_1\otimes P_2\otimes\cdots\otimes P_k)P_{k+1}\otimes P_{k+2}\otimes\cdots\otimes P_N\\ &= \left(\prod_{j=1}^{k}\mathrm{Tr}\,P_j\right)P_{k+1}\otimes P_{k+2}\otimes\cdots\otimes P_N.\end{aligned}$$

2.3　本章小结

本章首先介绍了齐次系统和非齐次系统的概念，接着介绍了乘积态和纠缠态概念，最后介绍了态的区分和局部区分的概念。这些概念将为后面的研究奠定基础。

第 3 章　不可扩充乘积基

不可扩充乘积基表明了无纠缠的量子非局域性现象，从而可以保障量子通信的安全性。本章将研究多体系统中的不可扩充乘积基与纠缠辅助区分。3.1 节介绍了不可扩充乘积基和纠缠辅助区分的背景和研究进展。3.2 节介绍了砖块结构。3.3 节给出了砖块结构与两体系统中不可扩充乘积基的对应关系，并利用砖块结构构造了两体系统中一系列较大数目的不可扩充乘积基。3.4 节构造了三体系统中的不可扩充乘积基。3.5 节构造了四体系统中的不可扩充乘积基。3.6 节研究了两体系统中不可扩充乘积基的纠缠辅助区分。3.7 节为本章小结。

3.1　引言

不可扩充乘积基指的是多体系统中的一个正交乘积集（非正交乘积基），其生成的子空间的正交补空间中没有乘积态。它在量子信息中扮演着重要的角色，可以用来构造束缚纠缠态[30]，其构造方法如下：给定 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中的一个不可扩充乘积基 $\{|\psi_i\rangle\}_{i=1}^t$，那么 $\rho = \frac{1}{mn-t}(\mathbb{I} - \sum_{i=1}^t |\psi_i\rangle\langle\psi_i|)$ 是一个束缚纠缠态。不可扩充乘积基还可以表明无纠缠的量子非局域性现象[4,30]，它与费米子系统和无量子违反的 Bell 不等式相关联[31-33]。目前，虽然在构造较小数目的不可扩充乘积基方面有了很多结果[30,34-38]，但在构造较大数目的不可扩充乘积基方面进展较少[4,39-40]。Bennett 等人首先在 $\mathbb{C}^3 \otimes \mathbb{C}^3$ 和 $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中分别构造了数目为 5 和 4 的不可扩充乘积基[30]；利用砖块结构，对于 $n \geqslant 4$，DiVincenzo 等人[4]在 $\mathbb{C}^n \otimes \mathbb{C}^n$ 中给出了数目为 $n^2 - 2n + 1$ 的 GenTiles1 不可扩充乘积基，并对于 $3 \leqslant m \leqslant n$，在 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中给出了数目为 $mn - 2m + 1$ 的 GenTiles2 不可扩充乘积基。利用砖块结构，当 $m \geqslant 3$ 为奇数时，Halder 等人在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中构造了数目为 $(m-1)^2 + 1$ 的不可扩充乘积基[39]，并且他们提出了一个公开问题[39]：当 $m \geqslant 3$ 为偶数时，是否可以将他们的构造推广到 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中？我们将对这一问题给予肯定回答。对于 $d \geqslant 3$，Agrawal 等人[92]利用三维立方体的分解给出了 $(\mathbb{C}^d)^{\otimes 3}$ 中数目为 $d^3 - 8(\lfloor\frac{d-3}{2}\rfloor + 1)$ 的不可扩充乘积基。

如果通过一系列 LOCC 操作不能区分一组多体正交态，那么这组正交态被称为局部不可区分的。虽然不可扩充乘积基是局部不可区分的[4,30,41]，但是可以借助于纠缠辅助区分协议来区分不可扩充乘积基[42]，例如 GenTiles2 不可扩充乘积基可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil} \otimes \mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分[42]；Halder 等人[39]构造的不可扩充乘积基也被证明可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil} \otimes \mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分[119]。纠缠辅助区分吸引了越来越多研究者的关

注[91,120-123]。

3.2　准备工作

本章中，我们只考虑纯态，且不归一化态和算子。对于 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个正交集 $\mathcal{S}$，我们记 span $\mathcal{S}$ 为 $\mathcal{S}$ 生成的子空间。

定义 3.1　假设 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中有一个正交乘积集，它生成一个子空间 $\mathcal{H}$，如果 $\mathcal{H}$ 的正交补空间 $\mathcal{H}^{\perp}$ 中没有乘积态，那么这个正交乘积集被称为 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个*不可扩充乘积基*。

由定义可知，$\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一组正交基一定是 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个不可扩充乘积基，这种不可扩充基是平凡的，本章中只考虑非平凡的不可扩充乘积基，即不可扩充乘积基的数目小于 $d_1d_2\cdots d_N$。

下面我们考虑两体系统 $\mathbb{C}^m\otimes\mathbb{C}^n$。我们定义 $\mathbb{C}^m\otimes\mathbb{C}^n$ 中的*砖块结构*，它是一个由互不相交的砖块 $\{t_i\}$ 铺设而成的 $m\times n$ 矩形 $\mathcal{T}$，我们用 $\mathcal{T}=\cup_i t_i$ 来表示。任意一个砖块 t_i 都是矩形，在我们的符号中，这个矩形的行坐标和列坐标都可以不连续。如图3.1所示，这是 $\mathbb{C}^4\otimes\mathbb{C}^4$ 中的一个砖块结构 $\mathcal{T}=\cup_{i=1}^{6}t_i$，它由 6 个互不相交的砖块铺设而成，其中标有相同数字 i 的网格表示砖块 t_i。接下来我们通过图3.1来构造 $\mathbb{C}^4\otimes\mathbb{C}^4$ 中的数目为 11 的不可扩充乘积基。

		B			
		0	1	2	3
A	0	1	1	2	3
	1	6	4	6	3
	2	6	4	6	3
	3	5	4	2	5

图 3.1　$\mathbb{C}^4\otimes\mathbb{C}^4$ **中的砖块结构，这个砖块结构可以表示为** $\mathcal{T}=\cup_{i=1}^{6}t_i$，**其中标有相同数字** i **的网格表示砖块** t_i。

例 3.1　在图3.1中，砖块 t_1 可以构造 $\mathbb{C}^4\otimes\mathbb{C}^4$ 中的两个正交乘积态：$|0\rangle_A(|0\rangle+|1\rangle)_B$，$|0\rangle_A(|0\rangle-|1\rangle)_B$；砖块 t_2 可以构造 $\mathbb{C}^4\otimes\mathbb{C}^4$ 中的两个正交乘积态 $(|0\rangle+|3\rangle)_A|2\rangle_B$，$(|0\rangle-|3\rangle)_A|2\rangle_B$。同样其它砖块可以构造相应的正交乘积态。对于 $1\leqslant i\neq j\leqslant 6$，由于砖块 t_i 和 t_j 是不相交的，砖块 t_i 构造的乘积态必然与砖块 t_j 构造的乘积态正交。从而我们得到 $\mathbb{C}^4\otimes\mathbb{C}^4$ 中的一组正交乘积基 $\mathcal{B}$：

$$|\psi_1^{(1)}\rangle=|0\rangle_A(|0\rangle+|1\rangle)_B,\quad |\psi_1^{(2)}\rangle=|0\rangle_A(|0\rangle-|1\rangle)_B,$$

$$
\begin{aligned}
&|\psi_2^{(1)}\rangle = (|0\rangle + |3\rangle)_A|2\rangle_B, && |\psi_2^{(2)}\rangle = (|0\rangle - |3\rangle)_A|2\rangle_B,\\
&|\psi_3^{(1)}\rangle = (|0\rangle + |1\rangle + |2\rangle)_A|3\rangle_B, && |\psi_3^{(2)}\rangle = (|0\rangle + w_3|1\rangle + w_3^2|2\rangle)_A|3\rangle_B,\\
&|\psi_3^{(3)}\rangle = (|0\rangle + w_3^2|1\rangle + w_3|2\rangle)_A|3\rangle_B, && |\psi_4^{(1)}\rangle = (|1\rangle + |2\rangle + |3\rangle)_A|1\rangle_B,\\
&|\psi_4^{(2)}\rangle = (|1\rangle + w_3|2\rangle + w_3^2|3\rangle)_A|1\rangle_B, && |\psi_4^{(3)}\rangle = (|1\rangle + w_3^2|2\rangle + w_3|3\rangle)_A|1\rangle_B,\\
&|\psi_5^{(1)}\rangle = |3\rangle_A(|0\rangle + |3\rangle)_B, && |\psi_5^{(2)}\rangle = |3\rangle_A(|0\rangle - |3\rangle)_B,\\
&|\psi_6^{(1)}\rangle = (|1\rangle + |2\rangle)_A(|0\rangle + |2\rangle)_B, && |\psi_6^{(2)}\rangle = (|1\rangle + |2\rangle)_A(|0\rangle - |2\rangle)_B,\\
&|\psi_6^{(3)}\rangle = (|1\rangle - |2\rangle)_A(|0\rangle + |2\rangle)_B, && |\psi_6^{(4)}\rangle = (|1\rangle - |2\rangle)_A(|0\rangle - |2\rangle)_B.
\end{aligned}
$$

我们定义一个“停止态”:

$$|S\rangle = (|0\rangle + |1\rangle + |2\rangle + |3\rangle)_A(|0\rangle + |1\rangle + |2\rangle + |3\rangle)_B,$$

那么我们断言

$$\mathcal{U} = \{|S\rangle\} \cup \mathcal{B} \setminus \{|\psi_i^{(1)}\rangle\}_{i=1}^6$$

是 $\mathbb{C}^4 \otimes \mathbb{C}^4$ 中的一个数目为 11 的不可扩充乘积基。令 $\mathcal{H}$ 为 $\mathcal{U}$ 生成的子空间，对于任何 $|\psi\rangle \in \mathcal{H}^\perp$，我们只需验证 $|\psi\rangle$ 是一个纠缠态。我们采用反证法，假设 $\mathcal{H}^\perp$ 中存在一个乘积态 $|\psi\rangle$。令 $\mathcal{H}_1$ 为 $\mathcal{B} \setminus \{|\psi_i^{(1)}\rangle\}_{i=1}^6$ 生成的子空间，则 $\mathcal{H}_1 \subset \mathcal{H}$，$\mathcal{H}^\perp \subset \mathcal{H}_1^\perp = \text{span}\,\{|\psi_i^{(1)}\rangle\}_{i=1}^6$。那么存在 $a_i \in \mathbb{C}$，$1 \leqslant i \leqslant 6$，使得

$$|\psi\rangle = a_1|\psi_1^{(1)}\rangle + a_2|\psi_2^{(1)}\rangle + a_3|\psi_3^{(1)}\rangle + a_4|\psi_4^{(1)}\rangle + a_5|\psi_5^{(1)}\rangle + a_6|\psi_6^{(1)}\rangle.$$

由于 $|S\rangle \in \mathcal{H}$，$\langle S|\psi\rangle = 0$，这意味着至少有两个非零的 a_i。下面我们考虑态对应的矩阵，$|S\rangle$ 和 $|\psi\rangle$ 分别对应于矩阵

$$J = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad M = \begin{pmatrix} a_1 & a_1 & a_2 & a_3 \\ a_6 & a_4 & a_6 & a_3 \\ a_6 & a_4 & a_6 & a_3 \\ a_5 & a_4 & a_2 & a_5 \end{pmatrix}.$$

由于 $\text{rank}(M) = 1$，我们可以推出 $a_1 = a_2 = a_3 = a_4 = a_5 = a_6 \neq 0$。然而此时 $\text{Tr}(J^\dagger M) \neq 0$, 即 $\langle S|\psi\rangle \neq 0$, 矛盾, 这推出 $|\psi\rangle$ 是一个纠缠态。所以 $\mathcal{U}$ 是 $\mathbb{C}^4 \otimes \mathbb{C}^4$ 中的一个数目为 11 的不可扩充乘积基。

虽然 $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中没有数目为 11 的不可扩充乘积基[94]，但是我们构造了 $\mathbb{C}^4 \otimes \mathbb{C}^4$ 中的一个数目为 11 的不可扩充乘积基，这也说明了四体系统 $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 与两体系统 $\mathbb{C}^4 \otimes \mathbb{C}^4$ 的区别。

从例3.1出发, 我们接下来想探究哪些砖块结构可以构造不可扩充乘积基。出于这个动机，我们在定义3.2中引入了 U-砖块结构。对于 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中的砖块结构

$\mathcal{T}$，令 $T=\cup_{j=1}^{k}t_{i_j}$ $(k\geqslant 2)$，其中 t_{i_j} 是一个砖块。如果 T 是 $\mathcal{T}$ 的子矩形，那么 T 被称为 $\mathcal{T}$ 的一个*特殊矩形*。在图3.2中，t_1 和 t_2 组成一个特殊矩形；t_3 和 t_5 组成一个特殊矩形；t_3，t_4 和 t_5 组成一个特殊矩形等等。但图3.1中的砖块结构只有一个特殊矩形，即它本身 $\cup_{i=1}^{6}t_i$。为方便起见，我们用 R_i 和 C_i 分别表示 t_i 的行坐标和列坐标。例如，图3.2中的 t_1 有行坐标 $\{0\}_A$ 和列坐标 $\{0,1\}_B$，即 $R_1=\{0\}_A$ 和 $C_1=\{0,1\}_B$。现在我们可以定义 U-砖块结构。

	0	1	2	3
0	1	1	2	2
1	3	4	4	3
2	5	4	4	5
3	6	6	6	6

图 3.2　$\mathbb{C}^4\otimes\mathbb{C}^4$ **中的砖块结构**。

定义 3.2　给定一个砖块结构 $\mathcal{T}$，如果 $\mathcal{T}$ 中的任何特殊矩形 T 不能被分割成两个更小的特殊矩形或砖块，那么我们称 $\mathcal{T}$ 为 *U-砖块结构*。

由于所有砖块之间的顺序是无关紧要的，对于 $k\geqslant 2$，我们总是可以假设一个特殊矩形 $T=\cup_{i=1}^{k}t_i$。根据定义3.2，如果 $\mathcal{T}$ 是 U-砖块结构，那么 $\{R_i\}_{i=1}^{k}$（$\{C_i\}_{i=1}^{k}$）不能被划分为两个集合，使得其中一个集合的所有元素都与另一集合的所有元素不相交。例如图3.2 中的砖块结构不是 U-砖块结构，因为特殊矩形 $t_1\cup t_2$ 可以划分为两个砖块。很容易检查出图3.1 是一个 U-砖块结构，因为它只有一个特殊矩形 $\cup_{i=1}^{6}t_i$，其中 $\{C_i\}_{i=1}^{6}=\{\{0,1\}_A,\{2\}_A,\{3\}_A,\{1\}_A,\{0,3\}_A,\{0,2\}_A\}$ 不能划分成没有交叉元素的两个集合，对 $\{R_i\}_{i=1}^{6}$ 也是如此。在下一节中，我们将给出 U-砖块结构与不可扩充乘积基之间的关系。

3.3　两体系统中的不可扩充乘积基

在本节中，我们将研究 U-砖块结构和两体系统中的不可扩充乘积基之间的关系，并通过 U-砖块结构来构造一些具有较大数目的不可扩充乘积基。

定理 3.1　一个具有 s 个砖块的砖块结构对应于 $\mathbb{C}^m\otimes\mathbb{C}^n$ 中数目为 $mn-s+1$ 的不可扩充乘积基当且仅当此砖块结构是 U-砖块结构。

证明　首先，我们证明充分性。假设 U-砖块结构 $\mathcal{T}=\cup_{i=1}^{s}t_i$ 具有行坐标 $\{0,1,\cdots,m-1\}_A$ 和列坐标 $\{0,1,\cdots,n-1\}_B$。对于每个砖块 t_i，令 $R_i=\{r_0,r_1,\cdots,r_{p-1}\}_A$ 和 $C_i=\{c_0,c_1,\cdots,c_{q-1}\}_B$，我们可以构造 pq 个正交乘积态：对

于任何 $k \in \mathbb{Z}_p$ 和 $l \in \mathbb{Z}_q$，令

$$|\phi_i^{(k,l)}\rangle = \left(\sum_{e\in\mathbb{Z}_p} w_p^{ke}|r_e\rangle\right)_A \left(\sum_{e\in\mathbb{Z}_q} w_q^{le}|c_e\rangle\right)_B .$$

记 $\mathcal{B}_i := \{|\phi_i^{(k,l)}\rangle\}_{k\in\mathbb{Z}_p, l\in\mathbb{Z}_q}$，令 $|S\rangle = (\sum_{i\in\mathbb{Z}_m}|i\rangle)_A(\sum_{j\in\mathbb{Z}_n}|j\rangle)_B$ 为停止态，我们断言 $\mathcal{U} = \cup_{i=1}^{s}\left(\mathcal{B}_i \setminus \{|\phi_i^{(0,0)}\rangle\}\right) \cup \{|S\rangle\}$ 是 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中的一个数目为 $mn - s + 1$ 的不可扩充乘积基。

与例3.1分析相同，记 $\mathcal{H}$ 为 $\mathcal{U}$ 生成的子空间，假设 $|\psi\rangle$ 为 $\mathcal{H}^\perp$ 中的乘积态，则存在 $a_i \in \mathbb{C}$，$1 \leqslant i \leqslant s$，(其中至少有两个非零 a_i) 使得

$$|\psi\rangle = \sum_{i=1}^{s} a_i|\phi_i^{(0,0)}\rangle,$$

且 $\langle S|\psi\rangle = 0$。令 M_i 为 $|\phi_i^{(0,0)}\rangle$ 对应的 0-1 矩阵，其非零位置对应于砖块 t_i 的位置，那么 $|\psi\rangle$ 对应于矩阵 $M = \sum_{i=1}^{s} a_i M_i$，其中 a_i 的位置对应于砖块 t_i 的位置。由于 $\mathrm{rank}(M) = 1$，M 的非零项所在的位置必然形成 $\mathcal{T}$ 的特殊矩形，由于 $\mathcal{T}$ 是一个 U-砖块结构，可以推出 M 的所有非零项相等。此时 $\mathrm{Tr}(J^\dagger M) \neq 0$，即 $\langle S|\psi\rangle \neq 0$，矛盾，充分性得证。

下面我们也可以通过反证法来证明必要性。如果 $\mathcal{T}$ 不是一个 U-砖块结构，那么存在一个特殊矩阵 $T = \cup_{i=1}^{k} t_i$, $2 \leqslant k \leqslant s$, 使得 $\{R_i\}_{i=1}^{k}$ 或 $\{C_i\}_{i=1}^{k}$ 可以划分成有交叉元素的两个集合，不失一般性，我们可以假设 $\{C_i\}_{i=1}^{k} = \{C_i\}_{i=1}^{k'} \cup \{C_j\}_{j=k'+1}^{k}$，其中 $C_i \cap C_j = \varnothing$。因此我们可以假设 $\cup_{i=1}^{k'} C_i = \{0, 1, \cdots, \ell - 1\}$，$\cup_{j=k'+1}^{k} C_j = \{\ell, \ell + 1, \cdots, h - 1\}$。现在我们构造一个态 $|\psi\rangle = \sum_{i=1}^{k} a_i|\phi_i^{(0,0)}\rangle$，其中 $a_i = 1$，$1 \leqslant i \leqslant k'$；$a_j = -\frac{\ell}{h-\ell}$，$k' + 1 \leqslant j \leqslant k$。也就是说，$|\psi\rangle$ 对应于一个矩阵 M，其中非零项形成一个子矩阵

$$M' = \begin{pmatrix} 1 & \cdots & 1 & -\frac{\ell}{h-\ell} & \cdots & -\frac{\ell}{h-\ell} \\ 1 & \cdots & 1 & -\frac{\ell}{h-\ell} & \cdots & -\frac{\ell}{h-\ell} \\ \vdots & & \vdots & -\frac{\ell}{h-\ell} & & -\frac{\ell}{h-\ell} \\ 1 & \cdots & 1 & -\frac{\ell}{h-\ell} & \cdots & -\frac{\ell}{h-\ell} \end{pmatrix}.$$

那么 $\mathrm{rank}(M) = 1$ 并且 $\mathrm{Tr}(J^\dagger M) = 0$，这意味着我们可以在 $\mathcal{H}^\perp$ 中找到一个乘积态 $|\psi\rangle$，矛盾，必要性得证。 ∎

在图3.2中，由于此砖块结构不是 U-砖块结构，根据定理3.1可知，它对应的乘积集不是不可扩充乘积基。实际上我们可以找到一个乘积态 $|\psi\rangle = |0\rangle_A(|0\rangle +$

$|1\rangle)-|0\rangle(|2\rangle+|3\rangle)_B \in \mathcal{H}^{\perp}$，$|\psi\rangle$ 对应矩阵 $\boldsymbol{M}=\begin{pmatrix} 1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

当 $m \geqslant 3$ 为奇数时，Halder 等人[39]在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中给出了一个具有 $2m-1$ 个砖块的 U-砖块结构，他们还提出了一个公开问题：是否可以将它们的构造推广到偶数维系统中？下面我们通过在任意两体系统 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中构造 U-砖块结构来回答这个问题。

	0	1	2	$\cdots$	n-3	n-2	n-1
0	1	1	1	$\cdots$	1	1	2
1	4	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\vdots$	2
2	4	$\vdots$	$2m$-3	$\cdots$	$2m$-3	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$2m$-3	$\cdots$	$2m$-3	$\vdots$	2
m-2	4	$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	2
m-1	4	3	3	$\cdots$	3	3	3

图 3.3　当 $m \geqslant 4$ 为偶数时，$\mathbb{C}^m \otimes \mathbb{C}^n$ 中具有 $2m-3$ 个砖块的 U-砖块结构。

	0	1	2	3	$\cdots$	n-4	n-3	n-2	n-1
0	1	1	1	1	$\cdots$	1	1	1	2
1	4	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\vdots$	2
2	4	$\vdots$	$2m$-5	$\cdots$	$2m$-5	$2m$-5	$2m$-4	$\vdots$	2
$\vdots$	$\vdots$	$\vdots$	$2m$-2	$2m$-1	$\cdots$	$2m$-1	$2m$-4	$\vdots$	$\vdots$
m-3	4	$\vdots$	$2m$-2	$2m$-3	$\cdots$	$2m$-3	$2m$-3	$\vdots$	2
m-2	4	$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	2
m-1	4	3	3	3	$\cdots$	3	3	3	3

图 3.4　当 $m \geqslant 3$ 为奇数时，$\mathbb{C}^m \otimes \mathbb{C}^n$ 中具有 $2m-1$ 个砖块的 U-砖块结构。

引理 3.2　对于 $3 \leqslant m \leqslant n$，$\mathbb{C}^m \otimes \mathbb{C}^n$ 中存在一个数目为 $(mn-4\lfloor\frac{m-1}{2}\rfloor)$ 的不可扩充乘积基。

证明　当 $m \geqslant 4$ 为偶数时，我们可以在 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中构造一个具有 $2m-3$ 个砖块的 U-砖块结构，如图3.3所示；当 $m \geqslant 3$ 为奇数时，我们可以在 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中

构造一个具有 $2m-1$ 个砖块的 U-砖块结构，如图3.4所示。根据定理3.1可知，引理得证。 ∎

引理 3.3　对于 $4 \leqslant m \leqslant n$ 和 $4 \leqslant k \leqslant 2m-1$，$\mathbb{C}^m \otimes \mathbb{C}^n$ 中存在一个数目为 $mn-k$ 的不可扩充乘积基。对于 $3 \leqslant m \leqslant n$，$F(m,n) = mn-4$，其中 $F(m,n)$ 是 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中不可扩充乘积基的最大数目。

证明　首先，对于 $m=n$，$m \geqslant 4$ 和 $4 \leqslant k \leqslant 2m-1$，我们在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中构造一个数目为 m^2-k 的不可扩充乘积基。由定理3.1可知，对于 $m \geqslant 4$ 和 $5 \leqslant t \leqslant 2m$，我们只需要在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中构造一个具有 t 个砖块的 U-砖块结构。

1	1	1	2
4	5	5	2
4	5	5	2
4	3	3	3

1	1	6	2
4	5	5	2
4	5	5	2
4	3	6	3

1	1	6	2
7	5	5	7
4	5	5	2
4	3	6	3

1	1	7	8
5	2	2	8
5	6	3	3
4	6	7	4

图 3.5　$\mathbb{C}^4 \otimes \mathbb{C}^4$ **中分别具有** $5,6,7,8$ **个砖块的 U-砖块结构**。

当 $m=4$ 时，我们可以在 $\mathbb{C}^4 \otimes \mathbb{C}^4$ 中分别构造具有 $5,6,7,8$ 个砖块的 U-砖块结构，如图3.5 所示。

1	1	1	2	2
1	1	1	2	2
4	5	5	2	2
4	5	5	2	2
4	3	3	3	3

1	1	6	2	2
1	1	6	2	2
4	5	5	2	2
4	5	5	2	2
4	3	6	3	3

1	1	6	2	2
1	1	6	2	2
7	5	5	7	7
4	5	5	2	2
4	3	6	3	3

图 3.6　$\mathbb{C}^5 \otimes \mathbb{C}^5$ **中分别具有** $5,6,7$ **个砖块的 U-砖块结构**。

1	1	7	8	8
1	1	7	8	8
5	2	2	8	8
5	6	3	3	3
4	6	7	4	4

1	1	7	8	9
1	1	7	8	9
5	2	2	8	9
5	6	3	3	9
4	6	7	4	4

10	10	10	10	9
1	1	7	8	9
5	2	2	8	9
5	6	3	3	9
4	6	7	4	4

图 3.7　$\mathbb{C}^5 \otimes \mathbb{C}^5$ **中分别具有** $8,9,10$ **个砖块的 U-砖块结构**。

当 $m=5$ 时，通过 $\mathbb{C}^4 \otimes \mathbb{C}^4$ 中分别具有 $5,6,7$ 个砖块的 U-砖块结构，我们可以在 $\mathbb{C}^5 \otimes \mathbb{C}^5$ 中分别构造具有 $5,6,7$ 个砖块的 U-砖块结构，如图3.6所示；通

过 $\mathbb{C}^4 \otimes \mathbb{C}^4$ 中具有 8 个砖块的 U-砖块结构，我们可以在 $\mathbb{C}^5 \otimes \mathbb{C}^5$ 中分别构造具有 $8, 9, 10$ 个砖块的 U-砖块结构，如图3.7所示。具体构造方法是在图3.5中的每个 U-砖块结构的顶部和右侧分别附加一行和一列。

5	$2m$-1	$\cdots$	$2m$-1	$2m$-1	$2m$-1
i_1	i_2	$\cdots$	i_{m-2}	i_{m-1}	i_{m-1}
				j_1	j_1
				$\vdots$	$\vdots$
				j_{m-3}	j_{m-3}
				j_{m-2}	4

5	$2m$-1	$\cdots$	$2m$-1	$2m$-1	$2m$-1
i_1	i_2	$\cdots$	i_{m-2}	i_{m-1}	$2m$
				j_1	$2m$
				$\vdots$	$\vdots$
				j_{m-3}	$2m$
				j_{m-2}	$2m$

图 3.8　当 $m \geqslant 6$ 为偶数时，$\mathbb{C}^m \otimes \mathbb{C}^m$ 中分别具有 $2m-1, 2m$ 个砖块的 U-砖块结构。

5	i_2	$\cdots$	i_{m-2}	i_{m-1}	$2m$-1
i_1	i_2	$\cdots$	i_{m-2}	i_{m-1}	$2m$-1
				j_1	$2m$-1
				$\vdots$	$\vdots$
				j_{m-3}	$2m$-1
				j_{m-2}	4

$2m$	$2m$	$\cdots$	$2m$	$2m$	$2m$-1
i_1	i_2	$\cdots$	i_{m-2}	i_{m-1}	$2m$-1
				j_1	$2m$-1
				$\vdots$	$\vdots$
				j_{m-3}	$2m$-1
				j_{m-2}	4

图 3.9　当 $m \geqslant 6$ 为奇数时，$\mathbb{C}^m \otimes \mathbb{C}^m$ 中分别具有 $2m-1, 2m$ 个砖块的 U-砖块结构。

下面我们可以归纳构造。当 $m \geqslant 6$，对于 $5 \leqslant t \leqslant 2(m-1)$，通过 $\mathbb{C}^{m-1} \otimes \mathbb{C}^{m-1}$ 中具有 t 个砖块的 U-砖块结构，我们可以在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中构造具有 t 个砖块的 U-砖块结构：在顶部附加一行 $m-1$ 个格子，使得每个格子里面的数字与底部相邻格子中的数字相等；在右侧附加一列 m 个格子，使得每个格子里面的数字与左边相邻格子中的数字相等。有关示例参见图3.6和图3.7左边第一个 U-砖块结构。对于 $t = 2m-1$ 和 $2m$，通过 $\mathbb{C}^{m-1} \otimes \mathbb{C}^{m-1}$ 中具有 $2(m-1)$ 个砖块的 U-砖块结构，我们可以在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中构造具有 t 个砖块的 U-砖块结构：构造分偶数 m 和奇数 m 两种情况，分别参见图3.8 和3.9。注意新添加的行和列分别位于顶部和右侧。

由归纳可知，对于 $m \geqslant 4$ 和 $5 \leqslant t \leqslant 2m$，我们在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中成功地构造了具有 t 个砖块的 U-砖块结构。在此 U-砖块结构的右侧附加一列 m 个格子，使

得每个格子里面的数字与左边相邻格子中的数字相等，按照这种方式添加 $n-m$ 列，我们可以在 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中构造一个具有 t 个砖块的 U-砖块结构。因此，根据定理3.1可知，对于 $4 \leqslant m \leqslant n$ 和 $4 \leqslant k \leqslant 2m-1$，$\mathbb{C}^m \otimes \mathbb{C}^n$ 中存在一个数目为 $mn-k$ 的不可扩充乘积基。

	0	1	⋯	$n-2$	$n-1$
0	1	1	⋯	1	2
1	4	5	⋯	5	2
⋮	⋮	⋮	5	⋮	⋮
$m-2$	4	5	⋯	5	2
$m-1$	4	3	⋯	3	3

图 3.10　$\mathbb{C}^m \otimes \mathbb{C}^n$ 中具有 5 个砖块的 U-砖块结构。

对于 $m,n \geqslant 3$，$\mathbb{C}^m \otimes \mathbb{C}^n$ 中不存在数目为 $mn-1$，$mn-2$，$mn-3$ 的不可扩充乘积基[93]，那么不可扩充乘积基的数目小于等于 $mn-4$。为了证明 $F(m,n)=mn-4$，我们只需在 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中构造具有 5 个砖块的 U-砖块结构，如图3.10所示。 ∎

在引理3.3中，当 $m \geqslant 3$ 为奇数时，我们也在 $\mathbb{C}^m \otimes \mathbb{C}^m$ 中给出了一个具有 $2m-1$ 个砖块的 U-砖块结构，但这个 U-砖块结构只有一个特殊矩形，这与 Halder 等人[39]构造的有所不同，当 $m \geqslant 5$ 为奇数时，他们的 U-砖块结构至少有两个特殊矩形。

3.4　三体系统中的不可扩充乘积基

在本节及其下节中，我们将构造三体和四体系统中的不可扩充乘积基。方法与两体系统类似，即对多维超立方体进行分解，然后在此分解的基础上构造一个正交乘积集。针对其不可扩充性，上一章的 U-砖块结构也可以推广到多体系统中，显然也是成立的，不过值得注意的是此时每个砖块为多维超立方体。区别于两体系统中的 U-砖块结构，由于多维超立方体的分解情况无法全方位地画出来，不能很直观地去验证它是 U-砖块结构。在本节中，我们将采用另一种方法来验证其不可扩充性。

首先我们从一个简单的例子出发。给定一个坐标为 $\{0,1,2\}_A \times \{0,1,2\}_B \times \{0,1,2\}_C$ 的三维立方体。我们可以这样分解：$\mathcal{C}_1 = \{1,2\}_A \times \{0\}_B \times \{0,1\}_C$，$\mathcal{C}_2 = \{1,2\}_A \times \{0,1\}_B \times \{2\}_C$，$\mathcal{C}_3 = \{2\}_A \times \{1,2\}_B \times \{0,1\}_C$，$\mathcal{C}_4 = \{2\}_A \times \{2\}_B \times \{2\}_C$，$\mathcal{D}_1 = \{0,1\}_A \times \{2\}_B \times \{1,2\}_C$，$\mathcal{D}_2 = \{0,1\}_A \times \{1,2\}_B \times \{0\}_C$，$\mathcal{D}_3 = \{0\}_A \times \{0,1\}_B \times \{1,2\}_C$，

$\mathcal{D}_4 = \{0\}_A \times \{0\}_B \times \{0\}_C$，$\mathcal{E} = \{1\}_A \times \{1\}_B \times \{1\}_C$，如图3.11所示。

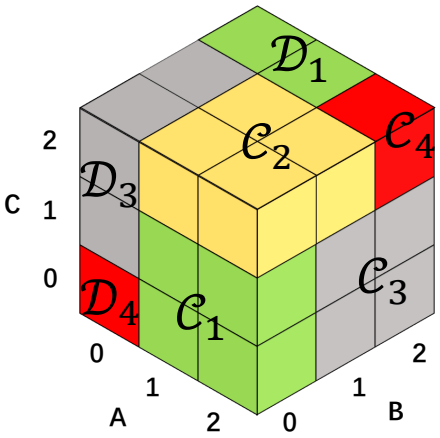

图 3.11　坐标为 $\{0,1,2\}_A \times \{0,1,2\}_B \times \{0,1,2\}_C$ 的三维立方体的分解。

从该分解我们可以获得 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 中的一组正交乘积基：

$$
\begin{aligned}
\mathcal{C}_1 &:= \{|\psi_1(i,j)\rangle = |\xi_i\rangle_A|0\rangle_B|\eta_j\rangle_C : (i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_2\},\\
\mathcal{C}_2 &:= \{|\psi_2(i,j)\rangle = |\xi_i\rangle_A|\eta_j\rangle_B|2\rangle_C : (i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_2\},\\
\mathcal{C}_3 &:= \{|\psi_3(i,j)\rangle = |2\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C : (i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_2\},\\
\mathcal{C}_4 &:= \{|\psi_4\rangle = |2\rangle_A|2\rangle_B|2\rangle_C\},\\
\mathcal{D}_1 &:= \{|\phi_1(i,j)\rangle = |\eta_i\rangle_A|2\rangle_B|\xi_j\rangle_C : (i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_2\},\\
\mathcal{D}_2 &:= \{|\phi_2(i,j)\rangle = |\eta_i\rangle_A|\xi_j\rangle_B|0\rangle_C : (i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_2\},\\
\mathcal{D}_3 &:= \{|\phi_3(i,j)\rangle = |0\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C : (i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_2\},\\
\mathcal{D}_4 &:= \{|\phi_4\rangle = |0\rangle_A|0\rangle_B|0\rangle_C\},\\
\mathcal{E} &:= \{|\varphi\rangle = |1\rangle_A|1\rangle_B|1\rangle_C\},
\end{aligned}
\tag{3.1}
$$

其中 $|\eta_s\rangle_X = |0\rangle_X + (-1)^s|1\rangle_X$，$|\xi_s\rangle_X := |1\rangle_X + (-1)^s|2\rangle_X$，$s \in \mathbb{Z}_2$，$X \in \{A,B,C\}$。

对于任意 $1 \leqslant i \leqslant 3$，令 $\mathcal{A}_i := \mathcal{C}_i \backslash \{|\psi_i(0,0)\rangle\}$，$\mathcal{B}_i := \mathcal{D}_i \backslash \{|\phi_i(0,0)\rangle\}$，$\mathcal{A}_4 = \mathcal{C}_4$，$\mathcal{B}_4 = \mathcal{D}_4$，$\mathcal{F} = \mathcal{E}$，

$$
|S\rangle = \left(\sum_{i=0}^{2}|i\rangle\right)_A \left(\sum_{j=0}^{2}|j\rangle\right)_B \left(\sum_{k=0}^{2}|k\rangle\right)_C,
$$

则 $\cup_{i=1}^{3}(\mathcal{A}_i, \mathcal{B}_i) \cup \{|S\rangle\}$ 是 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 中的一个不可扩充乘积基[92]。但文献[92]没有给出证明其不可扩充性的具体方法，我们将在下面给出具体方法。在此之前，我们考虑 $\cup_{i=1}^{4}\{\mathcal{A}_i, \mathcal{B}_i\} \cup \mathcal{F}$ 在两体划分 $A|BC$ 下对应的 3×9 网格，如图3.12所示。

例 3.2　在 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 中，上述给出的 $\cup_{i=1}^{3}(\mathcal{A}_i \cup \mathcal{B}_i) \cup \{|S\rangle\}$ 是一个不可扩充乘积基，且 $|\cup_{i=1}^{3}(\mathcal{A}_i \cup \mathcal{B}_i) \cup \{|S\rangle\}| = 19$。

证明

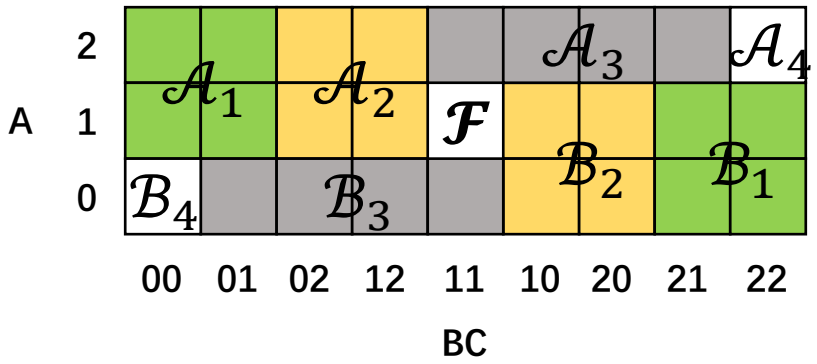

图 3.12　$\cup_{i=1}^{4}\{\mathcal{A}_i,\mathcal{B}_i\}\cup\mathcal{F}$ **在两体划分** $A|BC$ **下对应的** 3×9 **网格。例如，** $\mathcal{A}_1$ **对应于** 2×2 **网格** $\{1,2\}_A\times\{00,01\}_{BC}$。**此外，对于** $1\leqslant i\leqslant 4$，$\mathcal{A}_i$ **与** $\mathcal{B}_i$ **是对称的。**

令 $\mathcal{H}$ 为 $\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\{|S\rangle\}$ 生成的子空间，对于任何 $|\psi\rangle\in\mathcal{H}^{\perp}$，我们只需验证 $|\psi\rangle$ 是一个纠缠态。我们采用反证法，假设 $\mathcal{H}^{\perp}$ 中存在一个乘积态 $|\psi\rangle$。令 $\mathcal{H}_1$ 为 $\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)$ 生成的子空间，由于 $\mathcal{H}_1\subset\mathcal{H}$，$\mathcal{H}^{\perp}\subset\mathcal{H}_1^{\perp}$。此外由于

$$\begin{aligned}\mathcal{H}_1^{\perp}=\mathrm{span}\{&|\psi_1(0,0)\rangle,|\psi_2(0,0)\rangle,|\psi_3(0,0)\rangle,|\psi_4\rangle,|\phi_1(0,0)\rangle,\\&|\phi_2(0,0)\rangle,|\phi_3(0,0)\rangle,|\phi_4\rangle,|\varphi\rangle\},\end{aligned}$$

存在 $a_0,b_0,c_0,d_0,a_1,b_1,c_1,d_1,e\in\mathbb{C}$，使得

$$\begin{aligned}|\psi\rangle=&a_0|\psi_1(0,0)\rangle+b_0|\psi_2(0,0)\rangle+c_0|\psi_3(0,0)\rangle+d_0|\psi_4\rangle+a_1|\phi_1(0,0)\rangle\\&+b_1|\phi_2(0,0)\rangle+c_1|\phi_3(0,0)\rangle+d_1|\phi_4\rangle+e|\varphi\rangle,\end{aligned}$$

且有 $\langle S|\psi\rangle=0$。

下面我们考虑 $|\psi\rangle$ 在两体划分 $A|BC$ 下对应的矩阵，则它对应于一个 3×9 的矩阵

$$\begin{array}{cc} & \begin{matrix}00&01&02&12&11&10&20&21&22\end{matrix}\\ \begin{matrix}2\\1\\0\end{matrix}\ \mathrm{A} & \begin{bmatrix}a_0&a_0&b_0&b_0&c_0&c_0&c_0&c_0&d_0\\a_0&a_0&b_0&b_0&e&b_1&b_1&a_1&a_1\\d_1&c_1&c_1&c_1&c_1&b_1&b_1&a_1&a_1\end{bmatrix}\end{array}=M,$$

BC

且 $\mathrm{rank}(M)=1$。注意，M 与图3.12有相同的结构。对于 $x\in\{a,b,c,d\}$，这意味着 x_0 与 x_1 是对称的。由于 $|S\rangle$ 在两体划分 $A|BC$ 下对应于一个 3×9 的全 1 矩阵 J_S，

$$\langle S|\psi\rangle=\mathrm{Tr}(J_S^{\dagger}M)=\mathrm{sum}(M)=0.\tag{3.2}$$

M 中每一个元素都有坐标，例如 d_0 有坐标 $\{2\}_A\times\{22\}_{BC}$。如果我们考虑两体划分 $AB|C$，那么我们将 M 的第一行取出，按照坐标 $\{X\}_{AB}\times\{Y\}_C$ 的方式排成一个 3×3 的矩阵 M_2，例如，d_0 在 M_2 中的坐标为 $\{22\}_A\times\{2\}_{BC}$。同样，

我们将 M 的第三行取出，按照坐标 $\{X\}_{AB}\times\{Y\}_C$ 的方式排成一个 3×3 的矩阵 M_0。那么 M_2 和 M_0 如下所示:

$$\begin{array}{cc} & \begin{matrix}22 & 21 & 20\end{matrix} \\ \mathbf{AB} & \begin{bmatrix} c_0 & c_0 & d_0 \\ c_0 & c_0 & b_0 \\ a_0 & a_0 & b_0 \end{bmatrix} \\ & \begin{matrix}0 & 1 & 2\end{matrix} \\ & \mathbf{C} \end{array} = M_2, \qquad \begin{array}{cc} & \begin{matrix}02 & 01 & 00\end{matrix} \\ \mathbf{AB} & \begin{bmatrix} b_1 & a_1 & a_1 \\ b_1 & c_1 & c_1 \\ d_1 & c_1 & c_1 \end{bmatrix} \\ & \begin{matrix}0 & 1 & 2\end{matrix} \\ & \mathbf{C} \end{array} = M_0.$$

由于 $|\psi\rangle$ 在两体划分 $\boldsymbol{AB}|\boldsymbol{C}$ 下仍然是乘积态，我们有

$$\operatorname{rank} M_2 = 0 \quad 或 \quad 1, \tag{3.3}$$

$$\operatorname{rank} M_0 = 0 \quad 或 \quad 1. \tag{3.4}$$

假设 $a_0 \neq 0$。由于 $\operatorname{rank}(M)=1$，我们有 $c_1=d_1$，并且 $c_0=e=b_1=a_1=d_0$。

(i) 如果 $c_0=0$，那么由公式(3.3)得到 $b_0=0$，由公式(3.4) 得到 $c_1=0$。这与公式(3.2)相矛盾。

(ii) 如果 $c_0\neq0$，那么由公式(3.3) 得到 $c_0=a_0=b_0$，由公式(3.4)得到 $c_0=c_1$。这与公式(3.2)相矛盾。

因此我们有 $a_0=0$。根据 M 的对称性，我们有 $a_1=0$。

假设 $b_0\neq0$。由于 $\operatorname{rank}(M)=1$，我们有 $c_1=d_1=0$，并且 $c_0=e=b_1=a_1=d_0=0$。这与公式(3.2)相矛盾，因此我们有 $b_0=b_1=0$。

假设 $d_1\neq0$。由于 $\operatorname{rank}(M)=1$，我们有 $e=c_0=d_0=0$。再通过公式(3.4)得到 $c_1=0$。这与公式(3.2)相矛盾，因此我们有 $d_0=d_1=0$。

假设 $c_1\neq0$。由于 $\operatorname{rank}(M)=1$，我们有 $e=c_0=0$。这与公式(3.2)相矛盾，因此我们有 $c_0=c_1=0$。

由于 $\operatorname{sum}(M)=0$，我们有 $e=0$，这与 $\operatorname{rank}(M)=1$ 矛盾。因此 $|\psi\rangle$ 是一个纠缠态，$\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\{|S\rangle\}$ 是一个不可扩充乘积基。 ∎

下面我们将上面的不可扩充乘积基推广到 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}$ 中。令

$$\begin{aligned}
\mathcal{A}_1 &:= \{|\xi_i\rangle_A|0\rangle_B|\eta_j\rangle_C : (i,j)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}\},\\
\mathcal{A}_2 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|d_C-1\rangle_C : (i,j)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_B-1}\setminus\{(0,0)\}\},\\
\mathcal{A}_3 &:= \{|d_A-1\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C : (i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}\},\\
\mathcal{A}_4 &:= \{|d_A-1\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C\},\\
\mathcal{B}_1 &:= \{|\eta_i\rangle_A|d_B-1\rangle_B|\xi_j\rangle_C : (i,j)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}\},\\
\mathcal{B}_2 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|0\rangle_C : (i,j)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_B-1}\setminus\{(0,0)\}\},\\
\mathcal{B}_3 &:= \{|0\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C : (i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}\},\\
\mathcal{B}_4 &:= \{|0\rangle_A|0\rangle_B|0\rangle_C\},\\
\mathcal{F} &:= \{|\beta_i\rangle_A|\beta_j\rangle_B|\beta_k\rangle_C : (i,j,k)\in\mathbb{Z}_{d_A-2}\times\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}\setminus\{(0,0,0)\}\},\\
|S\rangle &:= \left(\sum_{i=0}^{d_A-1}|i\rangle\right)_A\left(\sum_{j=0}^{d_B-1}|j\rangle\right)_B\left(\sum_{k=0}^{d_C-1}|k\rangle\right)_C,
\end{aligned} \tag{3.5}$$

其中 $|\eta_s\rangle_X = \sum_{t=0}^{d_X-2} w_{d_X-1}^{st}|t\rangle_X$，$|\xi_s\rangle_X = \sum_{t=0}^{d_X-2} w_{d_X-1}^{st}|t+1\rangle_X$，$s \in \mathbb{Z}_{d_X-1}$，$X \in \{A,B,C\}$；且 $|\beta_s\rangle_X = \sum_{t=0}^{d_X-3} w_{d_X-2}^{st}|t+1\rangle_X$，$s \in \mathbb{Z}_{d_X-2}$，$X \in \{A,B,C\}$。

注意，对于 $X \in \{A,B,C\}$，$\{|\eta_s\rangle_X\}_{s\in\mathbb{Z}_{d_X-1}}$，$\{|\xi_s\rangle_X\}_{s\in\mathbb{Z}_{d_X-1}}$ 和 $\{|\beta_s\rangle_X\}_{s\in\mathbb{Z}_{d_X-2}}$ 是三个正交乘积集，它们由分别由 $\{|t\rangle_X\}_{t=0}^{d_X-2}$，$\{|t\rangle_X\}_{t=1}^{d_X-1}$ 和 $\{|t\rangle_X\}_{t=1}^{d_X-2}$ 生成。这推广了公式(3.1)中给出的态的定义。这 9 个子集 $\cup_{i=1}^{4}\{\mathcal{A}_i,\mathcal{B}_i\}\cup\mathcal{F}$ 在两体划分 $A|BC$ 下对应于图3.13中 $d_A \times d_B d_C$ 网格的 9 块。那么我们有以下引理。

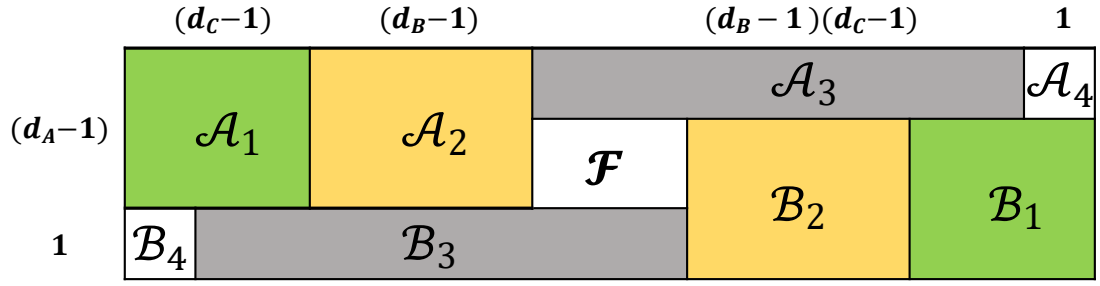

图 3.13　公式(3.5)给出的 $\cup_{i=1}^{4}\{\mathcal{A}_i,\mathcal{B}_i\}\cup\mathcal{F}$ 在两体划分 $A|BC$ 下对应的 $d_A \times d_B d_C$ 网格。此外，对于 $1 \leqslant i \leqslant 4$，$\mathcal{A}_i$ 与 $\mathcal{B}_i$ 是对称的。

引理 3.4　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}$ 中，$3 \leqslant d_A \leqslant d_B \leqslant d_C$，公式(3.5)给出的 $\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}$ 是一个不可扩充基。且 $|\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}| = d_A d_B d_C - 8$。

证明　与例3.2一样进行类似的讨论，我们可以假设 $|\psi\rangle$ 是 $\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}$ 所生成的子空间的正交补空间中的乘积态，然后我们考虑 $|\psi\rangle$ 在两体划分 $A|BC$ 和 $AB|C$ 下对应的矩阵。首先，考虑两体划分 $A|BC$，我们有

$$M = \begin{bmatrix} a_0 & a_0 & \cdots & a_0 & b_0 & \cdots & b_0 & c_0 & \cdots & c_0 & c_0 & \cdots & c_0 & c_0 & \cdots & c_0 & d_0 \\ a_0 & a_0 & \cdots & a_0 & b_0 & \cdots & b_0 & e & \cdots & e & b_1 & \cdots & b_1 & a_1 & \cdots & a_1 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_0 & a_0 & \cdots & a_0 & b_0 & \cdots & b_0 & e & \cdots & e & b_1 & \cdots & b_1 & a_1 & \cdots & a_1 & a_1 \\ d_1 & c_1 & \cdots & c_1 & c_1 & \cdots & c_1 & c_1 & \cdots & c_1 & b_1 & \cdots & b_1 & a_1 & \cdots & a_1 & a_1 \end{bmatrix}, \tag{3.6}$$

且

$$\mathrm{rank}(M) = 1, \quad \mathrm{sum}(M) = 0. \tag{3.7}$$

然后我们考虑两体划分 $AB|C$。我们将 M 的第一行按照坐标 $\{X\}_{AB}\times\{Y\}_C$ 的方式排成一个 $d_B\times d_C$ 的矩阵 $M_{(d_A-1)}$,同样将 M 的最后一行按照坐标 $\{X\}_{AB}\times\{Y\}_C$ 的方式排成一个 $d_B \times d_C$ 的矩阵 M_0，那么

$$M_{(d_A-1)} = \begin{bmatrix} c_0 & c_0 & \cdots & c_0 & d_0 \\ c_0 & c_0 & \cdots & c_0 & b_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_0 & c_0 & \cdots & c_0 & b_0 \\ a_0 & a_0 & \cdots & a_0 & b_0 \end{bmatrix}, \quad \mathrm{rank}(M_{(d_A-1)}) = 0 \text{ 或 } 1, \tag{3.8}$$

且

$$M_0=\begin{bmatrix} b_1 & a_1 & \cdots & a_1 & a_1 \\ b_1 & c_1 & \cdots & c_1 & c_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_1 & c_1 & \cdots & c_1 & c_1 \\ d_1 & c_1 & \cdots & c_1 & c_1 \end{bmatrix},\quad \operatorname{rank}(M_0)=0 \text{ 或 } 1. \tag{3.9}$$

与例3.2的证明类似，我们通过公式(3.7)，(3.8) 和 (3.9)可以证明 $|\psi\rangle$ 必然是一个纠缠态，从而引理得证。 ∎

请注意，公式(3.5)中 $\cup_{i=1}^{4}\{\mathcal{A}_i,\mathcal{B}_i\}$ 中的态由 $d_A\times d_B\times d_C$ 的立方体的最外层 $\{0,1,\cdots,d_A-1\}_A\times\{0,1,\cdots,d_B-1\}_B\times\{0,1,\cdots,d_C-1\}_C\setminus\{1,\cdots,d_A-2\}_A\times\{1,\cdots,d_B-2\}_B\times\{1,\cdots,d_C-2\}_C$ 给出，$\mathcal{F}$ 中的态由所有立方体的内层 $\{1,\cdots,d_A-2\}_A\times\{1,\cdots,d_B-2\}_B\times\{1,\cdots,d_C-2\}_C$ 给出。通过观察这一点，我们可以使用最外层的分解方法来继续分解内层，这样可以在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}$ 中构造更多的不可扩充乘积基。假设最外层是第 0 层，这样最多可以分解到第 $\lfloor\frac{d_A-3}{2}\rfloor$ 层。假设立方体处于从外到内的第 n 层，则 $0\leqslant n\leqslant\lfloor\frac{d_A-3}{2}\rfloor$。令 $X_n:=d_X-2n$，其中 $X\in\{A,B,C\}$。然后我们可以定义以下态:

$$\begin{aligned}
\mathcal{A}_1^{(n)} &:= \{|\xi_i^{(n)}\rangle_A|n\rangle_B|\eta_j^{(n)}\rangle_C : (i,j)\in\mathbb{Z}_{A_n-1}\times\mathbb{Z}_{C_n-1}\setminus\{(0,0)\}\},\\
\mathcal{A}_2^{(n)} &:= \{|\xi_i^{(n)}\rangle_A|\eta_j^{(n)}\rangle_B|d_C-1-n\rangle_C : (i,j)\in\mathbb{Z}_{A_n-1}\times\mathbb{Z}_{B_n-1}\setminus\{(0,0)\}\},\\
\mathcal{A}_3^{(n)} &:= \{|d_A-1-n\rangle_A|\xi_i^{(n)}\rangle_B|\eta_j^{(n)}\rangle_C : (i,j)\in\mathbb{Z}_{B_n-1}\times\mathbb{Z}_{C_n-1}\setminus\{(0,0)\}\},\\
\mathcal{A}_4^{(n)} &:= \{|d_A-1-n\rangle_A|d_B-1-n\rangle_B|d_C-1-n\rangle_C\},\\
\mathcal{B}_1^{(n)} &:= \{|\eta_i^{(n)}\rangle_A|d_B-1-n\rangle_B|\xi_j^{(n)}\rangle_C : (i,j)\in\mathbb{Z}_{A_n-1}\times\mathbb{Z}_{C_n-1}\setminus\{(0,0)\}\},\\
\mathcal{B}_2^{(n)} &:= \{|\eta_i^{(n)}\rangle_A|\xi_j^{(n)}\rangle_B|n\rangle_C : (i,j)\in\mathbb{Z}_{A_n-1}\times\mathbb{Z}_{B_n-1}\setminus\{(0,0)\}\},\\
\mathcal{B}_3^{(n)} &:= \{|n\rangle_A|\eta_i^{(n)}\rangle_B|\xi_j^{(n)}\rangle_C : (i,j)\in\mathbb{Z}_{B_n-1}\times\mathbb{Z}_{C_n-1}\setminus\{(0,0)\}\},\\
\mathcal{B}_4^{(n)} &:= \{|n\rangle_A|n\rangle_B|n\rangle_C\},\\
\mathcal{F}^{(n)} &:= \{|\beta_i^{(n)}\rangle_A|\beta_j^{(n)}\rangle_B|\beta_k^{(n)}\rangle_C : (i,j,k)\in\mathbb{Z}_{A_n-2}\times\mathbb{Z}_{B_n-2}\times\mathbb{Z}_{C_n-2}\setminus\{(0,0,0)\}\},\\
|S\rangle &= \left(\sum_{i=0}^{d_A-1}|i\rangle\right)_A\left(\sum_{j=0}^{d_B-1}|j\rangle\right)_B\left(\sum_{k=0}^{d_C-1}|k\rangle\right)_C,
\end{aligned}\tag{3.10}$$

其中 $|\eta_s^{(n)}\rangle_X=\sum_{t=n}^{X_n+n-2}w_{X_n-1}^{s(t-n)}|t\rangle_X$，$|\xi_s^{(n)}\rangle_X=\sum_{t=n}^{X_n+n-2}w_{X_n-1}^{s(t-n)}|t+1\rangle_X$，$s\in\mathbb{Z}_{X_n-1}$，$X\in\{A,B,C\}$；且 $|\beta_s^{(n)}\rangle_X=\sum_{t=n}^{X_n+n-3}w_{X_n-2}^{s(t-n)}|t+1\rangle_X$，$s\in\mathbb{Z}_{X_n-2}$，$X\in\{A,B,C\}$。

注意对于 $X\in\{A,B,C\}$，$\{|\eta_s^{(n)}\rangle_X\}_{s\in\mathbb{Z}_{X_n-1}}$，$\{|\xi_s^{(n)}\rangle_X\}_{s\in\mathbb{Z}_{X_n-1}}$，和 $\{|\beta_s^{(n)}\rangle_X\}_{s\in\mathbb{Z}_{X_n-2}}$ 是三个正交乘积集，它们分别由 $\{|t\rangle_X\}_{t=n}^{X_n+n-2}$，$\{|t\rangle_X\}_{t=n+1}^{X_n+n-1}$，和 $\{|t\rangle_X\}_{t=n+1}^{X_n+n-2}$ 生成。当 $n=0$ 时，公式(3.10)将变为公式(3.5)，因此公式(3.10)把 $n=0$ 的情形推广到了一般的 n。特别地，如果 $d_A\geqslant 5$，那么 $\cup_{i=1}^{4}\{\mathcal{A}_i^{(0)},\mathcal{B}_i^{(0)},\mathcal{A}_i^{(1)},\mathcal{B}_i^{(1)}\}\cup\mathcal{F}^{(1)}$ 在两体划分 $A|BC$ 下对应于图3.14。那我们有以下定理。

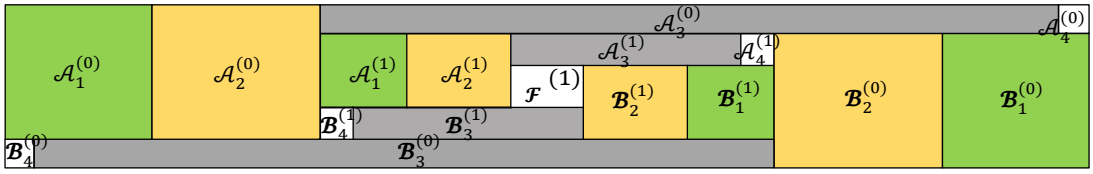

图 3.14　当 $d_A \geqslant 5$ 时，公式(3.10)给出的 $\cup_{i=1}^{4}\{\mathcal{A}_i^{(0)}, \mathcal{B}_i^{(0)}, \mathcal{A}_i^{(1)}, \mathcal{B}_i^{(1)}\} \cup \mathcal{F}^{(1)}$ 在两体划分 $A|BC$ 下对应的 $d_A \times d_B d_C$ 网格。对于 $1 \leqslant i \leqslant 4$，$\mathcal{A}_i^{(0)}$ 与 $\mathcal{B}_i^{(0)}$ 是对称的；$\mathcal{A}_i^{(1)}$ 与 $\mathcal{B}_i^{(1)}$ 是对称的。

定理 3.5　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}$ 中，$3 \leqslant d_A \leqslant d_B \leqslant d_C$，对于任何 $0 \leqslant n \leqslant \lfloor \frac{d_A-3}{2} \rfloor$，公式(3.10)给出的

$$\mathcal{U}_n := \cup_{t=0}^{n}(\cup_{i=1}^{3}(\mathcal{A}_i^{(t)} \cup \mathcal{B}_i^{(t)})) \cup \mathcal{F}^{(n)} \cup \{|S\rangle\}$$

是一个不可扩充乘积基，且 $|\mathcal{U}_n| = d_A d_B d_C - 8(n+1)$。

证明　像引理3.4一样讨论，我们可以得到矩阵，

$$M^{(d_A)} = \begin{bmatrix} a_0 & a_0 & \cdots & a_0 & b_0 & \cdots & b_0 & c_0 & \cdots & c_0 & c_0 & \cdots & c_0 & c_0 & \cdots & c_0 & d_0 \\ a_0 & a_0 & \cdots & a_0 & b_0 & \cdots & b_0 & & & & b_1 & \cdots & b_1 & a_1 & \cdots & a_1 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & & M^{(d_A-2)} & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_0 & a_0 & \cdots & a_0 & b_0 & \cdots & b_0 & & & & b_1 & \cdots & b_1 & a_1 & \cdots & a_1 & a_1 \\ d_1 & c_1 & \cdots & c_1 & c_1 & \cdots & c_1 & c_1 & \cdots & c_1 & b_1 & \cdots & b_1 & a_1 & \cdots & a_1 & a_1 \end{bmatrix},$$

$$M^{(d_A-2)} = \begin{bmatrix} a_0^{(1)} & a_0^{(1)} & \cdots & a_0^{(1)} & b_0^{(1)} & \cdots & b_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & d_0^{(1)} \\ a_0^{(1)} & a_0^{(1)} & \cdots & a_0^{(1)} & b_0^{(1)} & \cdots & b_0^{(1)} & & & & b_1^{(1)} & \cdots & b_1^{(1)} & a_1^{(1)} & \cdots & a_1^{(1)} & a_1^{(1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & & M^{(d_A-4)} & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_0^{(1)} & a_0^{(1)} & \cdots & a_0^{(1)} & b_0^{(1)} & \cdots & b_0^{(1)} & & & & b_1^{(1)} & & b_1^{(1)} & a_1^{(1)} & \cdots & a_1^{(1)} & a_1^{(1)} \\ d_1^{(1)} & c_1^{(1)} & \cdots & c_1^{(1)} & c_1^{(1)} & \cdots & c_1^{(1)} & c_1^{(1)} & \cdots & c_1^{(1)} & b_1^{(1)} & \cdots & b_1^{(1)} & a_1^{(1)} & \cdots & a_1^{(1)} & a_1^{(1)} \end{bmatrix},$$

$$\vdots$$

$$M^{(d_A-2s)} = \begin{bmatrix} a_0^{(s)} & a_0^{(s)} & \cdots & a_0^{(s)} & b_0^{(s)} & \cdots & b_0^{(s)} & c_0^{(s)} & \cdots & c_0^{(s)} & c_0^{(s)} & \cdots & c_0^{(s)} & c_0^{(s)} & \cdots & c_0^{(s)} & d_0^{(s)} \\ a_0^{(s)} & a_0^{(s)} & \cdots & a_0^{(s)} & b_0^{(s)} & \cdots & b_0^{(s)} & e^{(s)} & \cdots & e^{(s)} & b_1^{(s)} & \cdots & b_1^{(s)} & a_1^{(s)} & \cdots & a_1^{(s)} & a_1^{(s)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_0^{(s)} & a_0^{(s)} & \cdots & a_0^{(s)} & b_0^{(s)} & \cdots & b_0^{(s)} & e^{(s)} & \cdots & e^{(s)} & b_1^{(s)} & & b_1^{(s)} & a_1^{(s)} & \cdots & a_1^{(s)} & a_1^{(s)} \\ d_1^{(s)} & c_1^{(s)} & \cdots & c_1^{(s)} & c_1^{(s)} & \cdots & c_1^{(s)} & c_1^{(s)} & \cdots & c_1^{(s)} & b_1^{(s)} & \cdots & b_1^{(s)} & a_1^{(s)} & \cdots & a_1^{(s)} & a_1^{(s)} \end{bmatrix},$$

其中 $M^{(d_A-2s)}$ 与公式(3.6)中的 M 类似。下面我们有

$$\mathrm{rank}(M^{(d_A)}) = 1, \quad \mathrm{sum}(M^{(d_A)}) = 0. \tag{3.11}$$

然后我们考虑两体划分 $AB|C$。我们将 $M^{(d_A)}$ 的第一行按照坐标 $\{X\}_{AB} \times \{Y\}_C$ 的方式排成一个 $d_B \times d_C$ 的矩阵 $M_{(d_A-1)}$，同样将 $M^{(d_A)}$ 的最后一行按照坐标 $\{X\}_{AB} \times \{Y\}_C$ 的方式排成一个 $d_B \times d_C$ 的矩阵 M_0，那么

$$M_{(d_A-1)} = \begin{bmatrix} c_0 & c_0 & \cdots & c_0 & d_0 \\ c_0 & c_0 & \cdots & c_0 & b_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_0 & c_0 & \cdots & c_0 & b_0 \\ a_0 & a_0 & \cdots & a_0 & b_0 \end{bmatrix}, \quad \mathrm{rank}(M_{(d_A-1)}) = 0 \text{ 或 } 1, \tag{3.12}$$

且

$$M_0 = \begin{bmatrix} b_1 & a_1 & \cdots & a_1 & a_1 \\ b_1 & c_1 & \cdots & c_1 & c_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_1 & c_1 & \cdots & c_1 & c_1 \\ d_1 & c_1 & \cdots & c_1 & c_1 \end{bmatrix}, \quad \text{rank}(M_0) = 0 \text{ 或 } 1. \tag{3.13}$$

与例3.2的证明类似，通过公式(3.11)，(3.12)，和 (3.13)，我们可以得到 $a_0 = a_1 = b_0 = b_1 = c_0 = c_1 = d_0 = d_1 = 0$。然后我们有

$$\text{rank}(M^{(d_A-2)}) = 1, \quad \text{sum}(M^{(d_A-2)}) = 0. \tag{3.14}$$

我们将 $M^{(d_A)}$ 的第二行按照坐标 $\{X\}_{AB} \times \{Y\}_C$ 的方式排成一个 $d_B \times d_C$ 的矩阵 $M_{(d_A-2)}$，同样将 $M^{(d_A)}$ 的倒数第二行按照坐标 $\{X\}_{AB} \times \{Y\}_C$ 的方式排成一个 $d_B \times d_C$ 的矩阵 M_1，那么

$$M_{(d_A-2)} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & c_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & d_0^{(1)} & 0 \\ 0 & c_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & b_0^{(1)} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & c_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & b_0^{(1)} & 0 \\ 0 & a_0^{(1)} & a_0^{(1)} & \cdots & a_0^{(1)} & b_0^{(1)} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}, \quad \text{rank}(M_{d_A-2}) = 0 \text{ 或 } 1, \tag{3.15}$$

且

$$M_1 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & b_0^{(1)} & a_0^{(1)} & \cdots & a_0^{(1)} & a_0^{(1)} & 0 \\ 0 & b_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & c_0^{(1)} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & b_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & c_0^{(1)} & 0 \\ 0 & d_0^{(1)} & c_0^{(1)} & \cdots & c_0^{(1)} & c_0^{(1)} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}, \quad \text{rank}(M_1) = 0 \text{ 或 } 1. \tag{3.16}$$

类似地，我们通过公式(3.14)，(3.15)，和 (3.16)同样可以推出 $a_0^{(1)} = a_1^{(1)} = b_0^{(1)} = b_1^{(1)} = c_0^{(1)} = c_1^{(1)} = d_0^{(1)} = d_1^{(1)} = 0$。重复这个过程 s 次，我们得到

$$\text{rank}(M^{(d_A-2s)}) = 1, \quad \text{sum}(M^{(d_A-2s)}) = 0. \tag{3.17}$$

由于 $M^{(d_A-2s)}$ 与公式(3.6) 中的 M 类似，由引理3.4的证明可知，我们也有 $a_0^{(s)} = a_1^{(s)} = b_0^{(s)} = b_1^{(s)} = c_0^{(s)} = c_1^{(s)} = d_0^{(s)} = d_1^{(s)} = e^{(s)} = 0$。从而我们得到 $M^{(d_A)} = \mathbf{0}$，这与 $\text{rank}(M^{(d_A)}) = 1$ 矛盾，定理得证。 ∎

值得注意的是，当 $d_A = d_B = d_C$，$n = \lfloor \frac{d_A-3}{2} \rfloor$ 时，定理3.5给出的不可扩充乘积基恰好是文献[92]中构造的不可扩充乘积基，所以我们的结果更加广泛。

3.5　四体系统中的不可扩充乘积基

下面我们考虑四体系统中的不可扩充乘积基，需要对四维超立方体 $\{0,1,\cdots,d_A-1\}_A \times \{0,1,\cdots,d_B-1\}_B \times \{0,1,\cdots,d_C-1\}_C \times \{0,1,\cdots,d_D-1\}_D$ 进行分解，我们的分解方式由下面态给出：

$$
\begin{aligned}
\mathcal{A}_1 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|0\rangle_C|\xi_k\rangle_D : (i,j,k) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_D-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_2 &:= \{|\xi_i\rangle_A|d_B-1\rangle_B|\eta_j\rangle_C|\eta_k\rangle_D : (i,j,k) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_3 &:= \{|\xi_i\rangle_A|\xi_j\rangle_B|\xi_k\rangle_C|d_D-1\rangle_D : (i,j,k) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_4 &:= \{|\xi_i\rangle_A|d_B-1\rangle_B|0\rangle_C|d_D-1\rangle_D : i \in \mathbb{Z}_{d_A-1} \setminus \{0\}\},\\
\mathcal{A}_5 &:= \{|d_A-1\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C|\eta_k\rangle_D : (i,j,k) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_6 &:= \{|d_A-1\rangle_A|\eta_i\rangle_B|0\rangle_C|0\rangle_D : i \in \mathbb{Z}_{d_B-1} \setminus \{0\}\},\\
\mathcal{A}_7 &:= \{|d_A-1\rangle_A|0\rangle_B|\xi_i\rangle_C|d_D-1\rangle_D : i \in \mathbb{Z}_{d_C-1} \setminus \{0\}\},\\
\mathcal{A}_8 &:= \{|d_A-1\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C|\eta_i\rangle_D : i \in \mathbb{Z}_{d_D-1} \setminus \{0\}\},\\
\mathcal{B}_1 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|d_C-1\rangle_C|\eta_k\rangle_D : (i,j,k) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_D-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_2 &:= \{|\eta_i\rangle_A|0\rangle_B|\xi_j\rangle_C|\xi_k\rangle_D : (i,j,k) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_3 &:= \{|\eta_i\rangle_A|\eta_j\rangle_B|\eta_k\rangle_C|0\rangle_D : (i,j,k) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_4 &:= \{|\eta_i\rangle_A|0\rangle_B|d_C-1\rangle_C|0\rangle_D : i \neq 0 \in \mathbb{Z}_{d_A-1}\},\\
\mathcal{B}_5 &:= \{|0\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C|\xi_k\rangle_D : (i,j,k) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_6 &:= \{|0\rangle_A|\xi_i\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D : i \in \mathbb{Z}_{d_B-1} \setminus \{0\}\},\\
\mathcal{B}_7 &:= \{|0\rangle_A|d_B-1\rangle_B|\eta_i\rangle_C|0\rangle_D : i \in \mathbb{Z}_{d_C-1} \setminus \{0\}\},\\
\mathcal{B}_8 &:= \{|0\rangle_A|0\rangle_B|0\rangle_C|\xi_i\rangle_D : i \in \mathbb{Z}_{d_D-1} \setminus \{0\}\},\\
\mathcal{F} &:= \{|\beta_i\rangle_A|\beta_j\rangle_B|\beta_k\rangle_C|\beta_\ell\rangle_D : (i,j,k,\ell) \in \mathbb{Z}_{d_A-2} \times \mathbb{Z}_{d_B-2} \times \mathbb{Z}_{d_C-2} \times \mathbb{Z}_{d_D-2} \setminus \{(0,0,0,0)\}\},\\
|S\rangle &:= \left(\sum_{i=0}^{d_A-1}|i\rangle\right)_A \left(\sum_{j=0}^{d_B-1}|j\rangle\right)_B \left(\sum_{k=0}^{d_C-1}|k\rangle\right)_C \left(\sum_{\ell=0}^{d_D-1}|\ell\rangle\right)_D ,
\end{aligned}
\tag{3.18}
$$

其中 $|\eta_s\rangle_X = \sum_{t=0}^{d_X-2} w_{d_X-1}^{st}|t\rangle_X$，$|\xi_s\rangle_X = \sum_{t=0}^{d_X-2} w_{d_X-1}^{st}|t+1\rangle_X$，$s \in \mathbb{Z}_{d_X-1}$，$X \in \{A,B,C,D\}$；且 $|\beta_s\rangle_X = \sum_{t=0}^{d_X-3} w_{d_X-2}^{st}|t+1\rangle_X$，$s \in \mathbb{Z}_{d_X-2}$，$X \in \{A,B,C,D\}$。

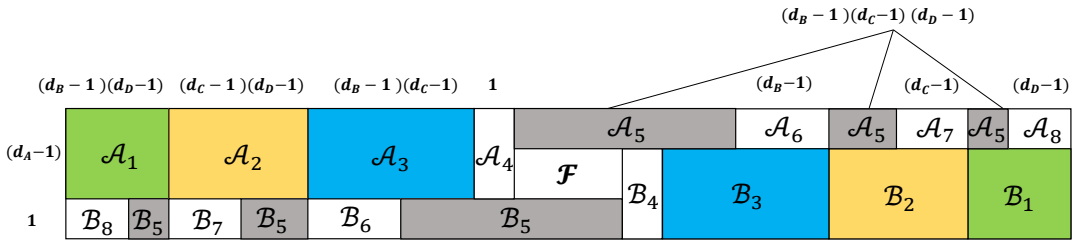

图 3.15　公式(3.18)给出的 $\cup_{i=1}^{8}\{\mathcal{A}_i,\mathcal{B}_i\}\cup\mathcal{F}$ 在两体划分 $A|BCD$ 下对应的 $d_A \times d_B d_C d_D$ 网格。此外，对于 $1 \leqslant i \leqslant 8$，$\mathcal{A}_i$ 与 $\mathcal{B}_i$ 是对称的。

注意对于 $X \in \{A,B,C,D\}$，$\{|\eta_s\rangle_X\}_{s\in\mathbb{Z}_{d_X-1}}$，$\{|\xi_s\rangle_X\}_{s\in\mathbb{Z}_{d_X-1}}$ 和 $\{|\beta_s\rangle_X\}_{s\in\mathbb{Z}_{d_X-2}}$

是三个正交集，它们分别由 $\{|t\rangle_X\}_{t=0}^{d_X-2}$，$\{|t\rangle_X\}_{t=1}^{d_X-1}$ 和 $\{|t\rangle_X\}_{t=1}^{d_X-2}$ 生成。这 17 个子集 $\cup_{i=1}^{8}\{\mathcal{A}_i,\mathcal{B}_i\}\cup\mathcal{F}$ 在两体划分 $A|BCD$ 下对应于图3.15中 $d_A\times d_Bd_Cd_D$ 网格的 17 块。现在我们可以给出四体系统中的不可扩充乘积基。

引理 3.6　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}\otimes\mathbb{C}^{d_D}$ 中，$3\leqslant d_A\leqslant d_B\leqslant d_C\leqslant d_D$，公式(3.18)给出的 $\cup_{i=1}^{8}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}$ 是一个不可扩充乘积基，且 $|\cup_{i=1}^{8}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}|=d_Ad_Bd_Cd_D-16$。

证明　由图3.15可知，对于任何 $3\leqslant d_A\leqslant d_B\leqslant d_C\leqslant d_D$，$\cup_{i=1}^{8}\{\mathcal{A}_i,\mathcal{B}_i\}\cup\mathcal{F}\cup\{|S\rangle\}$ 具有类似的结构。不失一般性，我们只考虑 $d_A=d_B=d_C=d_D=3$ 的情况。注意，在这种情况下，$\mathcal{F}=\varnothing$。与例3.2的证明类似，我们用反证法证明。假设在 $\cup_{i=1}^{8}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\{|S\rangle\}$ 生成的子空间的正交补空间中存在一个乘积态 $|\psi\rangle$。然后我们考虑 $|\psi\rangle$ 在两体划分 $A|BCD$、$AB|CD$ 和 $ABC|D$ 下的矩阵形式。首先，考虑两体划分 $A|BCD$，我们有

$$M=\begin{bmatrix}
a_0&a_0&a_0&a_0&b_0&b_0&b_0&b_0&c_0&c_0&c_0&c_0&d_0&e_0&e_0&e_0&e_0&f_0&f_0&e_0&e_0&g_0&g_0&e_0&e_0&h_0&h_0\\
a_0&a_0&a_0&a_0&b_0&b_0&b_0&b_0&c_0&c_0&c_0&c_0&d_0&s&d_1&c_1&c_1&c_1&c_1&b_1&b_1&b_1&b_1&a_1&a_1&a_1&a_1\\
h_1&h_1&e_1&e_1&g_1&g_1&e_1&e_1&f_1&f_1&e_1&e_1&e_1&e_1&d_1&c_1&c_1&c_1&c_1&b_1&b_1&b_1&b_1&a_1&a_1&a_1&a_1
\end{bmatrix},$$

$$\operatorname{rank}(M)=1,\quad \operatorname{sum}(M)=0. \tag{3.19}$$

然后我们考虑两体划分 $AB|CD$。我们将 M 的第一行按照坐标 $\{X\}_{AB}\times\{Y\}_{CD}$ 的方式排成一个 3×9 的矩阵 M_2，同样将 M 的最后一行按照坐标 $\{X\}_{AB}\times\{Y\}_{CD}$ 的方式排成一个 3×9 的矩阵 M_0，那么

$$M_2=\begin{bmatrix}
b_0&b_0&d_0&b_0&b_0&h_0&h_0&c_0&c_0\\
f_0&a_0&a_0&e_0&e_0&e_0&e_0&c_0&c_0\\
f_0&a_0&a_0&e_0&e_0&e_0&e_0&g_0&g_0
\end{bmatrix},\quad \operatorname{rank}(M_2)=0\text{ 或 }1, \tag{3.20}$$

$$M_0=\begin{bmatrix}
g_1&g_1&e_1&e_1&e_1&e_1&a_1&a_1&f_1\\
c_1&c_1&e_1&e_1&e_1&e_1&a_1&a_1&f_1\\
c_1&c_1&h_1&h_1&b_1&b_1&d_1&b_1&b_1
\end{bmatrix},\quad \operatorname{rank}(M_0)=0\text{ 或 }1, \tag{3.21}$$

下面我们考虑两体划分 $ABC|D$。我们将 M 的第一行按照坐标 $\{X\}_{ABC}\times\{Y\}_D$ 的方式排成一个 9×3 的矩阵 N_2，同样将 M 的最后一行按照坐标 $\{X\}_{ABC}\times\{Y\}_D$ 的方式排成一个 9×3 的矩阵 N_0，那么

$$N_2=\begin{bmatrix}
h_0&b_0&b_0&e_0&e_0&e_0&e_0&f_0&f_0\\
h_0&b_0&b_0&e_0&e_0&e_0&e_0&a_0&a_0\\
c_0&c_0&d_0&c_0&c_0&g_0&g_0&a_0&a_0
\end{bmatrix}^T,\quad \operatorname{rank}(N_2)=0\text{ 或 }1, \tag{3.22}$$

$$N_0=\begin{bmatrix} a_1 & a_1 & g_1 & g_1 & c_1 & c_1 & d_1 & c_1 & c_1 \\ a_1 & a_1 & e_1 & e_1 & e_1 & e_1 & b_1 & b_1 & h_1 \\ f_1 & f_1 & e_1 & e_1 & e_1 & e_1 & b_1 & b_1 & h_1 \end{bmatrix}^T, \quad \mathrm{rank}(N_0)=0 \text{ 或 } 1. \tag{3.23}$$

假设 $a_0\neq 0$。由于 $\mathrm{rank}(M)=1$，我们有 $h_1=e_1$ 和 $e_0=s=d_1=c_1=f_0=b_1=g_0=a_1=h_0$。通过公式(3.22)，我们得到 $e_0=c_0=b_0=d_0$。

(i) 如果 $e_0\neq 0$，那么由公式(3.20)得出 $e_0=a_0$，由公式(3.21) 得出 $e_0=g_1=e_1=f_1$。这与 $\mathrm{sum}(M)=0$ 相矛盾。

(ii) 如果 $e_0=0$, 那么通过 $\mathrm{rank}(M)=1$ 可知, $g_1=e_1=f_1=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾。

因此我们有 $a_0=0$。根据 M 的对称性，我们有 $a_1=0$。

假设 $b_0\neq 0$。由于 $\mathrm{rank}(M)=1$，我们有 $h_1=e_1=g_1=0$，并且 $e_0=s=d_1=c_1=f_0=b_1=g_0=a_1=h_0=0$。通过公式(3.22)，我们得到 $c_0=d_0=0$。此外，由于 $\mathrm{rank}(M)=1$，我们有 $f_1=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾，因此我们有 $b_0=b_1=0$。

假设 $c_0\neq 0$。由于 $\mathrm{rank}(M)=1$，我们有 $h_1=e_1=g_1=f_1=0$，并且 $e_0=s=d_1=c_1=f_0=b_1=g_0=a_1=h_0=0$。通过公式(3.20)，我们得到 $d_0=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾，因此我们有 $c_0=c_1=0$。

假设 $d_0\neq 0$。由于 $\mathrm{rank}(M)=1$，我们有 $h_1=e_1=g_1=f_1=0$，并且 $e_0=s=d_1=c_1=f_0=b_1=g_0=a_1=h_0=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾，因此我们有 $d_0=d_1=0$。

假设 $h_1\neq 0$。由于 $\mathrm{rank}(M)=1$，我们有 $e_0=s=f_0=g_0=h_0=0$。通过公式(3.21)，我们得到 $e_1=g_1=f_1=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾，因此我们有 $h_0=h_1=0$。

假设 $e_1\neq 0$。由于 $\mathrm{rank}(M)=1$, 我们有 $e_0=s=f_0=g_0=0$。通过公式(3.23), 我们得到 $f_1=g_1=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾，因此我们有 $e_0=e_1=0$。

假设 $g_1\neq 0$。由于 $\mathrm{rank}(M)=1$，我们有 $s=f_0=g_0=0$。通过公式(3.21), 我们得到 $f_1=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾，因此从而我们有 $g_0=g_1=0$。

假设 $f_1\neq 0$。由于 $\mathrm{rank}(M)=1$，我们有 $s=f_0=0$。这与 $\mathrm{sum}(M)=0$ 相矛盾，因此我们有 $f_0=f_1=0$。

因为 $\mathrm{sum}(M)=0$，所以我们必然有 $s=0$，但这与 $\mathrm{rank}(M)=1$ 相矛盾。因此 $|\psi\rangle$ 是一个纠缠态，从而 $\cup_{i=1}^{8}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\{|S\rangle\}$ 是一个不可扩充乘积基。当 $3\leqslant d_A\leqslant d_B\leqslant d_C\leqslant d_D$ 时，证明与上述证明类似。 ∎

与三体系统情况类似，我们可以在四体系统中构造更多的不可扩充乘积基。假设四维超立方体处于从外到内的第 n 层, 则 $0\leqslant n\leqslant\lfloor\frac{d_A-3}{2}\rfloor$。令 $X_n:=d_X-2n$,

其中 $X \in \{A, B, C, D\}$。然后我们可以定义以下态:

$$
\begin{aligned}
\mathcal{A}_1^{(n)} :=& \{|\xi_i^{(n)}\rangle_A|\eta_j^{(n)}\rangle_B|n\rangle_C|\xi_k^{(n)}\rangle_D : (i,j,k) \in \mathbb{Z}_{A_n-1} \times \mathbb{Z}_{B_n-1} \times \mathbb{Z}_{D_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_2^{(n)} :=& \{|\xi_i^{(n)}\rangle_A|d_B-1-n\rangle_B|\eta_j^{(n)}\rangle_C|\eta_k^{(n)}\rangle_D : (i,j,k) \in \mathbb{Z}_{A_n-1} \times \mathbb{Z}_{C_n-1} \times \mathbb{Z}_{D_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_3^{(n)} :=& \{|\xi_i^{(n)}\rangle_A|\xi_j^{(n)}\rangle_B|\xi_k^{(n)}\rangle_C|d_C-1-n\rangle_D : (i,j,k) \in \mathbb{Z}_{A_n-1} \times \mathbb{Z}_{B_n-1} \times \mathbb{Z}_{C_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_4^{(n)} :=& \{|\xi_i^{(n)}\rangle_A|d_B-1-n\rangle_B|n\rangle_C|d_D-1-n\rangle_D : i \in \mathbb{Z}_{A_n-1} \setminus \{0\}\},\\
\mathcal{A}_5^{(n)} :=& \{|d_A-1-n\rangle_A|\eta_i^{(n)}\rangle_B|\xi_j^{(n)}\rangle_C|\eta_k^{(n)}\rangle_D : (i,j,k) \in \mathbb{Z}_{B_n-1} \times \mathbb{Z}_{C_n-1} \times \mathbb{Z}_{D_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{A}_6^{(n)} :=& \{|d_A-1-n\rangle_A|\eta_i^{(n)}\rangle_B|n\rangle_C|n\rangle_D : i \in \mathbb{Z}_{B_n-1} \setminus \{0\}\},\\
\mathcal{A}_7^{(n)} :=& \{|d_A-1-n\rangle_A|n\rangle_B|\xi_i^{(n)}\rangle_C|d_D-1-n\rangle_D : i \in \mathbb{Z}_{C_n-1} \setminus \{0\}\},\\
\mathcal{A}_8^{(n)} :=& \{|d_A-1-n\rangle_A|d_B-1-n\rangle_B|d_C-1-n\rangle_C|\eta_i^{(n)}\rangle_D : i \in \mathbb{Z}_{D_n-1} \setminus \{0\}\},\\
\mathcal{B}_1^{(n)} :=& \{|\eta_i^{(n)}\rangle_A|\xi_j^{(n)}\rangle_B|d_C-1-n\rangle_C|\eta_k^{(n)}\rangle_D : (i,j,k) \in \mathbb{Z}_{A_n-1} \times \mathbb{Z}_{B_n-1} \times \mathbb{Z}_{D_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_2^{(n)} :=& \{|\eta_i^{(n)}\rangle_A|n\rangle_B|\xi_j^{(n)}\rangle_C|\xi_k^{(n)}\rangle_D : (i,j,k) \in \mathbb{Z}_{A_n-1} \times \mathbb{Z}_{C_n-1} \times \mathbb{Z}_{D_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_3^{(n)} :=& \{|\eta_i^{(n)}\rangle_A|\eta_j^{(n)}\rangle_B|\eta_k^{(n)}\rangle_C|0\rangle_D : (i,j,k) \in \mathbb{Z}_{A_n-1} \times \mathbb{Z}_{B_n-1} \times \mathbb{Z}_{C_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_4^{(n)} :=& \{|\eta_i^{(n)}\rangle_A|n\rangle_B|d_C-1-n\rangle_C|n\rangle_D : i \in \mathbb{Z}_{A_n-1} \setminus \{0\}\},\\
\mathcal{B}_5^{(n)} :=& \{|n\rangle_A|\xi_i^{(n)}\rangle_B|\eta_j^{(n)}\rangle_C|\xi_k^{(n)}\rangle_D : (i,j,k) \in \mathbb{Z}_{B_n-1} \times \mathbb{Z}_{C_n-1} \times \mathbb{Z}_{D_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{B}_6^{(n)} :=& \{|n\rangle_A|\xi_i^{(n)}\rangle_B|d_C-1-n\rangle_C|d_D-1-n\rangle_D : i \in \mathbb{Z}_{B_n-1} \setminus \{0\}\},\\
\mathcal{B}_7^{(n)} :=& \{|n\rangle_A|d_B-1-n\rangle_B|\eta_i^{(n)}\rangle_C|n\rangle_D : i \in \mathbb{Z}_{C_n-1} \setminus \{0\}\},\\
\mathcal{B}_8^{(n)} :=& \{|n\rangle_A|n\rangle_B|n\rangle_C|\xi_i^{(n)}\rangle_D : i \in \mathbb{Z}_{D_n-1} \setminus \{(0,0,0)\}\},\\
\mathcal{F}^{(n)} :=& \{|\beta_i^{(n)}\rangle_A|\beta_j^{(n)}\rangle_B|\beta_k^{(n)}\rangle_C|\beta_\ell^{(n)}\rangle_D : (i,j,k,\ell) \in \mathbb{Z}_{A_n-2} \times \mathbb{Z}_{B_n-2} \times \mathbb{Z}_{C_n-2} \times \mathbb{Z}_{D_n-2} \setminus \{(0,0,0,0)\}\},\\
|S\rangle :=& \left(\sum_{i=0}^{d_A-1}|i\rangle\right)_A\left(\sum_{j=0}^{d_B-1}|j\rangle\right)_B\left(\sum_{k=0}^{d_C-1}|k\rangle\right)_C\left(\sum_{\ell=0}^{d_D-1}|\ell\rangle\right)_D,
\end{aligned}
\tag{3.24}
$$

其中 $|\eta_s^{(n)}\rangle_X = \sum_{t=n}^{X_n+n-2} w_{X_n-1}^{s(t-n)}|t\rangle_X$，$|\xi_s^{(n)}\rangle_X = \sum_{t=n}^{X_n+n-2} w_{X_n-1}^{s(t-n)}|t+1\rangle_X$，$s \in \mathbb{Z}_{X_n-1}$，$X \in \{A, B, C, D\}$；且 $|\beta_s^{(n)}\rangle_X = \sum_{t=n}^{X_n+n-3} w_{X_n-2}^{s(t-n)}|t+1\rangle_X$，$s \in \mathbb{Z}_{X_n-2}$，$X \in \{A, B, C, D\}$。

注意对于 $X \in \{A, B, C, D\}$，$\{|\eta_s^{(n)}\rangle_X\}_{s\in\mathbb{Z}_{X_n-1}}$，$\{|\xi_s^{(n)}\rangle_X\}_{s\in\mathbb{Z}_{X_n-1}}$，和 $\{|\beta_s^{(n)}\rangle_X\}_{s\in\mathbb{Z}_{X_n-2}}$ 是三个正交乘积集，它们分别由 $\{|t\rangle_X\}_{t=n}^{X_n+n-2}$，$\{|t\rangle_X\}_{t=n+1}^{X_n+n-1}$，和 $\{|t\rangle_X\}_{t=n+1}^{X_n+n-2}$ 生成。那我们有以下定理。

定理 3.7　在 $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_C} \otimes \mathbb{C}^{d_D}$ 中，$3 \leqslant d_A \leqslant d_B \leqslant d_C \leqslant d_D$，对于任何 $0 \leqslant n \leqslant \lfloor \frac{d_A-3}{2} \rfloor$，公式(3.24)给出的

$$
\mathcal{U}_n := \cup_{t=0}^{n}(\cup_{i=1}^{8}(\mathcal{A}_i^{(t)} \cup \mathcal{B}_i^{(t)})) \cup \mathcal{F}^{(n)} \cup \{|S\rangle\}
$$

是一个不可扩充乘积基，且 $|\mathcal{U}_n| = d_A d_B d_C d_D - 16(n+1)$。

定理3.7的证明与定理3.5的证明类似。

3.6　不可扩充乘积基的纠缠辅助区分

由于不可扩充乘积基是局部不可区分的，我们在本节中将研究引理3.2构造的不可扩充乘积基的纠缠辅助区分。当 $m=n\geqslant 3$ 为偶数时，引理3.2构造的不可扩充乘积基可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil}\otimes\mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分[119]。我们将证明这个性质对引理3.2中所有的不可扩充乘积基都成立。我们首先讨论 $4=m\leqslant n$ 的情形。在引理3.2中，$\mathbb{C}^4\otimes\mathbb{C}^n$ 中数目为 $4n-4$ 的不可扩充乘积基如下所示：

$$
\begin{aligned}
|\psi_i\rangle =&|0\rangle_A\left(\sum_{j=0}^{n-2}w_{n-1}^{ij}|j\rangle\right)_B, \quad 1\leqslant i\leqslant n-2,\\
|\psi_{i+n-2}\rangle =&\left(\sum_{j=0}^{2}w_3^{ij}|j\rangle\right)_A|n-1\rangle_B, \quad 1\leqslant i\leqslant 2,\\
|\psi_{i+n}\rangle =&|3\rangle_A\left(\sum_{j=1}^{n-1}w_{n-1}^{ij}|j\rangle\right)_B, \quad 1\leqslant i\leqslant n-2,\\
|\psi_{i+2n-2}\rangle =&\left(\sum_{j=1}^{3}w_3^{ij}|j\rangle\right)_A|0\rangle_B, \quad 1\leqslant i\leqslant 2,\\
|\psi_{i+2n}\rangle =&(|1\rangle+|2\rangle)_A\left(\sum_{j=1}^{n-2}w_{n-2}^{ij}|j\rangle\right)_B, \quad 1\leqslant i\leqslant n-3,\\
|\psi_{i+3n-2}\rangle =&(|1\rangle-|2\rangle)_A\left(\sum_{j=1}^{n-2}w_{n-2}^{ij}|j\rangle\right)_B, \quad 0\leqslant i\leqslant n-3,\\
|S\rangle =&(|0\rangle+|1\rangle+|2\rangle+|3\rangle)_A(|0\rangle+|1\rangle+\cdots+|n-1\rangle)_B.
\end{aligned}
\tag{3.25}
$$

我们有如下引理：

引理 3.8　在 $\mathbb{C}^4\otimes\mathbb{C}^n$ 中，公式(3.25)给出的不可扩充乘积基可以借助于 $\mathbb{C}^2\otimes\mathbb{C}^2$ 中的一个最大纠缠态来完成局部区分。

证明　令 Alice 和 Bob 两个人分享 $\mathbb{C}^2\otimes\mathbb{C}^2$ 中的一个最大纠缠态 $|\psi\rangle_{ab}=|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b$，那么最开始的态为：

$$
\begin{aligned}
&|\psi_i\rangle\to|\psi_i\rangle|\psi\rangle_{ab}, \quad 1\leqslant i\leqslant 4n-5;\\
&|S\rangle\to|S\rangle|\psi\rangle_{ab},
\end{aligned}
\tag{3.26}
$$

其中 a 和 b 分别是 Alice 和 Bob 的辅助系统，那么区分过程如下：

步骤 1 Alice 进行测量

$$\begin{aligned}\{M_1 =&|0\rangle_A\langle 0|\otimes|0\rangle_a\langle 0|+|1\rangle_A\langle 1|\otimes|0\rangle_a\langle 0|\\ &+|2\rangle_A\langle 2|\otimes|0\rangle_a\langle 0|+|3\rangle_A\langle 3|\otimes|1\rangle_a\langle 1|;\\ \overline{M_2} =&|0\rangle_A\langle 0|\otimes|1\rangle_a\langle 1|+|1\rangle_A\langle 1|\otimes|1\rangle_a\langle 1|\\ &+|2\rangle_A\langle 2|\otimes|1\rangle_a\langle 1|+|3\rangle_A\langle 3|\otimes|0\rangle_a\langle 0|\}.\end{aligned}$$

如果点击 M_1（即 M_1 作用在公式(3.26)上），那么测量后的态为

$$\begin{aligned}|\psi_i\rangle \to&|0\rangle_A\left(\sum_{j=0}^{n-2}w_{n-1}^{ij}|j\rangle\right)_B|0\rangle_a|0\rangle_b,\quad 1\leqslant i\leqslant n-2;\\ |\psi_{i+n-2}\rangle \to&\left(\sum_{j=0}^{2}w_3^{ij}|j\rangle\right)_A|n-1\rangle_B|0\rangle_a|0\rangle_b,\quad 1\leqslant i\leqslant 2;\\ |\psi_{i+n}\rangle \to&|3\rangle_A\left(\sum_{j=1}^{n-1}w_{n-1}^{ij}|j\rangle\right)_B|1\rangle_a|1\rangle_b,\quad 1\leqslant i\leqslant n-2;\\ |\psi_{i+2n-2}\rangle \to&\left(\sum_{j=1}^{2}w_3^{ij}|j\rangle\right)_A|0\rangle_B|0\rangle_a|0\rangle_b+w_3^{3i}|3\rangle_A|0\rangle_B|1\rangle_a|1\rangle_b,\quad 1\leqslant i\leqslant 2;\\ |\psi_{i+2n}\rangle \to&(|1\rangle+|2\rangle)_A\left(\sum_{j=1}^{n-2}w_{n-2}^{ij}|j\rangle\right)_B|0\rangle_a|0\rangle_b,\quad 1\leqslant i\leqslant n-3;\\ |\psi_{i+3n-2}\rangle \to&(|1\rangle-|2\rangle)_A\left(\sum_{j=1}^{n-2}w_{n-2}^{ij}|j\rangle\right)_B|0\rangle_a|0\rangle_b,\quad 0\leqslant i\leqslant n-3;\\ |S\rangle \to&(|0\rangle+|1\rangle+|2\rangle)_A(|0\rangle+|1\rangle+\cdots+|n-1\rangle)_B|0\rangle_a|0\rangle_b\\ &+|3\rangle_A(|0\rangle+|1\rangle+\cdots+|n-1\rangle)_B|1\rangle_a|1\rangle_b.\end{aligned}\tag{3.27}$$

步骤 2 Bob 进行测量

$$\left\{\{M_{2,i}\}_{i=1}^{n-1};M_{2,n}=|n-1\rangle_B\langle n-1|\otimes|0\rangle_b\langle 0|;\overline{M_2}=\mathbb{I}-\sum_{i=1}^{n}M_{2,i}\right\},$$

其中 $M_{2,i}=\left(\sum_{j=1}^{n-1}w_{n-1}^{ij}|j\rangle\right)_B\left(\sum_{j=1}^{n-1}w_{n-1}^{ij}\langle j|\right)\otimes|1\rangle_b\langle 1|$，$1\leqslant i\leqslant n-1$。对于 $1\leqslant i\leqslant n-2$，如果点击 $M_{2,i}$，那么可区分出 $|\psi_{i+n}\rangle$; 如果点击 $M_{2,n-1}$，那么 $|S\rangle\to|3\rangle_A(|1\rangle+\cdots+|n-1\rangle)_B|1\rangle_a|1\rangle_b$; 如果点击 $M_{2,n}$，那么剩下 $\{|\psi_{i+n-2}\rangle\}_{i=1}^{2}$ 和 $|S\rangle\to(|0\rangle+|1\rangle+|2\rangle)_A(|n-1\rangle)_B|0\rangle_a|0\rangle_b$，很显然 Alice 可以区分出这三个态; 如果点击 $\overline{M_2}$，那么剩下 $\{|\psi_i\rangle\}_{i=1}^{n-2}$，$\{|\psi_{i+2n-2}\rangle\}_{i=1}^{2}$，$\{|\psi_{i+2n}\rangle\}_{i=1}^{n-3}$，$\{|\psi_{i+3n-2}\rangle\}_{i=0}^{n-3}$，$|S\rangle\to(|0\rangle+|1\rangle+|2\rangle)_A\left(\sum_{j=0}^{n-2}|j\rangle\right)_B|0\rangle_a|0\rangle_b+|3\rangle_A|0\rangle_B|1\rangle_a|1\rangle_b$。

步骤 3 Alice 进行测量

$$\{M_3 = |0\rangle_A\langle 0| \otimes |0\rangle_a\langle 0|; \overline{M_3} = \mathbb{I} - M_3\},$$

如果点击 M_3, 那么剩下 $\{|\psi_i\rangle\}_{i=1}^{n-2}$ 和 $|S\rangle \to |0\rangle_A \left(\sum_{j=0}^{n-2} |j\rangle\right)_B |0\rangle_a|0\rangle_b$, Bob 可以区分出这些态; 如果点击 $\overline{M_3}$, 那么剩下 $\{|\psi_{i+2n-2}\rangle\}_{i=1}^{2}$, $\{|\psi_{i+2n}\rangle\}_{i=1}^{n-3}$, $\{|\psi_{i+3n-2}\rangle\}_{i=0}^{n-3}$, $|S\rangle \to (|1\rangle + |2\rangle)_A \left(\sum_{j=0}^{n-2} |j\rangle\right)_B |0\rangle_a|0\rangle_b + |3\rangle_A|0\rangle_B|1\rangle_a|1\rangle_b$。

步骤 4 Bob 进行测量

$$\{M_4 = |0\rangle_B\langle 0|; \overline{M_4} = \mathbb{I} - M_4\},$$

如果点击 M_4，那么剩下 $\{|\psi_{i+2n-2}\rangle\}_{i=1}^{2}$ 和 $|S\rangle \to (|1\rangle + |2\rangle)_A|0\rangle_B|0\rangle_a|0\rangle_b + |3\rangle_A|0\rangle_B|1\rangle_a|1\rangle_b$。然后 Bob 进行测量 $\{(|0\rangle+|1\rangle)_b(\langle 0|+\langle 1|); (|0\rangle-|1\rangle)_b(\langle 0|-\langle 1|)\}$, 点击其中任意一个测量算子，测量后 Bob 部分有相同的态，Alice 部分有相互正交的态，从而 Alice 可以区分出 $\{|\psi_{i+2n-2}\rangle\}_{i=1}^{2}$ 和 $|S\rangle$。如果点击 $\overline{M_4}$，那么剩下 $\{|\psi_{i+2n}\rangle\}_{i=1}^{n-3}$，$\{|\psi_{i+3n-2}\rangle\}_{i=0}^{n-3}$，$|S\rangle \to (|1\rangle + |2\rangle)_A \left(\sum_{j=1}^{n-2} |j\rangle\right)_B |0\rangle_a|0\rangle_b$。

步骤 5 Alice 进行测量

$$\{M_5 = (|1\rangle + |2\rangle)_A(\langle 1| + \langle 2|); \overline{M_5} = \mathbb{I} - M_5\},$$

如果点击 M_5，那么剩下 $\{|\psi_{i+2n}\rangle\}_{i=1}^{n-3}$ 和 $|S\rangle \to (|1\rangle + |2\rangle)_A \left(\sum_{j=1}^{n-2} |j\rangle\right)_B |0\rangle_a|0\rangle_b$, Bob 可以区分出这些态；如果点击 $\overline{M_5}$，那么剩下 $\{|\psi_{i+3n-2}\rangle\}_{i=0}^{n-3}$，Bob 也可以区分出这些态。

如果在步骤 1 中，Alice 点击 $\overline{M_2}$，将会得到一个类似的区分过程，所以引理得证。 ∎

接下来，我们考虑引理3.2所有的不可扩充乘积基的纠缠辅助区分。当 $4 \leqslant m \leqslant n$ 且 m 为偶数时，引理3.2给出的数目为 $mn - 2m + 4$ 的不可扩充乘积基所下所示。为了方便起见，我们记 $\iota \triangleq \frac{m}{2}$。

$$|\psi_i\rangle = |0\rangle_A \left(\sum_{j=0}^{n-2} w_{n-1}^{ij} |j\rangle\right)_B, \quad 1 \leqslant i \leqslant n-2;$$

$$|\psi_{i+n-2}\rangle = \left(\sum_{j=0}^{m-2} w_{m-1}^{ij} |j\rangle\right)_A |n-1\rangle_B, \quad 1 \leqslant i \leqslant m-2;$$

$$|\psi_{i+m+n-4}\rangle = |m-1\rangle_A \left(\sum_{j=1}^{n-1} w_{n-1}^{ij} |j\rangle\right)_B, \quad 1 \leqslant i \leqslant n-2;$$

$$|\psi_{i+m+2n-6}\rangle = \left(\sum_{j=1}^{m-1} w_{m-1}^{ij} |j\rangle\right)_A |0\rangle_B, \quad 1 \leqslant i \leqslant m-2;$$

$$
\begin{aligned}
|\psi_{i+2m+2n-8}\rangle =& |1\rangle_A \left(\sum_{j=1}^{n-3} w_{n-3}^{ij}|j\rangle\right)_B, \quad 1 \leqslant i \leqslant n-4;\\
|\psi_{i+2m+3n-12}\rangle =& \left(\sum_{j=1}^{m-3} w_{m-3}^{ij}|j\rangle\right)_A |n-2\rangle_B, \quad 1 \leqslant i \leqslant m-4;\\
|\psi_{i+3m+3n-16}\rangle =& |m-2\rangle_A \left(\sum_{j=2}^{n-2} w_{n-3}^{ij}|j\rangle\right)_B, \quad 1 \leqslant i \leqslant n-4;\\
|\psi_{i+3m+4n-20}\rangle =& \left(\sum_{j=2}^{m-2} w_{m-3}^{ij}|j\rangle\right)_A |1\rangle_B, \quad 1 \leqslant i \leqslant m-4;\\
&\cdots\\
|\psi_{mn-2n+i}\rangle =& (|\iota-1\rangle + |\iota\rangle)_A \left(\sum_{j=\iota-1}^{n-\iota} w_{n-m+2}^{ij}|j\rangle\right)_B, \quad 1 \leqslant i \leqslant n-m+1;\\
|\psi_{mn-n-m+2+i}\rangle =& (|\iota-1\rangle - |\iota\rangle)_A \left(\sum_{j=\iota-1}^{n-\iota} w_{n-m+2}^{ij}|j\rangle\right)_B, \quad 0 \leqslant i \leqslant n-m+1;\\
|S\rangle =& (|0\rangle + |1\rangle + \cdots + |m-1\rangle)_A (|0\rangle + |1\rangle + \cdots + |n-1\rangle)_B . \qquad (3.28)
\end{aligned}
$$

首先我们证明公式(3.28)给出的不可扩充乘积基可以借助于 $\mathbb{C}^\iota \otimes \mathbb{C}^\iota$ 中的一个最大纠缠态来完成局部区分，然后我们再考虑 m 为奇数的情形。

定理 3.9　在 $\mathbb{C}^m \otimes \mathbb{C}^n$ 中，引理3.2给出的不可扩充乘积基可以借助于 $\mathbb{C}^{\lceil \frac{m}{2} \rceil} \otimes \mathbb{C}^{\lceil \frac{m}{2} \rceil}$ 中的一个最大纠缠态来完成局部区分。

证明　令 $m \geqslant 4$ 为偶数，我们通过对 m 归纳来证明。当 $m = 4$ 时，我们在引理3.8中已经证明了该定理成立。我们将公式(3.28)中的参数 m 全部替换为参数 k，并假设当 $k = m-2$ 时，公式(3.28)可以借助于 $\mathbb{C}^{\iota-1} \otimes \mathbb{C}^{\iota-1}$ 中的一个最大纠缠态来完成局部区分。我们只需证明当 $k = m$ 时，公式(3.28)可以借助于 $\mathbb{C}^\iota \otimes \mathbb{C}^\iota$ 中的一个最大纠缠态来完成局部区分。

令 Alice 和 Bob 两个人分享 $\mathbb{C}^\iota \otimes \mathbb{C}^\iota$ 中的一个最大纠缠态 $|\psi\rangle_{ab} = \sum_{i=0}^{\iota-1} |i\rangle_a |i\rangle_b$，那么最开始的态为：$|\psi_i\rangle \to |\psi_i\rangle|\psi\rangle_{ab}$，$1 \leqslant i \leqslant mn-2m+3$；$|S\rangle \to |S\rangle|\psi\rangle_{ab}$。其中 a 和 b 分别是 Alice 和 Bob 的辅助系统。Alice 进行测量

$$
\begin{aligned}
\{M_1 =& |0\rangle_A\langle 0| \otimes |0\rangle_a\langle 0| + |1\rangle_A\langle 1| \otimes |0\rangle_a\langle 0| + \cdots + |\iota\rangle_A\langle \iota| \otimes |0\rangle_a\langle 0|\\
&+ |\iota+1\rangle_A\langle \iota+1| \otimes |1\rangle_a\langle 1| + \cdots + |m-1\rangle_A\langle m-1| \otimes |\iota-1\rangle_a\langle \iota-1|;\\
\{M_i =& \sum_{j=0}^{\iota-1} |j\rangle_A\langle 0| \otimes |0\rangle_a\langle 0| + \sum_{j=0}^{\iota-1} |\iota+j\rangle_A\langle \iota+j| \otimes |j+i-1\rangle_a\langle j+i-1|\}_{i=2}^{\iota}\}.
\end{aligned}
$$

那么后面的过程与引理3.8类似，我们剩下 $\{|\psi_i\rangle\}_{i=2m+2n-7}^{mn-2m+3}$ 和 $|S\rangle \to$

$\left(\sum_{j=1}^{\iota-1}|j\rangle\right)_A\left(\sum_{e=1}^{n-2}|e\rangle\right)_B|0\rangle_a|0\rangle_b+\sum_{j=0}^{\iota-2}|\iota+j\rangle_A\left(\sum_{e=1}^{n-2}|e\rangle\right)_B|j\rangle_a|j\rangle_b$。由归纳假设可知，上面这些态可以局部区分。从而公式(3.28)可以借助于 $\mathbb{C}^{\iota}\otimes\mathbb{C}^{\iota}$ 中的一个最大纠缠态来完成局部区分。

当 $m=n\geqslant 3$ 为奇数时，引理3.2给出的不可扩充乘积基可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil}\otimes\mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分。当 $3\leqslant m\leqslant n$，且 m 为奇数时，采用相同的方法，我们可以证明该定理也成立。综上，定理得证。 ∎

当 $m\leqslant n$ 时，通过隐形传态协议，$\mathbb{C}^m\otimes\mathbb{C}^n$ 中任意一组正交态都可以借助于 $\mathbb{C}^m\otimes\mathbb{C}^m$ 中的一个最大纠缠态来完成局部区分[49,98]，这说明我们的区分协议所消耗的纠缠资源比隐形传态协议所消耗的要少。注意 Gentiles2 不可扩充乘积基也可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil}\otimes\mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分[42]，但 Gentiles2 不可扩充乘积基的数目与引理3.2中的不可扩充乘积基的数目不同，因此我们猜测，当 $m\leqslant n$ 时，$\mathbb{C}^m\otimes\mathbb{C}^n$ 中所有不可扩充乘积基都可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil}\otimes\mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分。

3.7　本章小结

本章中，我们建立了两体系统中的不可扩充乘积基与砖块结构之间的关系，利用这个关系，我们构造了两体系统中一系列较大数目的不可扩充乘积基，由此回答了文献[39]中的一个公开问题。我们同样将这种方法推广到了多体系统，即利用多维超立方体的分解来构造多体系统中的不可扩充乘积基，并成功地构造了三体和四体系统中数目较大的不可扩充乘积基。此外，由于不可扩充乘积基是局部不可区分的，我们研究了两体系统中的不可扩充乘积基的纠缠辅助区分。下面我们给出几个遗留的问题：

1. 对于任何的 $N\geqslant 5$，$d_i\geqslant 3$，$1\leqslant i\leqslant N$，是否可以利用多维超立方体的分解来构造 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的不可扩充乘积基？
2. 利用多维超立方体的分解来构造的不可扩充乘积基的最小数目是多少？
3. 对于 $m\leqslant n$，$\mathbb{C}^m\otimes\mathbb{C}^n$ 中所有的不可扩充乘积基是否都可以借助于 $\mathbb{C}^{\lceil\frac{m}{2}\rceil}\otimes\mathbb{C}^{\lceil\frac{m}{2}\rceil}$ 中的一个最大纠缠态来完成局部区分？

第 4 章　强量子非局域性

强量子非局域性可以阻止合谋情形下的信息获取, 从而进一步提高信息的安全性。本章将研究具有强量子非局域性的正交集。4.1 节介绍了强量子非局域性的研究背景及其现状。4.2 节介绍了强量子非局域性的基本概念和主要方法。4.3 节构造了三体、四体和五体系统中的强非局域的正交乘积集。4.4 节证明了 3.4 节和 3.5 节中的不可扩充乘积基具有强量子非局域性。4.5 节给出了 N 体齐次系统中的强非局域的正交纠缠集。4.6 节为本章小结。

4.1　引言

量子非局域性是量子力学中最重要的性质之一。如果纠缠态违反 Bell 型不等式, 那么它具有 Bell 型非局域性[1-2]。如果一组正交态是局部不可区分的, 那么这组正交态也具有量子非局域性, 但与 Bell 型非局域性不同, 原因是 Bell 型非局域性只发生在纠缠态中, 而基于局部不可区分性的非局域性不限于于此。Bennett 等人[3]首先在 $\mathbb{C}^3\otimes\mathbb{C}^3$ 中构造了一个局部不可区分的正交乘积基，这表明了无纠缠的量子非局域性现象。后来, 局部不可区分的正交乘积集和正交纠缠集被广泛地研究[4-21]。当信息被编码在复合子系统中一个局部不可区分的集合中时, 这个信息将不能通过 LOCC 操作在空间分离的子系统之间完全检索。因此，局部不可区分性可用于量子数据隐藏[22-25] 和量子秘密共享[26-28]。

最近，Halder 等人[43]引入了局部不可约性和强量子非局域性的概念。如果通过正交保持的局部测量不能从一组多体正交态中消除一个或多个态，那么这组正交态被称为局部不可约的。一个局部不可约集一定是一个局部不可区分集, 反之则不一定成立。此外, 如果一组多体正交态在任意两体划分下都是局部不可约的，那么它被称为强非局域的。Halder 等人在 $\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3$ 和 $\mathbb{C}^4\otimes\mathbb{C}^4\otimes\mathbb{C}^4$ 中分别构造了强非局域的正交乘积基，这表明了无纠缠的强量子非局域性现象。此外 Halder 等人提出了几个公开问题:

1. 对于任何 $N\geqslant 4$，$d\geqslant 3$，如何构造 $(\mathbb{C}^d)^{\otimes N}$ 中强非局域的正交乘积集?
2. 是否存在强非局域的不可扩充乘积基?
3. 是否存在强非局域的正交纠缠集?

之后, 对于 $d\geqslant 3$, Yuan 等人[95]在 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 和 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^{d+1}$ 中分别构造了数目为 $6(d-1)^2$ 和 $6d^2-8d+4$ 的强非局域的正交乘积集（非不可扩充乘积基), 并在 $\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3$ 和 $\mathbb{C}^4\otimes\mathbb{C}^4\otimes\mathbb{C}^4\otimes\mathbb{C}^4$ 中分别构造了强非局域的正交乘积基[95]。利用图的连通性, 当 $d\geqslant 3$ 为奇数（偶数）时, Li 等人[96]在 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$

中构造了数目为 $d^3-(d-2)^2$（$d^3-(d-2)^2+2$）的强非局域的正交真实纠缠集。此外，强量子非定域性的概念也被扩展到更一般的情形[97-98,100-101,124]。尽管如此，上述 3 个问题没有被完全解决。

4.2　准备工作

在本节中，我们将介绍 Halder 等人[43]提出的局部不可约性和强量子非局域性的概念，并给出证明强量子非局域性的方法。

4.2.1　局部不可约性和强量子非局域性

在本章中，我们只考虑纯态，为了简单起见，我们不归一化态和算子。下面我们介绍局部不可约性的概念。

定义 4.1　在 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中，如果通过正交保持的局部测量不能从一组多体正交态中消除一个或多个态，那么这组正交态被称为*局部不可约的*。

一个局部可约的正交集意味着可以通过正交保持的局部测量将这个集合分成一些真子集。由定义可知，局部不可约性可以推出局部不可区分性，反之则不然。例如，考虑 $\mathbb{C}^2\otimes\mathbb{C}^3$ 中的一组正交态：

$$\begin{aligned}&|\psi_{1,2}\rangle=|0\rangle_A|0\rangle_B\pm|1\rangle_A|1\rangle_B,\quad |\psi_{3,4}\rangle=|0\rangle_A|1\rangle_B\pm|1\rangle_A|0\rangle_B,\\&|\psi_5\rangle=|0\rangle_A|2\rangle_B,\end{aligned}\tag{4.1}$$

由于 Bell 基 $\{|\psi_i\rangle\}_{i=1}^4$ 是局部不可区分的[120]，公式(4.1)给出的 $\{|\psi_i\rangle\}_{i=1}^5$ 也是局部不可区分的。然而，$\{|\psi_i\rangle\}_{i=1}^5$ 是局部可约的，这是因为 Bob 可以使用测量 $\{|2\rangle_B\langle 2|,\mathbb{I}_B-|2\rangle_B\langle 2|\}$ 分别消除 $\{|\psi_i\rangle\}_{i=1}^4$ 和 $|\psi_5\rangle$。

如何证明一组多体正交态是局部不可约的？这里存在一个充分条件[43]：对于一组多体正交态，如果作用在任何单体子系统上的任何正交保持的局部测量是平凡的，那么这组多体正交态是局部不可约的。例如，对于 Bell 基 $\{|\psi_i\rangle\}_{i=1}^4$，假设 Alice 进行一个正交保持的局部测量 $\{E=M^\dagger M\}$，且每个 POVM 元素 E 在基 $\{|0\rangle,|1\rangle\}$ 下可以表示为一个 2×2 的矩阵：

$$E=\begin{pmatrix}a_{0,0}&a_{0,1}\\a_{1,0}&a_{1,1}\end{pmatrix}.$$

那么测量后的态 $\{M\otimes\mathbb{I}_B|\psi_k\rangle\}_{k=1}^4$ 是相互正交的，即对于任何 $1\leqslant i\neq j\leqslant 4$，有

$$\langle\psi_i|E\otimes\mathbb{I}_B|\psi_j\rangle=0.$$

我们需要利用上述正交关系证明 $E\propto\mathbb{I}$。由于 $\langle\psi_1|E\otimes\mathbb{I}_B|\psi_2\rangle=0$，这推出 $a_{0,0}=a_{1,1}$。此外，由于 $\langle\psi_1|E\otimes\mathbb{I}_B|\psi_3\rangle=\langle\psi_1|E\otimes\mathbb{I}_B|\psi_4\rangle=0$，我们得到 $a_{0,1}\pm a_{1,0}=0$，

这推出 $a_{0,1}=a_{1,0}=0$。那么 $E\propto\mathbb{I}$，则该正交保持的局部测量是平凡的。由于 Bell 基的对称性，我们同样可以证明 Bob 进行的正交保持的局部测量也是平凡的。因此，Bell 基是局部不可约的。在本章中，我们主要利用此方法证明局部不可约性。下面我们介绍强量子非局域性。

定义 4.2　在 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中，如果一组多体正交态在任意两体划分下都是局部不可约的，那么这组正交态被称为*强非局域的*。

下面我们给出一个证明强量子非局域性的引理。

引理 4.1　假设 $\{|\psi\rangle\}$ 是 $\otimes_{i=1}^{N}\mathcal{H}_{A_i}$ 中的一组正交态。定义 $B_1:=\{A_2A_3\cdots A_N\}$，$B_2:=\{A_3\cdots A_NA_1\}$，$B_3:=\{A_4\cdots A_NA_1A_2\}$，$\cdots$，$B_N:=\{A_1\cdots A_{N-1}\}$。对于任何 $1\leqslant i\leqslant N$，如果 B_i 进行的任何正交保持的局部测量是平凡的，那么 $\{|\psi\rangle\}$ 是强非局域的。

证明　对于任何非平凡的两体划分 $A_{i_1}\cdots A_{i_j}|A_{i_{j+1}}\cdots A_{i_N}$，其中 $(i_1,i_2,\cdots,i_N)$ 是 $(1,2,\cdots,N)$ 的一个置换，且 $1\leqslant j\leqslant N-1$，则一定存在 $r,s\in\{1,2,\cdots,n\}$，使得 $A_{i_1}\cdots A_{i_j}\subset B_r$ 和 $A_{i_{j+1}}\cdots A_{i_n}\subset B_s$。因此，$A_{i_1}\cdots A_{i_j}$ 和 $A_{i_{j+1}}\cdots A_{i_n}$ 进行的正交保持的局部测量一定是平凡的。∎

本章中，我们主要利用此引理证明强量子非局域性。根据此引理，当 N 较大时，我们需要验证每个 B_i 进行的正交保持的局部测量是平凡的。如果 $\{|\psi\rangle\}$ 在子系统的循环置换下都有相同的结构，那么我们只需验证其中一个 B_i 进行的正交保持的局部测量是平凡的，这将大大降低计算难度。因此在本章中，我们所构造的 $\{|\psi\rangle\}$，在子系统的循环置换下都有相同的结构。

4.2.2　证明的基本方法

当正交态非常多的时候，测量后有很多的正交关系，证明正交保持的局部测量是平凡的将非常困难。因此，针对一难点，我们将给出两个重要的引理。在此之前，我们简化一下记号。

记 $\mathcal{H}_n$ 为 n 维 Hilbert 空间，并令 $\{|0\rangle,|1\rangle,\cdots,|n-1\rangle\}$ 为 $\mathcal{H}_n$ 中的一组计算基。对于任何作用在 $\mathcal{H}_n$ 上的算子 M，我们记矩阵 M 为算子 M 在计算基下的矩阵表示，一般情况下，我们不区分算子 M 和矩阵 M。我们可以把一个 $n\times n$ 的矩阵 E 表示为 $E:=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}a_{i,j}|i\rangle\langle j|$。令 $\mathcal{S},\mathcal{T}\subseteq\{|0\rangle,|1\rangle,\cdots,|n-1\rangle\}$，我们记

$$_{\mathcal{S}}E_{\mathcal{T}}:=\sum_{|s\rangle\in\mathcal{S}}\sum_{|t\rangle\in\mathcal{T}}a_{s,t}|s\rangle\langle t|.$$

这意味着 $_{\mathcal{S}}E_{\mathcal{T}}$ 为 E 的子矩阵，其中行坐标为 $\mathcal{S}$，列坐标为 $\mathcal{T}$。为了简单起见，当 $\mathcal{S}=\mathcal{T}$ 时，我们记 $E_{\mathcal{S}}:=_{\mathcal{S}}E_{\mathcal{S}}$。给定一个集合 $\mathcal{S}\subseteq\{|0\rangle,|1\rangle,\cdots,|n-1\rangle\}$ 和一个正交集 $\{|\psi_i\rangle\}_{i\in\mathbb{Z}_s}$，对于任何 $i\in\mathbb{Z}_s$，如果 $|\psi_i\rangle$ 是 $\mathcal{S}$ 中态的线性组合，那么称正

交集 $\{|\psi_i\rangle\}_{i\in\mathbb{Z}_s}$ 由 $\mathcal{S}$ 生成。记 span $\mathcal{S}$ 为 $\mathcal{S}$ 生成的子空间，dim(span $\mathcal{S}$) 为这个子空间的维数。现在，我们给出两个基本的引理。

引理 4.2　设一个 $n\times n$ 的矩阵 $E=(a_{i,j})_{i,j\in\mathbb{Z}_n}$ 是 Hermitian 算子 E 在基 $\mathcal{B}:=\{|0\rangle,|1\rangle,\cdots,|n-1\rangle\}$ 下的矩阵表示。给定 $\mathcal{B}$ 的两个非空不相交子集 $\mathcal{S}$ 和 $\mathcal{T}$，假设 $\{|\psi_i\rangle\}_{i=0}^{s-1}$，$\{|\phi_j\rangle\}_{j=0}^{t-1}$ 分别为 $\mathcal{S}$ 和 $\mathcal{T}$ 生成的正交集，其中 $s=|\mathcal{S}|$，$t=|\mathcal{T}|$。对于任何 $i\in\mathbb{Z}_s$，$j\in\mathbb{Z}_t$，如果 $\langle\psi_i|E|\phi_j\rangle=0$，那么 ${}_{\mathcal{S}}E_{\mathcal{T}}=\mathbf{0}$ 和 ${}_{\mathcal{T}}E_{\mathcal{S}}=\mathbf{0}$。

证明　由于 $\{|\psi_i\rangle\}_{i=0}^{s-1}$，$\{|\phi_j\rangle\}_{j=0}^{t-1}$ 分别为 $\mathcal{S}$ 和 $\mathcal{T}$ 生成的正交集，且 dim(span $\mathcal{S}$) $=s$，dim(span $\mathcal{T}$) $=t$，这推出

$$\begin{aligned}\text{span}\{|\psi_0\rangle,|\psi_1\rangle,\cdots,|\psi_{s-1}\rangle\}&=\text{span}\,\mathcal{S},\\ \text{span}\{|\phi_0\rangle,|\phi_1\rangle,\cdots,|\phi_{t-1}\rangle\}&=\text{span}\,\mathcal{T}.\end{aligned}\tag{4.2}$$

对于任何的 $|k\rangle\in\mathcal{S}$ 和 $|\ell\rangle\in\mathcal{T}$，由公式(4.2)可知，它们分别是 $\{|\psi_i\rangle\}_{i=0}^{s-1}$ 和 $\{|\phi_j\rangle\}_{j=0}^{t-1}$ 的线性组合。然后根据给定的条件，对于任何 $i\in\mathbb{Z}_s$，$j\in\mathbb{Z}_t$，有 $\langle\psi_i|E|\phi_j\rangle=0$，我们得到

$$a_{k,\ell}=\langle k|E|\ell\rangle=0.$$

这意味着 ${}_{\mathcal{S}}E_{\mathcal{T}}=\mathbf{0}$。由于 $E^\dagger=E$，我们也有 ${}_{\mathcal{T}}E_{\mathcal{S}}=\mathbf{0}$。∎

引理 4.3　设一个 $n\times n$ 的矩阵 $E=(a_{i,j})_{i,j\in\mathbb{Z}_n}$ 是 Hermitian 算子 E 在基 $\mathcal{B}:=\{|0\rangle,|1\rangle,\cdots,|n-1\rangle\}$ 下的矩阵表示。给定 $\mathcal{B}$ 的一个非空子集 $\mathcal{S}:=\{|u_0\rangle,|u_1\rangle,\cdots,|u_{s-1}\rangle\}$，令 $\{|\psi_j\rangle\}_{j=0}^{s-1}$ 为 $\mathcal{S}$ 生成的正交集。对于任何 $i\neq j\in\mathbb{Z}_s$，假设 $\langle\psi_i|E|\psi_j\rangle=0$。如果存在态 $|u_t\rangle\in\mathcal{S}$，使得 ${}_{\{|u_t\rangle\}}E_{\mathcal{S}\setminus\{|u_t\rangle\}}=\mathbf{0}$，且对于任何 $j\in\mathbb{Z}_s$，$\langle u_t|\psi_j\rangle\neq0$，那么 $E_{\mathcal{S}}\propto\mathbb{I}_{\mathcal{S}}$。（注意，如果 $\{|\psi_j\rangle\}_{j=0}^{s-1}$ 为 Fourier 基，即 $|\psi_j\rangle=\sum_{i=0}^{s-1}w_s^{ij}|u_i\rangle$，那么对于任何 $j\in\mathbb{Z}_s$，一定满足 $\langle u_t|\psi_j\rangle\neq0$。）

证明　不失一般性，对于任何 $i\in\mathbb{Z}_s$，我们可以假设 $|u_i\rangle=|i\rangle$。在这个假设下，每个态 $\{|\psi_j\rangle\}_{j=0}^{s-1}$ 可以表示为 $\{|i\rangle\}_{i=0}^{s-1}$ 的线性组合，即 $|\psi_j\rangle=\sum_{i=0}^{s-1}h_{i,j}|i\rangle$。态集 $\{|\psi_j\rangle=\sum_{i=0}^{s-1}h_{i,j}|i\rangle\}_{j=0}^{s-1}$ 可以归一化为 $\{|\varphi_j\rangle=\sum_{i=0}^{s-1}\widetilde{h}_{i,j}|i\rangle\}_{j=0}^{s-1}$，那么 $H:=(\widetilde{h}_{i,j})_{i,j\in\mathbb{Z}_s}$ 是一个 $s\times s$ 的酉矩阵。令

$$F=\begin{pmatrix}H & \mathbf{0}_{s\times(n-s)}\\ \mathbf{0}_{(n-s)\times s} & \mathbf{0}_{(n-s)\times(n-s)}\end{pmatrix}$$

是一个 $n\times n$ 的矩阵。我们可以在空间 $\mathcal{H}_n$ 上定义一个算子，

$$F=\sum_{i=0}^{s-1}\sum_{j=0}^{s-1}\widetilde{h}_{i,j}|i\rangle\langle j|.$$

那么矩阵 F 就是算子 F 在基 $\{|0\rangle,|1\rangle,\cdots,|n-1\rangle\}$ 下的矩阵表示。

态集 $\{|\varphi_j\rangle = \sum_{i=0}^{s-1} \widetilde{h}_{i,j}|i\rangle\}_{j=0}^{s-1}$ 可以写成 $\{|\varphi_j\rangle = F|j\rangle\}_{j=0}^{s-1}$。对于任何 $i \neq j \in \mathbb{Z}_s$，由于 $\langle\psi_i|E|\psi_j\rangle = 0$，这意味着 $\langle\varphi_i|E|\varphi_j\rangle = 0$。对于任何 $i \neq j \in \mathbb{Z}_s$，我们有

$$\langle i|F^\dagger EF|j\rangle = 0. \tag{4.3}$$

公式(4.3) 意味着

$$H^\dagger E_S H = \mathrm{diag}(\alpha_0\ \alpha_1\ \cdots\ \alpha_{s-1}),$$

其中对于任何 $i \in \mathbb{Z}_s$，$\alpha_i \in \mathbb{C}$。由于 H 是一个酉矩阵，我们有

$$E_S H = H\,\mathrm{diag}(\alpha_0\ \alpha_1\ \cdots\ \alpha_{s-1}).$$

由于 ${}_{\{|t\rangle\}}E_{S\setminus\{|t\rangle\}} = \mathbf{0}$，即 E_S 的第 t 行为 $(0\ 0\ \cdots\ a_{t,t}\ \cdots\ 0)$，$E_S H$ 的第 t 行是 $(a_{t,t}\widetilde{h}_{t,0}\ a_{t,t}\widetilde{h}_{t,1}\ \cdots\ a_{t,t}\widetilde{h}_{t,t}\ \cdots\ a_{t,t}\widetilde{h}_{t,s-1})$。此外，$H\,\mathrm{diag}(\alpha_0\ \alpha_1\ \cdots\ \alpha_{s-1})$ 的第 t 行是 $(\alpha_0\widetilde{h}_{t,0}\ \alpha_1\widetilde{h}_{t,1}\ \cdots\ \alpha_{s-1}\widetilde{h}_{t,s-1})$。对于任何 $j \in \mathbb{Z}_s$，那么 $a_{t,t}\widetilde{h}_{t,j} = \alpha_j\widetilde{h}_{t,j}$。对于任何 $j \in \mathbb{Z}_s$，由于 $\langle t|\psi_j\rangle = h_{t,j} \neq 0$，即对于任何 $j \in \mathbb{Z}_s$，$\widetilde{h}_{t,j} \neq 0$。因此对于任何 $j \in \mathbb{Z}_s$，我们都有 $\alpha_j = a_{t,t}$。从而

$$E_S = H\,\mathrm{diag}(a_{t,t}\ \ a_{t,t}\ \cdots\ a_{t,t})H^\dagger = \mathrm{diag}(a_{t,t}\ \ a_{t,t}\ \cdots\ a_{t,t}).$$

即 $E_S \propto \mathbb{I}_S$。 ∎

在下一节中，我们将看到这两个引理在证明强量子非局域性时非常高效。

4.3　强非局域的正交乘积集

在本节中，我们将给出三体、四体和五体系统中强非局域的正交乘积集的构造。由于在3.4和3.5节中，我们给出了三维和四维超立方体的分解，并给出了对应乘积态。在本节中，我们将证明这些三维和四维超立方体最外层 (即第 $n = 0$ 层) 所对应的乘积集是强非局域的。此外我们将给出五维超立方体的分解，并用同样的方式构造强非局域的正交乘积集。

4.3.1　三体系统中强非局域的正交乘积集

我们通过一个例子开始。在 $\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3$ 中，由图3.11和公式(3.1)可知，3×3×3 立方体的最外层对应的乘积态为：

$$\begin{aligned}
C_1 &:= \{|\xi_i\rangle_A|0\rangle_B|\eta_j\rangle_C : (i,j) \in \mathbb{Z}_2\times\mathbb{Z}_2\},\\
C_2 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|2\rangle_C : (i,j) \in \mathbb{Z}_2\times\mathbb{Z}_2\},\\
C_3 &:= \{|2\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C : (i,j) \in \mathbb{Z}_2\times\mathbb{Z}_2\},\\
C_4 &:= \{|2\rangle_A|2\rangle_B|2\rangle_C\},
\end{aligned}$$

$$
\begin{aligned}
\mathcal{D}_1 &:= \{|\eta_i\rangle_A|2\rangle_B|\xi_j\rangle_C : (i,j)\in\mathbb{Z}_2\times\mathbb{Z}_2\},\\
\mathcal{D}_2 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|0\rangle_C : (i,j)\in\mathbb{Z}_2\times\mathbb{Z}_2\},\\
\mathcal{D}_3 &:= \{|0\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C : (i,j)\in\mathbb{Z}_2\times\mathbb{Z}_2\},\\
\mathcal{D}_4 &:= \{|0\rangle_A|0\rangle_B|0\rangle_C\},
\end{aligned}
\tag{4.4}
$$

其中 $|\eta_s\rangle_X = |0\rangle_X + (-1)^s|1\rangle_X$，$|\xi_s\rangle_X := |1\rangle_X + (-1)^s|2\rangle_X$，$s\in\mathbb{Z}_2$，$X\in\{A,B,C\}$。现在我们证明 $\cup_{i=1}^4(\mathcal{C}_i\cup\mathcal{D}_i)$ 具有强量子非局域性。

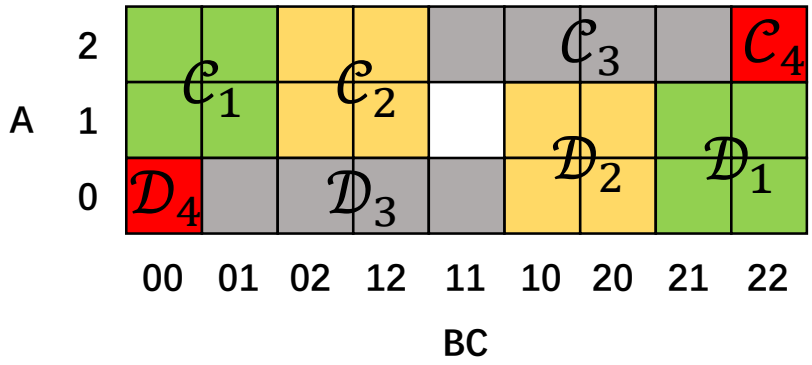

图 4.1　公式(4.4)给出的 $\cup_{i=1}^4\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BC$ 下对应的 3×9 网格。例如，$\mathcal{C}_1$ 对应于 2×2 网格 $\{1,2\}_A\times\{00,01\}_{BC}$。此外，对于 $1\leqslant i\leqslant4$，$\mathcal{C}_i$ 与 $\mathcal{D}_i$ 是对称的。

例 4.1　在 $\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3$ 中，公式(4.4)给出的 $\cup_{i=1}^4(\mathcal{C}_i\cup\mathcal{D}_i)$ 是一个强非局域的正交乘积集，且 $|\cup_{i=1}^4(\mathcal{C}_i\cup\mathcal{D}_i)| = 26$。

证明　这 8 个子集 $\cup_{i=1}^4\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BC$ 下对应于图4.1中 3×9 网格的 8 块。由于这 8 个子集 $\cup_{i=1}^4\{\mathcal{C}_i,\mathcal{D}_i\}$ 在任意两体划分 $\{A|BC, C|AB, B|CA\}$ 下都对应于与图4.1相同的结构，我们只需要考虑图4.1。

令 B 和 C 一起进行一个正交保持的局部测量 $\{E = M^\dagger M\}$，其中 $E = (a_{ij,k\ell})_{i,j,k,\ell\in\mathbb{Z}_3}$，那么测量后的态 $\{\mathbb{I}_A\otimes M|\psi\rangle \big| |\psi\rangle\in\cup_{i=1}^4(\mathcal{C}_i,\mathcal{D}_i)\}$ 是相互正交的，即

$$
\begin{aligned}
0 =& {}_A\langle\phi_1|_B\langle\phi_2|_C\langle\phi_3|\mathbb{I}_A\otimes E|\psi_1\rangle_A|\psi_2\rangle_B|\psi_3\rangle_C\\
=& \langle\phi_1|\psi_1\rangle_A({}_B\langle\phi_2|_C\langle\phi_3|E|\psi_2\rangle_B|\psi_3\rangle_C),
\end{aligned}
\tag{4.5}
$$

其中 $|\phi_1\rangle_A|\phi_2\rangle_B|\phi_3\rangle_C\neq|\psi_1\rangle_A|\psi_2\rangle_B|\psi_3\rangle_C\in\cup_{i=1}^4(\mathcal{C}_i\cup\mathcal{D}_i)$。通过观察可知，如果 $\langle\phi_1|\psi_1\rangle_A\neq0$，那么 ${}_B\langle\phi_2|_C\langle\phi_3|E|\psi_2\rangle_B|\psi_3\rangle_C = 0$。我们的目的是通过这个观察来证明 $E\propto\mathbb{I}$。

下面我们介绍几个符号。令 $\mathcal{S} = \{|\psi_1\rangle_A|\psi_2\rangle_B|\psi_3\rangle\}$ 为一个三体系统中的正交乘积集，定义

$$
\mathcal{S}(|\psi\rangle_A) := \{|\psi_2\rangle_B|\psi_3\rangle_C : |\psi\rangle_A|\psi_2\rangle_B|\psi_3\rangle_C\in\mathcal{S}\}.
$$

此外，将 $\mathcal{S}^{(A)}$ 定义为 $\mathcal{S}(|\psi\rangle_A)$ 的支撑集，即它生成 $\mathcal{S}(|\psi\rangle_A)$，且 $\mathcal{S}^{(A)}\subset\{|j\rangle_B|k\rangle_C\}_{j,k\in\mathbb{Z}_3}$。例如，在公式(4.4)中，$\mathcal{C}_1 := \{|\xi_i\rangle_A|0\rangle_B|\eta_j\rangle_C : (i,j)\in\mathbb{Z}_2\times\mathbb{Z}_2\}$，

那么 $\mathcal{C}_1(|\xi_1\rangle_A)=\{|0\rangle_A|\eta_j\rangle_C\}_{j\in\mathbb{Z}_2}$, $\mathcal{C}_1^{(A)}=\{|0\rangle_B|0\rangle_C,|0\rangle_B|1\rangle_C\}$, 且 $\mathcal{C}_1(|\xi_1\rangle_A)$ 由 $\mathcal{C}_1^{(A)}$ 生成。实际上，$\{\mathcal{C}_i^{(A)},\mathcal{D}_i^{(A)}\}_{i=1}^4$ 可以很容易地通过图4.1观察得到，它们是图4.1中 $\{\mathcal{C}_i,\mathcal{D}_i\}_{i=1}^4$ 在 BC 部分的投影集。

令 $\mathcal{V}:=\{|j\rangle_B|k\rangle_C\}_{j,k\in\mathbb{Z}_3}$ 为 BC 所属空间的计算基，我们发现 $\mathcal{V}$ 是 4 个互不相交的子集 $\mathcal{C}_1^{(A)},\mathcal{C}_2^{(A)},\mathcal{C}_3^{(A)},\mathcal{C}_4^{(A)}$ 的并集，即

$$\mathcal{V}=\mathcal{C}_1^{(A)}\cup\mathcal{C}_2^{(A)}\cup\mathcal{C}_3^{(A)}\cup\mathcal{C}_4^{(A)},\ \text{且}\ \mathcal{C}_i^{(A)}\cap\mathcal{C}_j^{(A)}=\varnothing$$

其中 $i\neq j$。

步骤 1 取任意的 $|\Phi_1\rangle\in\mathcal{C}_1(|\xi_0\rangle_A)$，$|\Phi_2\rangle\in\mathcal{C}_2(|\xi_0\rangle_A)$，$|\Phi_3\rangle\in\mathcal{C}_3(|2\rangle_A)$，$|\Phi_4\rangle\in\mathcal{C}_4(|2\rangle_A)$，由于 $|\xi_0\rangle_A$，$|\xi_0\rangle_A$，$|2\rangle_A$，$|2\rangle_A$ 相互不正交，通过公式(4.5)，我们得到

$$\langle\Phi_i|E|\Phi_j\rangle=0,\quad 1\leqslant i\neq j\leqslant 4.$$

注意 $\mathcal{C}_1(|\xi_0\rangle_A)$，$\mathcal{C}_2(|\xi_0\rangle_A)$，$\mathcal{C}_3(|2\rangle_A)$，$\mathcal{C}_4(|2\rangle_A)$ 分别由 $\mathcal{C}_1^{(A)}$，$\mathcal{C}_2^{(A)}$，$\mathcal{C}_3^{(A)}$，$\mathcal{C}_4^{(A)}$ 生成。对 $\{\mathcal{C}_1(|\xi_0\rangle_A),\mathcal{C}_2(|\xi_0\rangle_A),\mathcal{C}_3(|2\rangle_A),\mathcal{C}_4(|2\rangle_A)\}$ 中任意两个元素运用引理 4.2，我们得到

$$_{\mathcal{C}_i^{(A)}}E_{\mathcal{C}_j^{(A)}}=\mathbf{0},\quad 1\leqslant i\neq j\leqslant 4.$$

因此，E 是一个分块对角矩阵，即

$$E=E_{\mathcal{C}_1^{(A)}}\oplus E_{\mathcal{C}_2^{(A)}}\oplus E_{\mathcal{C}_3^{(A)}}\oplus E_{\mathcal{C}_4^{(A)}}.$$

参见图4.2(I)。

步骤 2 对 $\mathcal{D}_4(|0\rangle_A)$ 和 $\mathcal{D}_3(|0\rangle_A)$ 运用引理4.2，我们得到 $_{\{|0\rangle_B|0\rangle_C\}}E_{\mathcal{D}_3^{(A)}}=\mathbf{0}$。由于 $\mathcal{C}_1^{(A)}\backslash\{|0\rangle_B|0\rangle_C\}\subset\mathcal{D}_3^{(A)}$，我们也可以得到 $_{\{|0\rangle_B|0\rangle_C\}}E_{\mathcal{C}_1^{(A)}\backslash\{|0\rangle_B|0\rangle_C\}}=\mathbf{0}$。对 $\mathcal{C}_1(|\xi_0\rangle_A)$

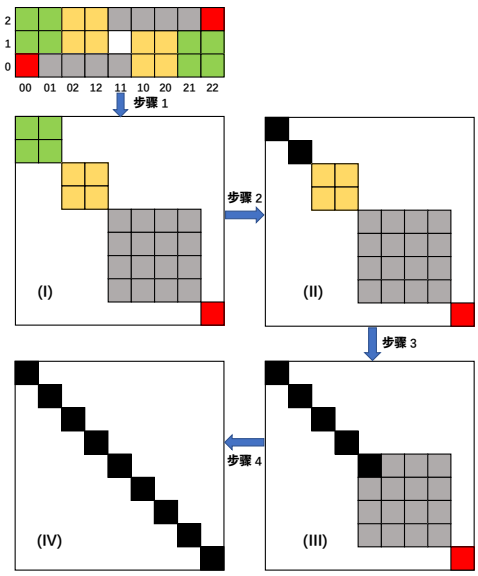

图 4.2　例4.1中强量子非局域性的证明步骤。

运用引理 4.3，我们得到

$$E_{C_1^{(A)}} = a\mathbb{I}_{C_1^{(A)}}.$$

参见图4.2(II)。

步骤 3 由图4.2(II) 可知，$_{\{|0\rangle_B|1\rangle_C\}}E_{D_3^{(A)}\setminus\{|0\rangle_B|1\rangle_C\}} = \mathbf{0}$。对集合 $\mathcal{D}_3(|0\rangle_A)$ 运用引理4.3，我们有 $E_{D_3^{(A)}} = b\mathbb{I}_{D_3^{(A)}}$。注意 $D_3^{(A)} \cap C_1^{(A)} \neq \varnothing$，那么 $b = a$。所以

$$E_{C_1^{(A)}\cup D_3^{(A)}} = a\mathbb{I}_{C_1^{(A)}\cup D_3^{(A)}}.$$

参见图4.2(III)。

步骤 4 由于图4.1的对称性，我们可以得到 $E = a\mathbb{I}$。参见图4.2(IV)。 ∎

上述结构及其证明可以直接推广到高维系统。由公式(3.5)可知，立方体最外层对应的乘积态为:

$$\begin{aligned}
\mathcal{C}_1 &:= \{|\xi_i\rangle_A|0\rangle_B|\eta_j\rangle_C : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{C}_2 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|d_C-1\rangle_C : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1}\},\\
\mathcal{C}_3 &:= \{|d_A-1\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{C}_4 &:= \{|d_A-1\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C\},\\
\mathcal{D}_1 &:= \{|\eta_i\rangle_A|d_B-1\rangle_B|\xi_j\rangle_C : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{D}_2 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|0\rangle_C : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1}\},\\
\mathcal{D}_3 &:= \{|0\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{D}_4 &:= \{|0\rangle_A|0\rangle_B|0\rangle_C\},
\end{aligned} \tag{4.6}$$

其中 $|\eta_s\rangle_X = \sum_{t=0}^{d_X-2} w_{d_X-1}^{st}|t\rangle_X$，$|\xi_s\rangle_X = \sum_{t=0}^{d_X-2} w_{d_X-1}^{st}|t+1\rangle_X$，$s \in \mathbb{Z}_{d_X-1}$，$X \in \{A,B,C\}$。因此我们有以下定理。

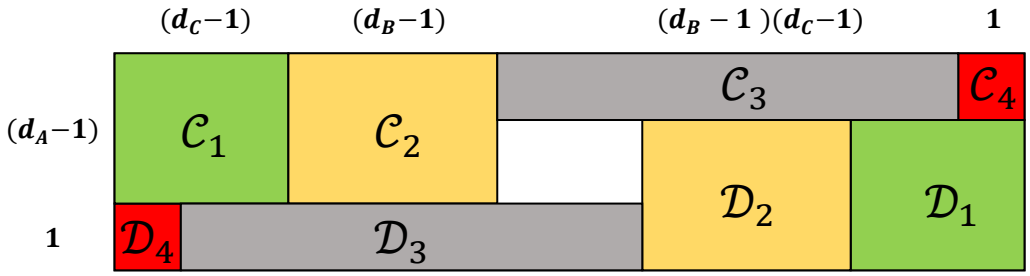

图 4.3　公式(4.6)给出的 $\cup_{i=1}^4\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BC$ 下对应的 $d_A \times d_Bd_C$ 网格。此外，对于 $1 \leqslant i \leqslant 4$，$\mathcal{C}_i$ 与 $\mathcal{D}_i$ 是对称的。

定理 4.4　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}$ 中，$d_A, d_B, d_C \geqslant 3$，公式(4.6)给出的 $\cup_{i=1}^4(\mathcal{C}_i\cup\mathcal{D}_i)$ 是一个强非局域的正交乘积集，且 $|\cup_{i=1}^4(\mathcal{C}_i\cup\mathcal{D}_i)| = d_Ad_Bd_C-(d_A-2)(d_B-2)(d_C-2)$。

证明　这 8 个子集 $\cup_{i=1}^{4}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BC$ 下对应于图4.3中 $d_A\times d_Bd_C$ 网格的 8 块。由于这 8 个子集 $\cup_{i=1}^{4}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在任意两体划分 $\{A|BC,C|AB,B|CA\}$ 下都对应于与图4.3相同的结构，我们只需要考虑图4.3。注意，

$$\mathcal{D}_3^{(A)}\cap\mathcal{C}_j^{(A)}\neq\varnothing \text{ 且 } \mathcal{D}_4^{(A)}\cap\mathcal{C}_1^{(A)}\neq\varnothing,\quad j=1,2,3.$$

令 $\boldsymbol{B}$ 和 $\boldsymbol{C}$ 一起进行一个正交保持的局部测量 $\{E=M^{\dagger}M\}$，其中 $E=(a_{ij,k\ell})_{i,k\in\mathbb{Z}_{d_B},j,\ell\in\mathbb{Z}_{d_C}}$，那么测量后的态 $\{\mathbb{I}_A\otimes M|\psi\rangle\big||\psi\rangle\in\cup_{i=1}^{4}(\mathcal{C}_i\cup\mathcal{D}_i)\}$ 是相互正交的。类似于例4.1的步骤 1，对 $\mathcal{C}_1(|\xi_0\rangle_A),\mathcal{C}_2(|\xi_0\rangle_A),\mathcal{C}_3(|d_A-1\rangle),\mathcal{C}_4(|d_A-1\rangle)$ 中任意两个子集运用引理 4.2，我们可以得到

$$E=E_{\mathcal{C}_1^{(A)}}\oplus E_{\mathcal{C}_2^{(A)}}\oplus E_{\mathcal{C}_3^{(A)}}\oplus E_{\mathcal{C}_4^{(A)}}.$$

我们可以像例4.1的其他步骤一样完成证明，见下面的分析草图：

$$\begin{aligned}
\mathcal{D}_4(|0\rangle_A),\mathcal{D}_3(|0\rangle_A)&\xrightarrow{\text{引理4.2}}E_{\mathcal{D}_4^{(A)}}E_{\mathcal{D}_3^{(A)}}=\mathbf{0},\\
\mathcal{C}_1(|\xi_0\rangle_A)&\xrightarrow{\text{引理4.3}}E_{\mathcal{C}_1^{(A)}}=a\mathbb{I}_{\mathcal{C}_1^{(A)}},\\
\mathcal{D}_3(|0\rangle_A)&\xrightarrow{\text{引理4.3}}E_{\mathcal{D}_3^{(A)}}=b\mathbb{I}_{\mathcal{D}_3^{(A)}},\\
\mathcal{C}_1^{(A)}\cap\mathcal{D}_3^{(A)}\neq\varnothing&\longrightarrow E_{\mathcal{C}_1^{(A)}\cup\mathcal{D}_3^{(A)}}=a\mathbb{I}_{\mathcal{C}_1^{(A)}\cup\mathcal{D}_3^{(A)}}.
\end{aligned}$$

由于图4.1的对称性，我们可以得到 $E=a\mathbb{I}$。这就完成了证明过程。 ∎

4.3.2　四体系统中强非局域的正交乘积集

由公式(3.18)可知，四维超立方体的最外层对应的乘积态为：

$$\begin{aligned}
\mathcal{C}_1&:=\{|\xi_i\rangle_A|\eta_j\rangle_B|0\rangle_C|\xi_k\rangle_D:(i,j,k)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_2&:=\{|\xi_i\rangle_A|d_B-1\rangle_B|\eta_j\rangle_C|\eta_k\rangle_D:(i,j,k)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_3&:=\{|\xi_i\rangle_A|\xi_j\rangle_B|\xi_k\rangle_C|d_D-1\rangle_D:(i,j,k)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_4&:=\{|\xi_i\rangle_A|d_B-1\rangle_B|0\rangle_C|d_D-1\rangle_D:i\in\mathbb{Z}_{d_A-1}\},\\
\mathcal{C}_5&:=\{|d_A-1\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C|\eta_k\rangle_D:(i,j,k)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_6&:=\{|d_A-1\rangle_A|\eta_i\rangle_B|0\rangle_C|0\rangle_D:i\in\mathbb{Z}_{d_B-1}\},\\
\mathcal{C}_7&:=\{|d_A-1\rangle_A|0\rangle_B|\xi_i\rangle_C|d_D-1\rangle_D:i\in\mathbb{Z}_{d_C-1}\},\\
\mathcal{C}_8&:=\{|d_A-1\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C|\eta_i\rangle_D:i\in\mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_1&:=\{|\eta_i\rangle_A|\xi_j\rangle_B|d_C-1\rangle_C|\eta_k\rangle_D:(i,j,k)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_2&:=\{|\eta_i\rangle_A|0\rangle_B|\xi_j\rangle_C|\xi_k\rangle_D:(i,j,k)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_3&:=\{|\eta_i\rangle_A|\eta_j\rangle_B|\eta_k\rangle_C|0\rangle_D:(i,j,k)\in\mathbb{Z}_{d_A-1}\times\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_4&:=\{|\eta_i\rangle_A|0\rangle_B|d_C-1\rangle_C|0\rangle_D:i\in\mathbb{Z}_{d_A-1}\},\\
\mathcal{D}_5&:=\{|0\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C|\xi_k\rangle_D:(i,j,k)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_6&:=\{|0\rangle_A|\xi_i\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D:i\in\mathbb{Z}_{d_B-1}\},\\
\mathcal{D}_7&:=\{|0\rangle_A|d_B-1\rangle_B|\eta_i\rangle_C|0\rangle_D:i\in\mathbb{Z}_{d_C-1}\},\\
\mathcal{D}_8&:=\{|0\rangle_A|0\rangle_B|0\rangle_C|\xi_i\rangle_D:i\in\mathbb{Z}_{d_D-1}\},
\end{aligned}\tag{4.7}$$

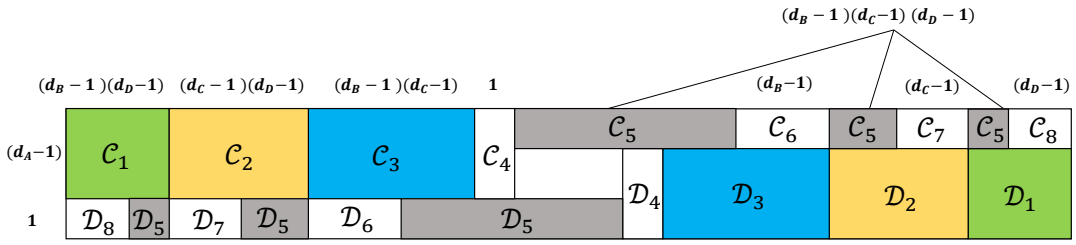

图 4.4　公式(4.7)给出的 $\cup_{i=1}^{8}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BCD$ 下对应的 $d_A\times d_Bd_Cd_D$ 网格。此外，对于 $1\leqslant i\leqslant 8$，$\mathcal{C}_i$ 与 $\mathcal{D}_i$ 是对称的。

其中 $|\eta_s\rangle_X=\sum_{t=0}^{d_X-2}w_{d_X-1}^{st}|t\rangle_X$，$|\xi_s\rangle_X=\sum_{t=0}^{d_X-2}w_{d_X-1}^{st}|t+1\rangle_X$，$s\in\mathbb{Z}_{d_X-1}$，$X\in\{A,B,C,D\}$。现在我们可以证明上述正交乘积集是强非局域的。

定理 4.5　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}\otimes\mathbb{C}^{d_D}$ 中，d_A，d_B，d_C，$d_D\geqslant 3$，公式(4.7)给出的 $\cup_{i=1}^{8}(\mathcal{C}_i\cup\mathcal{D}_i)$ 是一个强非局域的正交乘积集，且 $|\cup_{i=1}^{8}(\mathcal{C}_i\cup\mathcal{D}_i)|=d_Ad_Bd_Cd_D-(d_A-2)(d_B-2)(d_C-2)(d_D-2)$。

证明　这 16 个子集 $\cup_{i=1}^{8}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BCD$ 下对应于图4.4中 $d_A\times d_Bd_Cd_D$ 网格的 16 块。由于这 16 个子集 $\cup_{i=1}^{8}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在任意两体划分 $\{A|BCD,D|ABC,C|DAB,B|CDA\}$ 下都对应于与图4.4相同的结构，我们只需要考虑图4.4。对于 $1\leqslant j\leqslant 5$，注意

$$\mathcal{D}_5^{(A)}\cap\mathcal{C}_j^{(A)}\neq\varnothing;\ \mathcal{D}_6^{(A)}\cap\mathcal{C}_3^{(A)}\neq\varnothing;\ \mathcal{D}_7^{(A)}\cap\mathcal{C}_2^{(A)}\neq\varnothing;\ \mathcal{D}_8^{(A)}\cap\mathcal{C}_1^{(A)}\neq\varnothing.\tag{4.8}$$

令 B，C 和 D 一起进行一个正交保持的局部测量 $\{E=M^\dagger M\}$，其中 $E=(a_{ijk,\ell mn})_{i,\ell\in\mathbb{Z}_{d_B},j,m\in\mathbb{Z}_{d_C},k,n\in\mathbb{Z}_{d_D}}$，那么测量后的态 $\{\mathbb{I}_A\otimes M|\psi\rangle\big||\psi\rangle\in\cup_{i=1}^{8}(\mathcal{C}_i\cup\mathcal{D}_i)\}$ 是相互正交的。

步骤 1 对 $\{\{\mathcal{C}_i(|\xi_0\rangle_A)\}_{j=1}^{4},\{\mathcal{C}_j(|d_A-1\rangle)\}_{j=5}^{8}\}$ 中任意两个元素运用引理4.2，我们有

$$E=\oplus_{j=1}^{8}E_{\mathcal{C}_j^{(A)}}.\tag{4.9}$$

步骤 2 通过公式(4.9)，我们知道 ${}_{\mathcal{C}_4^{(A)}}E_{\mathcal{D}_5^{(A)}\setminus\mathcal{C}_4^{(A)}}=\mathbf{0}$。注意 $|\mathcal{C}_4^{(A)}|=1$，即 $\mathcal{C}_4^{(A)}=\{|d_B-1\rangle_B|0\rangle_C|d_D-1\rangle_D\}$。对 $\mathcal{D}_5(|0\rangle_A)$ 运用引理4.3，我们有

$$E_{\mathcal{D}_5^{(A)}}=a\mathbb{I}_{\mathcal{D}_5^{(A)}}.\tag{4.10}$$

接下来，我们对 $\mathcal{D}_5(|0\rangle_A)$ 和 $\mathcal{D}_i(|0\rangle_A)$ 运用引理4.2，其中 $i=6,7,8$，于是我们有

$${}_{\mathcal{D}_5^{(A)}}E_{\mathcal{D}_i^{(A)}}=\mathbf{0},\quad i=6,7,8.\tag{4.11}$$

步骤 3 注意 $\mathcal{D}_6^{(A)}=\mathcal{C}_3^{(A)}\setminus\mathcal{D}_5^{(A)}$，$\mathcal{D}_7^{(A)}=\mathcal{C}_2^{(A)}\setminus\mathcal{D}_5^{(A)}$，$\mathcal{D}_8^{(A)}=\mathcal{C}_1^{(A)}\setminus\mathcal{D}_5^{(A)}$。通过公式(4.10)和 (4.11)可知，对任何 $|j\rangle_B|k\rangle_C|\ell\rangle_D\in\mathcal{D}_5^{(A)}\cap\mathcal{C}_i^{(A)}$，其中 $i=1,2,3$，我们有 ${}_{\{|j\rangle_B|k\rangle_C|\ell\rangle_D\}}E_{\mathcal{C}_i^{(A)}\setminus\{|j\rangle_B|k\rangle_C|\ell\rangle_D\}}=\mathbf{0}$。对 $\mathcal{C}_i(|\xi_0\rangle_A)$ 运用引理4.3，我们得到

$$E_{\mathcal{C}_i^{(A)}}=a_i\mathbb{I}_{\mathcal{C}_i^{(A)}},\quad i=1,2,3.$$

由于 $\mathcal{D}_5^{(A)} \cap \mathcal{C}_i^{(A)} \neq \varnothing$，其中 $i = 1,2,3$，这推出 $a_i = a$。因此

$$E_{\{\cup_{i=1}^3 \mathcal{C}_i^{(A)}\} \cup \mathcal{D}_5^{(A)}} = a\mathbb{I}_{\{\cup_{i=1}^3 \mathcal{C}_i^{(A)}\} \cup \mathcal{D}_5^{(A)}}.$$

步骤 4 由于图4.4的对称性，我们得到 $E = a\mathbb{I}$。这就完成了证明过程。 ∎

4.3.3　五体系统中强非局域的正交乘积集

对于坐标为 $\{0,1,\cdots,d_A-1\}_A \times \{0,1,\cdots,d_B-1\}_B \times \{0,1,\cdots,d_C-1\}_C \times \{0,1,\cdots,d_D-1\}_D \times \{0,1,\cdots,d_E-1\}_E$ 的五维超立方体的最外层，我们可以给出如下分解：

$$
\begin{aligned}
\mathcal{C}_1 &:= \{|\xi_i\rangle_A|d_B-1\rangle_B|\eta_j\rangle_C|\xi_k\rangle_D|\eta_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{C}_2 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|0\rangle_C|\xi_k\rangle_D|\eta_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{C}_3 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|\xi_k\rangle_C|d_D-1\rangle_D|\eta_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{C}_4 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|\xi_k\rangle_C|\eta_\ell\rangle_D|0\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_5 &:= \{|\xi_i\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C|\eta_j\rangle_D|0\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_6 &:= \{|\xi_i\rangle_A|d_B-1\rangle_B|\eta_j\rangle_C|0\rangle_D|0\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{C}_7 &:= \{|\xi_i\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D|\eta_j\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{C}_8 &:= \{|\xi_i\rangle_A|\eta_j\rangle_B|0\rangle_C|0\rangle_D|0\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1}\},\\
\mathcal{C}_9 &:= \{|d_A-1\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C|\eta_k\rangle_D|\xi_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{C}_{10} &:= \{|d_A-1\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D|d_E-1\rangle_E\},\\
\mathcal{C}_{11} &:= \{|d_A-1\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C|d_D-1\rangle_D|d_E-1\rangle_E : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{C}_{12} &:= \{|d_A-1\rangle_A|\eta_i\rangle_B|0\rangle_C|0\rangle_D|\xi_j\rangle_E : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{C}_{13} &:= \{|d_A-1\rangle_A|\eta_i\rangle_B|0\rangle_C|\xi_j\rangle_D|d_E-1\rangle_E : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_{14} &:= \{|d_A-1\rangle_A|d_B-1\rangle_B|\eta_i\rangle_C|\xi_j\rangle_D|d_E-1\rangle_E : (i,j) \in \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{C}_{15} &:= \{|d_A-1\rangle_A|d_B-1\rangle_B|\eta_i\rangle_C|0\rangle_D|\xi_j\rangle_E : (i,j) \in \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{C}_{16} &:= \{|d_A-1\rangle_A|d_B-1\rangle_B|d_C-1\rangle_C|\eta_i\rangle_D|\xi_j\rangle_E : (i,j) \in \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_1 &:= \{|\eta_i\rangle_A|0\rangle_B|\xi_j\rangle_C|\eta_k\rangle_D|\xi_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_2 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|d_C-1\rangle_C|\eta_k\rangle_D|\xi_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_3 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|\eta_k\rangle_C|0\rangle_D|\xi_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_4 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D|d_E-1\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_5 &:= \{|\eta_i\rangle_A|0\rangle_B|0\rangle_C|\xi_j\rangle_D|d_E-1\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_6 &:= \{|\eta_i\rangle_A|0\rangle_B|\xi_j\rangle_C|d_D-1\rangle_D|d_E-1\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{D}_7 &:= \{|\eta_i\rangle_A|0\rangle_B|0\rangle_C|0\rangle_D|\xi_j\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_8 &:= \{|\eta_i\rangle_A|\xi_j\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D|d_E-1\rangle_E : (i,j) \in \mathbb{Z}_{d_A-1} \times \mathbb{Z}_{d_B-1}\},\\
\mathcal{D}_9 &:= \{|0\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C|\xi_k\rangle_D|\eta_\ell\rangle_E : (i,j,k,\ell) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_{10} &:= \{|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_D|0\rangle_E\},\\
\mathcal{D}_{11} &:= \{|0\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C|0\rangle_D|0\rangle_E : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1}\},\\
\mathcal{D}_{12} &:= \{|0\rangle_A|\xi_i\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D|\eta_j\rangle_E : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_{13} &:= \{|0\rangle_A|\xi_i\rangle_B|d_C-1\rangle_C|\eta_j\rangle_D|0\rangle_E : (i,j) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_{14} &:= \{|0\rangle_A|0\rangle_B|\xi_i\rangle_C|\eta_j\rangle_D|0\rangle_E : (i,j) \in \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1}\},\\
\mathcal{D}_{15} &:= \{|0\rangle_A|0\rangle_B|\xi_i\rangle_C|d_D-1\rangle_D|\eta_j\rangle_E : (i,j) \in \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_E-1}\},\\
\mathcal{D}_{16} &:= \{|0\rangle_A|0\rangle_B|0\rangle_C|\xi_i\rangle_D|\eta_j\rangle_E : (i,j) \in \mathbb{Z}_{d_D-1} \times \mathbb{Z}_{d_E-1}\},
\end{aligned}
\tag{4.12}
$$

其中 $|\eta_s\rangle_X=\sum_{t=0}^{d_X-2}w_{d_X-1}^{st}|t\rangle_X$，$|\xi_s\rangle_X=\sum_{t=0}^{d_X-2}w_{d_X-1}^{st}|t+1\rangle_X$，$s\in\mathbb{Z}_{d_X-1}$，$X\in\{A,B,C,D,E\}$。那么我们有如下定理。

定理 4.6　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}\otimes\mathbb{C}^{d_D}\otimes\mathbb{C}^{d_E}$ 中，d_A，d_B，d_C，d_D，$d_E\geqslant 3$，公式(4.12)给出的 $\cup_{i=1}^{16}(\mathcal{C}_i\cup\mathcal{D}_i)$ 是一个强非局域的正交乘积集，且 $|\cup_{i=1}^{16}(\mathcal{C}_i\cup\mathcal{D}_i)|=d_Ad_Bd_Cd_Dd_E-(d_A-2)(d_B-2)(d_C-2)(d_D-2)(d_E-2)$。

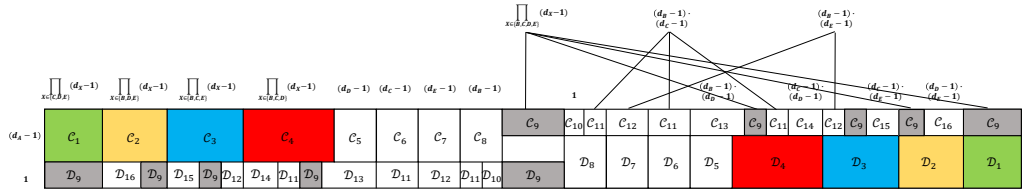

图 4.5　**公式(4.12)给出的 $\cup_{i=1}^{16}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BCDE$ 下对应的 $d_A\times d_Bd_Cd_Dd_E$ 网格。此外，对于 $1\leqslant i\leqslant 16$，$\mathcal{C}_i$ 与 $\mathcal{D}_i$ 是对称的。**

证明　这 32 个子集 $\cup_{i=1}^{16}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在两体划分 $A|BCDE$ 下对应于图4.5中 $d_A\times d_Bd_Cd_Dd_E$ 网格的 32 块。由于这 32 个子集 $\cup_{i=1}^{16}\{\mathcal{C}_i,\mathcal{D}_i\}$ 在任意两体划分 $\{A|BCDE,E|ABCD,D|EABC,C|DEAB,B|CDEA\}$ 下都对应于与图4.5相同的结构，我们只需要考虑图4.5。注意

$$\mathcal{D}_9^{(A)}\cap\mathcal{C}_j^{(A)}\neq\varnothing,\ j=1,2,3,4,9;\ \mathcal{D}_{11}^{(A)}\cap\mathcal{C}_j^{(A)}\neq\varnothing,\ j=4,6,8;$$
$$\mathcal{D}_{12}^{(A)}\cap\mathcal{C}_j^{(A)}\neq\varnothing,\ j=3,7;\ \mathcal{D}_{13}^{(A)}\cap\mathcal{C}_j^{(A)}\neq\varnothing,\ j=4,5;\ \mathcal{D}_{10}^{(A)}\cap\mathcal{C}_8^{(A)}\neq\varnothing;$$
$$\mathcal{D}_{14}^{(A)}\cap\mathcal{C}_4^{(A)}\neq\varnothing;\ \mathcal{D}_{15}^{(A)}\cap\mathcal{C}_3^{(A)}\neq\varnothing;\ \mathcal{D}_{16}^{(A)}\cap\mathcal{C}_2^{(A)}\neq\varnothing.$$

令 B，C，D 和 E 一起进行一个正交保持的局部测量 $\{E=M^\dagger M\}$，其中 $E=(a_{ijk\ell,mnst})_{i,m\in\mathbb{Z}_{d_B},j,n\in\mathbb{Z}_{d_C},k,s\in\mathbb{Z}_{d_D},\ell,t\in\mathbb{Z}_{d_E}}$，那么测量后的态 $\{\mathbb{I}_A\otimes M|\psi\rangle\big||\psi\rangle\in\cup_{i=1}^{16}(\mathcal{C}_i\cup\mathcal{D}_i)\}$ 是相互正交的。

步骤 1 对集合 $\{\{\mathcal{C}_j(|\xi_0\rangle_A)\}_{j=1}^{8},\{\mathcal{C}_j(|d_A-1\rangle_A)\}_{j=9}^{16}\}$ 中任意两个元素运用引理4.2，我们有

$$E=\oplus_{j=1}^{16}E_{\mathcal{C}_j^{(A)}}.\tag{4.13}$$

步骤 2 对集合 $\{\mathcal{D}_i(|0\rangle_A)\}_{i=9}^{16}$ 中任意两个元素运用引理4.2，我们有

$$_{\mathcal{D}_{i_1}^{(A)}}E_{\mathcal{D}_{i_2}^{(A)}}=\mathbf{0},\quad 9\leqslant i_1\neq i_2\leqslant 16.\tag{4.14}$$

接下来，由于 $\mathcal{C}_8^{(A)}\setminus\mathcal{D}_{10}^{(A)}\subset\mathcal{D}_{11}^{(A)}$，我们有 $_{\mathcal{D}_{10}^{(A)}}E_{\mathcal{C}_8^{(A)}\setminus\mathcal{D}_{10}^{(A)}}=\mathbf{0}$。注意 $|\mathcal{D}_{10}^{(A)}|=1$，即 $\mathcal{D}_{10}^{(A)}=\{|0\rangle_B|0\rangle_C|0\rangle_D|0\rangle_E\}$。对 $\mathcal{C}_8(|\xi_0\rangle_A)$ 运用引理4.3，我们得到

$$E_{\mathcal{C}_8^{(A)}}=a\mathbb{I}_{\mathcal{C}_8^{(A)}}.\tag{4.15}$$

步骤 3 通过公式(4.13)和(4.15)，对于任何 $|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\in\mathcal{D}_{11}^{(A)}\cap\mathcal{C}_8^{(A)}$，我们有 $_{\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}}E_{\mathcal{D}_{11}^{(A)}\setminus\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}}=\mathbf{0}$。对 $\mathcal{D}_{11}(|0\rangle_A)$ 运用引理4.3，我们有

$$E_{\mathcal{D}_{11}^{(A)}}=a\mathbb{I}_{\mathcal{D}_{11}^{(A)}}.\tag{4.16}$$

接下来，通过公式(4.14)和(4.16)，对于任何 $|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E \in \mathcal{D}_{11}^{(A)} \cap \mathcal{C}_4^{(A)}$，我们有 $_{\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}}E_{\mathcal{C}_4^{(A)}\setminus\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}} = \mathbf{0}$。对 $\mathcal{C}_4(|\xi_0\rangle_A)$ 运用引理4.3，我们有

$$E_{\mathcal{C}_4^{(A)}} = a\mathbb{I}_{\mathcal{C}_4^{(A)}}. \tag{4.17}$$

步骤 4 通过公式(4.13)和(4.17)，对于任何 $|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E \in \mathcal{D}_i^{(A)} \cap \mathcal{C}_4^{(A)}$，$i = 9, 13$，我们有 $_{\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}}E_{\mathcal{D}_i^{(A)}\setminus\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}} = \mathbf{0}$。对 $\mathcal{D}_i(|0\rangle_A)$ 运用引理4.3，$i = 9, 13$，我们有

$$E_{\mathcal{D}_i^{(A)}} = a\mathbb{I}_{\mathcal{D}_i^{(A)}}, \quad i = 9, 13. \tag{4.18}$$

通过公式(4.14)和(4.18), 对于任何 $|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E \in \mathcal{D}_9^{(A)} \cap \mathcal{C}_i^{(A)}, i = 2, 3$, 我们有 $_{\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}}E_{\mathcal{C}_i^{(A)}\setminus\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}} = \mathbf{0}$。对 $\mathcal{C}_i(|\xi_0\rangle_A)$ 运用引理4.3，$i = 2, 3$，我们有

$$E_{\mathcal{C}_i^{(A)}} = a\mathbb{I}_{\mathcal{C}_i^{(A)}}, \quad i = 2, 3. \tag{4.19}$$

步骤 5 通过公式(4.13)和(4.19)，对于任何 $|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E \in \mathcal{D}_{12}^{(A)} \cap \mathcal{C}_3^{(A)}$，我们有 $_{\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}}E_{\mathcal{D}_{12}^{(A)}\setminus\{|j\rangle_B|k\rangle_C|\ell\rangle_D|m\rangle_E\}} = \mathbf{0}$。对 $\mathcal{D}_{12}(|0\rangle_A)$ 运用引理4.3，我们有

$$E_{\mathcal{D}_{12}^{(A)}} = a\mathbb{I}_{\mathcal{D}_{12}^{(A)}}.$$

由于 $\{\cup_{i=1}^{8}\mathcal{C}_i^{(A)}\} \cup \mathcal{D}_9^{(A)} = \mathcal{C}_8^{(A)} \cup \mathcal{D}_{11}^{(A)} \cup \mathcal{C}_4^{(A)} \cup \mathcal{D}_9^{(A)} \cup \mathcal{D}_{13}^{(A)} \cup \mathcal{C}_2^{(A)} \cup \mathcal{C}_3^{(A)} \cup \mathcal{D}_{12}^{(A)}$，我们有

$$E_{\{\cup_{i=1}^{8}\mathcal{C}_i^{(A)}\}\cup\mathcal{D}_9^{(A)}} = \mathbb{I}_{\{\cup_{i=1}^{8}\mathcal{C}_i^{(A)}\}\cup\mathcal{D}_9^{(A)}}.$$

步骤 6 由于图4.5的对称性，我们得到 $E = a\mathbb{I}$。这就完成了证明过程。 ∎

基于这个五维超立方体的分解，我们很大可能可以按照第3章的方法来构造五体系统中的不可扩充乘积基。但由于讨论的情况过多，我们在这里不作讨论。

4.4　强非局域的不可扩充乘积基

在本节中，我们将证明3.4和3.5节中构造的三体和四体系统中的不可扩充乘积基具有强非局域性。由于当 $d_A = d_B = d_C$，$n = \lfloor\frac{d_A-3}{2}\rfloor$ 时，定理3.5给出的不可扩充乘积基恰好是文献[92]中构造的不可扩充乘积基。虽然文献[92]在第 6 节指出“例如在文献[43] 中，作者引入了一个新概念：无纠缠的强量子非局域性，但是我们已经检查过本文的不可扩充乘积基，没有表现出这种性质。”实际上我们将证明这些不可扩充乘积基确实具有强量子非局域性。值得注意的是，3.4和3.5节所有的不可扩充乘积基在子系统的循环置换下有相同的结构，因此为了证明这些不可扩充乘积基具有强量子非局域性，我们只需要证明 $\boldsymbol{B}$ 和 $\boldsymbol{C}$（或 $\boldsymbol{B}$，$\boldsymbol{C}$ 和 $\boldsymbol{D}$）进行的正交保持的局部测量是平凡的。

4.4.1　三体系统中强非局域的不可扩充乘积基

首先，我们验证公式(3.5)给出的不可扩充乘积基具有强量子非局域性。

引理 4.7　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}$ 中，$3\leqslant d_A\leqslant d_B\leqslant d_C$，公式(3.5)给出的 $\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}$ 是一个强非局域的不可扩充乘积基，且 $|\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}|=d_Ad_Bd_C-8$。

证明　令 B 和 C 一起进行一个正交保持的局部测量 $\{E=M^{\dagger}M\}$，其中 $E=(a_{ij,k\ell})_{i,k\in\mathbb{Z}_{d_B},j,\ell\in\mathbb{Z}_{d_C}}$，那么测量后的态 $\{\mathbb{I}_A\otimes M|\psi\rangle:|\psi\rangle\in\cup_{i=1}^{3}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}\}$ 是相互正交的。

步骤 1 由于 $\langle\xi_1|\eta_1\rangle_A\neq0$，对 $\{\mathcal{A}_1(|\xi_1\rangle_A),\mathcal{A}_2(|\xi_1\rangle_A),\mathcal{B}_2(|\eta_1\rangle_A),\mathcal{B}_1(|\eta_1\rangle_A)\}$ 中任意两个元素运用引理4.2，我们有

$$\begin{aligned}&{}_{\mathcal{A}_i^{(A)}}E_{\mathcal{A}_j^{(A)}}=\mathbf{0},\ {}_{\mathcal{A}_i^{(A)}}E_{\mathcal{B}_k^{(A)}}=\mathbf{0},\ {}_{\mathcal{B}_k^{(A)}}E_{\mathcal{B}_\ell^{(A)}}=\mathbf{0},\ {}_{\mathcal{B}_k^{(A)}}E_{\mathcal{A}_i^{(A)}}=\mathbf{0},\\&1\leqslant i\neq j\leqslant2,\ 1\leqslant k\neq\ell\leqslant2.\end{aligned}\tag{4.20}$$

注意如果 $d_A=3$，那么 $|\beta_i\rangle_A$ 在 $\mathcal{F}$ 中只能取 $|\beta_0\rangle_A$。因此我们对 $\mathcal{F}(|\beta_1\rangle_A)$ 和 $\mathcal{A}_1(|\xi_1\rangle_A)$ 无法运用引理4.2。为了得到 ${}_{\mathcal{F}^{(A)}}E_{\mathcal{A}_1^{(A)}}=\mathbf{0}$，我们需要考虑 $\mathcal{A}_3(|d_A-1\rangle_A)$ 和 $\mathcal{A}_1(|\xi_1\rangle_A)$。对于 $(j,k)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}$ 和 $i\in\mathbb{Z}_{d_C-1}$，我们有

$$\begin{aligned}{}_B\langle\xi_j|_C\langle\eta_k|E|0\rangle_B|\eta_i\rangle_C=&{}_B\left(\sum_{t_1=0}^{d_B-2}w_{d_B-1}^{-jt_1}\langle t_1+1|\right)_C\left(\sum_{t_2=0}^{d_C-2}w_{d_C-1}^{-kt_2}\langle t_2|\right)E\times\\&|0\rangle_B\left(\sum_{t_3=0}^{d_C-2}w_{d_C-1}^{it_3}|t_3\rangle\right)_C=0.\end{aligned}\tag{4.21}$$

由公式(4.20)可知，对于 $j\in\mathbb{Z}_{d_B-1}$，$i\in\mathbb{Z}_{d_C-1}$，我们有 ${}_B\langle j+1|_C\langle0|E|0\rangle_B|i\rangle_C=0$；对于 $k,i\in\mathbb{Z}_{d_C-1}$，我们有 ${}_B\langle d_B-1|_C\langle k+1|E|0\rangle_B|i\rangle_C=0$。那么公式(4.21)可以表示为

$${}_B\left(\sum_{t_1=0}^{d_B-3}w_{d_B-1}^{-jt_1}\langle t_1+1|\right)_C\left(\sum_{t_2=1}^{d_C-2}w_{d_C-1}^{-kt_2}\langle t_2|\right)E|0\rangle_B\left(\sum_{t_3=0}^{d_C-2}w_{d_C-1}^{it_3}|t_3\rangle\right)_C=0,$$

也即对于任何 $0\leqslant j\leqslant d_B-3$，$1\leqslant k\leqslant d_C-2$，$0\leqslant i\leqslant d_C-2$，我们有

$$\sum_{t_1=0}^{d_B-3}\sum_{t_2=1}^{d_C-2}\sum_{t_3=0}^{d_C-2}w_{d_B-1}^{-jt_1}w_{d_C-1}^{-kt_2}w_{d_C-1}^{it_3}{}_B\langle t_1+1|_C\langle t_2|E|0\rangle_B|t_3\rangle_C=0.$$

这意味着

$$[H_1^{\dagger}\otimes H_2^{\dagger}\otimes H_3]X=\mathbf{0},$$

其中

$$H_1=\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & w_{d_B-1} & \cdots & w_{d_B-1}^{(d_B-3)}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & w_{d_B-1}^{(d_B-3)} & \cdots & w_{d_B-1}^{(d_B-3)^2}\end{pmatrix},\quad H_2=\begin{pmatrix}w_{d_C-1} & w_{d_C-1}^2 & \cdots & w_{d_C-1}^{(d_C-2)}\\ w_{d_C-1}^2 & w_{d_C-1}^4 & \cdots & w_{d_C-1}^{2(d_C-2)}\\ \vdots & \vdots & \ddots & \vdots\\ w_{d_C-1}^{(d_C-2)} & w_{d_C-1}^{2(d_C-2)} & \cdots & w_{d_C-1}^{(d_C-2)^2}\end{pmatrix},$$

$H_3=(w_{d_C-1}^{ij})_{i,j\in\mathbb{Z}_{d_C-1}}$，并且 X 是一个列向量，

$$X=({}_B\langle t_1+1|_C\langle t_2|E|0\rangle_B|t_3\rangle_C)_{\{0\leqslant t_1\leqslant d_B-3,\ 1\leqslant t_2\leqslant d_C-2,\ 0\leqslant t_3\leqslant d_C-2\}}.$$

由于 H_1,H_2,H_3 都是满秩矩阵，这推出 $H_1^\dagger\otimes H_2^\dagger\otimes H_3$ 也是一个满秩矩阵，那么我们有 $X=\mathbf{0}$，即

$${}_B\langle t_1+1|_C\langle t_2|E|0\rangle_B|t_3\rangle_C=0,\ 0\leqslant t_1\leqslant d_B-3,\ 1\leqslant t_2\leqslant d_C-2,\ 0\leqslant t_3\leqslant d_C-2.$$

这也意味着

$$\mathcal{F}^{(A)}E_{\mathcal{A}_1^{(A)}}=\mathbf{0}. \tag{4.22}$$

类似地，通过 $\mathcal{A}_3(|d_A-1\rangle_A)$ 和 $\mathcal{A}_2(|\xi_1\rangle_A)$，我们也可以得到

$$\mathcal{F}^{(A)}E_{\mathcal{A}_2^{(A)}}=\mathbf{0}. \tag{4.23}$$

此外，由于图3.13的对称性，我们也能得到

$$\mathcal{F}^{(A)}E_{\mathcal{B}_1^{(A)}}=\mathbf{0},\quad \mathcal{F}^{(A)}E_{\mathcal{B}_2^{(A)}}=\mathbf{0}. \tag{4.24}$$

因此，由公式(4.20)，(4.22)，(4.23)和(4.24)可知，E 是一个分块对角矩阵，它可以表示为：

$$E=E_{\mathcal{A}_1^{(A)}}\oplus E_{\mathcal{A}_2^{(A)}}\oplus E_{\mathcal{F}^{(A)}}\oplus E_{\mathcal{B}_2^{(A)}}\oplus E_{\mathcal{B}_1^{(A)}}. \tag{4.25}$$

步骤 2 考虑 $|S\rangle$ 和 $\{|\beta_0\rangle_A|\beta_j\rangle_B|\beta_k\rangle_C\}_{(j,k)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}\setminus\{(0,0)\}}\subset\mathcal{F}$，其中 $d_C\geqslant 4$，那么由公式(4.25)可知，对于 $(j,k)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}\setminus\{(0,0)\}$，有

$${}_B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_C-1}\langle i_2|\right)E|\beta_j\rangle_B|\beta_k\rangle_C={}_B\left(\sum_{i_1=1}^{d_B-2}\langle i_1|\right)_C\left(\sum_{i_2=1}^{d_C-2}\langle i_2|\right)E|\beta_j\rangle_B|\beta_k\rangle_C=0.$$

此外，我们有

$$\left(\sum_{i_1=1}^{d_B-2}|i_1\rangle\right)_B\left(\sum_{i_2=1}^{d_C-2}|i_2\rangle\right)_C=|\beta_0\rangle_B|\beta_0\rangle_C.$$

因此，通过 $\{|S\rangle\}\cup\{|\beta_0\rangle_A|\beta_j\rangle_B|\beta_k\rangle_C\}_{(j,k)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}}\setminus\{(0,0)\}$，我们有

$${}_B\langle\beta_i|_C\langle\beta_j|E|\beta_k\rangle_B|\beta_\ell\rangle_C=0,\quad (i,j)\neq(k,\ell)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}. \tag{4.26}$$

通过公式(4.26)可知，对于 $(s,t)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}$，必然存在实数 $e_{s,t}$（$E^\dagger=E$），使得

$$E_{\mathcal{F}^{(A)}}=\sum_{s=0}^{d_B-3}\sum_{t=0}^{d_C-3}e_{s,t}|\beta_s\rangle_B\langle\beta_s|\otimes|\beta_t\rangle_C\langle\beta_t|. \tag{4.27}$$

注意公式(4.27)对 $d_C=3$ 同样成立，这是因为在这种情况下 $E_{\mathcal{F}^{(A)}}=e_{0,0}|\beta_0\rangle_B\langle\beta_0|\otimes|\beta_0\rangle_C\langle\beta_0|$, 其中 $|\beta_0\rangle_X=|1\rangle_X$, $X\in\{B,C\}$。接下来, 通过 $\mathcal{A}_1(|\xi_1\rangle_A)$, 我们有

$${}_B\langle 0|_C\langle\eta_i|E|0\rangle_B|\eta_j\rangle_C=0,\quad i\neq j\in\mathbb{Z}_{d_C-1}.$$

然后 $s\in\mathbb{Z}_{d_C-1}$，必然存在实数 a_s 使得

$$E_{\mathcal{A}_1^{(A)}}=\sum_{s=0}^{d_C-2}a_s|0\rangle_B\langle 0|\otimes|\eta_s\rangle_C\langle\eta_s|.$$

同样，以类似的方式，必然存在实数 $a_s,b_s,c_t,d_t,e_{s,t}$ 使得

$$\begin{aligned}E=&\sum_{s=0}^{d_C-2}a_s|0\rangle_B\langle 0|\otimes|\eta_s\rangle_C\langle\eta_s|+\sum_{s=0}^{d_B-2}b_s|\eta_s\rangle_B\langle\eta_s|\otimes|d_C-1\rangle_C\langle d_C-1|\\&+\sum_{s=0}^{d_B-3}\sum_{t=0}^{d_C-3}e_{s,t}|\beta_s\rangle_B\langle\beta_s|\otimes|\beta_t\rangle_C\langle\beta_t|+\sum_{t=0}^{d_B-2}c_t|\xi_t\rangle_B\langle\xi_t|\otimes|0\rangle_C\langle 0|\\&+\sum_{t=0}^{d_C-2}d_t|d_B-1\rangle_B\langle d_B-1|\otimes|\xi_t\rangle_C\langle\xi_t|.\end{aligned} \tag{4.28}$$

通过 $\{|0\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C\}_{(i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}}=\mathcal{B}_3$，我们可以得到

$${}_B\langle\eta_k|_C\langle\xi_\ell|E|\eta_i\rangle_B|\xi_j\rangle_C=0,\quad(k,\ell)\neq(i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}.$$

假设 $k=0$，$\ell\neq 0$，$i\neq 0$，$j=0$，由公式(4.28)，可知

$$\begin{aligned}0=&{}_B\langle\eta_0|_C\langle\xi_\ell|E|\eta_i\rangle_B|\xi_0\rangle_C\\=&\sum_{s=0}^{d_C-2}a_s\langle\eta_0|0\rangle_B\langle 0|\eta_i\rangle_B\langle\xi_\ell|\eta_s\rangle_C\langle\eta_s|\xi_0\rangle_C\\&+\sum_{s=0}^{d_B-3}\sum_{t=0}^{d_C-3}e_{s,t}\langle\eta_0|\beta_s\rangle_B\langle\beta_s|\eta_i\rangle_B\langle\xi_\ell|\beta_t\rangle_C\langle\beta_t|\xi_0\rangle_C\\=&\sum_{s=0}^{d_C-2}a_s\langle\xi_\ell|\eta_s\rangle_C\langle\eta_s|\xi_0\rangle_C+w_{d_C-1}^{\ell}(d_B-2)(d_C-2)e_{0,0}.\end{aligned} \tag{4.29}$$

上个等式的最后一个求和项有三种情况:

(a) 如果 $s=0$，那么

$$\langle\xi_\ell|\eta_0\rangle_C\langle\eta_0|\xi_0\rangle_C=(d_C-2)\sum_{n=1}^{d_C-2}w_{d_C-1}^{-(n-1)\ell}=-(d_C-2)w_{d_C-1}^{\ell}.$$

(b) 如果 $s=\ell$，那么

$$\langle\xi_\ell|\eta_\ell\rangle_C\langle\eta_\ell|\xi_0\rangle_C=-\sum_{n=1}^{d_C-2}w_{d_C-1}^{\ell}=-(d_C-2)w_{d_C-1}^{\ell}.$$

(c) 如果 $s\neq 0,\ell$，那么

$$\langle\xi_\ell|\eta_s\rangle_C\langle\eta_s|\xi_0\rangle_C=-\sum_{n=1}^{d_C-2}w_{d_C-1}^{ns-(n-1)\ell}=-w_{d_C-1}^{\ell}\sum_{n=1}^{d_C-2}w_{d_C-1}^{(s-\ell)n}=w_{d_C-1}^{\ell}.$$

因此，由公式(4.29)可知

$$\sum_{s=0}^{d_C-2}a_s-(d_C-1)(a_0+a_\ell)+(d_B-2)(d_C-2)e_{0,0}=0. \tag{4.30}$$

由于 $\ell\neq 0\in\mathbb{Z}_{d_C-1}$，我们一定有 $a_1=a_2=\cdots=a_{d_C-2}$。那么公式(4.30)可以表示为:

$$-(d_C-2)a_0-a_1+(d_B-2)(d_C-2)e_{0,0}=0. \tag{4.31}$$

此外，通过 $|S\rangle$，$|0\rangle_A|\eta_1\rangle_B|\xi_0\rangle\in\mathcal{B}_3$ 和公式(4.28)，我们得到

$$\begin{aligned}&{}_B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_B-1}\langle i_2|\right)E|\eta_1\rangle_B|\xi_0\rangle_C\\&=(d_C-1)(d_C-2)a_0-(d_B-2)(d_C-2)^2e_{0,0}=0,\end{aligned}$$

即

$$(d_C-1)a_0-(d_B-2)(d_C-2)e_{0,0}=0. \tag{4.32}$$

那么由公式(4.31)和(4.32)可知，$a_0=a_1$。因此 $a_0=a_1=\cdots=a_{d_C-2}=a$，这意味着

$$E_{\mathcal{A}_1^{(A)}}=a\sum_{s=0}^{d_C-2}|0\rangle_B\langle 0|\otimes|\eta_s\rangle_C\langle\eta_s|,$$

也等价于

$$E_{\mathcal{A}_1^{(A)}}=a\mathbb{I}_{\mathcal{A}_1^{(A)}}. \tag{4.33}$$

步骤 3 考虑 $|S\rangle$ 和 $\{|0\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C\}_{(i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}}=\mathcal{B}_3$，通过公式(4.25)和(4.33)，我们有

$${}_B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_C-1}\langle i_2|\right)E|\eta_i\rangle_B|\xi_j\rangle_C={}_B\left(\sum_{i_1=0}^{d_B-2}\langle i_1|\right)_C\left(\sum_{i_2=1}^{d_C-1}\langle i_2|\right)E|\eta_i\rangle_B|\xi_j\rangle_C=0.$$

此外，我们有

$$\left(\sum_{i_1=0}^{d_B-2}|i_1\rangle\right)_B\left(\sum_{i_2=1}^{d_C-1}|i_2\rangle\right)_C=|\eta_0\rangle_B|\xi_0\rangle_C.$$

因此，通过 $\{|S\rangle\}\cup\{|0\rangle_A|\eta_i\rangle_B|\xi_j\rangle_C\}_{(i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\setminus\{(0,0)\}}$，我们有

$$_B\langle\eta_k|_C\langle\xi_\ell|E|\eta_i\rangle_B|\xi_j\rangle_C=0,\quad (k,\ell)\neq(i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}.$$

对于任何 $|j\rangle_B|k\rangle_C\in\mathcal{A}_1^{(A)}\cap\mathcal{B}_3^{(A)}$，通过公式(4.25)和(4.33)，我们有 $_{\{|j\rangle_B|k\rangle_C\}}E_{\mathcal{B}_3^{(A)}\setminus\{|j\rangle_B|k\rangle_C\}}=\mathbf{0}$。对 $\{|\eta_i\rangle_B|\xi_j\rangle_C\}_{(i,j)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}}$ 运用引理4.3，我们有

$$E_{\mathcal{B}_3^{(A)}}=a_1\mathbb{I}_{\mathcal{B}_3^{(A)}}. \tag{4.34}$$

由于 $\mathcal{A}_1^{(A)}\cap\mathcal{B}_3^{(A)}\neq\varnothing$，这推出 $a=a_1$。因此，再通过公式(4.33)和(4.34)，我们得到

$$E_{\mathcal{A}_1^{(A)}\cup\mathcal{B}_3^{(A)}}=a\mathbb{I}_{\mathcal{A}_1^{(A)}\cup\mathcal{B}_3^{(A)}}.$$

由于图3.13的对称性，我们得到 $E=a\mathbb{I}$。引理得证。 ∎

下面我们有更一般的结论。

定理 4.8　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}$ 中，$3\leqslant d_A\leqslant d_B\leqslant d_C$，对于任何 $0\leqslant n\leqslant\lfloor\frac{d_A-3}{2}\rfloor$，公式(3.10)给出的

$$\mathcal{U}_n:=\cup_{t=0}^{n}(\cup_{i=1}^{3}(\mathcal{A}_i^{(t)}\cup\mathcal{B}_i^{(t)}))\cup\mathcal{F}^{(n)}\cup\{|S\rangle\}$$

是一个强非局域的不可扩充乘积基，且 $|\mathcal{U}_n=d_Ad_Bd_C-8(n+1)|$。

我们只需在引理4.7的基础上，对 $\mathcal{U}_n$ 中的 t 进行归纳，即可验证 $\mathcal{U}_n$ 具有强量子非局域性。

4.4.2　四体系统中强非局域的不可扩充乘积基

首先，我们验证公式(3.18)给出的不可扩充乘积基具有强量子非局域性。

引理 4.9　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}\otimes\mathbb{C}^{d_D}$ 中，$3\leqslant d_A\leqslant d_B\leqslant d_C\leqslant d_D$，公式(3.18)给出的 $\cup_{i=1}^{8}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}$ 是一个强非局域的不可扩充乘积基，且 $|\cup_{i=1}^{8}(\mathcal{A}_i\cup\mathcal{B}_i)\cup\mathcal{F}\cup\{|S\rangle\}|=d_Ad_Bd_Cd_D-16$。

证明　令 B，C 和 D 一起进行一个正交保持的局部测量 $\{E=M^\dagger M\}$，其中 $E=(a_{ijk,\ell mn})_{i,\ell\in\mathbb{Z}_{d_B},j,m\in\mathbb{Z}_{d_C},k,n\in\mathbb{Z}_{d_D}}$，那么测量后的态 $\{\mathbb{I}_A\otimes M|\psi\rangle:|\psi\rangle\in\mathcal{U}\}$ 是相互正交的。

步骤 1 由于 $\langle\xi_1|\eta_1\rangle_A\neq0$，对 $\cup_{i=1}^{4}\{\mathcal{A}_i(|\xi_1\rangle_A),\mathcal{B}_i(|\eta_1\rangle_A)\}$ 中任意两个元素运用引理4.2，我们有

$$\begin{aligned}&\mathcal{A}_i^{(A)}E_{\mathcal{A}_j^{(A)}}=\mathbf{0},\ \mathcal{A}_i^{(A)}E_{\mathcal{B}_k^{(A)}}=\mathbf{0},\ \mathcal{B}_k^{(A)}E_{\mathcal{B}_\ell^{(A)}}=\mathbf{0},\ \mathcal{B}_k^{(A)}E_{\mathcal{A}_i^{(A)}}=\mathbf{0}.\\&1\leqslant i\neq j\leqslant4,\ 1\leqslant k\neq\ell\leqslant4.\end{aligned} \tag{4.35}$$

接下来，我们考虑 $\mathcal{A}_5(|d_A-1\rangle_A)$ 和 $\mathcal{A}_1(|\xi_1\rangle_A)$，对于 $(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}$ 和 $(m,n)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_D-1}$，我们有

$$
\begin{aligned}
&{}_B\langle\eta_j|_C\langle\xi_k|_D\langle\eta_\ell|E|\eta_m\rangle_B|0\rangle_C|\xi_n\rangle_D=\\
&{}_B\left(\sum_{t_1=0}^{d_B-2}w_{d_B-1}^{-jt_1}\langle t_1|\right)_C\left(\sum_{t_2=0}^{d_C-2}w_{d_C-1}^{-kt_2}\langle t_2+1|\right)_D\left(\sum_{t_3=0}^{d_D-2}w_{d_D-1}^{-\ell t_3}\langle t_3|\right)E\\
&\left(\sum_{t_4=0}^{d_B-2}w_{d_B-1}^{mt_4}|t_4\rangle\right)_B|0\rangle_C\left(\sum_{t_5=0}^{d_D-2}w_{d_D-1}^{nt_5}|t_5+1\rangle\right)_D=0.
\end{aligned}
\tag{4.36}
$$

由公式(4.35)可知，对于 $1\leqslant i\leqslant 4$，${}_{\mathcal{B}_i^{(A)}}E_{\mathcal{A}_1^{(A)}}=\mathbf{0}$。对于 $1\leqslant i\leqslant 4$，这意味着 ${}_{\mathcal{B}_i^{(A)}\cap\mathcal{A}_5^{(A)}}E_{\mathcal{A}_1^{(A)}}=\mathbf{0}$。那么公式(4.36)可以表示为

$$
\begin{aligned}
&{}_B\left(\sum_{t_1=1}^{d_B-2}w_{d_B-1}^{-jt_1}\langle t_1|\right)_C\left(\sum_{t_2=0}^{d_C-3}w_{d_C-1}^{-kt_2}\langle t_2+1|\right)_D\left(\sum_{t_3=1}^{d_D-2}w_{d_D-1}^{-\ell t_3}\langle t_3|\right)E\\
&\left(\sum_{t_4=0}^{d_B-2}w_{d_B-1}^{mt_4}|t_4\rangle\right)_B|0\rangle_C\left(\sum_{t_5=0}^{d_D-2}w_{d_D-1}^{nt_5}|t_5+1\rangle\right)_D=0,
\end{aligned}
$$

即对于任何 $1\leqslant j\leqslant d_B-2$，$0\leqslant k\leqslant d_C-3$，$1\leqslant\ell\leqslant d_D-2$，$0\leqslant m\leqslant d_B-2$，$0\leqslant n\leqslant d_D-2$，有

$$
\begin{aligned}
&\sum_{t_1=1}^{d_B-2}\sum_{t_2=0}^{d_C-3}\sum_{t_3=1}^{d_D-2}\sum_{t_4=0}^{d_B-2}\sum_{t_5=0}^{d_D-2}w_{d_B-1}^{-jt_1}w_{d_C-1}^{-kt_2}w_{d_D-1}^{-\ell t_3}w_{d_B-1}^{mt_4}w_{d_D-1}^{nt_5}\times\\
&{}_B\langle t_1|_C\langle t_2+1|_D\langle t_3|E|t_4\rangle_B|0\rangle_C|t_5+1\rangle_D=0.
\end{aligned}
$$

这意味着

$$
[H_1^\dagger\otimes H_2^\dagger\otimes H_3^\dagger\otimes H_4\otimes H_5]X=\mathbf{0},
$$

其中

$$
H_1=\begin{pmatrix}
w_{d_B-1} & w_{d_B-1}^2 & \cdots & w_{d_B-1}^{(d_B-2)}\\
w_{d_B-1}^2 & w_{d_B-1}^4 & \cdots & w_{d_B-1}^{2(d_B-2)}\\
\vdots & \vdots & \ddots & \vdots\\
w_{d_B-1}^{(d_B-2)} & w_{d_B-1}^{2(d_B-2)} & \cdots & w_{d_B-1}^{(d_B-2)^2}
\end{pmatrix},\quad
H_2=\begin{pmatrix}
1 & 1 & \cdots & 1\\
1 & w_{d_C-1} & \cdots & w_{d_C-1}^{(d_C-3)}\\
\vdots & \vdots & \ddots & \vdots\\
1 & w_{d_C-1}^{(d_C-3)} & \cdots & w_{d_C-1}^{(d_C-3)^2}
\end{pmatrix}
$$

$$
H_3=\begin{pmatrix}
w_{d_D-1} & w_{d_D-1}^2 & \cdots & w_{d_D-1}^{(d_D-2)}\\
w_{d_D-1}^2 & w_{d_D-1}^4 & \cdots & w_{d_D-1}^{2(d_D-2)}\\
\vdots & \vdots & \ddots & \vdots\\
w_{d_D-1}^{(d_D-2)} & w_{d_D-1}^{2(d_D-2)} & \cdots & w_{d_D-1}^{(d_D-2)^2}
\end{pmatrix},
$$

$H_4 = (w_{d_B-1}^{ij})_{i,j\in\mathbb{Z}_{d_B-1}}$，$H_5 = (w_{d_D-1}^{ij})_{i,j\in\mathbb{Z}_{d_D-1}}$，且 X 是一个列向量：

$$X = ({}_B\langle t_1|_C\langle t_2+1|_D\langle t_3|E|t_4\rangle_B|0\rangle_C|t_5+1\rangle_D)_{\{1\leqslant t_1\leqslant d_B-2,\ 0\leqslant t_2\leqslant d_C-3,\ 1\leqslant t_3\leqslant d_D-2\ 0\leqslant t_4\leqslant d_B-2,\ 0\leqslant t_5\leqslant d_D-2\}}.$$

由于 H_1, H_2, H_3, H_4, H_5 都是满秩矩阵，我们可以得到 $H_1^\dagger\otimes H_2^\dagger\otimes H_3^\dagger\otimes H_4\otimes H_5$ 也是一个满秩矩阵，这推出 $X=\mathbf{0}$，即对于 $1\leqslant t_1\leqslant d_B-2$，$0\leqslant t_2\leqslant d_C-3$，$1\leqslant t_3\leqslant d_D-2$，$0\leqslant t_4\leqslant d_B-2$，$0\leqslant t_5\leqslant d_D-2$，我们有

$${}_B\langle t_1|_C\langle t_2+1|_D\langle t_3|E|t_4\rangle_B|0\rangle_C(|t_5+1\rangle_D=0,$$

这也意味着

$$\mathcal{F}^{(A)}E_{\mathcal{A}_1^{(A)}}=\mathbf{0}.$$

类似地，对于 $1\leqslant i\leqslant 4$，通过 $\mathcal{A}_5(|d_A-1\rangle_A)$ 和 $\mathcal{A}_i(|\xi_1\rangle_A)$，我们能像上面一样推出

$$\mathcal{F}^{(A)}E_{\mathcal{A}_i^{(A)}}=\mathbf{0},\quad 1\leqslant i\leqslant 4. \tag{4.37}$$

此外，由于图3.15的对称性，我们也可以得到

$$\mathcal{F}^{(A)}E_{\mathcal{B}_j^{(A)}}=\mathbf{0},\quad 1\leqslant j\leqslant 4. \tag{4.38}$$

因此，由公式(4.35)，(4.37)和 (4.38)可知，E 是一个分块对角矩阵，它可以表示为：

$$E=E_{\mathcal{A}_1^{(A)}}\oplus E_{\mathcal{A}_2^{(A)}}\oplus E_{\mathcal{A}_3^{(A)}}\oplus E_{\mathcal{A}_4^{(A)}}\oplus E_{\mathcal{F}^{(A)}}\oplus E_{\mathcal{B}_4^{(A)}}\oplus E_{\mathcal{B}_3^{(A)}}\oplus E_{\mathcal{B}_2^{(A)}}\oplus E_{\mathcal{B}_1^{(A)}}. \tag{4.39}$$

步骤 2 考虑 $|S\rangle$ 和 $\{|\beta_0\rangle_A|\beta_j\rangle_B|\beta_k\rangle_C|\beta_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}\times\mathbb{Z}_{d_D-2}\setminus\{(0,0,0)\}}\subset\mathcal{F}$，其中 $d_D\geqslant 4$。对于 $(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}$，那我们有

$$\begin{aligned}&B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)C\left(\sum_{i_2=0}^{d_C-1}\langle i_2|\right)D\left(\sum_{i_3=0}^{d_D-1}\langle i_3|\right)E|\beta_j\rangle_B|\beta_k\rangle_C|\beta_\ell\rangle_D=\\&B\left(\sum_{i_1=1}^{d_B-2}\langle i_1|\right)C\left(\sum_{i_2=1}^{d_C-2}\langle i_2|\right)D\left(\sum_{i_3=1}^{d_D-2}\langle i_3|\right)E|\beta_j\rangle_B|\beta_k\rangle_C|\beta_\ell\rangle_D=0.\end{aligned}$$

此外我们有

$$\left(\sum_{i_1=1}^{d_B-2}|i_1\rangle\right)_B\left(\sum_{i_2=1}^{d_C-2}|i_2\rangle\right)_C\left(\sum_{i_3=1}^{d_D-2}|i_3\rangle\right)_D=|\beta_0\rangle_B|\beta_0\rangle_C|\beta_0\rangle_D.$$

因此通过 $\{|S\rangle\}\cup\{|\beta_0\rangle_A|\beta_j\rangle_B|\beta_k\rangle_C|\beta_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}\times\mathbb{Z}_{d_D-2}\setminus\{(0,0,0)\}}$，我们得到

$$\begin{aligned}&{}_B\langle\beta_i|_C\langle\beta_j|_D\langle\beta_k|E|\beta_\ell\rangle_B|\beta_m\rangle_C|\beta_n\rangle_D=0,\\&(i,j,k)\neq(\ell,m,n)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}\times\mathbb{Z}_{d_D-2}.\end{aligned}$$

对于 $(r,s,t)\in\mathbb{Z}_{d_B-2}\times\mathbb{Z}_{d_C-2}\times\mathbb{Z}_{d_D-2}$，存在实数 $e_{r,s,t}$ 使得

$$E_{\mathcal{F}^{(A)}}=\sum_{r=0}^{d_B-3}\sum_{s=0}^{d_C-3}\sum_{t=0}^{d_D-3}e_{r,s,t}|\beta_r\rangle_B\langle\beta_r|\otimes|\beta_s\rangle_C\langle\beta_s|\otimes|\beta_t\rangle_D\langle\beta_t|. \tag{4.40}$$

注意公式(4.40)对 $d_D=3$ 也成立。接下来，通过 $\mathcal{A}_1(|\xi_1\rangle_A)$，我们有

$${}_B\langle\eta_i|_C\langle 0|_D\langle\xi_j|E|\eta_k\rangle_B|0\rangle_C|\xi_\ell\rangle_D=0,\quad (i,j)\neq(k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_D-1}.$$

对于 $(s,t)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_D-1}$，存在实数 $a_{s,t}$ 使得

$$E_{\mathcal{A}_1^{(A)}}=\sum_{s=0}^{d_B-2}\sum_{t=0}^{d_D-2}a_{s,t}|\eta_s\rangle_B\langle\eta_s|\otimes|0\rangle_C\langle 0|\otimes|\xi_t\rangle_D\langle\xi_t|.$$

类似地，存在实数 $a_{s,t},b_{s,t},c_{s,t},p,e_{r.s,t},q,g_{s,t},h_{s,t},i_{s,t}$ 使得

$$\begin{aligned}
E=&\sum_{s=0}^{d_B-2}\sum_{t=0}^{d_D-2}a_{s,t}|\eta_s\rangle_B\langle\eta_s|\otimes|0\rangle_C\langle 0|\otimes|\xi_t\rangle_D\langle\xi_t|\\
&+\sum_{s=0}^{d_C-2}\sum_{t=0}^{d_D-2}b_{s,t}|d_B-1\rangle_B\langle d_B-1|\otimes|\eta_s\rangle_C\langle\eta_s|\otimes|\eta_t\rangle_D\langle\eta_t|\\
&+\sum_{s=0}^{d_B-2}\sum_{t=0}^{d_C-2}c_{s,t}|\xi_s\rangle_B\langle\xi_s|\otimes|\xi_t\rangle_C\langle\xi_t|\otimes|d_D-1\rangle_D\langle d_D-1|\\
&+p|d_B-1\rangle_B\langle d_B-1|\otimes|0\rangle_C\langle 0|\otimes|d_D-1\rangle_D\langle d_D-1|\\
&+\sum_{r=0}^{d_B-3}\sum_{s=0}^{d_C-3}\sum_{t=0}^{d_D-3}e_{r,s,t}|\beta_r\rangle_B\langle\beta_r|\otimes|\beta_s\rangle_C\langle\beta_s|\otimes|\beta_t\rangle_D\langle\beta_t|\\
&+q|0\rangle_B\langle 0|\otimes|d_C-1\rangle_C\langle d_C-1|\otimes|0\rangle_D\langle 0|\\
&+\sum_{s=0}^{d_B-2}\sum_{t=0}^{d_C-2}g_{s,t}|\eta_s\rangle_B\langle\eta_s|\otimes|\eta_t\rangle_C\langle\eta_t|\otimes|0\rangle_D\langle 0|\\
&+\sum_{s=0}^{d_C-2}\sum_{t=0}^{d_D-2}h_{s,t}|0\rangle_B\langle 0|\otimes|\xi_s\rangle_C\langle\xi_s|\otimes|\xi_t\rangle_D\langle\xi_t|\\
&+\sum_{s=0}^{d_B-2}\sum_{t=0}^{d_D-2}i_{s,t}|\xi_s\rangle_B\langle\xi_s|\otimes|d_C-1\rangle_C\langle d_C-1|\otimes|\eta_t\rangle_D\langle\eta_t|.
\end{aligned}\tag{4.41}$$

通过 $\{|0\rangle_A|\xi_i\rangle_B|\eta_j\rangle_C|\xi_k\rangle_D\}_{(i,j,k)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}}=\mathcal{B}_5$，对于 $(i,j,k)\neq(\ell,m,n)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}$，我们有

$${}_B\langle\xi_i|_C\langle\eta_j|_D\langle\xi_k|E|\xi_\ell\rangle_B|\eta_m\rangle_C|\xi_n\rangle_D=0.$$

那么有三种情况:

(i) 假设 $i\neq 0,\ j=0,\ k=0,\ \ell=0,\ m\neq 0,\ n=0$。由公式(4.41)可知

$$\begin{aligned}0=&{}_B\langle\xi_i|_C\langle\eta_0|_D\langle\xi_0|E|\xi_0\rangle_B|\eta_m\rangle_C|\xi_0\rangle_D\\=&(d_D-1)^2\sum_{s=0}^{d_B-2}a_{s,0}\langle\xi_i|\eta_s\rangle_B\langle\eta_s|\xi_0\rangle_B+w^i_{d_B-1}p\\&+w^i_{d_B-1}(d_B-2)(d_C-2)(d_D-2)^2e_{0,0,0}\\=&(d_D-1)^2w^i_{d_B-1}\left(\sum_{s=0}^{d_B-2}a_{s,0}-(d_B-1)(a_{0,0}+a_{i,0})\right)\\&+w^i_{d_B-1}p+w^i_{d_B-1}(d_B-2)(d_C-2)(d_D-2)^2e_{0,0,0},\end{aligned}\tag{4.42}$$

即

$$\begin{aligned}&(d_D-1)^2\left(\sum_{s=0}^{d_B-2}a_{s,0}-(d_B-1)(a_{0,0}+a_{i,0})\right)+p\\&+(d_B-2)(d_C-2)(d_D-2)^2e_{0,0,0}=0.\end{aligned}\tag{4.43}$$

由于 $i\in\mathbb{Z}_{d_B-1}\setminus\{0\}$，我们得到 $a_{1,0}=a_{2,0}=\cdots=a_{d_B-2,0}$。然后公式(4.43)可以表示为

$$-(d_D-1)^2((d_B-2)a_{0,0}+a_{1,0})+p+(d_B-2)(d_C-2)(d_D-2)^2e_{0,0,0}=0.\tag{4.44}$$

接下来，通过 $|S\rangle$ 和 $|0\rangle_A|\xi_1\rangle_B|\eta_1\rangle_C|\xi_0\rangle_D\in\mathcal{B}_5$，我们有

$$\begin{aligned}0=&{}_B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_C-1}\langle i_2|\right)_D\left(\sum_{i_3=0}^{d_D-1}\langle i_3|\right)E|\xi_1\rangle_B|\eta_1\rangle_C|\xi_0\rangle_D\\=&-w^{d_B-2}_{d_B-1}(d_B-1)(d_D-1)^2a_{0,0}+w^{d_B-2}_{d_B-1}p\\&+w^{d_B-2}_{d_B-1}(d_B-2)(d_C-2)(d_D-2)^2e_{0,0,0},\end{aligned}$$

即

$$-(d_B-1)(d_D-1)^2a_{0,0}+p+(d_B-2)(d_C-2)(d_D-2)^2e_{0,0,0}=0.\tag{4.45}$$

考虑公式(4.44)和(4.45)，那我们有 $a_{0,0}=a_{1,0}$。这意味着 $a_{0,0}=a_{1,0}=\cdots=a_{d_B-2,0}=a$。

接下来，我们考虑 $\{|0\rangle_A|0\rangle_B|0\rangle_C|\xi_i\rangle_D\}_{i\in\mathbb{Z}_{d_D-1}\setminus\{0\}}=\mathcal{B}_8$ 和 $\{|0\rangle_A|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}}=\mathcal{B}_5$，对于 $i\in\mathbb{Z}_{d_D-1}\setminus\{0\}$ 和 $(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}$，那么我们有

$${}_B\langle 0|_C\langle 0|_D\langle\xi_i|E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D=0.\tag{4.46}$$

由公式(4.41)可知，对于 $i \in \mathbb{Z}_{d_D-1} \setminus \{0\}$，$(j,k,\ell) = (0,0,0)$，

$$ {}_B\langle 0|_C\langle 0|_D\langle \xi_i|E|\xi_0\rangle_B|\eta_0\rangle_C|\xi_0\rangle_D = 0; \tag{4.47} $$

对于 $(j,k) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1}$，$\ell \in \mathbb{Z}_{d_D-1} \setminus \{0\}$，我们有

$$ {}_B\langle 0|_C\langle 0|_D\langle \xi_0|E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D = 0. \tag{4.48} $$

此外，通过公式(4.41)可知，对于 $(j,k) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1}$，有

$$ \begin{aligned} &{}_B\langle 0|_C\langle 0|_D\langle \xi_0|E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_0\rangle_D = (d_D-1)^2 \sum_{s=0}^{d_B-2} a_{s,0}\langle \eta_s|\xi_j\rangle_B \\ &= a(d_D-1)^2 \sum_{s=0}^{d_B-2} \langle \eta_s|\xi_j\rangle_B \\ &= a(d_D-1)^2 \sum_{s=0}^{d_B-2}\sum_{n=1}^{d_B-2} w_{d_B-1}^{j(n-1)-ns} = a(d_D-1)^2 w_{d_B-1}^{-j} \sum_{s=0}^{d_B-2}\sum_{n=1}^{d_B-2} w_{d_B-1}^{n(j-s)} = 0. \end{aligned} \tag{4.49} $$

因此通过公式(4.46)，(4.47)，(4.48)和 (4.49)，对于 $i \in \mathbb{Z}_{d_D-1}$ 和 $(j,k,\ell) \in \mathbb{Z}_{d_B-1} \times \mathbb{Z}_{d_C-1} \times \mathbb{Z}_{d_D-1}$，我们有

$$ {}_B\langle 0|_C\langle 0|_D\langle \xi_i|E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D = 0. $$

对 $\{|0\rangle_B|0\rangle_C|\xi_i\rangle_D\}_{i\in\mathbb{Z}_{d_D-1}}$ 和 $\{|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}}$ 运用引理4.2，我们得到

$$ \mathcal{B}_8^{(A)} E \mathcal{B}_5^{(A)} = \mathbf{0}. \tag{4.50} $$

(ii) 假设 $i \neq 0$，$j = 0$，$k = 0$，$\ell = 0$，$m = 0$，$n \neq 0$。通过公式(4.41)，我们有

$$ \begin{aligned} 0 =& {}_B\langle \xi_i|_C\langle \eta_0|_D\langle \xi_0|E|\xi_0\rangle_B|\eta_0\rangle_C|\xi_n\rangle_D \\ =& w_{d_B-1}^{i}(d_C-1)^2 w_{d_D-1}^{-n}\left(\sum_{t=0}^{d_D-2} b_{0,t} - (d_D-1)(b_{0,0}+b_{0,n})\right) \\ &+ w_{d_B-1}^{i} w_{d_D-1}^{-n} p + w_{d_B-1}^{i} w_{d_D-1}^{-n}(d_B-2)(d_C-2)^2(d_D-2)e_{0,0,0}, \end{aligned} $$

即

$$ \begin{aligned} &(d_C-1)^2\left(\sum_{t=0}^{d_D-2} b_{0,t} - (d_D-1)(b_{0,0}+b_{0,n})\right) \\ &+ p + (d_B-2)(d_C-2)^2(d_D-2)e_{0,0,0} = 0. \end{aligned} \tag{4.51} $$

由于 $n \in \mathbb{Z}_{d_D-1} \setminus \{0\}$，我们得到 $b_{0,1} = b_{0,2} = \cdots = b_{0,d_D-2}$。然后公式(4.51)可以表示为

$$ -(d_C-1)^2((d_D-2)b_{0,0}+b_{0,1}) + p + (d_B-2)(d_C-2)^2(d_D-2)e_{0,0,0} = 0. \tag{4.52} $$

接下来，通过 $|S\rangle$ 和 $|0\rangle_A|\xi_1\rangle_B|\eta_0\rangle_C|\xi_1\rangle_D \in \mathcal{B}_5$，我们有

$$\begin{aligned}0 =& {}_B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_C-1}\langle i_2|\right)_D\left(\sum_{i_3=0}^{d_D-1}\langle i_3|\right)E|\xi_1\rangle_B|\eta_0\rangle_C|\xi_1\rangle_D\\ =& -w_{d_B-1}^{d_B-2}w_{d_D-1}^{d_D-2}(d_C-1)^2(d_D-1)b_{0,0}+w_{d_B-1}^{d_B-2}w_{d_D-1}^{d_D-2}p\\ &+w_{d_B-1}^{d_B-2}w_{d_D-1}^{d_D-2}(d_B-2)(d_C-2)^2(d_D-2)e_{0,0,0},\end{aligned}$$

即

$$-(d_C-1)^2(d_D-1)b_{0,0}+p+(d_B-2)(d_C-2)^2(d_D-2)e_{0,0,0}=0. \tag{4.53}$$

考虑公式(4.52)和(4.53)，我们有 $b_{0,0}=b_{0,1}$。这意味着 $b_{0,0}=b_{0,1}=\cdots=b_{0,d_D-2}=b$。

接下来，我们考虑 $\{|0\rangle_A|d_B-1\rangle_B|\eta_i\rangle_C|0\rangle_D\}_{i\in\mathbb{Z}_{d_C-1}\setminus\{0\}}=\mathcal{B}_7$ 和 $\{|0\rangle_A|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}}=\mathcal{B}_5$，像公式(4.46), (4.47), (4.48) 和 (4.49)一样讨论，对于 $i\in\mathbb{Z}_{d_C-1}$ 和 $(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}$，我们得到

$${}_B\langle d_B-1|_C\langle\eta_i|_D\langle 0|E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D=0.$$

对 $\{|d_B-1\rangle_B|\eta_i\rangle_C|0\rangle_D\}_{i\in\mathbb{Z}_{d_C-1}}$ 和 $\{|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}}$ 运用引理4.2，我们得到

$$\mathcal{B}_7^{(A)}E_{\mathcal{B}_5^{(A)}}=\mathbf{0}. \tag{4.54}$$

(iii) 假设 $i=0$，$j=0$，$k\neq 0$，$\ell=0$，$m\neq 0$，$n=0$。通过公式(4.41)，我们有

$$\begin{aligned}0 =& {}_B\langle\xi_0|_C\langle\eta_0|_D\langle\xi_k|E|\xi_0\rangle_B|\eta_m\rangle_C|\xi_0\rangle_D\\ =& w_{d_D-1}^k(d_B-1)^2\left(\sum_{t=0}^{d_C-2}c_{0,t}-(d_C-1)(c_{0,0}+c_{0,m})\right)\\ &+w_{d_D-1}^kp+w_{d_D-1}^k(d_B-2)^2(d_C-2)(d_D-2)e_{0,0,0},\end{aligned}$$

即

$$\begin{aligned}&(d_B-1)^2\left(\sum_{t=0}^{d_C-2}c_{0,t}-(d_C-1)(c_{0,0}+c_{0,m})\right)\\ &+p+(d_B-2)^2(d_C-2)(d_D-2)e_{0,0,0}=0.\end{aligned} \tag{4.55}$$

由于 $m\in\mathbb{Z}_{d_C-1}\setminus\{0\}$，我们得到 $c_{0,1}=c_{0,2}=\cdots=c_{0,d_C-2}$。然后公式(4.55)可以表示为

$$-(d_B-1)^2((d_C-2)c_{0,0}+c_{0,1})+p+(d_B-2)^2(d_C-2)(d_D-2)e_{0,0,0}=0. \tag{4.56}$$

接下来，通过公式 $|S\rangle$ 和 $|0\rangle_A|\xi_0\rangle_B|\eta_1\rangle_C|\xi_1\rangle_D \in \mathcal{B}_5$，我们有

$$\begin{aligned}0 =& {}_B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_C-1}\langle i_2|\right)_D\left(\sum_{i_3=0}^{d_D-1}\langle i_3|\right)E|\xi_0\rangle_B|\eta_1\rangle_C|\xi_1\rangle_D\\ =& -w_{d_D-1}^{d_D-2}(d_B-1)^2(d_C-1)c_{0,0}+w_{d_D-1}^{d_D-2}p\\ &+w_{d_D-1}^{d_D-2}(d_B-2)^2(d_C-2)(d_D-2)e_{0,0,0},\end{aligned}$$

即

$$-(d_B-1)^2(d_C-1)c_{0,0}+p+(d_B-2)^2(d_C-2)(d_D-2)e_{0,0,0}=0. \tag{4.57}$$

考虑公式(4.56)和(4.57)，我们有 $c_{0,0}=c_{0,1}$，这意味着 $c_{0,0}=c_{0,1}=\cdots=c_{0,d_D-2}=c$。

接下来，考虑 $\{|0\rangle_A|\xi_i\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D\}_{i\in\mathbb{Z}_{d_B-1}\setminus\{0\}}=\mathcal{B}_6$ 和 $\{|0\rangle_A|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}}=\mathcal{B}_5$。像公式(4.46), (4.47), (4.48)和 (4.49)一样讨论，对于 $i\in\mathbb{Z}_{d_B-1}$ 和 $(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}$，我们有

$${}_B\langle\xi_i|_C\langle d_C-1|_D\langle d_D-1|E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D=0.$$

对 $\{|\xi_i\rangle_B|d_C-1\rangle_C|d_D-1\rangle_D\}_{i\in\mathbb{Z}_{d_B-1}}$ 和 $\{|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}}$ 运用引理4.2，我们得到

$$\mathcal{B}_6^{(A)}E_{\mathcal{B}_5^{(A)}}=\mathbf{0}. \tag{4.58}$$

步骤 3 考虑 $|S\rangle$ 和 $\{|0\rangle_A|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}}=\mathcal{B}_5$，通过公式(4.39)，(4.50)，(4.54) 和 (4.58)，我们有下面等式

$$\begin{aligned}&{}_B\left(\sum_{i_1=0}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_C-1}\langle i_2|\right)_D\left(\sum_{i_3=0}^{d_D-1}\langle i_3|\right)E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\\ =&{}_B\left(\sum_{i_1=1}^{d_B-1}\langle i_1|\right)_C\left(\sum_{i_2=0}^{d_C-2}\langle i_2|\right)_D\left(\sum_{i_3=1}^{d_D-1}\langle i_3|\right)E|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D=0.\end{aligned}$$

此外，我们有

$$\left(\sum_{i_1=1}^{d_B-1}|i_1\rangle\right)_B\left(\sum_{i_2=0}^{d_C-2}|i_2\rangle\right)_C\left(\sum_{i_3=1}^{d_D-1}|i_3\rangle\right)_D=|\xi_0\rangle_B|\eta_0\rangle_C|\xi_0\rangle_D.$$

因此通过 $\{|S\rangle\}\cup\{|0\rangle_A|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}\setminus\{(0,0,0)\}}$，对于 $(i,j,k)\neq(\ell,m,n)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}$，我们有

$${}_B\langle\xi_i|_C\langle\eta_j|_D\langle\xi_k|E|\xi_\ell\rangle_B|\eta_m\rangle_C|\xi_n\rangle_D=0.$$

由公式(4.39)可知，$_{\mathcal{A}_4^{(A)}}E_{\mathcal{B}_5^{(A)}\setminus\mathcal{A}_4^{(A)}}=\mathbf{0}$，其中 $\mathcal{A}_4^{(A)}=\{|d_B-1\rangle_B|0\rangle_C|d_D-1\rangle_D\}$，$\mathcal{A}_4^{(A)}\subset\mathcal{B}_5^{(A)}$。对 $\{|\xi_j\rangle_B|\eta_k\rangle_C|\xi_\ell\rangle_D\}_{(j,k,\ell)\in\mathbb{Z}_{d_B-1}\times\mathbb{Z}_{d_C-1}\times\mathbb{Z}_{d_D-1}}$ 运用引理4.3，我们有

$$E_{\mathcal{B}_5^{(A)}}=a\mathbb{I}_{\mathcal{B}_5^{(A)}}. \tag{4.59}$$

接下来，对于任意 $|j\rangle_B|k\rangle_C|\ell\rangle_D\in\mathcal{A}_i^{(A)}\cap\mathcal{B}_5^{(A)}$，$i=1,2,3$，通过公式(4.50)，(4.54)，(4.58) 和 (4.59)，我们有 $_{\{|j\rangle_B|k\rangle_C|\ell\rangle_D\}}E_{\mathcal{A}_i^{(A)}\setminus\{|j\rangle_B|k\rangle_C|\ell\rangle_D\}}=\mathbf{0}$，$i=1,2,3$。对于 $i=1,2,3$，我们对 $\mathcal{A}_i(|\xi_1\rangle)$ 运用引理4.3，从而得到

$$E_{\mathcal{A}_i^{(A)}}=a_i\mathbb{I}_{\mathcal{A}_i^{(A)}}. \tag{4.60}$$

对于 $i=1,2,3$，因为有 $\mathcal{A}_i^{(A)}\cap\mathcal{B}_5^{(A)}\neq\varnothing$，这推出 $a_i=a$，$i=1,2,3$。因此由公式(4.59)和(4.60)可知

$$E_{\{\cup_{i=1}^3\mathcal{A}_i^{(A)}\}\cup\mathcal{B}_5^{(A)}}=a\mathbb{I}_{\{\cup_{i=1}^3\mathcal{A}_i^{(A)}\}\cup\mathcal{B}_5^{(A)}}.$$

由于图3.15的对称性，我们得到 $E=a\mathbb{I}$。引理得证。 ∎

下面我们有更一般的结论。

定理 4.10　在 $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}\otimes\mathbb{C}^{d_C}\otimes\mathbb{C}^{d_D}$ 中，$3\leqslant d_A\leqslant d_B\leqslant d_C\leqslant d_D$，对于任何 $0\leqslant n\leqslant\lfloor\frac{d_A-3}{2}\rfloor$，公式(3.24)给出的

$$\mathcal{U}_n:=\cup_{t=0}^n(\cup_{i=1}^8(\mathcal{A}_i^{(t)}\cup\mathcal{B}_i^{(t)}))\cup\mathcal{F}^{(n)}\cup\{|S\rangle\}$$

是一个强非局域的不可扩充乘积基，且 $|\mathcal{U}_n|=d_Ad_Bd_Cd_D-16(n+1)$。

我们只需在引理4.9的基础上，对 $\mathcal{U}_n$ 中的 t 进行归纳，即可验证 $\mathcal{U}_n$ 具有强量子非局域性。

4.5　强非局域的正交纠缠集

在本节中，对于 $d\geqslant 3$，我们利用3.4节三维立方体的分解构造 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 中强非局域的正交纠缠集（非真实纠缠集）。对于 $N\geqslant 3$，$d\geqslant 2$，我们利用循环置换群作用构造 $(\mathbb{C}^d)^{\otimes N}$ 中强非局域的正交纠缠集。特别地，对于 $N=3,4$，我们构造强非局域的真实纠缠集。下面针对纠缠集，我们给出类似于引理4.2和4.3的两个引理。

引理 4.11　假设 $\mathcal{B}_i:=\{|0\rangle,|1\rangle,\cdots,|d_i-1\rangle\}$ 是 $\mathbb{C}^{d_i}$ 的计算基，其中 $i=1,2$，并令 $d_2\times d_2$ 的 Hermitian 矩阵 $E=(a_{i,j})_{i,j\in\mathbb{Z}_{d_2}}$ 为 Hermitian 算子 E 在 $\mathcal{B}_2$ 下的矩阵表示。假设 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}$ 中有两个正交集，

$$\{|\psi_i\rangle=\sum_{j\in\mathbb{Z}_m}b_{i,j}|p_j\rangle|r_j\rangle\}_{i\in\mathbb{Z}_m},$$

$$\{|\varphi_k\rangle=\sum_{\ell\in\mathbb{Z}_n}c_{k,\ell}|q_\ell\rangle|s_\ell\rangle\}_{k\in\mathbb{Z}_n},$$

其中 $\{|r_j\rangle\}_{j\in\mathbb{Z}_m}$ 和 $\{|s_\ell\rangle\}_{\ell\in\mathbb{Z}_n}$ 是 $\mathcal{B}_2$ 的两个非空子集，且 $|p_j\rangle$，$|q_\ell\rangle \in \mathcal{B}_1$，$j \in \mathbb{Z}_m$，$\ell \in \mathbb{Z}_n$。这里我们不要求这些 $p_j(q_\ell)$ 各不相同。此外，假设

$$\langle\psi_i|\mathbb{I}\otimes E|\varphi_k\rangle = 0,\ i \in \mathbb{Z}_m,\ k \in \mathbb{Z}_n.$$

对于 $j \in \mathbb{Z}_m$，$\ell \in \mathbb{Z}_n$，如果 $p_j = q_\ell$，那么

$$a_{r_j,s_\ell} = a_{s_\ell,r_j} = 0.$$

证明　根据引理4.2，我们有

$$\langle p_j|\langle r_j|\mathbb{I}\otimes E|q_\ell\rangle|s_\ell\rangle = \langle p_j|r_\ell\rangle a_{r_j,s_\ell} = 0.$$

此引理得证。 ∎

引理 4.12　假设 $\mathcal{B}_i := \{|0\rangle, |1\rangle, \cdots, |d_i - 1\rangle\}$ 是 $\mathbb{C}^{d_i}$ 的计算基，其中 $i = 1, 2$，并令 $d_2 \times d_2$ 的 Hermitian 矩阵 $E = (a_{i,j})_{i,j\in\mathbb{Z}_{d_2}}$ 为 Hermitian 算子 E 在 $\mathcal{B}_2$ 下的矩阵表示。假设 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ 中有一个正交集，

$$\{|\psi_i\rangle = \sum_{j\in\mathbb{Z}_m} b_{i,j}|p_j\rangle|r_j\rangle\}_{i\in\mathbb{Z}_m},$$

其中 $\{|r_j\rangle\}_{j\in\mathbb{Z}_m}$ 是 $\mathcal{B}_2$ 的非空子集，且 $|p_j\rangle \in \mathcal{B}_1$，$j \in \mathbb{Z}_m$。这里我们不要求这些 p_j 各不相同。此外，假设

$$\langle\psi_i|\mathbb{I}\otimes E|\psi_k\rangle = 0,\ i \neq k \in \mathbb{Z}_m.$$

如果存在 $t \in \mathbb{Z}_m$，使得 $a_{r_t,r_j} = 0$，$j \neq t \in \mathbb{Z}_m$，且 $b_{i,t} \neq 0$，$i \in \mathbb{Z}_m$，那么我们有

$$a_{r_i,r_j} = a_{r_j,r_i} = 0,\ i \neq j \text{ 且 } p_i = p_j,$$

此外

$$a_{r_0,r_0} = a_{r_i,r_i},\ i \neq 0 \in \mathbb{Z}_m.$$

证明　根据引理4.3，我们有

$$\langle p_i|\langle r_i|\mathbb{I}\otimes E|p_j\rangle|r_j\rangle = \langle p_i|p_j\rangle a_{r_i,r_j} = k\delta_{i,j}.$$

此引理得证。 ∎

4.5.1　三体系统中强非局域的正交纠缠集

首先我们考虑3.4节 3×3×3 立方体的分解。我们取出图3.11中的 $C_1 = \{1, 2\}_A \times \{0\}_B \times \{0, 1\}_C$ 中，如图4.6所示。

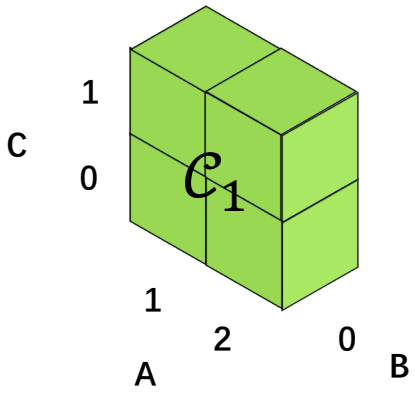

图 4.6　图3.11中的 $C_1 = \{1,2\}_A \times \{0\}_B \times \{0,1\}_C$。

由 $\mathcal{C}_1$，我们可以在 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 中构造 4 个相互正交的纠缠态:

$$\mathcal{C}_1 := \{|\psi_{1,2}\rangle = |1\rangle_A|0\rangle_B|0\rangle_C \pm |2\rangle_A|0\rangle_B|1\rangle_C, |\psi_{3,4}\rangle = |1\rangle_A|0\rangle_B|1\rangle_C \pm |2\rangle_A|0\rangle_B|0\rangle_C\}.$$

显然，对于 $1 \leqslant i \leqslant 4$，$|\psi_i\rangle$ 在两体划分 $A|BC$ 和 $AB|C$ 下是纠缠态，而在两体划分 $AC|B$ 下是乘积态。从而 $|\psi_i\rangle$ 是纠缠态，但不是真实纠缠态。按照上述方式，由图3.11中的 $\cup_{i=1}^3\{\mathcal{C}_i, \mathcal{D}_i\}$，我们可以在 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 中构造 24 个相互正交的纠缠态:

$$\begin{aligned}
\mathcal{C}_1 :=&\{|\psi_{1,2}\rangle = |1\rangle_A|0\rangle_B|0\rangle_C \pm |2\rangle_A|0\rangle_B|1\rangle_C, |\psi_{3,4}\rangle = |1\rangle_A|0\rangle_B|1\rangle_C \pm |2\rangle_A|0\rangle_B|0\rangle_C\},\\
\mathcal{C}_2 :=&\{|\psi_{5,6}\rangle = |1\rangle_A|0\rangle_B|2\rangle_C \pm |2\rangle_A|1\rangle_B|2\rangle_C, |\psi_{7,8}\rangle = |1\rangle_A|1\rangle_B|2\rangle_C \pm |2\rangle_A|0\rangle_B|2\rangle_C\},\\
\mathcal{C}_3 :=&\{|\psi_{9,10}\rangle = |2\rangle_A|1\rangle_B|0\rangle_C \pm |2\rangle_A|2\rangle_B|1\rangle_C, |\psi_{11,12}\rangle = |2\rangle_A|1\rangle_B|1\rangle_C \pm |2\rangle_A|2\rangle_B|0\rangle_C\},\\
\mathcal{D}_1 :=&\{|\psi_{13,14}\rangle = |0\rangle_A|2\rangle_B|1\rangle_C \pm |1\rangle_A|2\rangle_B|2\rangle_C, |\psi_{15,16}\rangle = |0\rangle_A|2\rangle_B|2\rangle_C \pm |1\rangle_A|2\rangle_B|1\rangle_C\},\\
\mathcal{D}_2 :=&\{|\psi_{17,18}\rangle = |0\rangle_A|1\rangle_B|0\rangle_C \pm |1\rangle_A|2\rangle_B|0\rangle_C, |\psi_{19,20}\rangle = |0\rangle_A|2\rangle_B|0\rangle_C \pm |1\rangle_A|1\rangle_B|0\rangle_C\},\\
\mathcal{D}_3 :=&\{|\psi_{21,22}\rangle = |0\rangle_A|0\rangle_B|1\rangle_C \pm |0\rangle_A|1\rangle_B|2\rangle_C, |\psi_{23,24}\rangle = |0\rangle_A|0\rangle_B|2\rangle_C \pm |0\rangle_A|1\rangle_B|1\rangle_C\}.
\end{aligned} \tag{4.61}$$

则公式(4.61)在两体划分 $A|BC$ 下对应于图4.7。注意，对于 $1 \leqslant i \leqslant 24$，$|\psi_i\rangle$ 在集合 $\{A|BC, AB|C, AC|B\}$ 中两个两体划分下是纠缠态，在剩下一个两体划分下是乘积态。那么下面我们证明 $\cup_{i=1}^3(\mathcal{C}_i \cup \mathcal{D}_i)$ 具有强量子非局域性。由于 $\cup_{i=1}^3\{\mathcal{C}_i, \mathcal{D}_i\}$ 在子系统的循环置换下有相同的结构，我们只需要验证 B 和 C 进行的正交保持的局部测量是平凡的。

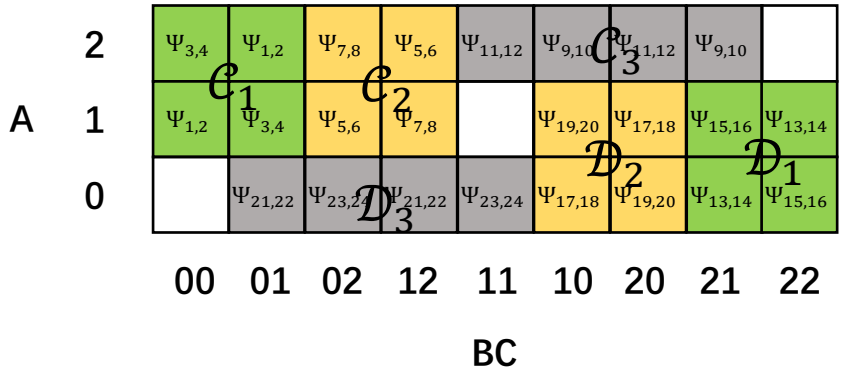

图 4.7　公式(4.61)在两体划分 $A|BC$ **下对应的** 3×9 **网格。**

引理 4.13　在 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ 中，公式(4.61)给出的 $\cup_{i=1}^3(\mathcal{C}_i \cup \mathcal{D}_i)$ 是一个强非局域的正交纠缠集，且 $|\cup_{i=1}^3(\mathcal{C}_i \cup \mathcal{D}_i)| = 24$。

证明　令 B 和 C 一起进行一个正交保持的局部测量 $\{E = M^\dagger M\}$，其中 $E = (a_{ij,k\ell})_{i,j,k,\ell\in\mathbb{Z}_3}$，那么测量后的态 $\{\mathbb{I}_A \otimes M|\psi\rangle : |\psi\rangle \in \cup_{i=1}^3(\mathcal{C}_i \cup \mathcal{D}_i)\}$ 是相互正交的。

首先我们需要证明 E 的对角元全为 0。观察图4.7可知，对于任意的 $(i,j) \neq (k,\ell) \in \mathbb{Z}_3 \times \mathbb{Z}_3$，总存在 $m \in \mathbb{Z}_3$，使得 $|m\rangle_A|i\rangle_B|j\rangle_C$ 和 $|m\rangle_A|k\rangle_B|\ell\rangle_C$ 分别出现在不同的 $|\psi_{n_1,n_1+1}\rangle$ 和 $|\psi_{n_2,n_2+1}\rangle$ 中，其中 n_1, n_2 都为奇数，且 $n_1 \neq n_2$。例如对于 $(0,0) \neq (1,1) \in \mathbb{Z}_3 \times \mathbb{Z}_3$，存在 $m = 2$，使得 $|2\rangle_A|0\rangle_B|0\rangle_C$ 出现在 $|\psi_{1,2}\rangle$ 中，$|2\rangle_A|1\rangle_B|1\rangle_C$ 出现在 $|\psi_{11,12}\rangle$ 中。下面对 $|\psi_{n_1,n_1+1}\rangle$ 和 $|\psi_{n_2,n_2+1}\rangle$ 运用引理4.11，我们得到 $a_{ij,k\ell} = 0$。从而 E 的对角元全为 0。

下面我们证明 E 的对角元都相等。观察图4.7，对 $|\psi_{1,2}\rangle$ 运用引理4.12，我们有 $a_{00,00} = a_{01,01}$；对 $|\psi_{5,6}\rangle$ 运用引理4.12，我们有 $a_{02,02} = a_{12,12}$；对 $|\psi_{21,22}\rangle$ 运用引理4.12，我们有 $a_{01,01} = a_{12,12}$；对 $|\psi_{23,24}\rangle$ 运用引理4.12，我们有 $a_{02,02} = a_{11,11}$，即 $a_{00,00} = a_{01,01} = a_{02,02} = a_{12,12} = a_{11,11}$。再根据图4.7的对称性，我们得到 E 的对角元都相等。

综上，$E \propto \mathbb{I}$，引理得证。 ∎

下面我们给出一般的结果。考虑3.4节 $d \times d \times d$ 立方体的分解，根据此分解，我们在 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ 中可以构造一组正交纠缠集：

$$
\begin{aligned}
\mathcal{C}_1 &:= \left\{ \mathcal{C}_{1,t} = \left\{ \sum_{j\in\mathbb{Z}_{d-1}} w_{d-1}^{jk} |j+1\rangle_A|0\rangle_B|j \oplus_{d-1} t\rangle_C \right\}_{k\in\mathbb{Z}_{d-1}} \right\}_{t\in\mathbb{Z}_{d-1}}, \\
\mathcal{C}_2 &:= \left\{ \mathcal{C}_{2,t} = \left\{ \sum_{j\in\mathbb{Z}_{d-1}} w_{d-1}^{jk} |j+1\rangle_A|j \oplus_{d-1} t\rangle_B|d-1\rangle_C \right\}_{k\in\mathbb{Z}_{d-1}} \right\}_{t\in\mathbb{Z}_{d-1}}, \\
\mathcal{C}_3 &:= \left\{ \mathcal{C}_{3,t} = \left\{ \sum_{j\in\mathbb{Z}_{d-1}} w_{d-1}^{jk} |d-1\rangle_A|j+1\rangle_B|j \oplus_{d-1} t\rangle_C \right\}_{k\in\mathbb{Z}_{d-1}} \right\}_{t\in\mathbb{Z}_{d-1}}, \\
\mathcal{D}_1 &:= \left\{ \mathcal{D}_{1,t} = \left\{ \sum_{j\in\mathbb{Z}_{d-1}} w_{d-1}^{jk} |j\rangle_A|d-1\rangle_B|(j \oplus_{d-1} t)+1\rangle_C \right\}_{k\in\mathbb{Z}_{d-1}} \right\}_{t\in\mathbb{Z}_{d-1}}, \\
\mathcal{D}_2 &:= \left\{ \mathcal{D}_{2,t} = \left\{ \sum_{j\in\mathbb{Z}_{d-1}} w_{d-1}^{jk} |j\rangle_A|(j \oplus_{d-1} t)+1\rangle_B|0\rangle_C \right\}_{k\in\mathbb{Z}_{d-1}} \right\}_{t\in\mathbb{Z}_{d-1}}, \\
\mathcal{D}_3 &:= \left\{ \mathcal{D}_{3,t} = \left\{ \sum_{j\in\mathbb{Z}_{d-1}} w_{d-1}^{jk} |0\rangle_A|j\rangle_B|(j \oplus_{d-1} t)+1\rangle_C \right\}_{k\in\mathbb{Z}_{d-1}} \right\}_{t\in\mathbb{Z}_{d-1}},
\end{aligned}
\tag{4.62}
$$

其中 $i \oplus_{d-1} j = i + j \mod (d-1)$。同样，对于任意的 $|\psi\rangle \in \cup_{i=1}^3(\mathcal{C}_i \cup \mathcal{D}_i)$，$|\psi_i\rangle$ 在集合 $\{A|BC, AB|C, AC|B\}$ 中两个两体划分下是纠缠态，在剩下一个两体划分

下是乘积态。公式(4.62)在两体划分 $A|BC$ 下对应于图4.8。

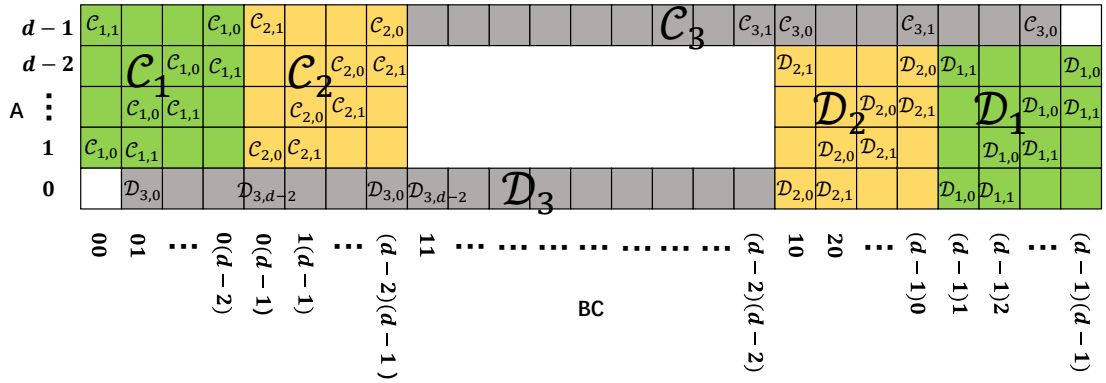

图 4.8　公式(4.62)在两体划分 $A|BC$ 下对应的 $d\times d^2$ 网格。

定理 4.14　在 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 中，$d\geqslant 3$，公式(4.62)给出的 $\cup_{i=1}^3(\mathcal{C}_i\cup\mathcal{D}_i)$ 是一个强非局域的正交纠缠集，且 $|\cup_{i=1}^3(\mathcal{C}_i\cup\mathcal{D}_i)|=6(d-1)^2$。

证明　由于 $\cup_{i=1}^3\{\mathcal{C}_i,\mathcal{D}_i\}$ 在子系统的循环置换下有相同的结构，我们只需要验证 B 和 C 进行的正交保持的局部测量是平凡的。令 B 和 C 一起进行一个正交保持的局部测量 $\{E=M^\dagger M\}$，其中 $E=(a_{ij,k\ell})_{i,j,k,\ell\in\mathbb{Z}_d}$，那么测量后的态 $\{\mathbb{I}_A\otimes M|\psi\rangle:|\psi\rangle\in\cup_{i=1}^3(\mathcal{C}_i\cup\mathcal{D}_i)\}$ 是相互正交的。

首先我们需要证明 E 的对角元全为 0。观察图4.8可知，对于任意的 $(i,j)\neq(k,\ell)\in\mathbb{Z}_d\times\mathbb{Z}_d$，有三种情况：

(i) (i,j) 和 (k,ℓ) 不同时属于 $\mathbb{Z}_d\backslash\{0,d-1\}\times\mathbb{Z}_d\backslash\{0,d-1\}$ 中。则一定存在 $m\in\mathbb{Z}_d$，使得 $|m\rangle_A|i\rangle_B|j\rangle_C$ 和 $|m\rangle_A|k\rangle_B|\ell\rangle_C$ 分别出现在 $\{\mathcal{C}_{s,t},\mathcal{D}_{s,t}\}_{1\leqslant s\leqslant 3;0\leqslant t\leqslant d-2}$ 的两个不同的集合中。例如 $(i,j)=(0,0),(k,\ell)=(d-2,d-2)$，则 $|d-1\rangle_A|0\rangle_B|0\rangle_C$ 和 $|d-1\rangle_A|d-2\rangle_B|d-2\rangle_C$ 分别出现在 $\mathcal{C}_{1,1}$ 和 $\mathcal{C}_{3,1}$ 中。那么对这两个集合运用引理4.11，我们有 $a_{ij,k\ell}=0$。

(ii) (i,j) 和 (k,ℓ) 同时属于 $\mathbb{Z}_d\setminus\{0,d-1\}\times\mathbb{Z}_d\setminus\{0,d-1\}$ 中，且 $|0\rangle_A|i\rangle_B|j\rangle_C$ 和 $|0\rangle_A|k\rangle_B|\ell\rangle_C$ 分别出现在 $\{\mathcal{D}_{3,t}\}_{0\leqslant t\leqslant d-2}$ 的两个不同的集合中。那么对这两个集合运用引理4.11，我们有 $a_{ij,k\ell}=0$。

(iii) (i,j) 和 (k,ℓ) 同时属于 $\mathbb{Z}_d\setminus\{0,d-1\}\times\mathbb{Z}_d\setminus\{0,d-1\}$ 中，且 $|0\rangle_A|i\rangle_B|j\rangle_C$ 和 $|0\rangle_A|k\rangle_B|\ell\rangle_C$ 出现在同一个 $\mathcal{D}_{3,t}$ 中，其中 $0\leqslant t\leqslant d-2$。考虑 $\mathcal{D}_{3,t}=\left\{\sum_{j\in\mathbb{Z}_{d-1}}w_{d-1}^{jk}|0\rangle_A|j\rangle_B|(j\oplus_{d-1}t)+1\rangle_C\right\}_{k\in\mathbb{Z}_{d-1}}$，由 (i) 可知，对于 $1\leqslant j\leqslant d-2$，$a_{0(t+1),j((j\oplus_{d-1}t)+1)}=0$。那么对 $\mathcal{D}_{3,t}$ 运用引理4.12，我们有 $a_{ij,k\ell}=0$。所以 E 的对角元全为 0。

下面我们证明 E 的对角元都相等。观察图4.8，对 $\mathcal{C}_{1,0}$，$\mathcal{C}_{2,0}$，$\mathcal{D}_{3,0}$ 分别运用引理4.12，我们有 $a_{00,00}=a_{01,01}=\cdots=a_{0(d-2),0(d-2)}=a_{0(d-1),0(d-1)}=a_{1(d-1),1(d-1)}=\cdots a_{(d-2)(d-1),(d-2)(d-1)}$。对于任意的 $(i,j)\in\mathbb{Z}_d\setminus\{0,d-1\}\times\mathbb{Z}_d\setminus\{0,d-1\}$，

$|0\rangle_A|i\rangle_B|j\rangle_C$ 出现在某个 $\mathcal{D}_{3,t}$ 中，其中 $0 \leqslant t \leqslant d-2$。对 $\mathcal{D}_{3,t}$ 运用引理4.12，我们有 $a_{ij,ij} = a_{0(t+1),0(t+1)}$。再根据图4.8的对称性，我们得到 $\boldsymbol{E}$ 的对角元都相等。

综上，$\boldsymbol{E} \propto \mathbb{I}$，定理得证。 ∎

4.5.2　N 体系统中强非局域的正交纠缠集

我们首先简要回顾一下群作用[125] 的概念和性质。如果 X 是一个集合并且 G 是一个群，如果存在函数 $G \times X \to X$，其中记 $(g,x) \rightarrowtail gx$，使得

(i) $(gh)x = g(hx)$，$g,h \in G$ 且 $x \in X$；

(ii) $1x = x$，$x \in X$，1 是 G 的单位元。

那么称 G 作用 在 X 上。对于 $x \in X$，令

$$\mathcal{O}_x := \{gx : g \in G\} \subseteq X,$$

则 $\mathcal{O}_x$ 被称为 x 的轨道，并且 x 被称为轨道 $\mathcal{O}_x$ 的一个代表元。如果 $y \in \mathcal{O}_x$，那么 $\mathcal{O}_x = \mathcal{O}_y$；如果 $y \notin \mathcal{O}_x$，那么 $\mathcal{O}_x \cap \mathcal{O}_y = \varnothing$。因此，$X$ 是互不相交的轨道的并集，

$$X = \bigcup_x \mathcal{O}_x,$$

其中 x 跑遍所有轨道的代表元。此外，$|\mathcal{O}_x|$ 整除 $|G|$。

在我们的构造中，我们考虑的集合是 $\mathbb{Z}_d^N$ 的子集 $\mathbb{X}_d^N$，其定义为

$$\mathbb{X}_d^N := \left\{ (i_1, i_2, \cdots, i_N) : \prod_{1\leqslant k\leqslant N} i_k = 0 \right\}.$$

也就是说，对于任何 $(i_1,i_2,\cdots,i_N) \in \mathbb{X}_d^N$，至少存在一个 $i_k = 0$，其中 $1 \leqslant k \leqslant N$，那么 $|\mathbb{X}_d^N| = d^N - (d-1)^N$。

假设

$$G_N = \{\sigma^k : k \in \mathbb{Z}_N\}$$

是阶数为 N 的循环置换群，其中对于 N-元组 $(i_1,i_2,\cdots,i_N) \in \mathbb{Z}_d^N$，我们有

$$\sigma(i_1,i_2,\cdots,i_N) = (i_2,\cdots,i_N,i_1).$$

根据定义可知 G_N 作用于 $\mathbb{X}_d^N$，那么 $\mathbb{X}_d^N$ 可以划分为不相交的轨道的并集。

例如，由于 G_3 作用在 $\mathbb{X}_2^3 = \mathbb{Z}_2^3 \setminus \{(1,1,1)\}$ 上，我们得到

$$\mathbb{X}_2^3 = \mathcal{O}_{(0,0,0)} \cup \mathcal{O}_{(0,0,1)} \cup \mathcal{O}_{(0,1,1)}, \tag{4.63}$$

其中

$$\mathcal{O}_{(0,0,0)} = \{(0,0,0)\},$$
$$\mathcal{O}_{(0,0,1)} = \{(0,0,1),(0,1,0),(1,0,0)\},$$
$$\mathcal{O}_{(0,1,1)} = \{(0,1,1),(1,1,0),(1,0,1)\}.$$

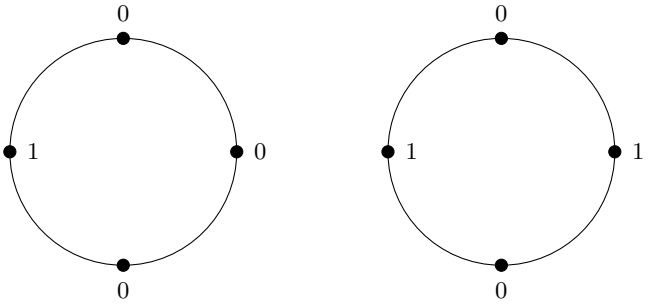

图 4.9　两个圈表示两个轨道。对于左边的圈，轨道为 $\mathcal{O}_{(0,0,0,1)} = \{(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0)\}$**，产生的态集为** $\mathcal{S}_{(0,0,0,1)} = \{|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|1\rangle_{A_4} + w_4^s|0\rangle_{A_1}|0\rangle_{A_2}|1\rangle_{A_3}|0\rangle_{A_4} + w_4^{2s}|0\rangle_{A_1}|1\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} + w_4^{3s}|1\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} : s \in \mathbb{Z}_4\}$。**对于右边的圈，轨道为** $\mathcal{O}_{(0,1,0,1)} = \{(0,1,0,1),(1,0,1,0)\}$**，产生的态集为** $\mathcal{S}_{(0,1,0,1)} = \{|0\rangle_{A_1}|1\rangle_{A_2}|0\rangle_{A_3}|1\rangle_{A_4} \pm |1\rangle_{A_1}|0\rangle_{A_2}|1\rangle_{A_3}|0\rangle_{A_4}\}$。

一般来说如果 $x \neq (0,0\cdots,0)$，那么我们记

$$\mathcal{O}_x = \{(i_1^{(j)}, i_2^{(j)}, \cdots, i_N^{(j)}) : j \in \mathbb{Z}_k\},$$

其中 $|\mathcal{O}_x| = k \geqslant 2$。注意不同轨道大小可能不同，以图4.9为例。

接下来，对于 $\mathbb{X}_d^N$ 的每个轨道 $\mathcal{O}_x$，我们在 $(\mathbb{C}^d)^{\otimes N}$ 中定义一组态 $\mathcal{S}_x$。如果 $x \neq (0,0\cdots,0)$，令

$$\mathcal{S}_x := \left\{ \sum_{j\in\mathbb{Z}_k} w_k^{sj} |i_1^{(j)}\rangle_{A_1} |i_2^{(j)}\rangle_{A_2} \cdots |i_N^{(j)}\rangle_{A_N} : s \in \mathbb{Z}_k \right\},$$

实际上系数矩阵

$$B = (w_k^{sj})_{s,j\in\mathbb{Z}_k} \tag{4.64}$$

是 k 阶复 Hadamard 矩阵。根据定义可知，$|\mathcal{S}_x| = |\mathcal{O}_x|$。图4.9中表明的是 $\mathcal{S}_{(0,0,0,1)}$ 和 $\mathcal{S}_{(0,1,0,1)}$。如果 $\mathcal{O}_x = \{(0,0,\cdots,0)\}$，那么我们定义

$$\mathcal{S}_{(0,0,\cdots,0)} := \{|0\rangle_{A_1}|0\rangle_{A_1}\cdots|0\rangle_{A_N} \pm |1\rangle_{A_1}|1\rangle_{A_1}\cdots|1\rangle_{A_N}\},$$

它比原轨道多一个元素。由于 $\mathbb{X}_d^N = \bigcup\limits_x \mathcal{O}_x$ 是不相交的并集，我们得到

$$\mathcal{B}_d^N := \bigcup_x \mathcal{S}_x \tag{4.65}$$

也是不相交的并集，其中 $|\mathcal{B}_d^N| = d^N - (d-1)^N + 1$。

例如在 $(\mathbb{C}^2)^{\otimes 3}$ 中，由公式(4.63)可知

$$\mathcal{B}_2^3 = \mathcal{S}_{(0,0,0)} \cup \mathcal{S}_{(0,0,1)} \cup \mathcal{S}_{(0,1,1)}, \tag{4.66}$$

其中

$$\begin{aligned}
\mathcal{S}_{(0,0,0)} &= \{|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3} \pm |1\rangle_{A_1}|1\rangle_{A_2}|1\rangle_{A_3}\},\\
\mathcal{S}_{(0,0,1)} &= \{|0\rangle_{A_1}|0\rangle_{A_2}|1\rangle_{A_3} + w_3^s|0\rangle_{A_1}|1\rangle_{A_2}|0\rangle_{A_3}\\
&\quad + w_3^{2s}|1\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3} : s \in \mathbb{Z}_3\},\\
\mathcal{S}_{(0,1,1)} &= \{|0\rangle_{A_1}|1\rangle_{A_2}|1\rangle_{A_3} + w_3^s|1\rangle_{A_1}|1\rangle_{A_2}|0\rangle_{A_3}\\
&\quad + w_3^{2s}|1\rangle_{A_1}|0\rangle_{A_2}|1\rangle_{A_3} : s \in \mathbb{Z}_3\},
\end{aligned}$$

且 $|\mathcal{B}_2^3| = 8$。我们可以很容易地看出 $\mathcal{B}_2^3$ 是 $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中的正交纠缠集。更一般地，我们有以下结果：

引理 4.15　在 $(\mathbb{C}^d)^{\otimes N}$ 中，$\mathcal{B}_d^N$ 是一个正交纠缠集，且 $|\mathcal{B}_d^N| = d^N - (d-1)^N + 1$。

证明　我们已经证明了 $|\mathcal{B}_d^N| = d^N - (d-1)^N + 1$，接下来，我们证明 $\mathcal{B}_d^N$ 是一个正交纠缠集。显然，$\mathcal{S}_{(0,0,\cdots,0)}$ 是一个正交纠缠集。我们只需要考虑 $\mathcal{S}_x$，其中 $x \neq (0,0\cdots,0) \in \mathbb{X}_d^N$。假设 $\mathcal{O}_x = \{(i_1^{(j)}, i_2^{(j)}, \cdots, i_N^{(j)}) : j \in \mathbb{Z}_k\}$，$k \geqslant 2$，由于 $\mathcal{O}_x = \{(i_1^{(j)}, i_2^{(j)}, \cdots, i_N^{(j)}) : j \in \mathbb{Z}_k\}$ 中任意两个元素是不同的，我们得到 $\{|i_1^{(j)}\rangle_{A_1}|i_2^{(j)}\rangle_{A_2}\cdots|i_N^{(j)}\rangle_{A_N} : j \in \mathbb{Z}_k\}$ 是相互正交的。由于系数矩阵 $\boldsymbol{B} = (w_k^{sj})_{s,j\in\mathbb{Z}_k}$ 是 k 阶复 Hadamard 矩阵，我们得到 $\mathcal{S}_x$ 中的态是相互正交的。接下来，我们需要证明 $\mathcal{S}_x$ 中的任何态都是纠缠态。

不失一般性，我们假设 $x = (i_1^{(0)}, i_2^{(0)}, \cdots, i_N^{(0)})$，根据定义，$\mathcal{O}_x = \{\sigma^r x : r \in \mathbb{Z}_N\}$。我们有以下两个断言：

(i) 我们断言 $(N-1)$-元组 $\{(i_2^{(j)}, \cdots, i_N^{(j)}) : j \in \mathbb{Z}_k\}$ 中的元素是互不相同的。对于某些 $j \neq j' \in \mathbb{Z}_k$，如果有 $(i_2^{(j)}, \cdots, i_N^{(j)}) = (i_2^{(j')}, \cdots, i_N^{(j')})$，那么 $i_1^{(j)} = i_1^{(j')}$。否则，如果 $i_1^{(j)} \neq i_1^{(j')}$，那么 $(i_1^{(j)}, i_2^{(j)}, \cdots, i_N^{(j)}) \notin \mathcal{O}_x$ 或 $(i_1^{(j')}, i_2^{(j')}, \cdots, i_N^{(j')}) \notin \mathcal{O}_x$。我们得到 $(i_1^{(j)}, i_2^{(j)}, \cdots, i_N^{(j)}) = (i_1^{(j')}, i_2^{(j')}, \cdots, i_N^{(j')})$，而这是不可能的，由此我们获得了这一断言。

(ii) 我们还断言必须存在 $j \neq j' \in \mathbb{Z}_k$，使得 $i_1^{(j)} = 0$ 和 $i_1^{(j')} \neq 0$。由于 $x \neq (0,0\cdots,0) \in \mathbb{X}_d^N$，这里必然存在 $1 \leqslant t \neq t' \leqslant N$，使得 $i_t^{(0)} = 0$ 和 $i_{t'}^{(0)} \neq 0$。进一步地，必然存在 $j \neq j' \in \mathbb{Z}_k$，使得 $(i_1^{(j)}, i_2^{(j)}, \cdots, i_N^{(j)}) = \sigma^{(t-1)}x$，和 $(i_1^{(j')}, i_2^{(j')}, \cdots, i_N^{(j')}) = \sigma^{(t'-1)}x$。那么 $i_1^{(j)} = i_t^{(0)} = 0$ 和 $i_1^{(j')} = i_{t'}^{(0)} \neq 0$，由此我们获得了这一断言。

对于任何 $s \in \mathbb{Z}_k$，令

$$|\psi_s\rangle = \sum_{j\in\mathbb{Z}_k} w_k^{sj}|i_1^{(j)}\rangle_{A_1}|i_2^{(j)}\rangle_{A_2}\cdots|i_N^{(j)}\rangle_{A_N} \in \mathcal{S}_x.$$

通过以上两个断言可知 $\mathrm{rank}(|\psi_s\rangle_{A_1|A_2\cdots A_N}) \geqslant 2$。因此，集合 $\mathcal{S}_x$ 是一个正交纠缠集。此外，如果 $\mathcal{O}_x \cap \mathcal{O}_y = \varnothing$，那么 $\mathcal{S}_x$ 中的任何态都与 $\mathcal{S}_y$ 中的任何态正交。引理得证。 ∎

下面，我们将证明公式(4.65)给出的 $\mathcal{B}_d^N$ 具有强量子非局域性。由于 $\mathcal{B}_d^N$ 在子系统的循环置换下有相同的结构，我们只需要验证 $A_2A_3\cdots A_N$ 进行的正交保持的局部测量是平凡的。我们从一个例子出发。

例 4.2　在 $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ 中，公式(4.66)给出的 $\mathcal{B}_2^3$ 是一个强非局域的正交纠缠集，且 $|\mathcal{B}_2^3|=8$。

证明　令 A_2 和 A_3 一起进行一个正交保持的局部测量 $\{E=M^\dagger M\}$，其中 $E=(a_{ij,k\ell})_{i,j,k,\ell\in\mathbb{Z}_2}$，那么测量后的态 $\{\mathbb{I}_{A_1}\otimes M|\psi\rangle:|\psi\rangle\in\mathcal{B}_2^3\}$ 是相互正交的。

对 $S_{(0,0,0)}$ 和 $S_{(0,0,1)}$ 运用引理4.11，我们有 $a_{00,01}=a_{00,10}=a_{00,11}=0$。接下来，对 $S_{(0,0,0)}$ 和 $S_{(0,1,1)}$ 运用引理4.11，我们得到 $a_{10,11}=a_{01,11}=0$。由于 $a_{00,01}=a_{00,10}=0$，我们对 $S_{(0,0,1)}$ 运用引理4.12，得到 $a_{01,10}=0$ 和 $a_{01,01}=a_{10,10}=a_{00,00}$。最后，对 $S_{(0,0,0)}$ 运用引理4.12，我们有 $a_{00,00}=a_{11,11}$。因此 $E\propto\mathbb{I}$，这就完成了证明。∎

下面我们给出一般性的结果。

定理 4.16　在 $(\mathbb{C}^d)^{\otimes N}$ 中，$d\geqslant 2$，$N\geqslant 3$，公式(4.65)给出的 $\mathcal{B}_d^N$ 是一个强非局域的正交纠缠集，且 $|\mathcal{B}_d^N|=d^N-(d-1)^N+1$。

证明　令 $A_2,A_3,\cdots,A_N$ 一起进行一个正交保持的局部测量 $\{E=M^\dagger M\}$，其中 $E=(a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}})_{i_k,j_k\in\mathbb{Z}_d,1\leqslant k\leqslant N-1}$，那么测量后的态 $\{\mathbb{I}_{A_1}\otimes M|\psi\rangle:|\psi\rangle\in\mathcal{B}_d^N\}$ 是相互正交的。

对于 $(i_1,i_2,\cdots,i_{N-1})\in\mathbb{Z}_d^{N-1}$，我们记 $wt(i_1,i_2,\cdots,i_{N-1})$ 为非零 i_k 的数量，其中 $1\leqslant k\leqslant N-1$。我们定义 $\mathbb{Z}_d^{N-1}$ 的 N 个子集，

$$\mathcal{A}_k:=\{(i_1,i_2,\cdots,i_{N-1})\in\mathbb{Z}_d^{N-1}:wt(i_1,i_2,\cdots,i_{N-1})=k\},\ k\in\mathbb{Z}_N.$$

注意 $\mathcal{A}_k\cap\mathcal{A}_\ell=\varnothing,k\neq\ell\in\mathbb{Z}_N$，且 $\mathbb{Z}_d^{N-1}=\bigcup\limits_{k\in\mathbb{Z}_N}\mathcal{A}_k$。首先，我们需要证明 E 的非对角元都是零，即 $a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}}=0,(i_1,i_2,\cdots,i_{N-1})\neq(j_1,j_2,\cdots,j_{N-1})\in\mathbb{Z}_d^{N-1}$。有两种情况：

(i) 假设 $(i_1,i_2,\cdots,i_{N-1})\in\mathcal{A}_k$，$(j_1,j_2,\cdots,j_{N-1})\in\mathcal{A}_\ell$，$k\neq\ell\in\mathbb{Z}_N$，那么我们必然有 $\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}\cap\mathcal{O}_{(0,j_1,j_2,\cdots,j_{N-1})}=\varnothing$ 和 $\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}\cap\mathcal{O}_{(0,j_1,j_2,\cdots,j_{N-1})}=\varnothing$。对 $S_{(0,i_1,i_2,\cdots,i_{N-1})}$ 和 $S_{(0,i_1,i_2,\cdots,i_{N-1})}$ 运用引理4.11，我们得到 $a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}}=0$。

(ii) 假设 $(i_1,i_2,\cdots,i_{N-1}),(j_1,j_2,\cdots,j_{N-1})\in\mathcal{A}_k$，$k\neq 0\in\mathbb{Z}_N$。

(1) 首先我们考虑 $k=1$ 的情况，那么必然存在 $i_\ell\neq 0$ 和 $i_m=0$，其中 $1\leqslant m\neq\ell\leqslant N-1$。如果 $\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}\cap\mathcal{O}_{(0,j_1,j_2,\cdots,j_{N-1})}=\varnothing$，那么像 (i) 一样讨论，我们也可以得到 $a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}}=0$。如果 $\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}=\mathcal{O}_{(0,j_1,j_2,\cdots,j_{N-1})}$，那么 $\sigma^\ell(0,i_1,i_2,\cdots,i_{N-1})=$

$(i_\ell,0,0,\cdots,0)\in\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}$，其中 $(0,0,\cdots,0)\in\mathcal{A}_0$。对于任何 $(n_0,n_1,\cdots,n_{N-1})\in\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}$，我们有 $(n_1,\cdots,n_{N-1})\in\mathcal{A}_0$ 或 $\mathcal{A}_1$。对于 $(i'_1,i'_2,\cdots,i'_{N-1})\neq(j'_1,j'_2,\cdots,j'_{N-1})\in\mathbb{Z}_d^{N-1}$，$(i'_1,i'_2,\cdots,i'_{N-1})\in\mathcal{A}_0$，$(j'_1,j'_2,\cdots,j'_{N-1})\in\mathcal{A}_1$，我们已经证明 $a_{i'_1i'_2\cdots i'_{N-1},j'_1j'_2\cdots j'_{N-1}}=0$。对于 $(n_0,n_1,\cdots,n_{N-1})\neq(i_\ell,0,\cdots,0)\in\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}$，这意味着 $a_{00\cdots0,n_1n_2\cdots n_{N-1}}=0$。然后对 $\mathcal{S}_{(0,i_1,i_2,\cdots,i_{N-1})}$ 运用引理4.12，我们得到 $a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}}=0$，其中 $(i_1,i_2,\cdots,i_{N-1})$，$(j_1,j_2,\cdots,j_{N-1})\in\mathcal{A}_1$。

(2) 下面我们考虑 $k=2$ 的情况，那么必须存在一个 $i_\ell\neq0$，其中 $1\leqslant\ell\leqslant N-1$。我们只需要考虑 $\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}=\mathcal{O}_{(0,j_1,j_2,\cdots,j_{N-1})}$ 的情况。记 $i_0=0$，那么 $\sigma^\ell(0,i_1,i_2,\cdots,i_{N-1})=(i_\ell,i_{\ell+1},i_{\ell+2},\cdots,i_{\ell-1})\in\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}$，其中 $(i_{\ell+1},i_{\ell+2},\cdots,i_{\ell-1})\in\mathcal{A}_1$。对于任何 $(n_0,n_1,\cdots,n_{N-1})\in\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}$，我们一定有 $(n_1,\cdots,n_{N-1})\in\mathcal{A}_1$ 或 $\mathcal{A}_2$。对于 $(i'_1,i'_2,\cdots,i'_{N-1})\neq(j'_1,j'_2,\cdots,j'_{N-1})\in\mathbb{Z}_d^{N-1}$，$(i'_1,i'_2,\cdots,i'_{N-1})\in\mathcal{A}_1$，$(j'_1,j'_2,\cdots,j'_{N-1})\in\mathcal{A}_2$，我们已经证明 $a_{i'_1i'_2\cdots i'_{N-1},j'_1j'_2\cdots j'_{N-1}}=0$，且对于 $(i'_1,i'_2,\cdots,i'_{N-1})$，$(j'_1,j'_2,\cdots,j'_{N-1})\in\mathcal{A}_1$，有 $a_{i'_1i'_2\cdots i'_{N-1},j'_1j'_2\cdots j'_{N-1}}=0$。对于任何 $(n_0,n_1,\cdots,n_{N-1})\neq(i_\ell,i_{\ell+1},\cdots,i_{\ell-1})\in\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}$，这意味着 $a_{i_{\ell+1},i_{\ell+2}\cdots,i_{\ell-1},n_1n_2\cdots n_{N-1}}=0$。对 $\mathcal{S}_{(0,i_1,i_2,\cdots,i_{N-1})}$ 运用引理4.12，我们得到 $a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}}=0$，其中 $(i_1,i_2,\cdots,i_{N-1})$，$(j_1,j_2,\cdots,j_{N-1})\in\mathcal{A}_2$。

(3) 通过重复这个过程 $N-2$ 次，我们得到 $a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}}=0$，其中 $(i_1,i_2,\cdots,i_{N-1})$，$(j_1,j_2,\cdots,j_{N-1})\in\mathcal{A}_k$，$1\leqslant k\leqslant N-2$。

(4) 最后，我们考虑 $k=N-1$ 的情况。如果 $(i_1,i_2,\cdots,i_{N-1})\neq(j_1,j_2,\cdots,j_{N-1})\in\mathcal{A}_{N-1}$，那么 $\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}\cap\mathcal{O}_{(0,j_1,j_2,\cdots,j_{N-1})}=\varnothing$。像 (i) 一样讨论，我们得到 $a_{i_1i_2\cdots i_{N-1},j_1j_2\cdots j_{N-1}}=0$，其中 $(i_1,i_2,\cdots,i_{N-1})$，$(j_1,j_2,\cdots,j_{N-1})\in\mathcal{A}_{N-1}$。

综上，$\boldsymbol{E}$ 的非对角元都是零。接下来，我们考虑 $\boldsymbol{E}$ 的对角元。

对于任何 $(i_1,i_2,\cdots,i_{N-1})\in\mathcal{A}_k$，$k\neq0\in\mathbb{Z}_N$，必然存在一个 $(n_{(0,k-1)},n_{(1,k-1)},\cdots,n_{(N-1,k-1)})\in\mathcal{O}_{(0,i_1,i_2,\cdots,i_{N-1})}$ 使得 $(n_{(1,k-1)},\cdots,n_{(N-1,k-1)})\in\mathcal{A}_{k-1}$。对 $\mathcal{S}_{(0,i_1,i_2,\cdots,i_{N-1})}$ 运用引理4.12，我们得到 $a_{i_1i_2\cdots i_{N-1},i_1i_2\cdots i_{N-1}}=a_{n_{(1,k-1)}n_{(2,k-1)}\cdots n_{(N-1,k-1)},n_{(1,k-1)}n_{(2,k-1)}\cdots n_{(N-1,k-1)}}$。接下来，必然存在一个 $(n_{(0,k-2)},n_{(1,k-2)},\cdots,n_{(N-1,k-2)})\in\mathcal{O}_{(0,n_{(1,k-1)},\cdots,n_{(N-1,k-1)})}$ 使得 $(n_{(1,k-2)},\cdots,n_{(N-1,k-2)})\in\mathcal{A}_{k-2}$。对 $\mathcal{S}_{(0,n_{(1,k-1)},\cdots,n_{(N-1,k-1)})}$ 运用引理4.12，我们得到 $a_{n_{(1,k-1)}n_{(2,k-1)}\cdots n_{(N-1,k-1)},n_{(1,k-1)}n_{(2,k-1)}\cdots n_{(N-1,k-1)}}=a_{n_{(1,k-2)}n_{(2,k-2)}\cdots n_{(N-1,k-2)},n_{(1,k-2)}n_{(2,k-2)}\cdots n_{(N-1,k-2)}}$。通过重复这个过程 k 次，我们得到 $a_{i_1i_2\cdots i_{N-1},i_1i_2\cdots i_{N-1}}=a_{n_{(1,0)}n_{(2,0)}\cdots n_{(N-1,0)},n_{(1,0)}n_{(2,0)}\cdots n_{(N-1,0)}}$，其中 $(n_{(1,0)},n_{(2,0)},\cdots,n_{(N-1,0)})\in\mathcal{A}_0$。即 $a_{i_1i_2\cdots i_{N-1},i_1i_2\cdots i_{N-1}}=a_{00\cdots0,00\cdots0}$。由此可

知 E 的对角元都是相等的。所以 $E \propto \mathbb{I}$，这样就完成了证明。 ∎

下面我们考虑三体和四体系统中强非局域的正交真实纠缠集。由引理4.15的证明可知，对于任意 $|\psi\rangle \in \mathcal{B}_d^N$，$|\psi\rangle$ 在两体划分 $A_1|A_2A_3\cdots A_N$ 下是纠缠态。由于 $\mathcal{B}_d^N$ 在子系统 $\{A_1, A_2, \cdots, A_N\}$ 的循环置换下具有相同的结构，对于任何 $1 \leqslant i \leqslant N$，我们得到 $|\psi\rangle$ 在两体划分 $A_i|\{A_1A_2\cdots A_N\}\setminus\{A_i\}$ 下是纠缠态。因此当 $N = 3$ 时，$\mathcal{B}_d^3$ 为正交真实纠缠集。那我们有以下结果。

引理 4.17　在 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ 中，$d \geqslant 2$，公式(4.65)给出的 $\mathcal{B}_d^3$ 是一个强非局域的正交真实纠缠集，且 $|\mathcal{B}_d^3| = d^3 - (d-1)^3 + 1$。

对于 $\mathcal{B}_d^N$，我们自然而然地会想到将引理4.17推广至所有的 $N \geqslant 4$。然而，当 $N = 4$ 时，$\mathcal{B}_d^4$ 不再是正交真实纠缠集。记 $[d-1] := \{1, 2, \cdots, d-1\}$，对于任何 $i \in [d-1]$，实际上

$$\begin{aligned}|\psi_i\rangle =& |0\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|i\rangle_{A_4} + |0\rangle_{A_1}|i\rangle_{A_2}|i\rangle_{A_3}|0\rangle_{A_4} \\ &+ |i\rangle_{A_1}|i\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} + |i\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4} \in \mathcal{S}_{(0,0,i,i)} \subset \mathcal{B}_d^4\end{aligned}$$

在两体划分 $A_1A_3|A_2A_4$ 下是乘积态，这是因为它可以被写成

$$|\psi_i\rangle = (|0\rangle|i\rangle + |i\rangle|0\rangle)_{A_1A_3}(|0\rangle|i\rangle + |i\rangle|0\rangle)_{A_2A_4}.$$

从而 $\mathcal{B}_d^4$ 不再是正交真实纠缠集。但是我们可以修改公式(4.64)中的系数矩阵 B，从而得到正交真实纠缠集。令

$$\widetilde{B} = (b_{i,j})_{i,j\in\mathbb{Z}_4} := \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & -1 & 2 & -1 \\ 5 & 5 & -2 & -4 \\ 5 & -5 & -4 & 2 \end{pmatrix},$$

显然，$\widetilde{B}$ 是一个行正交矩阵。对于任何 $i \in [d-1]$，定义

$$\begin{aligned}\overline{\mathcal{S}_{(0,0,i,i)}} :=& \{b_{s,0}|0\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|i\rangle_{A_4} + b_{s,1}|0\rangle_{A_1}|i\rangle_{A_2}|i\rangle_{A_3}|0\rangle_{A_4} + b_{s,2}|i\rangle_{A_1} \\ &|i\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} + b_{s,3}|i\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4} : s \in \mathbb{Z}_4\}.\end{aligned}$$

对于任何 $i \in [d-1]$，我们将 $\mathcal{B}_d^4$ 中的 $\mathcal{S}_{(0,0,i,i)}$ 替换成 $\overline{\mathcal{S}_{(0,0,i,i)}}$，其余态不变，则 $\mathcal{B}_d^4$ 变为 $\overline{\mathcal{B}_d^4}$。因此我们有以下结论。

引理 4.18　在 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ 中，$d \geqslant 2$，$\overline{\mathcal{B}_d^4}$ 是一个强非局域的正交真实纠缠集，且 $|\overline{\mathcal{B}_d^4}| = d^4 - (d-1)^4 + 1$。

证明　根据 $\overline{\mathcal{B}_d^4}$ 的定义可知，

$$\begin{aligned}\overline{\mathcal{B}_d^4} =& \mathcal{S}_{(0,0,0,0)} \bigcup \left(\bigcup_{i\in[d-1]} (\mathcal{S}_{(0,0,0,i)} \cup \overline{\mathcal{S}_{(0,0,i,i)}} \cup \mathcal{S}_{(0,i,0,i)}) \right) \\ & \bigcup \left(\bigcup_{i\neq j\in[d-1]} \mathcal{S}_{(0,0,i,j)} \right) \bigcup \left(\bigcup_{p<q\in[d-1]} \mathcal{S}_{(0,p,0,q)} \right) \bigcup \left(\bigcup_{k,\ell,m\in[d-1]} \mathcal{S}_{(0,k,\ell,m)} \right),\end{aligned}$$

其中对于 $i \neq j \in [d-1]$，$p < q \in [d-1]$ 和 $k, \ell, m \in [d-1]$，有

$$\begin{aligned}
\mathcal{S}_{(0,0,0,0)} =& \{|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} \pm |1\rangle_{A_1}|1\rangle_{A_2}|1\rangle_{A_3}|1\rangle_{A_4}\},\\
\mathcal{S}_{(0,0,0,i)} =& \{|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4} + w_4^s|0\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|0\rangle_{A_4} + w_4^{2s}|0\rangle_{A_1}\\
&|i\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} + w_4^{3s}|i\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} : s \in \mathbb{Z}_4\},\\
\overline{\mathcal{S}_{(0,0,i,i)}} =& \{b_{s,0}|0\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|i\rangle_{A_4} + b_{s,1}|0\rangle_{A_1}|i\rangle_{A_2}|i\rangle_{A_3}|0\rangle_{A_4} + b_{s,2}|i\rangle_{A_1}\\
&|i\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} + b_{s,3}|i\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4} : s \in \mathbb{Z}_4\},\\
\mathcal{S}_{(0,i,0,i)} =& \{|0\rangle_{A_1}|i\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4} \pm |i\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|0\rangle_{A_4}\},\\
\mathcal{S}_{(0,0,i,j)} =& \{|0\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|j\rangle_{A_4} + w_4^s|0\rangle_{A_1}|i\rangle_{A_2}|j\rangle_{A_3}|0\rangle_{A_4} + w_4^{2s}|i\rangle_{A_1}\\
&|j\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4} + w_4^{3s}|j\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4} : s \in \mathbb{Z}_4\},\\
\mathcal{S}_{(0,p,0,q)} =& \{|0\rangle_{A_1}|p\rangle_{A_2}|0\rangle_{A_3}|q\rangle_{A_4} + w_4^s|p\rangle_{A_1}|0\rangle_{A_2}|q\rangle_{A_3}|0\rangle_{A_4} + w_4^{2s}|0\rangle_{A_1}\\
&|q\rangle_{A_2}|0\rangle_{A_3}|p\rangle_{A_4} + w_4^{3s}|q\rangle_{A_1}|0\rangle_{A_2}|p\rangle_{A_3}|0\rangle_{A_4} : s \in \mathbb{Z}_4\},\\
\mathcal{S}_{(0,k,\ell,m)} =& \{|0\rangle_{A_1}|k\rangle_{A_2}|\ell\rangle_{A_3}|m\rangle_{A_4} + w_4^s|k\rangle_{A_1}|\ell\rangle_{A_2}|m\rangle_{A_3}|0\rangle_{A_4} + w_4^{2s}|\ell\rangle_{A_1}\\
&|m\rangle_{A_2}|0\rangle_{A_3}|k\rangle_{A_4} + w_4^{3s}|m\rangle_{A_1}|0\rangle_{A_2}|k\rangle_{A_3}|\ell\rangle_{A_4} : s \in \mathbb{Z}_4\}.
\end{aligned}$$

由于 $|\mathcal{B}_d^4| = d^4 - (d-1)^4 + 1$，并且 $|\overline{\mathcal{S}_{(0,0,i,i)}}| = |\mathcal{S}_{(0,0,i,i)}|$，对于 $i \in [d-1]$，我们有 $|\overline{\mathcal{B}_d^4}| = |\mathcal{B}_d^4| = d^4 - (d-1)^4 + 1$。根据定理4.16，我们知道 $\mathcal{B}_d^4$ 是强非局域的。由于 $\overline{\mathcal{B}_d^4}$ 与 $\mathcal{B}_d^4$ 具有相似的结构，我们推出 $\overline{\mathcal{B}_d^4}$ 也是强非局域的。我们只需要证明 $\overline{\mathcal{B}_d^4}$ 是一个正交真实纠缠集。首先我们给出一个断言。

断言: 对于 $|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}$，如果存在乘积算子 $P_1 \otimes P_2 \otimes \cdots \otimes P_N$ 使得

$$P_1 \otimes P_2 \otimes \cdots \otimes P_N|\psi\rangle$$

是一个真实纠缠态，那么 $|\psi\rangle$ 也是一个真实纠缠态。

上述断言的证明如下。如果 $|\psi\rangle$ 不是真实纠缠态，那么存在两体划分 $A|B$，使得 $|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$。对于任何乘积算子 $P_1 \otimes P_2 \otimes \cdots \otimes P_N$，

$$P_1 \otimes P_2 \otimes \cdots \otimes P_N(|\psi\rangle_A \otimes |\psi\rangle_B)$$

在两体划分 $A|B$ 下是乘积态，那么它不是真实纠缠态，矛盾，从而断言得证。

对于任何 $s \in \mathbb{Z}_4$，$i \neq j \in [d-1]$，令

$$\begin{aligned}
|\psi_s\rangle =& |0\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|j\rangle_{A_4} + w_4^s|0\rangle_{A_1}|i\rangle_{A_2}|j\rangle_{A_3}|0\rangle_{A_4} + w_4^{2s}|i\rangle_{A_1}|j\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4}\\
&+ w_4^{3s}|j\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4} \in \mathcal{S}_{(0,0,i,j)},
\end{aligned}$$

和

$$\begin{aligned}
P =& (|0\rangle\langle 0| + |0\rangle\langle j| + w_4^{-2s}|1\rangle\langle i|)_{A_1}(|0\rangle\langle 0| + |0\rangle\langle j| + w_4^{-s}|1\rangle\langle i|)_{A_2}\\
&(|0\rangle\langle 0| + |0\rangle\langle j| + |1\rangle\langle i|)_{A_3}(|0\rangle\langle 0| + |0\rangle\langle j| + w_4^{-3s}|1\rangle\langle i|)_{A_4}.
\end{aligned}$$

那么

$$\begin{aligned}P|\psi_s\rangle =&|0\rangle_{A_1}|0\rangle_{A_2}|1\rangle_{A_3}|0\rangle_{A_4}+|0\rangle_{A_1}|1\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4}\\&+|1\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4}+|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|1\rangle_{A_4}=|W\rangle_2^4.\end{aligned}$$

由于 W 态是真实纠缠态，根据上面的断言，我们得到 $|\psi_s\rangle$ 也是一个真实纠缠态。从而 $\mathcal{S}_{(0,0,i,j)}$ 是一个正交真实纠缠集。同理，其中对于 $i\in[d-1]$，$p<q\in[d-1]$ 和 $k,\ell,m\in[d-1]$，我们按照同样的方法可以证明 $\mathcal{S}_{(0,0,0,0)}$，$\mathcal{S}_{(0,0,0,i)}$，$\mathcal{S}_{(0,i,0,i)}$，$\mathcal{S}_{(0,p,0,q)}$，$\mathcal{S}_{(0,k,\ell,m)}$ 都是正交真实纠缠集。

最后，我们考虑 $\overline{\mathcal{S}_{(0,0,i,i)}}$。对于 $s\in\mathbb{Z}_4$ 和 $i\in[d-1]$，令

$$\begin{aligned}|\lambda_s\rangle =&b_{s,0}|0\rangle_{A_1}|0\rangle_{A_2}|i\rangle_{A_3}|i\rangle_{A_4}+b_{s,1}|0\rangle_{A_1}|i\rangle_{A_2}|i\rangle_{A_3}|0\rangle_{A_4}\\&+b_{s,2}|i\rangle_{A_1}|i\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4}+b_{s,3}|i\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{A_3}|i\rangle_{A_4}\in\overline{\mathcal{S}_{(0,0,i,i)}}.\end{aligned}$$

通过计算,我们有 $\mathrm{rank}(|\lambda_s\rangle_{A_1|A_2A_3A_4})=\mathrm{rank}(|\lambda_s\rangle_{A_2|A_3A_4A_1})=\mathrm{rank}(|\lambda_s\rangle_{A_3|A_4A_1A_2})=\mathrm{rank}(|\lambda_s\rangle_{A_4|A_1A_2A_3})=\mathrm{rank}(|\lambda_s\rangle_{A_1A_3|A_2A_4})=2$ 和 $\mathrm{rank}(|\lambda\rangle_{A_1A_2|A_3A_4})=\mathrm{rank}(|\lambda\rangle_{A_1A_4|A_2A_3})=4$。这推出 $|\lambda_s\rangle$ 在任意两体划分下都是纠缠态，从而它是真实纠缠态，且 $\overline{\mathcal{S}_{(0,0,i,i)}}$ 是正交真实纠缠集。

综上，$\overline{B_d^4}$ 是强非局域的正交真实纠缠集。 ∎

4.6　本章小结

在本章中，我们给出了证明强量子非局域性的有效方法。基于这种方法和多维超立方体的分解，我们构造出了一系列三、四、五体系统中强非局域的正交集。最后利用循环置换群作用，我们给出了 N 体齐次系统中强非局域的正交纠缠集。主要结果见表1.3。我们的结果对文献[43]中提出的三个公开问题给予了全面的回答。

对于强量子非局域性，我们提出几个值得研究的问题：

1. 对于任何 $d_i\geqslant 3$，$N\geqslant 6$，$1\leqslant i\leqslant N$，能否构造 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中强非局域的正交乘积集?
2. 对于任何 $d_i\geqslant 2$，$N\geqslant 3$，$1\leqslant i\leqslant N$，$(\mathbb{C}^d)^{\otimes N}$ 中强非局域的正交集所含态的个数最小是多少?
3. 对于任何 $d_i\geqslant 3$，$N\geqslant 3$，$1\leqslant i\leqslant N$，能否构造 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的不可扩充乘积基，使得它在任意两体划分下还是一个不可扩充乘积基?

第 5 章　k-均匀态和量子信息掩盖

目前多体系统中的量子信息掩盖要求任意单体子系统无法获取原始信息, 类似于量子非局域性，如果其中有 k 个子系统共谋，那么原始信息将有可能被获取。为了避免这种共谋，我们需要一种更强版本的量子信息掩盖。而 k-均匀态在量子信息掩盖中发挥着重要作用。本章将研究非齐次系统中的 k-均匀态和量子信息掩盖。5.1 节介绍了 k-均匀态和量子信息掩盖的研究背景及其现状。5.2 节介绍了 k-均匀态、混合正交阵列、量子信息掩盖和量子纠错码等概念。5.3 节构造了一系列非齐次系统中的 k-均匀态。5.4 节给出了一些非齐次系统中的绝对最大纠缠态的不存在性结果。5.5 节建立了量子纠错码与量子信息掩盖之间的关系。5.6 节给出了几种从已知的非齐次系统中的量子纠错码构造新的量子纠错码的方法。5.7 节为本章小结。

5.1　引言

如果齐次系统 $(\mathbb{C}^d)^{\otimes N}$ 中的一个纯态在任意 k 体上的约化密度算子是最大混合的, 那么它被称为 k-均匀态[51] 。$(\mathbb{C}^d)^{\otimes N}$ 中的 k-均匀态与参数为 $((N,1,k+1))_d$ 的量子纠错码一一对应[51]，并且它可以通过正交阵列[52]、拉丁方[57]、量子拉丁方[58]、对称矩阵和经典纠错码[53]来构造。根据施密特分解，$(\mathbb{C}^d)^{\otimes N}$ 中 k-均匀态存在的必要条件是 $k \leqslant \lfloor \frac{N}{2} \rfloor$[59]。特别地，$\lfloor \frac{N}{2} \rfloor$-均匀态被称为绝对最大纠缠态，它在任意两体划分下都是最大纠缠态。绝对最大纠缠态可用于阈值量子秘密共享方案[60]、并行和开放目标的远程传输协议[60] 和全息量子纠错码[61]。

k-均匀态和绝对最大纠缠态的概念也可以直接推广到非齐次系统中。类似地, 非齐次系统 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的 k-均匀态与非齐次系统中参数为 $((N,1,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码一一对应[66]。Bryan 等人[109-110] 给出了非齐次系统中存在 1-均匀态的充要条件。利用混合正交阵列，Goyeneche 等人[107]构造了一些 N 体非齐次系统中的 1, 2-均匀态。Shen 等人[108]构造了一些 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3}$ 中的绝对最大纠缠态。虽然非齐次系统中的 k-均匀态已经有了一些结果，但缺少一定的构造。特别地，Goyeneche 等人[107]提出了一个公开问题：非齐次系统中是否存在 3-均匀态？我们将对这个问题给予肯定的回答。

最近 Modi 等人提出了量子信息掩盖的概念[89]，这是一个将量子信息编码到两体系统中的物理过程，使得信息对于每个单体子系统来说是完全未知的。同时他们还强调了一个不可掩盖定理：不能掩盖任意量子态。Li 等人[111]表明了多体系统中的量子信息掩盖是可能的。在他们的掩盖协议中，同样要求每个单体子

系统都无法访问原始信息。最近，Liu 等人[118]给出了量子信息掩盖的光学实现。在之前的量子信息掩盖中，如果其中几个子系统共谋，那么有可能会导致信息泄露，为了避免这种情况发生，本章将提出 k-均匀量子信息掩盖。Li 等人[111]提出了两个公开问题：

(i) 是否能将 $\mathbb{C}^d$ 中所有态掩盖到 $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ 中，使得掩盖后的态的单体约化密度算子不等于 $\frac{1}{d}\mathbb{I}_d$？

(ii) 是否能将 $\mathbb{C}^d$ 中所有态掩盖到 $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$ 中，使得 $n < d$？

我们将对这两个问题给予否定回答。

当量子信息通过带有噪声的信道时，错误是不可避免的[73-75]。量子纠错码在量子信息处理中发挥着核心作用，它可以保护量子信息免受各种量子噪声的影响。齐次系统中的量子纠错码的研究较多[62,76-81]，但当编码后的态属于非齐次系统时，我们通常面临更复杂的情况，这使得研究非齐次系统中的量子纠错码更加复杂。我们将研究量子信息掩盖与量子纠错码之间的关系。

5.2　准备工作

本节将介绍非齐次系统中的 k-均匀态、混合正交阵列和相关引理，其次介绍量子信息掩盖和量子纠错码的概念。

5.2.1　非齐次系统中的 k-均匀态

本小节中，我们将介绍 k-均匀态的基本概念和引理。在 N 体非齐次系统 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中，如果没有特殊说明，我们总是假设 $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_N$。根据第2章中的预备知识可知，$\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_N} := \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中任意一个态 $|\psi\rangle$ 可以写为 $|\psi\rangle = \sum_{\mathbf{u}\in\mathbb{Z}_{d_1}\times\cdots\times\mathbb{Z}_{d_N}} a_{\mathbf{u}}|\mathbf{u}\rangle$，其中 $a_{\mathbf{u}} \in \mathbb{C}$，那么 $|\psi\rangle$ 的密度算子被定义为

$$\rho := \sum_{\mathbf{u},\mathbf{u}'\in\mathbb{Z}_{d_1}\times\cdots\times\mathbb{Z}_{d_N}} a_{\mathbf{u}}\overline{a_{\mathbf{u}'}}|\mathbf{u}\rangle\langle\mathbf{u}'|.$$

对于任何子集 $A \subset \{A_1, A_2, \cdots, A_N\}$，令 $A^c := \{A_1, A_2, \cdots, A_N\} \setminus A$。对于向量 $\mathbf{u} \in \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_N}$，令 $\mathbf{u}_A$ 为 $\mathbf{u}$ 在 A 上的投影，则 $|\psi\rangle$ 也可以写成 $|\psi\rangle = \sum_{\mathbf{u}\in\mathbb{Z}_{d_1}\times\cdots\times\mathbb{Z}_{d_N}} a_{\mathbf{u}}|\mathbf{u}_A\rangle|\mathbf{u}_{A^c}\rangle$。那么 $|\psi\rangle$ 在 A 上的约化密度算子为

$$\rho_A := \mathrm{Tr}_{A^c}\rho = \sum_{\mathbf{u},\mathbf{u}'\in\mathbb{Z}_{d_1}\times\cdots\times\mathbb{Z}_{d_N}} a_{\mathbf{u}}\overline{a_{\mathbf{u}'}}\langle\mathbf{u}_{A^c}|\mathbf{u}'_{A^c}\rangle|\mathbf{u}_A\rangle\langle\mathbf{u}'_A|,$$

其中 Tr_{A^c} 为偏迹运算符，如果 $\mathbf{u}_{A^c} = \mathbf{u}'_{A^c}$，那么 $\langle\mathbf{u}_{A^c}|\mathbf{u}'_{A^c}\rangle$ 为 1 ，否则为 0。

定义 5.1　假设 $|\psi\rangle$ 是 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个纯态，令 $A =$

$\{A_{i_1}, A_{i_2}, \cdots, A_{i_k}\} \subset \{A_1, A_2, \cdots, A_N\}$，其中 $|A| = k$。如果

$$\rho_A := \frac{1}{d_{i_1} d_{i_2} \cdots d_{i_k}} \sum_{\mathbf{u} \in \mathbb{Z}_{d_{i_1}} \times \cdots \times \mathbb{Z}_{d_{i_k}}} |\mathbf{u}\rangle\langle\mathbf{u}|. \tag{5.1}$$

那么称 $|\psi\rangle$ 在 A 上的约化密度算子是最大混合的。如果 $|\psi\rangle$ 在任意 k 体上的约化密度算子是最大混合的，那么 $|\psi\rangle$ 被称为k-均匀态。特别地，如果 $k = \lfloor \frac{N}{2} \rfloor$，那么 $|\psi\rangle$ 被称为绝对最大纠缠态。

若 $|\psi\rangle$ 是 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的 k-均匀态，根据两体纯态的施密特分解[59]，我们得到 $d_1 d_2 \cdots d_k \leqslant d_{k+1} d_{k+2} \cdots d_N$。因此 k 满足 $k \leqslant \lfloor \frac{N}{2} \rfloor$，极端情况下 $|\psi\rangle$ 就是绝对最大纠缠态。例如

$$|\phi\rangle = \frac{1}{\sqrt{6}}(|000\rangle + |011\rangle + |101\rangle + |110\rangle + |200\rangle - |211\rangle)$$

是 $\mathbb{C}^3 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中的 1-均匀态（绝对最大纠缠态）[107]。对 $|\phi\rangle$ 来说，可以验证 $\rho_{A_1} = \frac{1}{3} \sum_{i \in \mathbb{Z}_3} |i\rangle\langle i|$ 和 $\rho_{A_2} = \rho_{A_3} = \frac{1}{2} \sum_{i \in \mathbb{Z}_2} |i\rangle\langle i|$。

正交阵列和混合正交阵列是组合数学中的经典概念，它们与有限域、有限几何和经典纠错码相关，在统计学、计算机科学和密码学中有着广泛的应用[126]。

定义 5.2 [126] 一个参数为 $\mathrm{MOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$ 的混合正交阵列是一个 $r \times \sum_{i=1}^{\ell} n_i$ 的阵列，其中有 n_i 列的元素来自 $\mathbb{Z}_{d_i}, i = 1, 2, \cdots, \ell$。取任意一个 $r \times k$ 阶子矩阵，这个子矩阵的第 j 列元素来自 $\mathbb{Z}_{d_{i_j}}, j = 1, 2, \cdots, k$，使得 $\mathbb{Z}_{d_{i_1}} \times \mathbb{Z}_{d_{i_2}} \times \cdots \times \mathbb{Z}_{d_{i_k}}$ 中所有可能的长度为 k 的行向量在这个子矩阵的行向量中出现的次数相同。如果 $\ell = 1$，$d_1 = d$ 且 $n_1 = N$，那么这个混合正交阵列退化为正交阵列，参数为 $\mathrm{OA}(r, d^N, k)$。其中 k 被称为强度，d_i 被称为水平。

注意，改变混合正交阵列的列顺序并不会改变混合正交阵列的参数。因此，混合正交阵列中的 $d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}$ 并不意味着前 n_1 列中的元素来自 $\mathbb{Z}_{d_1}$，接下来的 n_2 列中的元素来自 $\mathbb{Z}_{d_2}$ 等等。但按照惯例，我们通常以 $d_1 > d_2 > \cdots > d_\ell$ 的方式编写符号，并按照这个方式列出相应的列。如果混合正交阵列的行向量两两不同，那么这个混合正交阵列是简单的。下面是两个简单的混合正交阵列。

例 5.1

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 & 0 \\ 3 & 0 & 1 & 1 & 0 \\ 3 & 1 & 0 & 0 & 1 \end{pmatrix}$$ 是一个 $\mathrm{MOA}(8, 4^1 2^4, 2)$;

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 1 & 0\\
0 & 0 & 1 & 0 & 1\\
0 & 1 & 1 & 1 & 1\\
1 & 0 & 1 & 1 & 0\\
1 & 1 & 1 & 0 & 0\\
1 & 0 & 0 & 0 & 1\\
1 & 1 & 0 & 1 & 1\\
2 & 0 & 1 & 1 & 0\\
2 & 1 & 0 & 0 & 0\\
2 & 0 & 0 & 1 & 1\\
2 & 1 & 1 & 0 & 1
\end{pmatrix}$$ 是一个 $\mathrm{MOA}(12, 3^1 2^4, 2)$.

利用例5.1中的 $\mathrm{MOA}(8, 4^1 2^4, 2)$，我们可以在 $\mathbb{C}^4 \otimes (\mathbb{C}^2)^{\otimes 4}$ 中构造一个 2-均匀态，

$$\begin{aligned}|\psi\rangle = \frac{1}{2\sqrt{2}}(&|00000\rangle + |01111\rangle + |10011\rangle + |11100\rangle + \\ &|20101\rangle + |21010\rangle + |30110\rangle + |31001\rangle).\end{aligned} \tag{5.2}$$

并非所有混合正交阵列都可以用于构造非齐次系统中的 k-均匀态。利用相同的方法，例5.1中的 $\mathrm{MOA}(12, 3^1 2^4, 2)$ 可构造态 $|\phi\rangle = \frac{1}{2\sqrt{3}}(|00000\rangle + |01010\rangle + |00101\rangle + |01111\rangle + |10110\rangle + |11100\rangle + |10001\rangle + |11011\rangle + |20110\rangle + |21000\rangle + |20011\rangle + |21101\rangle) \in \mathbb{C}^3 \otimes (\mathbb{C}^2)^{\otimes 4}$。但是，$|\phi\rangle$ 不是 2-均匀态，这是因为 $|\phi\rangle$ 在 A_1, A_2 上的约化密度算子不是最大混合的。为了描述混合正交阵列和 k-均匀态之间的关系，我们给出不可缩短的混合正交阵列的定义。

定义 5.3 [52,107] 如果从一个有 $N = \sum_{i=1}^{\ell} n_i$ 列的混合正交阵列 $\mathrm{MOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$ 中选取任意 $N-k$ 列，且限制在这 $N-k$ 列的 r 个行向量各不相同，那么这个混合正交阵列被称为不可缩短的。我们标记不可缩短的 $\mathrm{MOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$ 为 $\mathrm{IrMOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$，且标记不可缩短的 $\mathrm{OA}(r, d^N, k)$ 为 $\mathrm{IrOA}(r, d^N, k)$。

下面的引理表明不可缩短的混合正交阵列可用于构造非齐次系统中的 k-均匀态。

引理 5.1 [107] 如果陈列 $(m_{i,j})_{1\leqslant i\leqslant r; 1\leqslant j\leqslant N}$ 是 $\mathrm{IrMOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$，那么 $|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{i=1}^{r} |m_{i,1} m_{i,2} \cdots m_{i,N}\rangle$ 是 $(\mathbb{C}^{d_1})^{\otimes n_1} \otimes (\mathbb{C}^{d_2})^{\otimes n_2} \otimes \cdots \otimes (\mathbb{C}^{d_\ell})^{\otimes n_\ell}$ 中的一个 k-均匀态。

在例5.1中, 我们可以验证 MOA$(8, 4^1 2^4, 2)$ 是不可缩短的, 而 MOA$(12, 3^1 2^4, 2)$ 是非不可缩短的。所以通过引理5.1可知，我们在 $\mathbb{C}^4 \otimes (\mathbb{C}^2)^{\otimes 4}$ 中可以构造一个 2-均匀态。

5.2.2　k-均匀量子信息掩盖

本小节中，我们将介绍量子信息掩盖和量子纠错码的概念。文献[89]中提出了量子信息掩盖的概念。

定义 5.4　[89] 一个算子 S 可以掩盖量子信息 $\{|a_j\rangle_{A_1} \in \mathcal{H}_{A_1}\}$ 指的是 S 将这些态映射到 $\{|\psi_j\rangle \in \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}\}$，使得对于所有的 $|\psi_j\rangle$，它们的单体约化密度算子都相等，即

$$\rho_{A_1} = \mathrm{Tr}_{A_2} |\psi_j\rangle\langle\psi_j| \text{ 和 } \rho_{A_2} = \mathrm{Tr}_{A_1} |\psi_j\rangle\langle\psi_j|$$

没有任何 j 的信息。

文献[111]提出了多体系统中的量子信息掩盖的概念。

定义 5.5　[111] 一个算子 S 可以掩盖量子信息 $\{|a_j\rangle_{A_1} \in \mathcal{H}_{A_1}\}$ 指的是 S 将这些态映射到 $\{|\psi_j\rangle \in \otimes_{\ell=1}^{N} \mathcal{H}_{A_\ell}\}$，使得对于所有的 $|\psi_j\rangle$，它们的单体约化密度算子都相等，即对于任意的 $A_\ell \in \{A_1, A_2, \cdots, A_N\}$，

$$\rho_{A_\ell} = \mathrm{Tr}_{A_\ell^c} |\psi_j\rangle\langle\psi_j|$$

没有任何 j 的信息。

定义5.5同样要求 $\{|\psi_j\rangle \in \otimes_{\ell=1}^{N} \mathcal{H}_{A_\ell}\}$ 中的态的单体约化密度算子都相等。但是如果一些子系统 $\{A_1, A_2, \cdots, A_N\}$ 共谋，那么有可能揭露掩盖之前的信息。例如

$$\begin{aligned}
S:\ |0\rangle \to |\psi_0\rangle_{ABC} =& \frac{1}{\sqrt{3}}(|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C + |2\rangle_A|2\rangle_B|2\rangle_C),\\
|1\rangle \to |\psi_1\rangle_{ABC} =& \frac{1}{\sqrt{3}}(|0\rangle_A|1\rangle_B|2\rangle_C + |1\rangle_A|2\rangle_B|0\rangle_C + |2\rangle_A|0\rangle_B|1\rangle_C),\\
|2\rangle \to |\psi_2\rangle_{ABC} =& \frac{1}{\sqrt{3}}(|0\rangle_A|2\rangle_B|1\rangle_C + |1\rangle_A|0\rangle_B|2\rangle_C + |2\rangle_A|1\rangle_B|0\rangle_C).
\end{aligned}$$

则任意的一个量子态 $\alpha|0\rangle_A + \beta|1\rangle_A + \gamma|2\rangle_A \in \mathbb{C}^3$（$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$）可以被 S 掩盖成 $|\psi\rangle = \alpha|\psi_0\rangle_{ABC} + \beta|\psi_1\rangle_{ABC} + \gamma|\psi_2\rangle_{ABC} \in \mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$。如果 A 和 B 共谋，那么首先可以将 $|\psi\rangle$ 中 A 部分的态加到 B 部分（模 3），然后再将 B 部分的态加到 A 部分（模 3），则 $|\psi\rangle$ 变为

$$\frac{1}{\sqrt{3}}(\alpha|0\rangle_A + \beta|1\rangle_A + \gamma|2\rangle_A)(|0\rangle_B|0\rangle_C + |1\rangle_B|2\rangle_C + |2\rangle_B|1\rangle_C).$$

那么 A 部分已经揭露了掩盖之前的信息。为了避免这种共谋，我们提出 k-均匀量子信息掩盖的概念。

定义 5.6　一个算子 S 可以k-均匀地掩盖量子信息 $\{|a_j\rangle_{A_0} \in \mathcal{H}_{A_0}\}$ 指的是 S 将这些态映射到 $\{|\psi_j\rangle \in \otimes_{\ell=1}^{N}\mathcal{H}_{A_\ell}\}$，使得对于所有的 $|\psi_j\rangle$，它们的 k 体约化密度算子都相等，即对于任意的 $A = \{A_{\ell_1}, A_{\ell_2}, \cdots, A_{\ell_k}\}$，$A \subset \{A_1, A_2, \cdots, A_N\}$ 且 $|A| = k$,

$$\rho_A = \mathrm{Tr}_{A^c}|\psi_j\rangle\langle\psi_j|$$

没有任何 j 的信息。特别地，如果 $k = \lfloor\frac{N}{2}\rfloor$，那么 k-均匀量子信息掩盖被称为强量子信息掩盖。

值得注意的是当 $\mathcal{H}_{A_0} = \mathcal{H}_{A_1}$，$k = 1$ 和 $N = 2$ 时，定义5.6就是定义5.4；当 $\mathcal{H}_{A_0} = \mathcal{H}_{A_1}$ 和 $k = 1$ 时，定义5.6 就是定义5.5。我们的 k-均匀量子信息掩盖也是量子秘密分享的基础[127-128]。一个 (k, N) 量子秘密分享方案，指的是一组秘密量子态被分给了 N 个人，使得任意 k 个人可以恢复这个秘密，而任意 $k-1$ 个人无法恢复这个秘密。然而当 $N \geqslant 2k$ 时，任意 (k, N) 量子秘密分享方案不存在。在我们的 k-均匀量子信息掩盖中，即使 $N \geqslant 2(k+1)$，它也允许老板将秘密分享到他的 N 个下属中，使得任意 k 个下属共谋也无法得到这个秘密。注意在我们的方案中，不考虑恢复秘密。

接下来，我们考虑非齐次系统中的量子纠错码。令 $\{e_j\}_{j\in\mathbb{Z}_{d^2}}$ 为作用在 $\mathbb{C}^d$ 上的正交算子基，其中 $e_0 = \mathbb{I}_d$，$\mathrm{Tr}(e_i^\dagger e_j) = \delta_{ij}d$。那么 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个局部错误基 $\mathcal{E} = \{E_\alpha\}$ 由

$$E_\alpha = e_{\alpha_1}^{(1)} \otimes e_{\alpha_2}^{(2)} \otimes \cdots \otimes e_{\alpha_N}^{(N)}$$

组成，其中 $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_N) \in \mathbb{Z}_{d_1^2} \times \mathbb{Z}_{d_2^2} \times \cdots \times \mathbb{Z}_{d_N^2}$，$e_{\alpha_i}^{(i)}$ 作用在 $\mathbb{C}^{d_i}$ 上，且 $\mathrm{Tr}(E_\alpha^\dagger E_\beta) = \delta_{\alpha\beta}d_1d_2\cdots d_N$。一个局部错误 E_α 的支撑集被定义为 $supp(E_\alpha) := supp(\alpha) = \#\{i \mid \alpha_i \neq 0,\ 1 \leqslant i \leqslant N\}$，$E_\alpha$ 的权重为 $wt(E_\alpha) = |supp(E_\alpha)|$。任何一个作用在 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 上的算子 M 都可以被分解为:

$$M = \frac{1}{d_1d_2\cdots d_N}\sum_{E_\alpha\in\mathcal{E}}\mathrm{Tr}(E_\alpha^\dagger M)E_\alpha. \tag{5.3}$$

非齐次系统中的量子纠错码同样要满足 Knill-Laflamme 条件[74-75]。我们给出如下定义。

定义 5.7　令 Q 为 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 K 维子空间。对于 Q 中任意一组标准正交基 $\{|i_Q\rangle\}_{i\in\mathbb{Z}_K}$ 和任意一个 $E_\alpha \in \mathcal{E}$，且 $wt(E_\alpha) < k+1$，如果有

$$\langle i_Q|E_\alpha|j_Q\rangle = C(E_\alpha)\delta_{ij},$$

其中 $C(E_\alpha)$ 只依赖于 E_α，那么 Q 被称为一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码。这里 $k+1$ 被称为这个量子纠错码的距离。如果 $0<wt(E_\alpha)<k+1$，有 $C(E_\alpha)=\frac{\mathrm{Tr}(E_\alpha)}{d_1d_2\cdots d_N}=0$，那么这个量子纠错码被称为纯量子纠错码。按照惯例，$((N,1,k+1))_{d_1,d_2,\cdots,d_N}$ 只指纯量子纠错码。特别地，如果 $d_1=d_2=\cdots=d_N=d$，那么 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 被记为 $((N,K,k+1))_d$。

我们把参数为 $((N,K,k+1))_d$ 的量子纠错码称为齐次系统中的量子纠错码。齐次系统中的量子纠错码存在一个等价的定义[79,129]，类似地，我们也可以给出非齐次系统中的量子纠错码的一个等价定义。

定义 5.8　令 Q 为 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个 K 维子空间。对于任意的 $|\psi\rangle\in Q$ 和 $E_\alpha\in\mathcal{E}$，且 $wt(E_\alpha)<k+1$，如果有

$$\langle\psi|E_\alpha|\psi\rangle=C(E_\alpha),$$

其中 $C(E_\alpha)$ 只依赖于 E_α，那么 Q 被称为一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码。如果 $0<wt(E)<k+1$，有 $C(E_\alpha)=\frac{\mathrm{Tr}(E_\alpha)}{d_1d_2\cdots d_N}=0$，那么这个量子纠错码被称为纯量子纠错码。

下面我们证明定义5.7与定义5.8等价。

引理 5.2　定义5.7与定义5.8等价。

证明　定义5.7 “⇒”定义 5.8。我们可以在基 $\{|i_Q\rangle\}_{i\in\mathbb{Z}_K}$ 下分解 $|\psi\rangle$，使得 $|\psi\rangle=\sum_{i\in\mathbb{Z}_K}a_i|i_Q\rangle$，其中 $\sum_{i\in\mathbb{Z}_K}|a_i|^2=1, a_i\in\mathbb{C}, i\in\mathbb{Z}_K$。对于任何 $wt(E_\alpha)<k+1$，我们有

$$\begin{aligned}\langle\psi|E_\alpha|\psi\rangle&=\sum_{i\in\mathbb{Z}_K}\sum_{j\in\mathbb{Z}_K}\overline{a_i}a_j\langle i_Q|E_\alpha|j_Q\rangle=\sum_{i\in\mathbb{Z}_K}|a_i|^2\langle i_Q|E_\alpha|i_Q\rangle\\&=\sum_{i\in\mathbb{Z}_K}|a_i|^2C(E_\alpha)=C(E_\alpha).\end{aligned}$$

定义5.8 “⇒”定义 5.7。对于任何 $i\neq j\in\mathbb{Z}_k$ 和 $wt(E_\alpha)<k+1$，我们只需要验证 $\langle i_Q|E_\alpha|j_Q\rangle=0$。令 $|\psi\rangle=\lambda|i_Q\rangle+u|j_Q\rangle$，其中 $|\lambda|^2+|u|^2=1$，那么

$$\begin{aligned}\langle\psi|E_\alpha|\psi\rangle&=(\overline{\lambda}\langle i_Q|+\overline{u}\langle j_Q|)E_\alpha(\lambda|i_Q\rangle+u|j_Q\rangle)\\&=C(E_\alpha)+\overline{\lambda}u\langle i_Q|E_\alpha|j_Q\rangle+\lambda\overline{u}\langle j_Q|E_\alpha|i_Q\rangle=C(E_\alpha).\end{aligned}$$

这推出

$$\overline{\lambda}u\langle i_Q|E_\alpha|j_Q\rangle+\lambda\overline{u}\langle j_Q|E_\alpha|i_Q\rangle=0.$$

我们可以分别令 $\lambda=\frac{1}{\sqrt{2}}$，$u=\frac{1}{\sqrt{2}}$；$\lambda=\frac{1}{\sqrt{2}}$，$u=\frac{1}{\sqrt{2}}i$，即

$$\begin{cases}\frac{1}{2}\langle i_Q|E_\alpha|j_Q\rangle+\frac{1}{2}\langle j_Q|E_\alpha|i_Q\rangle=0,\\\frac{1}{2}i\langle i_Q|E_\alpha|j_Q\rangle-\frac{1}{2}i\langle j_Q|E_\alpha|i_Q\rangle=0.\end{cases}$$

从而我们得到 $\langle i_Q|E_\alpha|j_Q\rangle = 0$。 ∎

值得注意的是 E_α 可以被任何算子 M 替代，其中 M 至少在 $N-k$ 个子系统上是单位作用。在这种情况下，如果 $C(M) = \frac{\mathrm{Tr}(M)}{d_1 d_2 \cdots d_N}$，那么这个量子纠错码是纯量子纠错码[77,79]。对于一个参数为 $((N, K, k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码，它最多可以检测出作用于 k 个子系统的所有错误，并最多可以纠正作用于 $\lfloor \frac{k}{2} \rfloor$ 个子系统的所有错误。

5.3　非齐次系统中的 k-均匀态的构造

在本节中，我们将给出具有明确的最小汉明距离的混合正交阵列与不可缩短的混合正交阵列之间的关系。基于这个关系，我们将给出 $2,3$-均匀态的构造。此外，我们也给出两种从 k-均匀态获得 $(k-1)$-均匀态的方法。

5.3.1　混合正交阵列的最小汉明距离

当混合正交阵列有很多列时，根据定义决定混合正交阵列的不可缩短性并不容易，我们需要引入一种有效的方法，该方法首先用于决定正交阵列的不可缩短性[55]。我们需要先给出两个向量的汉明距离的定义，这个概念来自于编码理论。对于一个 $r \times N$ 的矩阵 M，它的 r 行为 $\mathbf{m}_i$，$i = 1, 2, \cdots, r$，则 $\mathbf{m}_i - \mathbf{m}_j$ 中非零的个数为 $\mathbf{m}_i$ 和 $\mathbf{m}_j$ 的*汉明距离*，用 $\mathrm{HD}(\mathbf{m}_i, \mathbf{m}_j)$ 表示。M 的*最小汉明距离*指的是 M 中任意两个行向量之间的最小汉明距离，用 $\mathrm{MD}(M)$ 表示。下面我们给出具有明确的最小汉明距离的混合正交阵列与不可缩短的混合正交阵列之间的关系。

引理 5.3　[130] 令 M 为 $\mathrm{MOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$，那么 M 是不可缩短的当且仅当 $\mathrm{MD}(M) \geqslant k+1$。

特别地，混合正交阵列是简单的当且仅当它的最小汉明距离大于等于 1。图5.1表明了我们构造非齐次系统中的 k-均匀态的主要方法。例5.1给出的 $\mathrm{MOA}(8, 4^1 2^4, 2)$ 和 $\mathrm{MOA}(12, 3^1 2^4, 2)$ 的最小汉明距离分别是 3 和 1，因此根据引理5.3，$\mathrm{MOA}(8, 4^1 2^4, 2)$ 是不可缩短的，而 $\mathrm{MOA}(12, 3^1 2^4, 2)$ 是非不可缩短的。

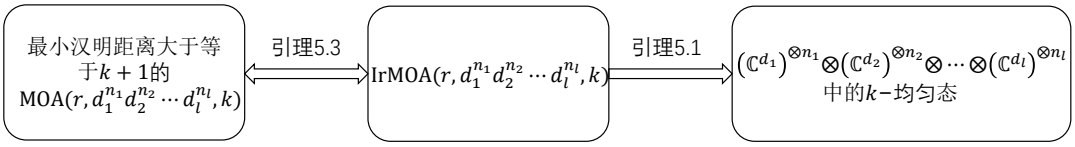

图 5.1　构造非齐次系统中的 k-均匀态的主要方法。

根据定义5.2，删除 $\mathrm{MOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$ 的一些列后仍然是强度为 k 的混合正交阵列，但这个混合正交阵列可能不再保持不可缩短的性质。文献[107]提出了*k 耐受性*的概念，它指的是强度为 k 的混合正交阵列可以删除的最大列数，使

得删除后的混合正交阵列仍然是不可缩短的。通过引理5.3，我们可以很容易地估计出混合正交阵列 $\boldsymbol{M}$ 的 k 耐受性，它至少是 $\mathrm{MD}(\boldsymbol{M})-(k+1)$。因此我们有以下引理。

引理 5.4　假设 $\boldsymbol{M}$ 是 $\mathrm{IrMOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, k)$，其中 $\mathrm{MD}(\boldsymbol{M}) = b \geqslant k+1$。如果我们删除 $\boldsymbol{M}$ 的任何 $c \leqslant b-(k+1)$ 列，那么它变为 $\mathrm{IrMOA}(r, d_1^{n_1'} d_2^{n_2'} \cdots d_\ell^{n_\ell'}, k)$，其中 $n_i' \leqslant n_i$，$1 \leqslant i \leqslant \ell$ 且 $(n_1+n_2+\cdots+n_\ell)-(n_1'+n_2'+\cdots+n_\ell') = c$。

下面我们给出一个简单的例子。

例 5.2

$$
\begin{pmatrix}
0&0&0&0&0&0&0&0\\
0&1&2&2&0&1&1&0\\
0&2&1&2&1&0&2&0\\
0&1&1&0&2&2&0&1\\
0&2&0&1&2&1&1&1\\
0&0&2&1&1&2&2&1\\
1&1&1&1&1&1&0&0\\
1&2&0&0&1&2&1&0\\
1&0&2&0&2&1&2&0\\
1&2&2&1&0&0&0&1\\
1&0&1&2&0&2&1&1\\
1&1&0&2&2&0&2&1\\
2&2&2&2&2&2&0&0\\
2&0&1&1&2&0&1&0\\
2&1&0&1&0&2&2&0\\
2&0&0&2&1&1&0&1\\
2&1&2&0&1&0&1&1\\
2&2&1&0&0&1&2&1
\end{pmatrix}
\text{是一个 } \mathrm{MOA}(18, 3^7 2^1, 2).
$$

它的最小汉明距离为 5，根据引理5.4，我们可以得到 $\mathrm{IrMOA}(18, 3^6 2^1, 2)$、$\mathrm{IrOA}(18, 3^7, 2)$、$\mathrm{IrMOA}(18, 3^5 2^1, 2)$ 和 $\mathrm{IrOA}(18, 3^6, 2)$。

5.3.2　非齐次系统中的 2-均匀态的构造

本小节中，我们将给出具有明确的最小汉明距离的 $\mathrm{MOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, 2)$ 的一些构造，第一个方法被称为广阔替换[126]。

引理 5.5　假设 A_1 是一个 $\mathrm{MOA}(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, 2)$，对于某个 $1 \leqslant i \leqslant \ell$，$A_2$ 是一个简单的 $\mathrm{MOA}(d_i, s_1^{t_1} s_2^{t_2} \cdots s_e^{t_e}, 2)$，且行向量为 $\mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_{d_i-1}$。令 $\mathbf{c}$ 为 A_1 中

任何一个水平为 d_i 的列向量，对于任何 $c \in \mathbb{Z}_{d_i}$，将 $\mathbf{c}$ 中的符号 c 替换为 $\mathbf{v}_c$，我们得到一个新的 MOA$(r, d_1^{n_1} d_2^{n_2} \cdots d_{i-1}^{n_{i-1}} s_1^{t_1} s_2^{t_2} \cdots s_e^{t_e} d_i^{n_i - 1} d_{i+1}^{n_{i+1}} \cdots d_\ell^{n_\ell}, 2)$[126]，记为 A_1'。如果 MD$(A_1) = b$，那么 MD$(A_1') \geqslant b$。因此，如果 A_1 是不可缩短的，那么 A_1' 也是不可缩短的。

证明　我们只需要讨论 A_1' 的最小汉明距离。假设 HD$(\mathbf{m}_p, \mathbf{m}_q) = b$，其中 $\mathbf{m}_p = (m_{p,s})$，$\mathbf{m}_j = (m_{q,s})$ 是 A_1 的两个行向量。令 $\mathbf{m}_p'$ $(\mathbf{m}_q')$ 表示 A_1' 中 $\mathbf{m}_p$ $(\mathbf{m}_q)$ 在经过替换之后的向量。如果替换之前的水平 d_i 中的 $m_{p,s}$ 和 $m_{q,s}$ 相等，那么替换之后 HD$(\mathbf{m}_p', \mathbf{m}_q') = b$；由于 A_2 是简单的，如果在被替换之前的水平 d_i 中的 $m_{p,s}$ 和 $m_{q,s}$ 不相等，那么 HD$(\mathbf{m}_p', \mathbf{m}_q') \geqslant b$。因此，我们有 MD$(A_1') \geqslant b$。 ∎

例如，给定一个最小汉明距离为 9 的 MOA$(36, 12^1 3^{12}, 2)$ 和一个简单的 MOA$(12, 3^1 2^4, 2)$[131]，根据引理5.5，我们得到一个最小汉明距离大于等于 9 的 MOA$(36, 3^{13} 2^4, 2)$。

文献[132]中给出了一个混合正交阵列的分裂方法。给定一个最小汉明距离为 b 的 MOA$(r, (d_1 d_2)^1 d_3^1 \cdots d_N^1, t)$，将水平 $d_1 d_2$ 中的符号按照引理5.5中的方法替换成平凡 MOA$(d_1 d_2, d_1^1 d_2^1, 2)$ 中的行向量，那么我们得到一个最小汉明距离大于等于 b 的 MOA$(r, d_1^1 d_2^1 d_3^1 \cdots d_N^1, t)$，其证明方法与引理5.5类似。例如，给定一个最小汉明距离为 5 的 MOA$(18, 3^6 6^1, 2)$[131]，那么我们得到一个最小汉明距离大于等于 5 的 MOA$(18, 3^7 2^1, 2)$。对于 k-均匀态，也存在一个分裂方法[107]。给定 $\mathbb{C}^{d_1 d_2} \otimes \mathbb{C}^{d_3} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 k-均匀态，将 $\mathbb{C}^{d_1 d_2}$ 中的态全部替换为 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ 中的态，则我们得到 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 k-均匀态。注意这种替换反过来是不正确的，例如我们无法从 $(\mathbb{C}^2)^{\otimes 4}$ 中的 $|\mathrm{GHZ}\rangle_2^4 = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ (1-均匀态) 上获得 $\mathbb{C}^4 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中的 1-均匀态。然而，$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 k-均匀态，通过将 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ 中的态全部替换为 $\mathbb{C}^{d_1 d_2}$ 中的态，我们可以得到 $\mathbb{C}^{d_1 d_2} \otimes \mathbb{C}^{d_3} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 $(k-1)$-均匀态，我们将在引理5.11中讨论这个问题。

接下来通过差矩阵，我们给出具有明确的最小汉明距离的 MOA$(r, d_1^{n_1} d_2^{n_2} \cdots d_\ell^{n_\ell}, 2)$ 的第二种构造。令 S 为 d 阶加法群，对于一个 $s \times N$ 的矩阵 D，其元素取自于 S，如果任意两列作差，使得 S 中的 d 个符号出现次数相同，那么 D 被称为*差矩阵*，并记为 $D(s, N, d)$。我们经常选择 S 为 $\mathbb{Z}_d$ 或伽罗瓦数域 GF(d)。特别地，差矩阵 $D(\lambda d, \lambda d, d)$ 也称为*广义 Hadamard 矩阵*。由于 S 是一个加法群，$D(\lambda d, \lambda d, d)$ 的转置仍然是一个广义 Hadamard 矩阵[126]。

对于矩阵 $A_1 = (a_{i,j})_{1 \leqslant i \leqslant r_1, 1 \leqslant j \leqslant N_1}$ 和 $A_2 = (f_{i,j})_{1 \leqslant i \leqslant r_2, 1 \leqslant j \leqslant N_2}$，令 $A_1 \oplus A_2 = (a_{i,j} + A_2)_{1 \leqslant i \leqslant r_1, 1 \leqslant j \leqslant N_1}$，其中 $a_{i,j} + A_2 = (a_{i,j} + f_{i',j'})_{1 \leqslant i' \leqslant r_2, 1 \leqslant j' \leqslant N_2}$。因此 $A_1 \oplus A_2$ 有 $r_1 r_2$ 行和 $N_1 N_2$ 列。对于 $N \geqslant 1$，给定一个 OA$(r, d^N, 2)$ 和一个 $D(\lambda d, \lambda d, d)$，我

们可以通过“$\oplus$”得到具有明确的最小汉明距离的混合正交阵列。注意当 $N=1$ 时，$\mathrm{OA}(d,d^1,2)$ 表示 $(0,1,\cdots,d-1)^T$。

引理 5.6　对于 $N\geqslant 1$, 令 A_1 为 $\mathrm{OA}(r,d^N,2)$, 其中 $\mathrm{MD}(A_1)=b$。假设 A_2 是广义 Hadamard 矩阵 $D(\lambda d,\lambda d,d)$, 则 $A_1'=(\mathbf{m}^T,A_1\oplus A_2)$ 是 $\mathrm{MOA}(r\lambda d,(\lambda d)^1 d^{N\lambda d},2)$, 且 $\mathrm{MD}(A_1')=\min\{\lambda(d-1)N+1,\lambda db\}$，其中行向量 $\mathbf{m}=(m_j)_{1\leqslant j\leqslant r\lambda d}$，$m_j=j-1 \pmod{\lambda d}$。

证明　$\mathrm{MOA}(r\lambda d,(\lambda d)^1 d^{N\lambda d},2)$ 的构造来自文献[126]，我们只需要证明 $\mathrm{MD}(A_1')=\min\{\lambda(d-1)N+1,\lambda db\}$。假设 $A_1=(a_{i,j})_{1\leqslant i\leqslant r,1\leqslant j\leqslant N}$，$A_2=(f_{i,j})_{1\leqslant i\leqslant \lambda d,1\leqslant j\leqslant \lambda d}$，则

$$A_1'=(\mathbf{m}^T,A_1\oplus A_2)=\begin{pmatrix}\mathbf{m}_1 & a_{1,1}+A_2 & a_{1,2}+A_2 & \cdots & a_{1,N}+A_2\\ \mathbf{m}_2 & a_{2,1}+A_2 & a_{2,2}+A_2 & \cdots & a_{2,N}+A_2\\ \vdots & \vdots & \vdots & \ddots & \cdots\\ \mathbf{m}_r & a_{r,1}+A_2 & a_{r,2}+A_2 & \cdots & a_{r,N}+A_2\end{pmatrix}=\begin{pmatrix}\mathbf{m}_1 & B_{1,1}\\ \mathbf{m}_2 & B_{2,1}\\ \vdots & \vdots\\ \mathbf{m}_r & B_{r,1}\end{pmatrix},$$

其中 $B_{i,1}=(a_{i,1}+A_2,\ a_{i,2}+A_2,\ \cdots,\ a_{i,N}+A_2)$, $\mathbf{m}_i=(0,1,\cdots,\lambda d-1)^T$, $1\leqslant i\leqslant r$。令 $\mathbf{v}_1'=(t,\mathbf{v}_1)$ 和 $\mathbf{v}_2'=(t',\mathbf{v}_2)$ 为 A_1' 的两个行向量，其中 $\mathbf{v}_1\in B_{i,1}$，$\mathbf{v}_2\in B_{j,1}$。那么有两种情况。

1. 如果 $i=j$，那么我们可以假设

$$\mathbf{v}_1=(a_{i,1}+f_{k,1},\ a_{i,1}+f_{k,2},\ \cdots,\ a_{i,1}+f_{k,\lambda d},\ \cdots,\ a_{i,N}+f_{k,1},\ \cdots,\ a_{i,N}+f_{k,\lambda d}),$$

$$\mathbf{v}_2=(a_{i,1}+f_{\ell,1},\ a_{i,1}+f_{\ell,2},\ \cdots,\ a_{i,1}+f_{\ell,\lambda d},\ \cdots,\ a_{i,N}+f_{\ell,1},\ \cdots,\ a_{i,N}+f_{\ell,\lambda d}),$$

其中 $k\neq\ell$。我们有 $t=k-1\neq\ell-1=t'$，$\mathrm{HD}(\mathbf{v}_1,\mathbf{v}_2)=\mathrm{HD}(\mathbf{v}_1-\mathbf{v}_1,\mathbf{v}_2-\mathbf{v}_1)$。由于 A_2 是广义 Hadamard 矩阵 $D(\lambda d,\lambda d,d)$，A_2 的转置仍然是广义 Hadamard 矩阵。那么 $\{0,1\cdots,d-1\}$ 中每个元素在 $\mathbf{v}_2-\mathbf{v}_1$ 中出现 λN 次，我们得到 $\mathrm{HD}(\mathbf{v}_1,\mathbf{v}_2)=\lambda(d-1)N$。由于 $t\neq t'$，$\mathrm{HD}(\mathbf{v}_1',\mathbf{v}_2')=\lambda(d-1)N+1$。

2. 如果 $i\neq j$，那么我们可以假设

$$\mathbf{v}_1=(a_{i,1}+f_{k,1},\ a_{i,1}+f_{k,2},\ \cdots,\ a_{i,1}+f_{k,\lambda d},\ \cdots,\ a_{i,N}+f_{k,1},\ \cdots,\ a_{i,N}+f_{k,\lambda d}),$$

$$\mathbf{v}_2=(a_{j,1}+f_{\ell,1},\ a_{j,1}+f_{\ell,2},\ \cdots,\ a_{j,1}+f_{\ell,\lambda d},\ \cdots,\ a_{j,N}+f_{\ell,1},\ \cdots,\ a_{j,N}+f_{\ell,\lambda d}).$$

如果 $k=\ell$，那么 $t=k-1=\ell-1=t'$。由于 $\mathrm{MD}(A_1)=b$，我们有 $\mathrm{HD}(\mathbf{v}_1',\mathbf{v}_2')=\mathrm{HD}(\mathbf{v}_1,\mathbf{v}_2)\geqslant\lambda db$。此外，$\min\{\mathrm{HD}(\mathbf{v}_1',\mathbf{v}_2')\}_{i\neq j,k=\ell}=\lambda db$。如果 $k\neq\ell$，那么 $t=k-1\neq\ell-1=t'$。令

$$\mathbf{e}=(f_{k,1},\ f_{k,2},\ \cdots,\ f_{k,\lambda d},\ \cdots,\ f_{k,1},\ \cdots,\ f_{k,\lambda d}).$$

我们有 $\mathrm{HD}(\mathbf{v}_1, \mathbf{v}_2) = \mathrm{HD}(\mathbf{v}_1 - \mathbf{e}, \mathbf{v}_2 - \mathbf{e})$，其中

$$\mathbf{v}_1 - \mathbf{e} = (a_{i,1},\ a_{i,1},\ \cdots,\ a_{i,1},\ \cdots,\ a_{i,N},\ \cdots,\ a_{i,N}),$$

$$\begin{aligned}\mathbf{v}_2 - \mathbf{e} = (&a_{j,1} + f_{\ell,1} - f_{k,1},\ a_{j,1} + f_{\ell,2} - f_{k,2},\ \cdots,\\ &a_{j,1} + f_{\ell,\lambda d} - f_{k,\lambda d},\ \cdots,\ a_{j,N} + f_{\ell,1} - f_{k,1},\\ &a_{j,N} + f_{\ell,2} - f_{k,2},\ \cdots,\ a_{j,N} + f_{\ell,\lambda d} - f_{k,\lambda d}).\end{aligned}$$

对 $\mathbf{v}_2 - \mathbf{e}$ 进行置换，我们有

$$\begin{aligned}(\mathbf{v}_2 - \mathbf{e})' = (&a_{j,1} + 0,\ a_{j,1} + 1,\ \cdots,\ a_{j,1} + d - 1,\\ &\cdots,\ a_{j,1} + 0, a_{j,1} + 1,\ \cdots,\ a_{j,1} + d - 1,\\ &\cdots,\ a_{j,N} + 0,\ a_{j,N} + 1,\ \cdots,\ a_{j,N} + d - 1,\\ &\cdots,\ a_{j,N} + 0,\ a_{j,N} + 1,\ \cdots,\ a_{j,N} + d - 1),\end{aligned}$$

$\mathrm{HD}(\mathbf{v}_1 - \mathbf{e}, (\mathbf{v}_2 - \mathbf{e})') = \mathrm{HD}(\mathbf{v}_1 - \mathbf{e}, \mathbf{v}_2 - \mathbf{e})$。因为 $\mathrm{HD}((a_{i,1},\ a_{i,1},\ \cdots,\ a_{i,1}),\ (a_{j,1}+0,\ a_{j,1}+1,\ \cdots,\ a_{j,1} + d - 1)) = d - 1$，所以 $\mathrm{HD}(\mathbf{v}_1, \mathbf{v}_2) = \mathrm{HD}(\mathbf{v}_1 - \mathbf{e}, (\mathbf{v}_2 - \mathbf{e})') = \lambda(d-1)N$，并且 $\mathrm{HD}(\mathbf{v}_1', \mathbf{v}_2') = \lambda(d-1)N + 1$。

综上，我们有 $\mathrm{MD}(A_1') = \min\{\lambda(d-1)N + 1, \lambda d b\}$。 ∎

通过引理5.6，我们将给出 2-均匀态的一些结果。

定理 5.7　对于任何 $d \geqslant 2$，下面两种情况都成立。

(i) 对于任何 $N \geqslant 7$ 且 $N \neq 4d+2, 4d+3$，$(\mathbb{C}^d)^{\otimes N} \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中存在一个 2-均匀态；

(ii) 对于任何 $N \geqslant 5$，$(\mathbb{C}^d)^{\otimes N} \otimes \mathbb{C}^2$ 中存在一个 2-均匀态。

证明　(i) 如果 d 为素数幂，对于任何 $n \geqslant 1$，那么都存在一个广义 Hadamard 矩阵 $D(4d^n, 4d^n, d)$[126]。令引理5.6中的 $A_1 = (0, 1, \cdots, d-1)^T$，$A_2$ 为 $D(4d^n, 4d^n, d)$，那么我们得到一个

$$\mathrm{MOA}(4d^{n+1}, (4d^n)^1 d^{4d^n}, 2),\quad \text{其最小汉明距离为 } 4d^{n-1}(d-1) + 1.$$

此外通过分裂方法，我们得到一个

$$\mathrm{MOA}(4d^{n+1}, d^{4d^n+n}2^2, 2),\quad \text{其最小汉明距离大于等于 } 4d^{n-1}(d-1) + 1.$$

由引理5.4可知，对于任何 $4d^{n-1} + n + 2 \leqslant N \leqslant 4d^n + n$ 和 $n \geqslant 1$，都存在一个

$$\mathrm{IrMOA}(4d^{n+1}, d^N 2^2, 2).$$

因此，对于 $n \geqslant 1$，我们只需要考虑 $N = 4d^n + n + 1, 4d^n + n + 2$ 的情形。

对于任何 $n \geqslant 2$, 都存在一个最小汉明距离为 d^{n-1} 的 $\mathrm{OA}(d^n, d^{\frac{d^n-1}{d-1}}, 2)$[55]。令引理5.6中的 A_1 为 $\mathrm{OA}(d^n, d^{\frac{d^n-1}{d-1}}, 2)$，$A_2$ 为 $D(4d, 4d, d)$，那么我们得到一个

$$\mathrm{MOA}(4d^{n+1}, (4d)^1 d^{\frac{4d(d^n-1)}{d-1}}, 2), \quad \text{其最小汉明距离为 } 4d^n - 3.$$

通过分裂方法，我们得到一个

$$\mathrm{MOA}(4d^{n+1}, d^{\frac{4d(d^n-1)}{d-1}+1}2^2, 2), \quad \text{其最小汉明距离大于等于 } 4d^n - 3.$$

由引理5.4可知，对于任何 $\frac{4d(d^n-1)}{d-1} - 4d^n + 7 \leqslant N' \leqslant \frac{4d(d^n-1)}{d-1} + 1$ 和 $n \geqslant 2$，都存在一个

$$\mathrm{IrMOA}(4d^{n+1}, d^{N'}2^2, 2).$$

因此

$$\frac{4d(d^n-1)}{d-1} - 4d^n + 7 \leqslant 4d^n + n + 1, 4d^n + n + 2 \leqslant \frac{4d(d^n-1)}{d-1} + 1, \ n \geqslant 2,$$

对于 $n \geqslant 2$，那么都存在一个 $\mathrm{IrMOA}(4d^{n+1}, d^{4d^n+n+1}2^2, 2)$ 和一个 $\mathrm{IrMOA}(4d^{n+1}, d^{4d^n+n+2}2^2, 2)$。从而当 d 为素数幂时，都存在一个

$$\mathrm{IrMOA}(r, d^N 2^2, 2), \quad N \geqslant 7 \text{ 且 } N \neq 4d+2, 4d+3.$$

由引理5.1可知，对于任何 $N \geqslant 7$ 且 $N \neq 4d+2, 4d+3$，$(\mathbb{C}^d)^{\otimes N} \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中存在一个 2-均匀态。

注意这里有一个事实：如果 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \mathbb{C}^{d_n}$ 中存在一个 n 体 k-均匀态 $|\psi\rangle_{A_1A_2\cdots A_n}$，以及 $\mathbb{C}^{s_1} \otimes \mathbb{C}^{s_2} \otimes \cdots \mathbb{C}^{s_n}$ 中存在一个 n 体 k-均匀态 $|\phi\rangle_{B_1B_2\cdots B_n}$，那么 $|\varphi\rangle_{(A_1B_1)(A_2B_2)\cdots(A_nB_n)} = |\psi\rangle_{A_1A_2\cdots A_n} \otimes |\phi\rangle_{B_1B_2\cdots B_n}$ 是 $\mathbb{C}^{d_1s_1} \otimes \mathbb{C}^{d_2s_2} \otimes \cdots \mathbb{C}^{d_ns_n}$ 中的一个 n 体 k-均匀态[108]。

当 d' 为素数幂时，对于任何 $N \geqslant 5$，$(\mathbb{C}^{d'})^{\otimes N} \otimes \mathbb{C}^1 \otimes \mathbb{C}^1$ 中存在一个 2-均匀态[54]。通过 $(\mathbb{C}^d)^{\otimes N} \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中的 2-均匀态和 $(\mathbb{C}^{d'})^{\otimes N} \otimes \mathbb{C}^1 \otimes \mathbb{C}^1$ 中的 2-均匀态作张量积，对于任何 $d \geqslant 2$，$N \geqslant 7$ 且 $N \neq 4d+2, 4d+3$，那么我们得到 $(\mathbb{C}^d)^{\otimes N} \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ 中的一个 2-均匀态。

(ii) 如果 d 为素数幂，对于任何 $n \geqslant 1$，那么都存在一个广义 Hadamard 矩阵 $D(2d^n, 2d^n, d)$[126]。那么像 (i) 一样分析，当 d 为素数幂时，对于任何 $N \geqslant 5$ 且 $N \neq 2d+2, 2d+3$，都存在一个

$$\mathrm{IrMOA}(r, d^N 2^1, 2).$$

我们只需要考虑 $N = 2d+2, 2d+3$ 的情形。由 (i) 可知，存在一个

$$\mathrm{IrMOA}(4d^2, d^{4d+1}2^2, 2), \quad \text{其最小汉明距离大于等于 } 4d - 3.$$

那么由引理5.4可知，对于任何 $8 \leqslant N \leqslant 4d+1$，都存在一个

$$\mathrm{IrMOA}(4d^2, d^N 2^1, 2).$$

当 $d \geqslant 3$ 为素数幂时，$8 \leqslant 2d+2, 2d+3 \leqslant 4d+1$。对于任何 $N \geqslant 5$ 和 $d \geqslant 3$，那么都存在一个 $\mathrm{IrMOA}(r, d^N 2^1, 2)$，其中 d 为素数幂。此外，对于任何 $N \geqslant 5$，都存在一个 $\mathrm{IrOA}(r, 2^N 2^1, 2)$[52]。因此，当 d 为素数幂时，对于 $N \geqslant 5$，我们得到一个 $\mathrm{IrMOA}(r, d^N 2^1, 2)$。像 (i) 一样讨论，对于任何 $d \geqslant 2$ 和 $N \geqslant 5$，我们得到 $(\mathbb{C}^d)^{\otimes N} \otimes \mathbb{C}^2$ 中的一个 2 均匀态。 ∎

其他类型的广义 Hadamard 矩阵可以在文献[133-134] 中找到。令 A_2 为引理5.6中的 $D(s, N_1, d)$，则 $A_1' = (\mathbf{m}^T, A_1 \oplus A_2)$ 是一个 $\mathrm{MOA}(rs, s^1 d^{NN_1}, 2)$，其中向量 $\mathbf{m} = (m_j)_{1 \leqslant j \leqslant rs}$，$m_j = j - 1 \pmod{s}$[126]。虽然不能直接确定 A_1' 的最小汉明距离，但是我们仍然可以用它来构造不可缩短的混合正交阵列。例如，文献[134]中存在一个差矩阵 $D(15, 9, 3)$，记为 A_2。令 $A_1 = (0, 1, 2)^T$，则 $A_1' = (\mathbf{m}^T, A_1 \oplus A_2)$ 是 $\mathrm{MOA}(45, 15^1 3^9, 2)$。通过数值计算我们可以确定 $\mathrm{MD}(A_1') = 5$。因此，对于 $8 \leqslant N \leqslant 10$，我们可以在 $\mathbb{C}^5 \otimes (\mathbb{C}^3)^{\otimes N}$ 中构造一个 2-均匀态。

显然，我们可以通过结合引理5.5和引理5.6在非齐次系统中得到更多的 2-均匀态。

例 5.3　如果 t 和 N 满足以下两个情况之一，那么 $(\mathbb{C}^3)^{\otimes N} \otimes (\mathbb{C}^2)^{\otimes t}$ 中存在一个 2-均匀态:

(a) $3 \leqslant t \leqslant 4$，$N \geqslant 7$;

(b) $5 \leqslant t \leqslant 11$，$N \geqslant 6$。

我们下面证明存在性。由定理5.7 (i)，我们可以得到一个

$$\mathrm{MOA}(4d^{n+1}, (4d^n)^1 d^{4d^n}, 2), \quad \text{其最小汉明距离为 } 4d^{n-1}(d-1)+1, \text{且 } n \geqslant 1,$$

和一个

$$\mathrm{MOA}(4d^{n+1}, (4d)^1 d^{\frac{4d(d^n-1)}{d-1}}, 2), \quad \text{其最小汉明距离为 } 4d^n - 3, \text{且 } n \geqslant 2,$$

其中 d 为素数幂。通过分裂方法，我们可以得到一个

$$\mathrm{MOA}(4d^{n+1}, (4d)^1 d^{4d^n+n-1}, 2), \quad \text{其最小汉明距离大于等于 } 4d^{n-1}(d-1)+1, \text{且 } n \geqslant 1.$$

像定理5.7 (i) 一样讨论，那么当 d 为素数幂时，对于任何 $N \geqslant 6$ 且 $N \neq 4d+1, 4d+2$，都存在一个

$$\mathrm{IrMOA}(r, (4d)^1 d^N, 2). \tag{5.4}$$

由于存在一个最小汉明距离为 17 的 MOA$(72, 3^{24}24^1, 2)$[131]，通过分裂方法和引理5.4，我们得到一个

$$\text{IrMOA}(72, (12)^1 3^N, 2), \quad 11 \leqslant N \leqslant 24. \tag{5.5}$$

令公式(5.4)中的 $d = 3$，那么存在一个

$$\text{IrMOA}(r, (12)^1 3^N, 2), \quad N \geqslant 6 \text{ 且 } N \neq 13, 14. \tag{5.6}$$

由于 $11 \leqslant 13, 14 \leqslant 24$，由公式(5.5)和(5.6)可知，我们得到一个

$$\text{IrMOA}(r, (12)^1 3^N, 2), \quad N \geqslant 6. \tag{5.7}$$

例5.1给出了一个简单的 MOA$(12, 3^1 2^4, 2)$，如果删除它的最后一列，那么我们得到一个简单的 MOA$(12, 3^1 2^3, 2)$。从而我们得到一个简单的

$$\text{MOA}(12, 3^1 2^t, 2), \quad 3 \leqslant t \leqslant 4. \tag{5.8}$$

通过引理5.5并结合公式(5.7)和(5.8)，我们可以得到一个

$$\text{IrMOA}(r, 3^{N+1} 2^t, 2), \quad 3 \leqslant t \leqslant 4 \text{ 且 } N \geqslant 6.$$

此外，对于 $5 \leqslant t \leqslant 11$，由于存在一个简单的 OA$(12, 2^t, 2)$[131]，按照上面同样的方法，对于 $5 \leqslant t \leqslant 11$ 和 $N \geqslant 6$，我们得到一个 IrMOA$(r, 3^N 2^t, 2)$。

通过采用与例5.3相同的方法，我们得到了表5.1。有关简单的混合正交阵列的更多构造，可以参考文献[126,131]。

表 5.1　非齐次系统中 2-均匀态的存在性，即强度为 2 的不可缩短的混合正交阵列的存在性。通过例5.3、引理5.5和引理5.6，我们可以由第一列的 IrMOA$(r, (4d)^1 d^N, 2)$ 和第二列的简单的混合正交阵列，得到第三列的 IrMOA$(r, d^N 2^t, 2)$。

IrMOA$(r, (4d)^1 d^N, 2)$ +	简单的混合正交阵列	$\Rightarrow$ IrMOA$(r, d^N 2^t, 2)$
$d = 3, N \geqslant 6$	MOA$(12, 3^1 2^t, 2), 3 \leqslant t \leqslant 4$ OA$(12, 2^t, 2), 5 \leqslant t \leqslant 11$	$d = 3, 3 \leqslant t \leqslant 4, N \geqslant 7$ $d = 3, 5 \leqslant t \leqslant 11, N \geqslant 6$
$d = 5, N \geqslant 6, N \neq 21, 22$	MOA$(20, 5^1 2^t, 2), 3 \leqslant t \leqslant 8$ OA$(20, 2^t, 2), 5 \leqslant t \leqslant 19$	$d = 5, 3 \leqslant t \leqslant 4, N \geqslant 7, N \neq 22, 23$ $d = 5, 5 \leqslant t \leqslant 8, N \geqslant 6, N \neq 22$ $d = 5, 9 \leqslant t \leqslant 19, N \geqslant 6, N \neq 21, 22$
$d = 7, N \geqslant 6, N \neq 29, 30$	MOA$(28, 7^1 2^t, 2), 3 \leqslant t \leqslant 12$ OA$(28, 2^t, 2), 6 \leqslant t \leqslant 27$	$d = 7, 3 \leqslant t \leqslant 5, N \geqslant 7, N \neq 30, 31$ $d = 7, 6 \leqslant t \leqslant 12, N \geqslant 6, N \neq 30$ $d = 7, 13 \leqslant t \leqslant 27, N \geqslant 6, N \neq 29, 30$

5.3.3　非齐次系统中的 3-均匀态的构造

文献[107]提出了一个公开问题：非齐次系统中是否存在 3-均匀态？我们将在本小节给出肯定的回答。

令 S 为 d 阶加法群，$S^k := \{(x_1, x_2, \cdots, x_k) \mid x_i \in S, 1 \leqslant i \leqslant k\}$ 为 d^k 阶加法群, 其加法为向量的加法。令 $S_0^k = \{(x_1, x_2, \cdots, x_k) : x_1 = x_2 = \cdots = x_k \in S\}$, 那么 S_0^k 为 S^k 的 d 阶加法子群。我们记 S_0^k 在 S^k 中的陪集为 S_i^k，$i = 0, 1, \cdots, d^{k-1} - 1$, 其中陪集的每个元素都是这个陪集的代表元。对于一个 $s \times N$ 的矩阵 $\boldsymbol{D}$，其元素取自于 S，如果从这个矩阵中任意选取 k 列形成一个子矩阵，这个子矩阵的每行看成陪集的代表元，每个陪集的代表元在这个子矩阵中出现的次数相同，那么 $\boldsymbol{D}$ 被称为*强度为 k 的差矩阵*[126]，并记为 $\boldsymbol{D}_k(s, N, d)$。当 $k = 2$ 时，很容易验证 $\boldsymbol{D}_2(s, N, d)$ 就是 $\boldsymbol{D}(s, N, d)$。

一个 Hadamard 矩阵 $\boldsymbol{H}_m$ 是一个 $m \times m$ 的矩阵, 其中元素取自于 $\{+1, -1\}$, 并满足 $\boldsymbol{H}_m^T \boldsymbol{H}_m = m\mathbb{I}_m$[126]。Hadamard 矩阵可以构造强度为 2 和 3 的差矩阵。如果我们将 $\boldsymbol{H}_m$ 中的 -1 替换为 0, 那么 $\boldsymbol{H}_m$ 是 $\mathbb{Z}_2$ 上的 $\boldsymbol{D}(m, m, 2)$, 也是 $\boldsymbol{D}_3(m, m, 2)$[135]。例如,

$$\boldsymbol{H}_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

是一个 4 阶 Hadamard 矩阵, 将 $\boldsymbol{H}_4$ 中的 -1 替换为 0, 那么我们得到一个 $\boldsymbol{D}(4, 4, 2)$, 它也是 $\boldsymbol{D}_3(4, 4, 2)$。其它 Hadamard 矩阵可以参考文献[126,134]。$\boldsymbol{D}_3(s, N, d)$ 可以用来构造强度为 3 的混合正交阵列。

引理 5.8　假设 $(\boldsymbol{A}_1, \boldsymbol{A}_2)$ 是 $\mathrm{MOA}(r, d^{n_1} 2^{n_2}, 3)$，且 $\mathrm{MD}(\boldsymbol{A}_2) = b$，其中 $\boldsymbol{A}_1$ 由混合正交阵列的前 n_1 列组成，$\boldsymbol{A}_2$ 由其最后 n_2 列组成。假设 $\boldsymbol{D}$ 为 $\boldsymbol{D}_3(m, N, d)$, $\boldsymbol{H}_m$ 为 m 阶 Hadamard 矩阵，则 $(\boldsymbol{A}_1 \oplus \boldsymbol{D}, \boldsymbol{A}_2 \oplus \boldsymbol{H}_m)$ 是 $\mathrm{MOA}(rm, d^{n_1 N} 2^{n_2 m}, 3)$，且 $\mathrm{MD}(\boldsymbol{A}_2 \oplus \boldsymbol{H}_m) = \min\{\frac{m}{2} n_2, mb\}$。

证明　$\mathrm{MOA}(rm, d^{n_1 N} 2^{n_2 m}, 3)$ 的构造来自于文献[135]，我们只需要证明 $\mathrm{MD}(\boldsymbol{A}_2 \oplus \boldsymbol{H}_m) = \min\{\frac{m}{2} n_2, mb\}$。由于 Hadamard 矩阵也是一个广义 Hadamard 矩阵，像引理5.6一样讨论，我们可以得到 $\mathrm{MD}(\boldsymbol{A}_2 \oplus \boldsymbol{H}_m) = \min\{\frac{m}{2} n_2, mb\}$。 ∎

现在，根据引理5.8，我们可以构造非齐次系统中的 3-均匀态。

定理 5.9　对于任何 $n \geqslant 1$，有:

(i) 对于任何 $0 \leqslant N \leqslant 4^n$ 和 $7 \times 36^n + 4 \leqslant t \leqslant 9 \times 36^n$，$(\mathbb{C}^3)^{\otimes N} \otimes (\mathbb{C}^2)^{\otimes t}$ 中存在一个 3-均匀态;

(ii) 对于任何 $0 \leqslant N \leqslant 6^n$ 和 $5 \times 100^n + 4 \leqslant t \leqslant 6 \times 100^n$，$(\mathbb{C}^5)^{\otimes N} \otimes (\mathbb{C}^2)^{\otimes t}$ 中存在一个 3-均匀态。

证明　(i) 令 $(\boldsymbol{A}_1, \boldsymbol{A}_2)$ 为 $\mathrm{MOA}(48, 3^1 2^9, 3)$，其中 $\boldsymbol{A}_1$ 为第 1 列，$\boldsymbol{A}_2$ 为最后 9

列，且 $\mathrm{MD}(A_2)=2$[136]。此外，一个 $D_3(36,4,3)$（记为 D）和一个 Hadamard 矩阵 H_{36} 可以在文献[136]中找到。那么根据引理5.8可知，

$$(A_1\oplus D, A_2\oplus H_{36})$$

是一个

$$\mathrm{MOA}(48\times 36, 3^4 2^{9\times 36}, 3).$$

其中 $\mathrm{MD}(A_2\oplus H_{36})=\min\{9\times 18, 2\times 36\}=2\times 36$。令 $B_1=A_1\oplus D\oplus\cdots\oplus D$，$B_2=A_2\oplus H_{36}\oplus\cdots\oplus H_{36}$，其中 D 和 H_{36} 分别重复 n 次。通过重复使用引理5.8 n 次，则 (B_1,B_2) 是一个

$$\mathrm{MOA}(48\times 36^n, 3^{4^n}2^{9\times 36^n}, 3),$$

其中 $\mathrm{MD}(B_2)=\min\left\{\frac{9\times 36^n}{2}, 2\times 36^n\right\}=2\times 36^n$。对于任何矩阵 B，令 $B-\{t\}$ 为从 B 中删去任意 t 列后的矩阵。由于 $\mathrm{MD}(B_2)=2\times 36^n$，对于任何 $0\leqslant t\leqslant 2\times 36^n-4$，我们可以从 B_2 中删去任意 t 列，使得 $\mathrm{MD}(B_2-\{t\})\geqslant 4$。此外，对于任何 $0\leqslant N\leqslant 4^n$，我们从 B_1 中删去任意 N 列，仍然有

$$\mathrm{MD}(B_1-\{N\}, B_2-\{t\})\geqslant \mathrm{MD}(B_2-\{t\})\geqslant 4.$$

从而对任意 $0\leqslant N\leqslant 4^n$ 和 $0\leqslant t\leqslant 2\times 36^n-4$，我们得到一个

$$\mathrm{MOA}(48\times 36^n, 3^{4^n-N}2^{9\times 36^n-t}, 3),\quad \text{其最小汉明距离大于等于 4.}$$

根据引理 5.3，对于任何 $0\leqslant N\leqslant 4^n$ 和 $7\times 36^n+4\leqslant t\leqslant 9\times 36^n$，都存在 $\mathrm{IrMOA}(r, 3^N 2^t, 3)$，再根据引理5.1，$(\mathbb{C}^3)^{\otimes N}\otimes(\mathbb{C}^2)^{\otimes t}$ 中存在一个 3-均匀态。

(ii) 由于存在一个 $\mathrm{MOA}(40, 5^1 2^6, 3)$，用矩阵 (A_1, A_2) 表示，其中 $\mathrm{MD}(A_2)=1$[132]，也存在一个 $D_3(100,6,5)$[135]和一个 Hadamard 矩阵 H_{100}[131]，像 (i) 一样讨论，对于任何 $0\leqslant N\leqslant 6^n$，$5\times 100^n+4\leqslant t\leqslant 6\times 100^n$ 和 $n\geqslant 1$，我们可以得到 $(\mathbb{C}^5)^{\otimes N}\otimes(\mathbb{C}^2)^{\otimes t}$ 中的 3-均匀态。 ∎

定理5.9中得到的最小情况是 $(\mathbb{C}^3)\otimes(\mathbb{C}^2)^{\otimes 256}$ 中的 3-均匀态，即 $\mathrm{IrMOA}(1728, 3^1 2^{256}, 3)$。由于这个混合正交阵列非常大，为了方便读者，我们在网站[136]中列出了这个 $\mathrm{IrMOA}(1728, 3^1 2^{256}, 3)$ 及其构造细节，并列出了一个 Matlab 程序，以此来检查其正确性。有关强度为 3 的混合正交阵列和强度为 3 的差矩阵的更多构造，请参考文献[132,135,137-138]。

5.3.4　从 k-均匀态到 $(k-1)$-均匀态的构造方法

在本小节中，我们将给出两种从非齐次系统中的 k-均匀态到 $(k-1)$-均匀态的构造方法。注意 $d_1, d_2, d_3, \cdots, d_N$ 在本小节中不是按照从大到小的方式排列的。第一个方法由文献[52,54]的启发得到。

引理 5.10　假设 $|\psi\rangle$ 是 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个 k-均匀态, 则它可以表示为 $|\psi\rangle=\frac{1}{\sqrt{d_1}}\sum_{j\in\mathbb{Z}_{d_1}}|j\rangle|\phi_j\rangle$。对于任何标准化向量 $\mathbf{v}=(\alpha_0,\alpha_1,\cdots,\alpha_{d_1-1})\in\mathbb{C}^{d_1}$ (即 $\sum_{j\in\mathbb{Z}_{d_1}}|\alpha_i|^2=1$)，我们得到

$$|\psi(\mathbf{v})\rangle=\sum_{j\in\mathbb{Z}_{d_1}}\alpha_j|\phi_j\rangle$$

是 $\mathbb{C}^{d_2}\otimes\mathbb{C}^{d_3}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个 $(k-1)$ 均匀态。

证明　我们选择任意 $(k-1)$ 个子系统 $\{A_{i_2},A_{i_3},\cdots,A_{i_k}\}$ 并使得 $A_1\notin\{A_{i_2},A_{i_3},\cdots,A_{i_k}\}$。由于 $|\psi\rangle$ 是 k-均匀态，我们得到 $\rho_{\{A_1,A_{i_2},A_{i_3},\cdots,A_{i_k}\}}=\frac{1}{d_1d_{i_2}\cdots d_{i_k}}\sum_{(j_1,j_{i_2},\cdots,j_{i_k})\in\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_{i_2}}\times\cdots\times\mathbb{Z}_{d_{i_k}}}|j_1,j_{i_2},\cdots,j_{i_k}\rangle\langle j_1,j_{i_2},\cdots,j_{i_k}|$。那么我们有

$$|\psi\rangle=\sum_{(j_1,j_{i_2},\cdots,j_{i_k})\in\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_{i_2}}\times\cdots\times\mathbb{Z}_{d_{i_k}}}c_{j_1,j_{i_2},\cdots,j_{i_k}}|j_1,j_{i_2},\cdots,j_{i_k}\rangle|\psi(j_1,j_{i_2},\cdots,j_{i_k})\rangle,\quad(5.9)$$

其中 $|c_{j_1,j_{i_2},\cdots,j_{i_k}}|=\frac{1}{\sqrt{d_1d_{i_2}\cdots d_{i_k}}}$，且

$$\langle\psi(j_1,j_{i_2},\cdots,j_{i_k})|\psi(j_1',j_{i_2}',\cdots,j_{i_k}')\rangle=\delta_{j_1,j_1'}\delta_{j_{i_2},j_{i_2}'}\cdots\delta_{j_{i_k},j_{i_k}'}.\quad(5.10)$$

根据公式(5.9)可知

$$|\phi_{j_1}\rangle=\sqrt{d_1}\sum_{(j_{i_2},\cdots,j_{i_k})\in\mathbb{Z}_{d_{i_2}}\times\cdots\times\mathbb{Z}_{d_{i_k}}}c_{j_1,j_{i_2},\cdots,j_{i_k}}|j_{i_2},\cdots,j_{i_k}\rangle|\psi(j_1,j_{i_2},\cdots,j_{i_k})\rangle.$$

接下来,

$$|\psi(\mathbf{v})\rangle=\sum_{j_1\in\mathbb{Z}_{d_1}}\alpha_{j_1}|\phi_{j_1}\rangle=\sum_{(j_1,j_{i_2},\cdots,j_{i_k})\in\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_{i_2}}\times\cdots\times\mathbb{Z}_{d_{i_k}}}\sqrt{d_1}\alpha_{j_1}\times$$

$$c_{j_1,j_{i_2},\cdots,j_{i_k}}|j_{i_2},\cdots,j_{i_k}\rangle|\psi(j_1,j_{i_2},\cdots,j_{i_k})\rangle.$$

通过公式(5.10)可知，$|\psi(\mathbf{v})\rangle$ 在 $\{A_{i_2},A_{i_3},\cdots,A_{i_k}\}$ 上的约化密度算子为

$$\begin{aligned}\rho_{\{A_{i_2},A_{i_3},\cdots,A_{i_k}\}}=&\frac{1}{d_{i_2}\cdots d_{i_k}}\sum_{(j_1,j_{i_2},\cdots,j_{i_k})\in\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_{i_2}}\times\cdots\times\mathbb{Z}_{d_{i_k}}}|\alpha_{j_1}|^2|j_{i_2},\cdots,j_{i_k}\rangle\langle j_{i_2},\cdots,j_{i_k}|\\=&\frac{1}{d_{i_2}\cdots d_{i_k}}\sum_{(j_{i_2},\cdots,j_{i_k})\in\mathbb{Z}_{d_{i_2}}\times\cdots\times\mathbb{Z}_{d_{i_k}}}|j_{i_2},\cdots,j_{i_k}\rangle\langle j_{i_2},\cdots,j_{i_k}|.\end{aligned}$$

引理得证。∎

回顾公式(5.2)在 $\mathbb{C}^4\otimes(\mathbb{C}^2)^{\otimes4}$ 中给出的一个 2-均匀态 $|\psi\rangle$，如果我们考虑子系统 A_1，那么根据引理5.10，$|\psi(\mathbf{v})\rangle=\sum_{j\in\mathbb{Z}_4}\alpha_j|\phi_j\rangle$ 是 $(\mathbb{C}^2)^{\otimes4}$ 中的一个 1-均匀态，其中 $|\phi_0\rangle=\frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)$，$|\phi_1\rangle=\frac{1}{\sqrt{2}}(|0011\rangle+|1100\rangle)$，$|\phi_2\rangle=$

$\frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle)$，$|\phi_3\rangle = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)$，且 $\sum_{j\in\mathbb{Z}_4} |\alpha_j|^2 = 1$。如果我们考虑子系统 A_5，那么根据引理5.10，$|\psi(\mathbf{v})\rangle = \sum_{j\in\mathbb{Z}_2} \beta_j |\phi_j'\rangle$ 是 $\mathbb{C}^4 \otimes (\mathbb{C}^2)^{\otimes 3}$ 中的一个 1-均匀态，其中 $|\phi_0'\rangle = \frac{1}{2}(|0000\rangle + |1110\rangle + |2101\rangle + |3011\rangle)$，$|\phi_1'\rangle = \frac{1}{2}(|0111\rangle + |1001\rangle + |2010\rangle + |3100\rangle)$，且 $\sum_{j\in\mathbb{Z}_2} |\beta_j|^2 = 1$。下面我们介绍第 2 种方法。

引理 5.11　假设 $|\psi\rangle$ 是 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 k-均匀态，那么 $|\psi\rangle$ 也是 $\mathbb{C}^{d_1 d_2} \otimes \mathbb{C}^{d_3} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 $(k-1)$-均匀态。

证明　如果我们将 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ 中的向量视为 $\mathbb{C}^{d_1 d_2}$ 中的向量，那么通过验证公式5.1可知，$|\psi\rangle$ 是 $\mathbb{C}^{d_1 d_2} \otimes \mathbb{C}^{d_3} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 $(k-1)$-均匀态。 ∎

特别地，我们可以通过引理5.11从齐次系统中的 k-均匀态构造非齐次系统中的 $(k-1)$-均匀态。例如，由于在 $(\mathbb{C}^3)^{\otimes 10}$ 中存在一个绝对最大纠缠态[64]，根据引理5.11，$\mathbb{C}^9 \otimes (\mathbb{C}^3)^{\otimes 8}$ 中存在一个 4-均匀态，同样它也是 $\mathbb{C}^9 \otimes (\mathbb{C}^3)^{\otimes 8}$ 中的一个绝对最大纠缠态。

5.4　非齐次系统中的绝对最大纠缠态

在本节中，我们将给出一些非齐次系统中的绝对最大纠缠态的不存在性结果。齐次系统中的绝对最大纠缠态引起了很多研究者的关注[51,62-63,65,106]，但是关于非齐次系统中的绝对最大纠缠态的结果很少。文献[108] 中研究了三体非齐次系统中的绝对最大纠缠态。对于 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的绝对最大纠缠态，其定义与齐次系统中的绝对最大纠缠态相同，它要求这个态在任意 $\lfloor \frac{N}{2} \rfloor$ 体上的约化密度算子是最大混合的，这是我们在本文中关注的定义。在 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中还有另一种绝对最大纠缠态的定义，即对于任意 $1 \leqslant s \leqslant N-1$，选取任意 $\{i_1, i_2, \cdots, i_s\}$，且 $d_{i_1} d_{i_2} \cdots d_{i_s} \leqslant \frac{d_1 d_2 \cdots d_N}{d_{i_1} d_{i_2} \cdots d_{i_s}}$，使得 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个态在 $\{i_1, i_2, \cdots, i_s\}$ 上的约化密度算子是最大混合的[106]。

对于 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的绝对最大纠缠态，如果 $d_1, d_2, \cdots, d_N$ 不完全相同，由于 $d_1 \cdots d_{\lfloor \frac{N}{2} \rfloor} \leqslant d_{\lfloor \frac{N}{2} \rfloor + 1} \cdots d_N$，$N$ 一定是奇数。除了三体非齐次系统中的绝对最大纠缠态之外，$N \geqslant 5$ 时的绝对最大纠缠态的示例很少。公式(5.2)给出的态是 $\mathbb{C}^4 \otimes (\mathbb{C}^2)^{\otimes 4}$ 中的绝对最大纠缠态。由于存在最小汉明距离为 4 的 $\mathrm{OA}(16, 4^5, 2)$[55,126]，通过分裂方法，我们可以得到最小汉明距离大于等于 4 的 $\mathrm{MOA}(16, 4^4 2^2, 2)$。然后通过引理 5.4，我们可以得到一个 $\mathrm{IrMOA}(16, 4^3 2^2, 2)$ 和一个 $\mathrm{IrMOA}(16, 4^4 2^1, 2)$，它们分别可以推出 $(\mathbb{C}^4)^{\otimes 3} \otimes (\mathbb{C}^2)^{\otimes 2}$ 和 $(\mathbb{C}^4)^{\otimes 4} \otimes \mathbb{C}^2$ 中的绝对最大纠缠态。进一步地，由引理5.11可知，如果 $(\mathbb{C}^d)^{\otimes N}$ 中存在一个绝对最大纠缠态，N 是偶数，那么在 $\mathbb{C}^{d^2} \otimes (\mathbb{C}^d)^{\otimes (N-2)}$ 中也存在一个绝对最大纠缠态。

如果非齐次系统中至少有两个局部维数互素时，那么这个非齐次系统被称为*真实非齐次系统*[107]。上面提到的大部分绝对最大纠缠态所在的非齐次系统不是真实非齐次系统。在文献[110]中，当 $n=0$，或者 $m=kn$，$k\geqslant 1$ 时，$\mathbb{C}^2\otimes\mathbb{C}^m\otimes\mathbb{C}^{m+n}$ 中存在绝对最大纠缠态，而当 m 或 n 为奇数时，这个非齐次系统是真实非齐次系统。对于 $N\geqslant 5$，N 体真实非齐次系统中构造绝对最大纠缠态是具有挑战性的，我们留待进一步研究。接下来，我们给出一些非齐次系统中的绝对最大纠缠态的不存在性结果。

表 5.2　非齐次系统中的绝对最大纠缠态的不存在性结果。例如 $\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes 8}$ 意味着 $\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes 8}$ 中不存在绝对最大纠缠态。

9 体	11 体	13 体
$\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes 8}$	$\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes 10}$	$(\mathbb{C}^3)^{\otimes n}\otimes(\mathbb{C}^2)^{\otimes(13-n)}$, $n=1,11,12$
$(\mathbb{C}^3)^{\otimes 7}\otimes(\mathbb{C}^2)^{\otimes 2}$	$\mathbb{C}^4\otimes(\mathbb{C}^2)^{\otimes 10}$	$\mathbb{C}^4\otimes(\mathbb{C}^2)^{\otimes 12}$
$\mathbb{C}^4\otimes(\mathbb{C}^2)^{\otimes 8}$		$(\mathbb{C}^4)^{\otimes n}\otimes(\mathbb{C}^3)^{\otimes(13-n)}$, $n=1,2,3$
$\mathbb{C}^4\otimes(\mathbb{C}^3)^{\otimes 6}\otimes(\mathbb{C}^2)^{\otimes 2}$		$(\mathbb{C}^5)^{\otimes n}\otimes(\mathbb{C}^3)^{\otimes(13-n)}$, $n=1,2$
		$\mathbb{C}^d\otimes(\mathbb{C}^3)^{\otimes 12}$, $d=6,7,8,9$
		$(\mathbb{C}^4)^{\otimes n_1}\otimes(\mathbb{C}^3)^{\otimes n_2}\otimes(\mathbb{C}^2)^{\otimes(13-n_1-n_2)}$, $(n_1,n_2)=(1,10),(1,11),(2,10)$
		$(\mathbb{C}^5)^{\otimes n_1}\otimes(\mathbb{C}^4)^{\otimes n_2}\otimes(\mathbb{C}^3)^{\otimes(13-n_1-n_2)}$, $(n_1,n_2)=(1,1),(1,2)$
		$\mathbb{C}^5\otimes(\mathbb{C}^3)^{\otimes 11}\otimes\mathbb{C}^2$
		$\mathbb{C}^6\otimes\mathbb{C}^4\otimes(\mathbb{C}^3)^{\otimes 11}$

在文献[106]中，作者通过影子不等式给出了一些齐次系统中的绝对最大纠缠态的不存在性结果。受到这个想法的启发，我们也可以证明某些非齐次系统中不存在绝对最大纠缠态。假设在 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中存在绝对最大纠缠态，其中 N 是奇数，那么有影子不等式成立：对于任何 $0\leqslant j\leqslant N$，有

$$S_j=\sum_{k=0}^{N}K_{N-j}(k;N)A'_k\geqslant 0, \tag{5.11}$$

其中 $K_{N-j}(k;N)=\sum_\alpha(-1)^\alpha\binom{N-k}{N-j-\alpha}\binom{k}{\alpha}$，$A'_0=1$，对于任何 $1\leqslant k\leqslant\frac{N-1}{2}$，有 $A'_k=\sum_{\{i_1,i_2,\cdots,i_k\}\subset\{1,2,\cdots,N\}}\frac{1}{d_{i_1}d_{i_2}\cdots d_{i_k}}$，$A'_k=A'_{N-k}$。特别地，如果 $d_1=d_2=\cdots=d_N=d$，那么 $A'_k=\binom{N}{k}d^{-\min(k,N-k)}$。

我们的主要思想是证明影子不等式不成立，首先我们给出一个例子。

引理 5.12　$\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes 8}$ 中不存在绝对最大纠缠态。

证明　对于 $2\leqslant i\leqslant 8$，$d_1=3$，$d_i=2$，我们可以计算出 $A'_0=1$，$A'_1=\frac{13}{3}$，$A'_2=\frac{25}{3}$，$A'_3=\frac{28}{3}$，$A'_4=\frac{161}{24}$，且对于 $5\leqslant j\leqslant 9$，$A'_j=A'_{9-j}$。此外 $K_8(0,9)=9$，$K_8(1,9)=-7$，$K_8(2,9)=5$，$K_8(3,9)=-3$，$K_8(4,9)=1$，且对于 $5\leqslant k\leqslant 9$，

$K_8(k,9)=K_8(9-k,9)$。那么我们有

$$S_1=\sum_{k=0}^{9}K_8(k,9)A'_k=-\frac{23}{12}<0.$$

从而影子不等式不成立，引理得证。 ∎

通过数值计算，我们在表5.2中列出了 9，11 和 13 体非齐次系统中的绝对最大纠缠态的不存在性。当 $N\leqslant 7$ 时，我们的策略不能轻易地给出 N 体非齐次系统中的绝对最大纠缠态的不存在性结果。以 $\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes n}$ 为例，首先，$\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes 2}$ 中的绝对最大纠缠态存在[107]；其次，当 $n=4$ 或 6 时，用引理5.12中的方法并不能确定 $\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes n}$ 中的绝对最大纠缠态的不存在性。事实上，通过数值计算，当 $n=4$ 时，我们可以得到

$$[S_0\ S_1\ S_2\ S_3\ S_4\ S_5]=[0\quad 0.333\quad 0\quad 20.667\quad 0\quad 11],$$

当 $n=6$ 时，我们可以得到

$$[S_0\ S_1\ S_2\ S_3\ S_4\ S_5\ S_6\ S_7]=[0\quad 1.667\quad 0\quad 11.667\quad 0\quad 89\quad 0\quad 25.667].$$

影子不等式都成立，从而当 $n=4$ 或 6 时，我们得不到 $\mathbb{C}^3\otimes(\mathbb{C}^2)^{\otimes n}$ 中的绝对最大纠缠态的不存在性结果。

5.5　量子纠错码与量子信息掩盖之间的关系

在本节中，我们将给出量子纠错码与量子信息掩盖之间的关系。我们将证明文献[89] 中的不可掩盖定理实际上是非齐次系统中量子纠错码的量子 Singleton 界的一个特例，并基于这个量子 Singleton 界，我们将给出更一般的不可掩盖定理。我们也将回答文献[111]中提出的两个公开问题。令 $\mathbb{I}_{d_{j_1},d_{j_2},\cdots,d_{j_k}}$ 为作用在空间 $\mathbb{C}^{d_{j_1}}\otimes\mathbb{C}^{d_{j_2}}\otimes\cdots\otimes\mathbb{C}^{d_{j_k}}$ 上的单位算子。首先我们证明参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码对应于 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中一类特殊的子空间。

引理 5.13　令 $\mathcal{Q}$ 为 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个 K 维子空间。如果 $\mathcal{Q}$ 是一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码，那么对于任意 k 体子系统，$\mathcal{Q}$ 中所有态在这 k 体上的约化密度算子是相等的，反之亦然。此外，如果 $\mathcal{Q}$ 是纯量子纠错码，那么 $\mathcal{Q}$ 中任意一个态都是 k-均匀态，反之亦然。

证明　“⇒”假设 $\mathcal{Q}$ 是一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码，对

于任何 $|\psi\rangle \in \mathcal{Q}$，根据公式(5.3)可知，

$$\begin{aligned}|\psi\rangle\langle\psi| =&\frac{1}{d_1 d_2 \cdots d_N}\mathbb{I}_{d_1,d_2,\cdots,d_N} + \frac{1}{d_1 d_2 \cdots d_N}\sum_{1\leqslant wt(E_\alpha)\leqslant k}\mathrm{Tr}(E_\alpha^\dagger|\psi\rangle\langle\psi|)E_\alpha \\ &+ \frac{1}{d_1 d_2 \cdots d_N}\sum_{wt(E_\alpha)\geqslant k+1}\mathrm{Tr}(E_\alpha^\dagger|\psi\rangle\langle\psi|)E_\alpha \\ =&\frac{1}{d_1 d_2 \cdots d_N}\mathbb{I}_{d_1,d_2,\cdots,d_N} + \frac{1}{d_1 d_2 \cdots d_N}\sum_{1\leqslant wt(E_\alpha)\leqslant k}\overline{\langle\psi|E_\alpha|\psi\rangle}E_\alpha \\ &+ \frac{1}{d_1 d_2 \cdots d_N}\sum_{wt(E_\alpha)\geqslant k+1}\overline{\langle\psi|E_\alpha|\psi\rangle}E_\alpha,\end{aligned} \tag{5.12}$$

其中 $\overline{\langle\psi|E_\alpha|\psi\rangle}$ 是 $\langle\psi|E_\alpha|\psi\rangle$ 的复共轭。对于任意子集 $S = \{j_1, j_2, \cdots, j_k\} \subset \{1, 2, \cdots, N\}$ 且 $|S| = k$，我们有

$$\begin{aligned}\mathrm{Tr}_{S^c}|\psi\rangle\langle\psi| =&\frac{1}{d_{j_1} d_{j_2} \cdots d_{j_k}}\mathbb{I}_{d_{j_1},d_{j_2},\cdots,d_{j_k}} \\ &+ \frac{1}{d_1 d_2 \cdots d_N}\sum_{1\leqslant wt(E_\alpha)\leqslant k}\overline{\langle\psi|E_\alpha|\psi\rangle}\mathrm{Tr}_{S^c}(E_\alpha) \\ =&\frac{1}{d_{j_1} d_{j_2} \cdots d_{j_k}}\mathbb{I}_{d_{j_1},d_{j_2},\cdots,d_{j_k}} \\ &+ \frac{1}{d_1 d_2 \cdots d_N}\sum_{1\leqslant wt(E_\alpha)\leqslant k,\ supp(E_\alpha)\subset S}\overline{C(E_\alpha)}\mathrm{Tr}_{S^c}(E_\alpha).\end{aligned}$$

注意当我们对 $|\psi\rangle\langle\psi|$ 进行偏迹运算时，公式(5.12)中的第三项消失了。这是因为当 $wt(E_\alpha) \geqslant k+1$ 时，如果 E_α 在 S^c 上进行偏迹运算，那么必然会对一个其中非单位算子 $e_{\alpha_j}^{(j)}$ 求迹，从而 $\mathrm{Tr}_{S^c}(E_\alpha) = 0$。由定义5.8可知，$C(E_\alpha)$ 是一个仅依赖于 E_α 的常数，那么对于所有的 $|\psi\rangle \in \mathcal{Q}$，$\mathrm{Tr}_{S^c}|\psi\rangle\langle\psi|$ 都是相等的。

特别地，如果 $\mathcal{Q}$ 是纯量子纠错码，那么对于 $0 < wt(E_\alpha) < k+1$，$C(E_\alpha) = 0$。这意味着 $\mathrm{Tr}_{S^c}|\psi\rangle\langle\psi| = \frac{1}{d_{j_1} d_{j_2} \cdots d_{j_k}}\mathbb{I}_{d_{j_1},d_{j_2},\cdots,d_{j_k}}$，即 $|\psi\rangle$ 是 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中的一个 k-均匀态。

“$\Leftarrow$”对于一个 $wt(E_\alpha) < k+1$ 的错误算子 $E_\alpha \in \mathcal{E}$，那么必然存在一个子集 $S = \{j_1, j_2, \cdots, j_k\} \subset \{1, 2, \cdots, N\}$，且 $|S| = k$，使得 $supp(E_\alpha) \subset S$。对于一个乘积算子 $P = P_1 \otimes P_2 \otimes \cdots \otimes P_N$，其中 P_i 作用在 $\mathbb{C}^{d_i}$ 上，$1 \leqslant i \leqslant N$，那么我们有

$$\mathrm{Tr}(PE_\alpha) = \frac{d_{j_1} d_{j_2} \cdots d_{j_k}}{d_1 d_2 \cdots d_N}\mathrm{Tr}_S(\mathrm{Tr}_{S^c} P \cdot \mathrm{Tr}_{S^c} E_\alpha). \tag{5.13}$$

对于任意的 $|\psi\rangle \in \mathcal{Q}$，根据公式(5.3)，算子 $|\psi\rangle\langle\psi|$ 可以被分解为一些乘积算子的求和。根据公式(5.13)和偏迹运算的线性性，我们有

$$\langle\psi|E_\alpha|\psi\rangle = \mathrm{Tr}(|\psi\rangle\langle\psi|E_\alpha) = \frac{d_{j_1} d_{j_2} \cdots d_{j_k}}{d_1 d_2 \cdots d_N}\mathrm{Tr}_S(\mathrm{Tr}_{S^c}|\psi\rangle\langle\psi| \cdot \mathrm{Tr}_{S^c} E_\alpha).$$

对于任何 $|\psi\rangle$，由于 $\mathrm{Tr}_{S^c}|\psi\rangle\langle\psi|$ 都是相等的，我们推出

$$\langle\psi|E_\alpha|\psi\rangle = \frac{d_{j_1}d_{j_2}\cdots d_{j_k}}{d_1d_2\cdots d_N}\mathrm{Tr}_S(\mathrm{Tr}_{S^c}|\psi\rangle\langle\psi|\cdot\mathrm{Tr}_{S^c}E_\alpha) = C(E_\alpha),$$

其中 $C(E_\alpha)$ 是一个仅依赖于 E_α 的常数。由定义5.8可知，$\mathcal{Q}$ 是一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码。

特别地，如果 $|\psi\rangle$ 是 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个 k-均匀态，那么 $\mathrm{Tr}_{S^c}|\psi\rangle\langle\psi| = \frac{1}{d_{j_1}d_{j_2}\cdots d_{j_k}}\mathbb{I}_{d_{j_1},d_{j_2},\cdots,d_{j_k}}$。对于 $0<wt(E_\alpha)<k+1$，我们有

$$\langle\psi|E_\alpha|\psi\rangle = \frac{1}{d_1d_2\cdots d_N}\mathrm{Tr}_S(\mathrm{Tr}_{S^c}E_\alpha) = \frac{1}{d_1d_2\cdots d_N}\mathrm{Tr}(E_\alpha) = C(E_\alpha) = 0,$$

从而根据定义5.8可知，$\mathcal{Q}$ 是一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的纯量子纠错码。∎

引理5.13也可以被看作是量子纠错码的定义[139]。现在我们给出一些量子纠错码的例子。

例 5.4　(i) 令 $\{|i_Q\rangle\}_{i\in\mathbb{Z}_3}$ 为 $\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^2$ 中子空间 $\mathcal{Q}$ 的一组标准正交基，其中

$$\begin{aligned}
|0_Q\rangle =& \frac{1}{\sqrt{6}}(|00000\rangle+|12111\rangle+|01210\rangle+|22021\rangle+|10220\rangle+|21101\rangle),\\
|1_Q\rangle =& \frac{1}{\sqrt{6}}(|21020\rangle+|02201\rangle+|11100\rangle+|20211\rangle+|12010\rangle+|00121\rangle),\\
|2_Q\rangle =& \frac{1}{\sqrt{6}}(|20110\rangle+|11221\rangle+|02120\rangle+|10001\rangle+|22200\rangle+|01011\rangle).
\end{aligned}$$

通过计算，对于任意的单位向量 (v_0,v_1,v_2)，我们可以发现 $\sum_{i\in\mathbb{Z}_3}v_i|i_Q\rangle$ 是 $\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^3\otimes\mathbb{C}^2$ 中的一个 2-均匀态，那么根据引理5.13可知，$\mathcal{Q}$ 是一个参数为 $((5,3,3))_{3,3,3,3,2}$ 的纯量子纠错码。

(ii) 令 $\{|i_Q\rangle\}_{i\in\mathbb{Z}_2}$ 为 $(\mathbb{C}^2)^{\otimes 9}$ 中子空间 $\mathcal{Q}$ 的一组标准正交基，其中

$$\begin{aligned}
|0_Q\rangle =& \frac{1}{\sqrt{8}}(|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle),\\
|1_Q\rangle =& \frac{1}{\sqrt{8}}(|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle).
\end{aligned}$$

那么 $\mathcal{Q}$ 是 Shor 提出的 9-比特码[73,140]，即是一个参数为 $((9,2,3))_2$ 的非纯量子纠错码。我们可以验证 $|0_Q\rangle$ 在前两体上的约化密度算子为 $\frac{1}{2}(|00\rangle\langle 00|+|11\rangle\langle 11|)$，这并不和单位算子成比例。

对于一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码 $\mathcal{Q}$ 来说，它可以将 $\mathbb{C}^K$ 中所有态编码到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 的子空间 $\mathcal{Q}$ 中。根据引理5.6和引理5.13可知，我们可以得到量子纠错码与量子信息掩盖之间的关系。

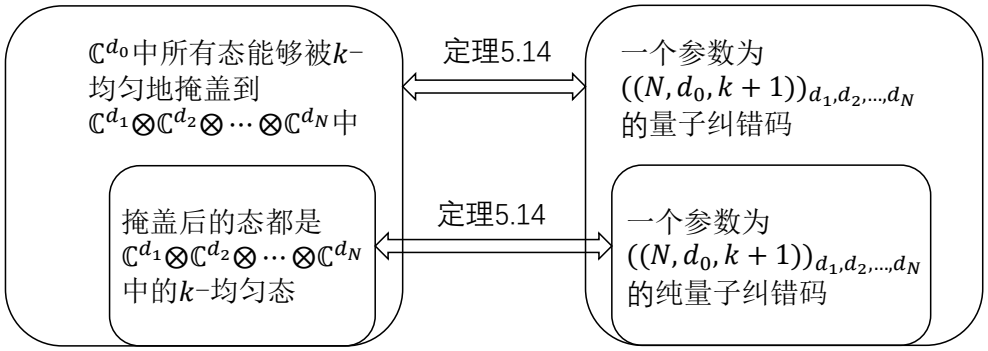

图 5.2　量子纠错码与量子信息掩盖之间的关系。

定理 5.14　如果 $\mathbb{C}^{d_0}$ 中所有态能够被 k-均匀地掩盖到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中，那么一定存在一个参数为 $((N,d_0,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码，反之亦然。此外，如果所有掩盖后的态都是 k-均匀态，那么这个量子纠错码是纯量子纠错码，反之亦然。

量子纠错码与量子信息掩盖之间的关系参见图5.2。k-均匀量子信息掩盖看起来与量子纠错码类似，实际上，k-均匀量子信息掩盖是一个比量子纠错码更加广泛的概念。对于 k-均匀量子信息掩盖，被掩盖之前的态来自于 $\mathcal{H}_{A_0}$ 的一个子集（不一定是一个子空间）。对于参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码来说，编码之前的态都来自于子空间 $\mathbb{C}^K$。文献[89]中强调了一个新的不可行定理：不可掩盖定理，它指的是 $\mathbb{C}^{d_1}$ 中所有态不能被 1-均匀地掩盖到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}$ 中。但是，文献[114-115]中确定了任何可掩盖的集合必须落在某些欧几里得空间中的球面上。

对于一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码来说，它必须满足量子 Singleton 界[66]：

$$\begin{aligned}&\text{对于 } N\geqslant 2k+1,\ \text{有 } K\leqslant \min\left\{\prod_{j\in C}d_j \mid C\subset\{1,2,\cdots,N\right\},|C|=N-2k\};\\&\text{对于 } N=2k,\ \text{有 } K\leqslant 1.\end{aligned}\tag{5.14}$$

特别地，对于一个参数为 $((N,K,k+1))_d$ 的量子纠错码，它有量子 Singleton 界[77]：

$$K\leqslant d^{N-2k}.\tag{5.15}$$

如果 $K=d^{N-2k}$，那么这个量子纠错码被称为最大距离可分量子码（quantum maximum distance separable code, quantum MDS code），即具有参数 $((N,d^{N-2k},k+1))_d$。根据定理5.14，我们有以下推论。

推论 5.15　不可掩盖定理是非齐次系统中量子纠错码的量子 Singleton 界的一个特例。

证明　对于一个参数为 $((2,d_1,2))_{d_1,d_2}$ 的量子纠错码，根据公式(5.14)中的量子 Singleton 界，我们有 $d_1 \leqslant 1$。因此如果 $d_1 \geqslant 2$，那么参数为 $((2,d_1,2))_{d_1,d_2}$ 的量子纠错码不存在。根据定理5.14可知，这等价于 $\mathbb{C}^{d_1}$ 中所有态不能被 1-均匀地掩盖到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}$ 中。∎

更一般地，由公式(5.14)中的量子 Singleton 界可知，当 N 为偶数时，参数为 $((N,d_0,\frac{N}{2}+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码不存在。根据定理5.14，我们可以得到一个推广的多体系统中的不可掩盖定理。

定理 5.16　当 N 为偶数时,$\mathbb{C}^{d_0}$ 中所有态不能被强掩盖到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中。

同样，人们也可以研究定理5.16 中的可掩盖集，我们将其作为一个公开问题。量子 Singleton 界实际上起源于不可克隆定理[79,82]，因此我们认为不可掩盖定理也起源于不可克隆定理。在文献[111] 中，作者留下了两个公开问题:

(i) 是否能将 $\mathbb{C}^d$ 中所有态 1-均匀地掩盖到 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 中，使得掩盖后的态的单体约化密度算子不等于 $\frac{1}{d}\mathbb{I}_d$?

(ii) 是否能将 $\mathbb{C}^d$ 中所有态 1-均匀地掩盖到 $\mathbb{C}^n\otimes\mathbb{C}^n\otimes\mathbb{C}^n$ 中，使得 $n<d$?

对于第二个问题，当 $d=3$ 和 $n=2$ 时，文献[112]给予了否定回答。现在针对这两个问题，我们可以完全地给出否定回答。

推论 5.17　不可能将 $\mathbb{C}^d$ 中所有态 1-均匀地掩盖到 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 中，使得掩盖后的态的单体约化密度算子不等于 $\frac{1}{d}\mathbb{I}_d$

证明　如果可以将 $\mathbb{C}^d$ 中所有态 1-均匀地掩盖到 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 中，使得掩盖后的态的单体约化态不等于 $\frac{1}{d}\mathbb{I}_d$，那么根据定理5.14，这等价于一个参数为 $((3,d,2))_d$ 非纯量子纠错码。注意参数为 $((3,d,2))_d$ 的量子纠错码是一个最大距离可分量子码。由于最大距离可分量子码一定是纯量子纠错码[77,129]，参数为 $((3,d,2))_d$ 非纯量子纠错码不存在。∎

推论 5.18　不可能将 $\mathbb{C}^d$ 中所有态 1-均匀地掩盖到 $\mathbb{C}^n\otimes\mathbb{C}^n\otimes\mathbb{C}^n$ 中，使得 $n<d$?

证明　如果可以将 $\mathbb{C}^d$ 中所有态 1-均匀地掩盖到 $\mathbb{C}^n\otimes\mathbb{C}^n\otimes\mathbb{C}^n$ 中，那么根据定理5.14，这等价于一个参数为 $((3,d,2))_n$ 的量子纠错码，再根据公式(5.15)，我们必然有 $d\leqslant n$。∎

文献[111]中也证明了如果 $d\neq 2,6$，那么 $\mathbb{C}^d$ 中所有态可以被 1-均匀地掩盖到 $\mathbb{C}^d\otimes\mathbb{C}^d\otimes\mathbb{C}^d$ 中。文献[112]证明了不可能将 $\mathbb{C}^2$ 中所有态 1-均匀地掩盖到 $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ 中。最近，文献[103]给出了一个参数为 $((3,6,2))_6$ 的最大距离可分量子码，它是由一个参数为 $((4,1,3))_6$ 的最大距离可分量子码得到的（我们将

在下一节给出几种从已知的量子纠错码构造新的量子纠错码的方法）。根据定理5.14可知，$\mathbb{C}^6$ 中所有态可以被 1-均匀地掩盖到 $\mathbb{C}^6\otimes\mathbb{C}^6\otimes\mathbb{C}^6$ 中，这也解决了文献[111]中最后一个未知的情况。

5.6　从已知的量子纠错码构造新的量子纠错码

本节中，我们将给出几种从已知的非齐次系统中的量子纠错码构造新的量子纠错码的方法。我们的一些方法受到齐次系统中的量子纠错码的构造的启发[76,129]。

引理 5.19　如果存在一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的纯量子纠错码，那么存在一个参数为 $((N-1,d_1K,k))_{d_2,d_3,\cdots,d_N}$ 的纯量子纠错码。

证明　假设 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中由 $\{|i_Q\rangle\}_{i\in\mathbb{Z}_K}$ 生成的子空间 Q 是一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的纯量子纠错码。令

$$|i_Q\rangle=\frac{1}{\sqrt{d_1}}\sum_{p\in\mathbb{Z}_{d_1}}|p^{(1)}\rangle|\psi_p^{(i_Q)}\rangle,$$

其中 $\{|p^{(1)}\rangle\}_{p\in\mathbb{Z}_{d_1}}$ 是 $\mathbb{C}^{d_1}$ 的一组标准正交基。那么下面我们将证明 $\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中由 $\{|\psi_p^{(i_Q)}\rangle\}_{p\in\mathbb{Z}_{d_1},i\in\mathbb{Z}_K}$ 生成的子空间是一个参数为 $((N-1,d_1K,k))_{d_2,d_3,\cdots,d_N}$ 的纯量子纠错码。

令

$$E_\beta=e_{\beta_2}^{(2)}\otimes e_{\beta_3}^{(3)}\otimes\cdots\otimes e_{\beta_N}^{(N)},$$

其中 $\beta=\{\beta_2,\beta_3,\cdots,\beta_N\}\in\mathbb{Z}_{d_2^2}\times\mathbb{Z}_{d_3^2}\times\cdots\times\mathbb{Z}_{d_N^2}$。那么 $\{E_\beta\}_{\beta\in\mathbb{Z}_{d_2^2}\times\mathbb{Z}_{d_3^2}\times\cdots\times\mathbb{Z}_{d_N^2}}$ 是作用在 $\mathbb{C}^{d_2}\otimes\mathbb{C}^{d_3}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 上的一组错误算子基。假设错误算子基 $\{e_{\alpha_1}^{(1)}\}_{\alpha_1\in\mathbb{Z}_{d_1^2}}$ 作用在 $\mathbb{C}^{d_1}$ 上，令一个 $d_1\times d_1$ 的矩阵 $M_{\alpha_1}=(m_{i,j})_{i,j\in\mathbb{Z}_{d_1}}$ 是错误算子 $e_{\alpha_1}^{(1)}$ 在基 $\{|p^{(1)}\rangle\}_{p\in\mathbb{Z}_{d_1}}$ 下的矩阵表示。我们可以定义一个行向量：

$$\begin{aligned}u_{\alpha_1}=(&m_{0,0},\ m_{0,1},\ \cdots,\ m_{0,d_1-1},\ m_{1,0},\ m_{1,1},\ \cdots,m_{1,d_1-1},\ \cdots,\\&m_{d_1-1,0},\ m_{d_1-1,1},\ \cdots,m_{d_1-1,d_1-1}).\end{aligned}$$

那么 $u_{\alpha_i}^\dagger\cdot u_{\alpha_j}=\mathrm{Tr}(M_{\alpha_i}^\dagger M_{\alpha_j})=d_1\delta_{i,j}$。这意味着

$$N=\begin{pmatrix}u_0\\u_1\\\vdots\\u_{d_1^2-1}\end{pmatrix}$$

是一个 $d_1^2 \times d_1^2$ 的满秩矩阵。

由于 $\mathcal{Q}$ 是纯量子纠错码，由定义5.7可知，对于 $0 < wt(e_{\alpha_1} \otimes E_\beta) = wt(e_{\alpha_1}) + wt(E_\beta) < k+1$，或 $i \neq j$，我们有

$$\langle i_Q | e_{\alpha_1}^{(1)} \otimes E_\beta | j_Q \rangle = \frac{1}{d_1} \sum_{p \in \mathbb{Z}_{d_1}} \sum_{q \in \mathbb{Z}_{d_1}} \langle p^{(1)} | e_{\alpha_1}^{(1)} | q^{(1)} \rangle \cdot \ \langle \psi_p^{(i_Q)} | E_\beta | \psi_q^{(j_Q)} \rangle = 0;$$

对于 $wt(e_{\alpha_1} \otimes E_\beta) = 0$，我们有

$$\langle i_Q | e_{\alpha_1}^{(1)} \otimes E_\beta | i_Q \rangle = \langle i_Q | i_Q \rangle = 1.$$

这里有两种情况。

(i) 如果 $0 < wt(E_\beta) < k$ 且 $i, j \in \mathbb{Z}_K$ 或 $wt(E_\beta) = 0$ 且 $i \neq j \in \mathbb{Z}_K$，对于 $\alpha_1 \in \mathbb{Z}_{d_1^2}$，那么我们有

$$\sum_{p \in \mathbb{Z}_{d_1}} \sum_{q \in \mathbb{Z}_{d_1}} \langle p^{(1)} | e_{\alpha_1}^{(1)} | q^{(1)} \rangle \langle \psi_p^{(i_Q)} | E_\beta | \psi_q^{(j_Q)} \rangle = 0. \tag{5.16}$$

令列向量

$$X^{(i,j)} = (\langle \psi_0^{(i_Q)} | E_\beta | \psi_0^{(j_Q)} \rangle, \langle \psi_0^{(i_Q)} | E_\beta | \psi_1^{(j_Q)} \rangle, \ \cdots, \langle \psi_0^{(i_Q)} | E_\beta | \psi_{d_1-1}^{(j_Q)} \rangle,), \ \cdots,$$
$$\langle \psi_{d_1-1}^{(i_Q)} | E_\beta | \psi_0^{(j_Q)} \rangle, \langle \psi_{d_1-1}^{(i_Q)} | E_\beta | \psi_1^{(j_Q)} \rangle, \ \cdots \langle \psi_{d_1-1}^{(i_Q)} | E_\beta | \psi_{d_1-1}^{(j_Q)} \rangle)^T.$$

由公式(5.16)可知

$$N X^{(i,j)} = \mathbf{0}.$$

这推出 $X^{(i,j)} = \mathbf{0}$，对于 $0 < wt(E_\beta) < k$，$i, j \in \mathbb{Z}_K$，$p, q \in \mathbb{Z}_{d_1}$，也意味着我们有

$$\langle \psi_p^{(i_Q)} | E_\beta | \psi_q^{(j_Q)} \rangle = 0; \tag{5.17}$$

对于 $wt(E_\beta) = 0$，$i \neq j \in \mathbb{Z}_K$，$p, q \in \mathbb{Z}_{d_1}$，我们有

$$\langle \psi_p^{(i_Q)} | E_\beta | \psi_q^{(j_Q)} \rangle = \langle \psi_p^{(i_Q)} | \psi_q^{(j_Q)} \rangle = 0. \tag{5.18}$$

(ii) 如果 $wt(E_\beta) = 0$ 和 $i = j \in \mathbb{Z}_K$，对于 $\alpha_1 \in \mathbb{Z}_{d_1^2}$，那么

$$\sum_{p \in \mathbb{Z}_{d_1}} \sum_{q \in \mathbb{Z}_{d_1}} \langle p^{(1)} | e_{\alpha_1}^{(1)} | q^{(1)} \rangle \langle \psi_p^{(i_Q)} | E_\beta | \psi_q^{(i_Q)} \rangle = d_1 \delta_{\alpha_1, 0}. \tag{5.19}$$

令 Y 为一个 $d_1^2 \times 1$ 的列向量 $Y = (d_1, 0, 0, \cdots, 0)^T$，根据公式(5.19)，我们有

$$N X^{(i,i)} = Y.$$

从而 $X^{(i,i)}$ 存在一个唯一的解，即对于 $wt(E_\beta) = 0$，$i \in \mathbb{Z}_K$，$p, q \in \mathbb{Z}_{d_1}$，有

$$\langle \psi_p^{(i_Q)} | E_\beta | \psi_q^{(i_Q)} \rangle = \langle \psi_p^{(i_Q)} | \psi_q^{(i_Q)} \rangle = \delta_{p,q}, \tag{5.20}$$

因此，根据公式(5.17)，(5.18)，(5.20)和定义5.7，$\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中由 $\{|\psi_p^{(i_Q)}\rangle\}_{p\in\mathbb{Z}_{d_1},i\in\mathbb{Z}_K}$ 生成的子空间是一个参数为 $((N-1,d_1K,k))_{d_2,d_3,\cdots,d_N}$ 的纯量子纠错码。 ∎

下面我们可以给出引理5.19的一个例子。

例 5.5　由公式5.2可知

$$|\psi\rangle=\frac{1}{2\sqrt{2}}(|00000\rangle+|01111\rangle+|10011\rangle+|11100\rangle+$$
$$|20101\rangle+|21010\rangle+|30110\rangle+|31001\rangle)$$

是 $\mathbb{C}^4\otimes(\mathbb{C}^2)^{\otimes4}$ 中的一个 2-均匀态，那么根据引理5.13可知，$\mathbb{C}^4\otimes(\mathbb{C}^2)^{\otimes4}$ 中由 $\{|\psi\rangle\}$ 生成的子空间是一个参数为 $((5,1,3))_{4,2,2,2,2}$ 的纯量子纠错码。令

$$|\psi_1\rangle=\frac{1}{2}(|0000\rangle+|1110\rangle+|2101\rangle+|3011\rangle);$$
$$|\psi_2\rangle=\frac{1}{2}(|0111\rangle+|1001\rangle+|2010\rangle+|3100\rangle).$$

根据引理5.19可知，$\mathbb{C}^4\otimes(\mathbb{C}^2)^{\otimes3}$ 中由 $\{|\psi_i\rangle\}_{i=1}^2$ 生成的子空间是一个参数为 $((4,2,2))_{4,2,2,2}$ 的纯量子纠错码。

由以上这个例子和定理5.14可知，非齐次系统中的 k-均匀态可以用于 k-均匀量子信息掩盖。

引理 5.20　(1) 如果存在一个参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码和一个参数为 $((N,L,k+1))_{s_1,s_2,\cdots,s_N}$ 的量子纠错码，那么存在一个参数为 $((N,KL,k+1))_{d_1s_1,d_2s_2,\cdots,d_Ns_N}$ 的量子纠错码。如果之前的是纯量子纠错码，那么之后的也是纯量子纠错码。

(2) 如果存在一个参数为 $((N_1,K,k+1))_{d_1,d_2,\cdots,d_{N_1}}$ 的量子纠错码和一个参数为 $((N_2,L,k+1))_{s_1,s_2,\cdots,s_{N_2}}$ 的量子纠错码，那么存在一个参数为 $((N_1+N_2,KL,k+1))_{d_1,d_2,\cdots,d_{N_1},s_1,s_2,\cdots,s_{N_2}}$ 的量子纠错码。如果之前的是纯量子纠错码，那么之后的也是纯量子纠错码。

证明

(1) 假设 Q_1 是一个由 $\{|i\rangle_{A_1,A_2,\cdots,A_N}\}_{i\in\mathbb{Z}_K}$ 生成的参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码，Q_2 是一个由 $\{|j\rangle_{B_1,B_2,\cdots,B_N}\}_{j\in\mathbb{Z}_L}$ 生成的参数为 $((N,L,k+1))_{s_1,s_2,\cdots,s_N}$ 的量子纠错码，那么我们下面证明由 $\{(|i\rangle\otimes|j\rangle)_{A_1B_1,A_2B_2,\cdots,A_NB_N}\}_{(i,j)\in\mathbb{Z}_K\times\mathbb{Z}_L}$ 生成的子空间 $Q_1\otimes Q_2$ 是一个参数为 $((N,KL,k+1))_{d_1s_1,d_2s_2,\cdots,d_Ns_N}$ 的量子纠错码。

令 $\{E_\alpha\}_{\alpha\in\mathbb{Z}_{d_1^2}\times\mathbb{Z}_{d_2^2}\times\cdots\times\mathbb{Z}_{d_N^2}}$ 和 $\{E_\beta\}_{\beta\in\mathbb{Z}_{s_1^2}\times\mathbb{Z}_{s_2^2}\times\cdots\times\mathbb{Z}_{s_N^2}}$ 分别为作用在 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes$

$\cdots\otimes\mathbb{C}^{d_N}$ 和 $\mathbb{C}^{s_1}\otimes\mathbb{C}^{s_2}\otimes\cdots\otimes\mathbb{C}^{s_N}$ 上的错误算子基，其中

$$E_\alpha = e_{\alpha_1}^{(1)}\otimes e_{\alpha_2}^{(2)}\otimes\cdots\otimes e_{\alpha_N}^{(N)};$$
$$E_\beta = e_{\beta_1}^{(1)}\otimes e_{\beta_2}^{(2)}\otimes\cdots\otimes e_{\beta_N}^{(N)}.$$

我们定义

$$E_{(\alpha,\beta)} = E_\alpha\otimes E_\beta = (e_{\alpha_1}^{(1)}\otimes e_{\beta_1}^{(1)})\otimes\ (e_{\alpha_2}^{(2)}\otimes e_{\beta_2}^{(2)})\otimes\cdots\otimes(e_{\alpha_N}^{(N)}\otimes e_{\beta_N}^{(N)}),$$

其中 $(\alpha,\beta)=((\alpha_1,\beta_1),(\alpha_2,\beta_2),\cdots,(\alpha_N,\beta_N))$。那么 $\{E_{(\alpha,\beta)}\}_{(\alpha,\beta)\in(\mathbb{Z}_{d_1^2}\times\mathbb{Z}_{s_1^2})\times(\mathbb{Z}_{d_2^2}\times\mathbb{Z}_{s_2^2})\times\cdots\times(\mathbb{Z}_{d_N^2}\times\mathbb{Z}_{s_N^2})}$ 是一个作用在 $\mathbb{C}^{d_1s_1}\otimes\mathbb{C}^{d_2s_2}\otimes\cdots\otimes\mathbb{C}^{d_Ns_N}$ 上的错误算子基。如果 $wt(E_{(\alpha,\beta)})<k+1$，那么 $wt(E_\alpha)<k+1$ 且 $wt(E_\beta)<k+1$。对于任意的 $wt(E_{(\alpha,\beta)})<k+1$，我们有

$$\begin{aligned}\langle i_1|\langle j_1|E_{(\alpha,\beta)}|i_2\rangle|j_2\rangle &= \langle i_1|E_\alpha|i_2\rangle\langle j_1|E_\beta|j_2\rangle = C(E_\alpha)C(E_\beta)\delta_{i_1,i_2}\delta_{j_1,j_2}\\ &= C(E_{(\alpha,\beta)})\delta_{((i_1,j_1),(i_2,j_2))}.\end{aligned}$$

因此根据定义5.7可知，$\mathcal{Q}_1\otimes\mathcal{Q}_2$ 是一个参数为 $((N,KL,k+1))_{d_1s_1,d_2s_2,\cdots,d_Ns_N}$ 的量子纠错码。

如果 $\mathcal{Q}_1$ 和 $\mathcal{Q}_2$ 都是纯量子纠错码，那么有 $C(E_\alpha)=\frac{\mathrm{Tr}(E_\alpha)}{d_1d_2\cdots d_N}$ 和 $C(E_\beta)=\frac{\mathrm{Tr}(E_\beta)}{s_1s_2\cdots s_N}$。从而我们有

$$\begin{aligned}C(E_{(\alpha,\beta)}) = C(E_\alpha)C(E_\beta) &= \frac{\mathrm{Tr}(E_\alpha)}{d_1d_2\cdots d_N}\cdot\frac{\mathrm{Tr}(E_\beta)}{s_1s_2\cdots s_N}\\ &= \frac{\mathrm{Tr}(E_\alpha\otimes E_\beta)}{d_1s_1d_2s_2\cdots d_Ns_N} = \frac{\mathrm{Tr}(E_{(\alpha,\beta)})}{d_1s_1d_2s_2\cdots d_Ns_N}.\end{aligned}$$

因此 $\mathcal{Q}_1\otimes\mathcal{Q}_2$ 也是纯量子纠错码。

(2) 假设 $\mathcal{Q}_1$ 是一个由 $\{|i\rangle_{A_1,A_2,\cdots,A_N}\}_{i\in\mathbb{Z}_K}$ 生成的参数为 $((N,K,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码，$\mathcal{Q}_2$ 是一个由 $\{|j\rangle_{B_1,B_2,\cdots,B_N}\}_{j\in\mathbb{Z}_L}$ 生成的参数为 $((N,L,k+1))_{s_1,s_2,\cdots,s_N}$ 的量子纠错码，那么我们下面证明由 $\{(|i\rangle\otimes|j\rangle)_{A_1,A_2,\cdots,A_{N_1},B_1,B_2,\cdots,B_{N_2}}\}_{(i,j)\in\mathbb{Z}_K\times\mathbb{Z}_L}$ 生成的子空间 $\mathcal{Q}_1\otimes\mathcal{Q}_2$ 是一个参数为 $((N_1+N_2,KL,k+1))_{d_1,d_2,\cdots,d_{N_1},s_1,s_2,\cdots,s_{N_2}}$ 的量子纠错码。

注意由 $\{|i\rangle_{A_1,A_2,\cdots,A_{N_1}}\}_{i\in\mathbb{Z}_K}$ 生成的参数为 $((N_1,K,k+1))_{d_1,d_2,\cdots,d_{N_1}}$ 的量子纠错码 $\mathcal{Q}_1$ 可以被看成一个由 $\{|i\rangle_{A_1,A_2,\cdots,A_{N_1},B_1,B_2,\cdots,B_{N_2}}\}_{i\in\mathbb{Z}_K}$ 生成的参数为 $((N_1+N_2,K,k+1))_{d_1,d_2,\cdots,d_{N_1},1,1,\cdots1}$ 的量子纠错码，由 $\{|j\rangle_{B_1,B_2,\cdots,B_{N_2}}\}$ 生成的参数为 $((N_2,L,k+1))_{s_1,s_2,\cdots,s_{N_2}}$ 的量子纠错码 $\mathcal{Q}_2$ 可以被看成一个由 $\{|j\rangle_{A_1,A_2,\cdots,A_{N_1},B_1,B_2,\cdots,B_{N_2}}\}_{j\in\mathbb{Z}_L}$ 生成的参数为 $((N_1+N_2,K,k+1))_{1,1,\cdots,1,s_1,s_1,\cdots s_{N_2}}$ 的量子纠错码。由 (i) 可知，$\{(|i\rangle\otimes|j\rangle)_{A_1,A_2,\cdots,A_{N_1},B_1,B_2,\cdots,B_{N_2}}\}_{(i,j)\in\mathbb{Z}_K\times\mathbb{Z}_L}$ 生成的

子空间 $\mathcal{Q}_1 \otimes \mathcal{Q}_2$ 是一个参数为 $((N_1+N_2, KL, k+1))_{d_1,d_2,\cdots,d_{N_1},s_1,s_2,\cdots,s_{N_2}}$ 的量子纠错码。显然如果 $\mathcal{Q}_1$ 和 $\mathcal{Q}_2$ 都是纯量子纠错码，那么 $\mathcal{Q}_1 \otimes \mathcal{Q}_2$ 也是纯量子纠错码。∎

引理 5.21　如果存在一个参数为 $((N, K, k+1))_{(d_0d_1),d_2,\cdots,d_N}$ 的量子纠错码，那么存在一个参数为 $((N+1, K, k+1))_{d_0,d_1,d_2,\cdots,d_N}$ 的量子纠错码。如果之前的是纯量子纠错码，那么之后的也是纯量子纠错码。

证明　假设 $\mathcal{Q}_1$ 是一个由 $\{|i\rangle_{A_1,A_2,\cdots,d_N}\}_{i\in\mathbb{Z}_K}$ 生成的参数为 $((N, K, k+1))_{(d_0d_1),d_2,\cdots,d_N}$ 的量子纠错码。通过将 $\mathbb{C}^{d_0d_1}$ 中的态替换为 $\mathbb{C}^{d_0} \otimes \mathbb{C}^{d_1}$ 中的态，下面我们将证明替换后的量子纠错码 $\mathcal{Q}_2$ 是一个由 $\{|i\rangle_{B_0,B_1,A_2,\cdots,d_N}\}_{i\in\mathbb{Z}_K}$ 生成的参数为 $((N+1, K, k+1))_{d_0,d_1,d_2,\cdots,d_N}$ 的量子纠错码。

令

$$E_\alpha = e^{(0)}_{\alpha_0} \otimes e^{(1)}_{\alpha_1} \otimes e^{(2)}_{\alpha_2} \otimes \cdots \otimes e^{(N)}_{\alpha_N},$$

其中 $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_N) \in \mathbb{Z}_{d_0^2} \times \mathbb{Z}_{d_1^2} \times \mathbb{Z}_{d_2^2} \times \cdots \times \mathbb{Z}_{d_N^2}$，那么 $\{E_\alpha\}_{\alpha\in\in\mathbb{Z}_{d_0^2}\times\mathbb{Z}_{d_1^2}\times\mathbb{Z}_{d_2^2}\times\cdots\times\mathbb{Z}_{d_N^2}}$ 是一个作用在 $\mathbb{C}^{d_0} \otimes \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 上的错误算子基。

令

$$E_\beta = (e^{(0)}_{\alpha_0} \otimes e^{(1)}_{\alpha_1}) \otimes e^{(2)}_{\alpha_2} \otimes \cdots \otimes e^{(N)}_{\alpha_N},$$

其中 $\beta = (\beta_{(\alpha_0,\alpha_1)}, \alpha_2, \cdots, \alpha_N) \in (\mathbb{Z}_{d_0^2} \times \mathbb{Z}_{d_1^2}) \times \mathbb{Z}_{d_2^2} \times \cdots \times \mathbb{Z}_{d_N^2}$，$\beta_{(\alpha_0,\alpha_1)} = (\alpha_0, \alpha_1)$。那么 $\{E_\beta\}_{\beta\in(\mathbb{Z}_{d_0^2}\times\mathbb{Z}_{d_1^2})\times\mathbb{Z}_{d_2^2}\times\cdots\times\mathbb{Z}_{d_N^2}}$ 是一个作用在 $\mathbb{C}^{d_0d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 上的错误算子基。如果 $wt(E_\alpha) < k+1$，那么 $wt(E_\beta) < k+1$。对于任意的 $wt(E_\alpha) < k+1$，我们有

$$\begin{aligned} {}_{B_0,B_1,A_2,\cdots,A_N}\langle i|E_\alpha|j\rangle_{B_0,B_1,A_2,\cdots,A_N} &= {}_{A_1,A_2,\cdots,A_N}\langle i|E_\beta|j\rangle_{A_1,A_2,\cdots,A_N} \\ &= C(E_\beta)\delta_{i,j} = C(E_\alpha)\delta_{i,j}. \end{aligned}$$

从而根据定义5.7, $\mathcal{Q}_2$ 是一个由 $\{|i\rangle_{B_0,B_1,A_2,\cdots,d_N}\}_{i\in\mathbb{Z}_K}$ 生成的参数为 $((N+1, K, k+1))_{d_0,d_1,d_2,\cdots,d_N}$ 的量子纠错码。如果 $\mathcal{Q}_1$ 是纯量子纠错码，那么很容易看出 $\mathcal{Q}_2$ 也是纯量子纠错码。∎

引理5.21的逆命题不一定正确，但是我们有以下结论。

引理 5.22　如果存在一个参数为 $((N+1, K, k+1))_{d_0,d_1,d_2,\cdots,d_N}$ 的量子纠错码，那么存在一个参数为 $((N, K, k))_{(d_0d_1),d_2,\cdots,d_N}$ 的量子纠错码。如果之前的是纯量子纠错码，那么之后的也是纯量子纠错码。

同样，我们也是通过将 $\mathbb{C}^{d_0} \otimes \mathbb{C}^{d_1}$ 中的态替换为 $\mathbb{C}^{d_0d_1}$ 中的态，从而得到参数为 $((N, K, k))_{(d_0d_1),d_2,\cdots,d_N}$ 的量子纠错码。原因是由引理5.21的证明可知，如果 $wt(E_\beta) < k$，那么 $wt(E_\alpha) < k+1$。从而引理5.22可以很容易地被证明。

根据引理5.13可知, 一个参数为 $((N,1,k+1))_{d_1,d_2,\cdots,d_N}$ 的量子纠错码是 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个 k-均匀态。本节所有量子纠错码的构造都可以用于非齐次系统中的 k-均匀态的构造。例如，5.3.2节中 k-均匀态的分裂方法是本节引理5.21的一个特例；5.3.4节中的引理5.10是本节引理5.19的一个特例；5.3.4节中的引理5.11是本节引理5.22的一个特例。但是本节的引理5.20可以构造更多未知的非齐次系统中的 k-均匀态。例如, 对于任何 $d\geqslant 3$, $N\geqslant 7$ 且 $N\neq 4d+2,4d+3$, 5.3.2节中的定理5.7证明了 $(\mathbb{C}^d)^{\otimes N}\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ 存在一个 2-均匀态。对于 $d\geqslant 3$, 通过对 $(\mathbb{C}^d)^{\otimes(2d+2)}\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ (或 $(\mathbb{C}^d)^{\otimes(2d+3)}\otimes\mathbb{C}^2\otimes\mathbb{C}^2$) 中的一个 2-均匀态和 $(\mathbb{C}^d)^{\otimes 2d}$ 中的一个 2-均匀态[54]运用引理5.20(2)，我们可以找到 $(\mathbb{C}^d)^{\otimes(4d+2)}\otimes\mathbb{C}^2\otimes\mathbb{C}^2$（或 $(\mathbb{C}^d)^{\otimes(4d+3)}\otimes\mathbb{C}^2\otimes\mathbb{C}^2$）中的一个 2-均匀态, 从而解决了定理5.7中 $N\neq 4d+2,4d+3$ 的情况。

5.7　本章小结

本章中，我们利用混合正交阵列，构造了一系列非齐次系统中的 2, 3-均匀态，由此回答了文献[107]中的一个公开问题。我们也给出了两种从 k-均匀态构造 $(k-1)$-均匀态的方法, 并利用影子不等式给出了一些非齐次系统中的绝对最大纠缠态的不存在性结果，主要结果见表1.4。我们提出了 k-均匀量子信息掩盖的概念，这个模型能很好地保证量子信息的安全。我们揭示了非齐次系统中的量子纠错码与 k-均匀量子信息掩盖之间的关系，利用这个关系，我们证明了文献[89]中的不可掩盖定理实际上是非齐次系统中量子纠错码的量子 Singleton 界的一个特例，也给出了多体系统中更一般的不可掩盖定理，并回答了文献[111]中提出的两个公开问题。最后我们给出了几种从已知的非齐次系统中的量子纠错码构造新的量子纠错码的方法，这几种方法也能够用来构造非齐次系统中的 k-均匀态。

此外，非齐次系统中的 k-均匀态也可以用于 k-均匀量子信息掩盖。虽然当 N 为偶数时，$\mathbb{C}^{d_0}$ 中所有态不能被强掩盖到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中，但是当 N 为奇数时，强量子信息掩盖是可能的，它与非齐次系统中的绝对最大纠缠态有关系。假设 N 为奇数，给定 $\mathbb{C}^{d_0}\otimes\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中的一个绝对最大纠缠态，它也是一个参数为 $((N+1,1,\lfloor\frac{N+1}{2}\rfloor+1))_{d_0,d_1,d_2,\cdots d_N}$ 的量子纠错码，那么根据引理5.19，我们可以得到一个参数为 $((N,d_0,\lfloor\frac{N+1}{2}\rfloor))_{d_1,d_2,\cdots d_N}$ 的量子纠错码，从而 $\mathbb{C}^{d_0}$ 中所有态可以被强掩盖到 $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}\otimes\cdots\otimes\mathbb{C}^{d_N}$ 中。

本章中还有一些遗留的问题：如何确定表1.1中的未知情况？即当 $d\geqslant 6$ 且 $d=2 \mod (4)$ 时，如何确定 $(\mathbb{C}^d)^{\otimes 7}$ 中的 3-均匀态（绝对最大纠缠态）的存在性？当 $N\geqslant 5$，是否可以构造 N 体真实非齐次系统中的绝对最大纠缠态？例如 $\mathbb{C}^3\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ 中是否存在绝对最大纠缠态？当 N 为偶数时，怎么刻

画 $\mathbb{C}^{d_0}$ 中的子集 S，使得 S 中所有态可以被强掩盖到 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中? 我们是否可以找到比量子 Singleton 界更紧的界?

第 6 章　总结与展望

6.1　工作总结

量子非局域性与多体纠缠在量子信息理论中扮演着重要的角色，它们同时在量子秘密分享，量子隐形传态和量子密钥分发等量子信息任务中发挥着至关重要的作用。本文主要从三个方面来研究量子非局域性与多体纠缠。

(1) 不可扩充乘积基是一类能够展示无纠缠量子非局域性现象的集合，而之前关于不可扩充乘积基的研究主要集中于它的最小数目的研究，并且缺少明确的构造。我们建立了多维超立方体与不可扩充乘积基之间的关系，利用多维超立方体的分解，我们明确地给出了二、三、四体系统中数目较大的不可扩充乘积基的构造。由于不可扩充乘积基是局部不可区分的，要区分它必须借助于纠缠资源。因此我们也研究了两体系统中的不可扩充乘积基的纠缠辅助区分。

(2) 强量子非局域性是一种更强版本的非局域性。我们给出了两个工具来验证正交集的强量子非局域性，这两个工具大大减少了计算量。利用前面提到的多维超立方体的分解和这两个工具，我们构造了三、四、五体系统中强非局域的正交乘积集，三体系统中强非局域的正交纠缠集，也验证了前面构造的三体和四体系统中的不可扩充乘积基具有强量子非局域性。最后，我们利用循环置换群作用，构造了一般 N 体齐次系统中的强非局域的正交纠缠集，并在 $N = 3, 4$ 的时候，找到了强非局域的正交真实纠缠集。

(3) 利用混合正交阵列，我们构造了一系列非齐次系统中的 $2, 3$-均匀态，并给出了两种从 k-均匀态到 $(k-1)$-均匀态的构造方法。此外利用影子不等式，我们给出了一些非齐次系统中的绝对最大纠缠态的不存在性结果。我们提出了 k-均匀量子信息掩盖的概念，它要求任意 k 个子系统都无法访问掩盖之前的信息。我们建立了非齐次系统中的量子纠错码与 k-均匀量子信息掩盖之间的关系，基于这个关系，我们证明了不可掩盖定理是量子纠错码的量子 Singleton 界的一个特例，并给出了一个更一般的不可掩盖定理。最后我们给出了几种从已知的非齐次系统中的量子纠错码构造新的量子纠错码的方法，这些方法还可以用来构造非齐次系统中的 k-均匀态。此外，我们也证明了非齐次系统中的 k-均匀态可以用于 k-均匀量子信息掩盖。

6.2　未来展望

本文研究了不可扩充乘积基、强量子非局域性、k-均匀态和 k-均匀量子信息掩盖。虽然不可扩充乘积基和强量子非局域性都能够对信息进行加密，并提高信息的安全性，但是关于它们的研究还需要进一步深入。此外，虽然 k-均匀态和 k-均匀量子信息掩盖与量子纠错码息息相关，但是对它们还需要进一步刻画。因此有几个问题是下一步需要考虑的。

(1) 给出一般 N 维超立方体的分解，利用它来构造一般 N 体系统中的强非局域的不可扩充乘积基，正交乘积集和正交纠缠集。

(2) 对于 $d_i \geqslant 2$，$N \geqslant 3$，$1 \leqslant i \leqslant N$，确定 $(\mathbb{C}^d)^{\otimes N}$ 中强非局域的正交集所含态的最小个数。

(3) 找到一个多体系统中的不可扩充乘积基，使得它在任意两体划分下仍然是不可扩充乘积基。

(4) 构造 N 体真实非齐次系统中的绝对最大纠缠态。

(5) 当 N 为偶数时，刻画 $\mathbb{C}^{d_0}$ 中的子集 S，使得 S 中所有态可以同时被强掩盖到 $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_N}$ 中。

(6) 找到比量子 Singleton 界更紧的界。

参 考 文 献

[1] HORODECKI R, HORODECKI P, HORODECKI M, et al. Quantum entanglement[J]. Reviews of Modern Physics, 2009, 81(2): 865.

[2] BRUNNER N, CAVALCANTI D, PIRONIO S, et al. Bell nonlocality[J]. Reviews of Modern Physics, 2014, 86(2): 419.

[3] BENNETT C H, DIVINCENZO D P, FUCHS C A, et al. Quantum nonlocality without entanglement[J]. Physical Review A, 1999, 59(2): 1070.

[4] DIVINCENZO D P, MOR T, SHOR P W, et al. Unextendible product bases, uncompletable product bases and bound entanglement[J]. Communications in Mathematical Physics, 2003, 238(3): 379-410.

[5] FENG Y, SHI Y. Characterizing locally indistinguishable orthogonal product states[J]. IEEE Transactions on Information Theory, 2009, 55(6): 2799-2806.

[6] NISET J, CERF N J. Multipartite nonlocality without entanglement in many dimensions[J]. Physical Review A, 2006, 74(5): 052103.

[7] YANG Y H, GAO F, TIAN G J, et al. Local distinguishability of orthogonal quantum states in a $2 \otimes 2 \otimes 2$ system[J]. Physical Review A, 2013, 88(2): 024301.

[8] HALDER S. Several nonlocal sets of multipartite pure orthogonal product states[J]. Physical Review A, 2018, 98(2): 022303.

[9] XU G B, WEN Q Y, GAO F, et al. Local indistinguishability of multipartite orthogonal product bases[J]. Quantum Information Processing, 2017, 16(11): 1-19.

[10] WANG Y L, LI M S, ZHENG Z J, et al. The local indistinguishability of multipartite product states[J]. Quantum Information Processing, 2017, 16(1): 1-13.

[11] ZHANG Z C, ZHANG K J, GAO F, et al. Construction of nonlocal multipartite quantum states[J]. Physical Review A, 2017, 95(5): 052344.

[12] GHOSH S, KAR G, ROY A, et al. Distinguishability of maximally entangled states[J]. Physical Review A, 2004, 70(2): 022304.

[13] FAN H. Distinguishability and indistinguishability by local operations and classical communication[J]. Physical Review Letters, 2004, 92(17): 177905.

[14] NATHANSON M. Distinguishing bipartitite orthogonal states using locc: Best and worst cases[J]. Journal of Mathematical Physics, 2005, 46(6): 062103.

[15] YU N, DUAN R, YING M. Any $2 \otimes n$ subspace is locally distinguishable[J]. Physical Review A, 2011, 84(1): 012304.

[16] DUAN R, FENG Y, JI Z, et al. Distinguishing arbitrary multipartite basis unambiguously

using local operations and classical communication[J]. Physical Review Letters, 2007, 98 (23): 230502.

[17] BANDYOPADHYAY S, GHOSH S, KAR G. Locc distinguishability of unilaterally transformable quantum states[J]. New Journal of Physics, 2011, 13(12): 123013.

[18] COSENTINO A. Positive-partial-transpose-indistinguishable states via semidefinite programming[J]. Physical Review A, 2013, 87(1): 012321.

[19] YU N, DUAN R, YING M. Four locally indistinguishable ququad-ququad orthogonal maximally entangled states[J]. Physical Review Letters, 2012, 109(2): 020506.

[20] BANDYOPADHYAY S. Entanglement, mixedness, and perfect local discrimination of orthogonal quantum states[J]. Physical Review A, 2012, 85(4): 042319.

[21] WANG Y L, LI M S, ZHENG Z J, et al. Nonlocality of orthogonal product-basis quantum states[J]. Physical Review A, 2015, 92(3): 032313.

[22] TERHAL B M, DIVINCENZO D P, LEUNG D W. Hiding bits in Bell states[J]. Physical Review Letters, 2001, 86(25): 5807.

[23] DIVINCENZO D P, LEUNG D, TERHAL B M. Quantum data hiding[J]. IEEE Transactions on Information Theory, 2002, 48(3): 580-598.

[24] EGGELING T, WERNER R F. Hiding classical data in multipartite quantum states[J]. Physical Review Letters, 2002, 89(9): 097905.

[25] MATTHEWS W, WEHNER S, WINTER A. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding[J]. Communications in Mathematical Physics, 2009, 291(3): 813-843.

[26] MARKHAM D, SANDERS B C. Graph states for quantum secret sharing[J]. Physical Review A, 2008, 78(4): 042309.

[27] HILLERY M, BUŽEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3): 1829.

[28] RAHAMAN R, PARKER M G. Quantum scheme for secret sharing based on local distinguishability[J]. Physical Review A, 2015, 91(2): 022330.

[29] BANDYOPADHYAY S, HALDER S. Genuine activation of nonlocality: From locally available to locally hidden information[J]. Physical Review A, 2021, 104(5): L050201.

[30] BENNETT C H, DIVINCENZO D P, MOR T, et al. Unextendible product bases and bound entanglement[J]. Physical Review Letters, 1999, 82(26): 5385.

[31] CHEN J, CHEN L, ZENG B. Unextendible product basis for fermionic systems[J]. Journal of Mathematical Physics, 2014, 55(8): 082207.

[32] AUGUSIAK R, FRITZ T, KOTOWSKI M, et al. Tight Bell inequalities with no quantum violation from qubit unextendible product bases[J]. Physical Review A, 2012, 85(4): 042113.

[33] AUGUSIAK R, STASIŃSKA J, HADLEY C, et al. Bell inequalities with no quantum violation and unextendable product bases[J]. Physical Review Letters, 2011, 107(7): 070401.

[34] JOHNSTON N. The minimum size of qubit unextendible product bases[M]//Proceedings of the 8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013): volume 22. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2013: 93–105.

[35] JOHNSTON N. The structure of qubit unextendible product bases[J]. Journal of Physics A: Mathematical and Theoretical, 2014, 47(42): 424034.

[36] ALON N, LOVÁSZ L. Unextendible product bases[J]. Journal of Combinatorial Theory, Series A, 2001, 95(1): 169-179.

[37] FENG K. Unextendible product bases and 1-factorization of complete graphs[J]. Discrete Applied Mathematics, 2006, 154(6): 942-949.

[38] CHEN J, JOHNSTON N. The minimum size of unextendible product bases in the bipartite case (and some multipartite cases)[J]. Communications in Mathematical Physics, 2015, 333 (1): 351-365.

[39] HALDER S, BANIK M, GHOSH S. Family of bound entangled states on the boundary of the peres set[J]. Physical Review A, 2019, 99(6): 062329.

[40] BEJ P, HALDER S. Unextendible product bases, bound entangled states, and the range criterion[J]. Physics Letters A, 2021, 386: 126992.

[41] DE RINALDIS S. Distinguishability of complete and unextendible product bases[J]. Physical Review A, 2004, 70(2): 022309.

[42] COHEN S M. Understanding entanglement as resource: Locally distinguishing unextendible product bases[J]. Physical Review A, 2008, 77(1): 012304.

[43] HALDER S, BANIK M, AGRAWAL S, et al. Strong quantum nonlocality without entanglement[J]. Physical Review Letters, 2019, 122(4): 040403.

[44] EKERT A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661.

[45] GISIN N, RIBORDY G, TITTEL W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145.

[46] BENNETT C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121.

[47] LIAO S K, CAI W Q, LIU W Y, et al. Satellite-to-ground quantum key distribution[J]. Nature, 2017, 549(7670): 43-47.

[48] CHEN Y A, ZHANG Q, CHEN T Y, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres[J]. Nature, 2021, 589(7841): 214-219.

[49] BENNETT C H, BRASSARD G, CRÉPEAU C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels[J]. Physical Review Letters, 1993, 70(13): 1895.

[50] BOUWMEESTER D, PAN J W, MATTLE K, et al. Experimental quantum teleportation[J]. Nature, 1997, 390(6660): 575.

[51] SCOTT A J. Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions[J]. Physical Review A, 2004, 69(5): 052330.

[52] GOYENECHE D, ŻYCZKOWSKI K. Genuinely multipartite entangled states and orthogonal arrays[J]. Physical Review A, 2014, 90(2): 022316.

[53] FENG K, JIN L, XING C, et al. Multipartite entangled states, symmetric matrices, and error-correcting codes[J]. IEEE Transactions on Information Theory, 2017, 63(9): 5618-5627.

[54] LI M S, WANG Y L. k-Uniform quantum states arising from orthogonal arrays[J]. Physical Review A, 2019, 99(4): 042332.

[55] PANG S Q, ZHANG X, LIN X, et al. Two and three-uniform states from irredundant orthogonal arrays[J]. npj Quantum Information, 2019, 5(1): 6.

[56] 吴长锋. “墨子号”量子卫星：太空最耀眼的“科学之星”[EB/OL]. http://www.stdaily.com/index/kejixinwen/2020-10/13/content_1027133.shtml.

[57] GOYENECHE D, ALSINA D, LATORRE J I, et al. Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices[J]. Physical Review A, 2015, 92(3): 032316.

[58] GOYENECHE D, RAISSI Z, DI MARTINO S, et al. Entanglement and quantum combinatorial designs[J]. Physical Review A, 2018, 97(6): 062326.

[59] NIELSEN M A, CHUANG I L. Quantum computation and quantum information[M]. Cambridge University Press, Cambridge, UK, 2004.

[60] HELWIG W, CUI W, LATORRE J I, et al. Absolute maximal entanglement and quantum secret sharing[J]. Physical Review A, 2012, 86(5): 052335.

[61] PASTAWSKI F, YOSHIDA B, HARLOW D, et al. Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence[J]. Journal of High Energy Physics, 2015, 2015(6): 149.

[62] RAINS E M. Quantum shadow enumerators[J]. IEEE Transactions on Information Theory, 1999, 45(7): 2361-2366.

[63] HUBER F, GÜHNE O, SIEWERT J. Absolutely maximally entangled states of seven qubits do not exist[J]. Physical Review Letters, 2017, 118(20): 200502.

[64] HUBER F, WYDERKA N. Table of absolutely maximally entangled states[EB/OL]. http://www.tp.nt.uni-siegen.de/+fhuber/ame.html.

[65] HORODECKI P, RUDNICKI Ł, ŻYCZKOWSKI K. Five open problems in quantum information theory[J]. PRX Quantum, 2022, 3(1): 010101.

[66] WANG Z, YU S, FAN H, et al. Quantum error-correcting codes over mixed alphabets[J]. Physical Review A, 2013, 88(2): 022328.

[67] KRENN M, MALIK M, ERHARD M, et al. Orbital angular momentum of photons and the entanglement of laguerre–gaussian modes[J]. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2017, 375(2087): 20150442.

[68] CAI Y, ROSLUND J, FERRINI G, et al. Multimode entanglement in reconfigurable graph states using optical frequency combs[J]. Nature Communications, 2017, 8: 15645.

[69] ERHARD M, FICKLER R, KRENN M, et al. Twisted photons: new quantum perspectives in high dimensions[J]. Light: Science & Applications, 2018, 7(3): 17146-17146.

[70] MALIK M, ERHARD M, HUBER M, et al. Multi-photon entanglement in high dimensions [J]. Nature Photonics, 2016, 10(4): 248-252.

[71] KRENN M, GU X, ZEILINGER A. Quantum experiments and graphs: Multiparty states as coherent superpositions of perfect matchings[J]. Physical Review Letters, 2017, 119(24): 240403.

[72] GU X, CHEN L, ZEILINGER A, et al. Quantum experiments and graphs. III. high-dimensional and multiparticle entanglement[J]. Physical Review A, 2019, 99(3): 032338.

[73] SHOR P W. Scheme for reducing decoherence in quantum computer memory[J]. Physical Review A, 1995, 52(4): R2493.

[74] KNILL E, LAFLAMME R. Theory of quantum error-correcting codes[J]. Physical Review A, 1997, 55(2): 900.

[75] KNILL E, LAFLAMME R, VIOLA L. Theory of quantum error correction for general noise [J]. Physical Review Letters, 2000, 84(11): 2525.

[76] RAINS E M. Quantum weight enumerators[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1388-1394.

[77] RAINS E M. Nonbinary quantum codes[J]. IEEE Transactions on Information Theory, 1999, 45(6): 1827-1832.

[78] RAINS E M. Polynomial invariants of quantum codes[J]. IEEE Transactions on Information Theory, 2000, 46(1): 54-59.

[79] GOTTESMAN D. An introduction to quantum error correction[C]//Proceedings of Symposia in Applied Mathematics: volume 58. 2002: 221-236.

[80] KETKAR A, KLAPPENECKER A, KUMAR S, et al. Nonbinary stabilizer codes over finite fields[J]. IEEE Transactions on Information Theory, 2006, 52(11): 4892-4914.

[81] GRASSL M, BETH T, ROETTELER M. On optimal quantum codes[J]. International Journal

of Quantum Information, 2004, 2(01): 55-64.

[82] CERF N J, CLEVE R. Information-theoretic interpretation of quantum error-correcting codes [J]. Physical Review A, 1997, 56(3): 1721.

[83] WOOTTERS W K, ZUREK W H. A single quantum cannot be cloned[J]. Nature, 1982, 299 (5886): 802-803.

[84] GISIN N, MASSAR S. Optimal quantum cloning machines[J]. Physical Review Letters, 1997, 79(11): 2153.

[85] LAMAS-LINARES A, SIMON C, HOWELL J C, et al. Experimental quantum cloning of single photons[J]. Science, 2002, 296(5568): 712-714.

[86] BARNUM H, CAVES C M, FUCHS C A, et al. Noncommuting mixed states cannot be broadcast[J]. Physical Review Letters, 1996, 76(15): 2818.

[87] KUMAR PATI A, BRAUNSTEIN S L. Impossibility of deleting an unknown quantum state [J]. Nature, 2000, 404(6774): 164-165.

[88] BRAUNSTEIN S L, PATI A K. Quantum information cannot be completely hidden in correlations: implications for the black-hole information paradox[J]. Physical Review Letters, 2007, 98(8): 080502.

[89] MODI K, PATI A K, SEN A, et al. Masking quantum information is impossible[J]. Physical Review Letters, 2018, 120(23): 230501.

[90] ZHANG Y, FEI S, XIANDE Z, et al. New results on unextendible product bases[J]. Scientia Sinica Mathematica, 2021, 51.

[91] ZHANG Z C, SONG Y Q, SONG T T, et al. Local distinguishability of orthogonal quantum states with multiple copies of $2 \otimes 2$ maximally entangled states[J]. Physical Review A, 2018, 97(2): 022334.

[92] AGRAWAL S, HALDER S, BANIK M. Genuinely entangled subspace with all-encompassing distillable entanglement across every bipartition[J]. Physical Review A, 2019, 99(3): 032335.

[93] CHEN L, ĐOKOVIĆ D Ž. Separability problem for multipartite states of rank at most 4[J]. Journal of Physics A: Mathematical and Theoretical, 2013, 46(27): 275304.

[94] CHEN L, ĐOKOVIĆ D Ž. Nonexistence of n-qubit unextendible product bases of size $2^n - 5$ [J]. Quantum Information Processing, 2018, 17(2): 1-10.

[95] YUAN P, TIAN G, SUN X. Strong quantum nonlocality without entanglement in multipartite quantum systems[J]. Physical Review A, 2020, 102(4): 042228.

[96] WANG Y L, LI M S, YUNG M H. Graph connectivity based strong quantum nonlocality with genuine entanglement[J]. Physical Review A, 2021, 104(1): 012424.

[97] ZHANG Z C, ZHANG X. Strong quantum nonlocality in multipartite quantum systems[J].

Physical Review A, 2019, 99(6): 062108.

[98] ROUT S, MAITY A G, MUKHERJEE A, et al. Genuinely nonlocal product bases: Classification and entanglement-assisted discrimination[J]. Physical Review A, 2019, 100(3): 032321.

[99] ROUT S, MAITY A G, MUKHERJEE A, et al. Multiparty orthogonal product states with minimal genuine nonlocality[J]. Physical Review A, 2021, 104(5): 052433.

[100] LI M S, WANG Y L, SHI F, et al. Local distinguishability based genuinely quantum nonlocality without entanglement[J]. Journal of Physics A: Mathematical and Theoretical, 2021, 54(44): 445301.

[101] ZHANG Z C, TIAN G J, CAO T Q. Strong quantum nonlocality for multipartite entangled states[J]. Quantum Information Processing, 2021, 20(10): 1-10.

[102] HIGUCHI A, SUDBERY A. How entangled can two couples get?[J]. Physics Letters A, 2000, 273(4): 213-217.

[103] RATHER S A, BURCHARDT A, BRUZDA W, et al. Thirty-six entangled officers of euler: quantum solution to a classically impossible problem[J]. Physical Review Letters, 2022, 128 (8): 080507.

[104] RAISSI Z, TEIXIDÓ A, GOGOLIN C, et al. Constructions of k-uniform and absolutely maximally entangled states beyond maximum distance codes[J]. Physical Review Research, 2020, 2(3): 033411.

[105] GRASSL M, RÖTTELER M. Quantum MDS codes over small fields[C]//2015 IEEE International Symposium on Information Theory (ISIT). IEEE, 2015: 1104-1108.

[106] HUBER F, ELTSCHKA C, SIEWERT J, et al. Bounds on absolutely maximally entangled states from shadow inequalities, and the quantum Macwilliams identity[J]. Journal of Physics A: Mathematical and Theoretical, 2018, 51(17): 175301.

[107] GOYENECHE D, BIELAWSKI J, ŻYCZKOWSKI K. Multipartite entanglement in heterogeneous systems[J]. Physical Review A, 2016, 94(1): 012346.

[108] SHEN Y, CHEN L. Absolutely maximally entangled states in tripartite heterogeneous systems [J]. Quantum Information Processing, 2021, 20(3): 1-23.

[109] BRYAN J, REICHSTEIN Z, VAN RAAMSDONK M. Existence of locally maximally entangled quantum states via geometric invariant theory[C]//Annales Henri Poincaré: volume 19. Springer, 2018: 2491-2511.

[110] BRYAN J, LEUTHEUSSER S, REICHSTEIN Z, et al. Locally maximally entangled states of multipart quantum systems[J]. Quantum, 2019, 3: 115.

[111] LI M S, WANG Y L. Masking quantum information in multipartite scenario[J]. Physical Review A, 2018, 98(6): 062306.

[112] HAN K, GUO Z, CAO H, et al. Quantum multipartite maskers vs. quantum error-correcting codes[J]. EPL (Europhysics Letters), 2020, 131(3): 30005.

[113] LI B, JIANG S H, LIANG X B, et al. Deterministic versus probabilistic quantum information masking[J]. Physical Review A, 2019, 99(5): 052343.

[114] LIANG X B, LI B, FEI S M. Complete characterization of qubit masking[J]. Physical Review A, 2019, 100(3): 030304.

[115] LIANG X B, LI B, FEI S M, et al. Impossibility of masking a set of quantum states of nonzero measure[J]. Physical Review A, 2020, 101(4): 042321.

[116] LI M S, MODI K. Probabilistic and approximate masking of quantum information[J]. Physical Review A, 2020, 102(2): 022418.

[117] LV Q Q, LIANG J M, WANG Z X, et al. Quantum information masking in non-hermitian systems and robustness[J]. Laser Physics Letters, 2022, 19(4): 045203.

[118] LIU Z H, LIANG X B, SUN K, et al. Photonic implementation of quantum information masking[J]. Physical Review Letters, 2021, 126(17): 170505.

[119] ZHANG Z C, WU X, ZHANG X. Locally distinguishing unextendible product bases by using entanglement efficiently[J]. Physical Review A, 2020, 101(2): 022306.

[120] GHOSH S, KAR G, ROY A, et al. Distinguishability of Bell states[J]. Physical Review Letters, 2001, 87(27): 277902.

[121] BANDYOPADHYAY S, HALDER S, NATHANSON M. Entanglement as a resource for local state discrimination in multipartite systems[J]. Physical Review A, 2016, 94(2): 022311.

[122] ZHANG Z C, GAO F, CAO T Q, et al. Entanglement as a resource to distinguish orthogonal product states[J]. Scientific Reports, 2016, 6(1): 1-7.

[123] GÜNGÖR Ö, TURGUT S. Entanglement-assisted state discrimination and entanglement preservation[J]. Physical Review A, 2016, 94(3): 032330.

[124] HALDER S, SENGUPTA R. Distinguishability classes, resource sharing, and bound entanglement distribution[J]. Physical Review A, 2020, 101(1): 012311.

[125] ROTMAN J J. Advanced modern algebra: volume 114[M]. American Mathematical Society, 2010.

[126] HEDAYAT A S, SLOANE N J A, STUFKEN J. Orthogonal arrays: theory and applications [M]. Springer-Verlag, New York, 1999.

[127] ŻUKOWSKI M, ZEILINGER A, HORNE M A, et al. Quest for GHZ states[J]. Acta Physica Polonica A, 1998, 93(1): 187-195.

[128] CLEVE R, GOTTESMAN D, LO H K. How to share a quantum secret[J]. Physical Review Letters, 1999, 83(3): 648.

[129] HUBER F, GRASSL M. Quantum codes of maximal distance and highly entangled subspaces

[J]. Quantum, 2020, 4: 284.

[130] PANG S, ZHANG R, ZHANG X. Quantum frequency arrangements, quantum mixed orthogonal arrays and entangled states[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020, 103(12): 1674-1678.

[131] SLOANE N J A. A library of orthogonal arrays[EB/OL]. http://neilsloane.com/oadir/.

[132] BROUWER A E, COHEN A M, NGUYEN M V. Orthogonal arrays of strength 3 and small run sizes[J]. Journal of Statistical Planning and Inference, 2006, 136(9): 3268-3280.

[133] COLBOURN D J H, Charles J. handbook of combinatorial designs[M]. 2nd ed, CRC Press, Boca Raton, FL, 2006.

[134] WARREN F K. Orthogonal arrays[EB/OL]. https://support.sas.com/techsup/technote/ts723b.pdf.

[135] CHEN G Z, LEI J G. Constructions of mixed orthogonal arrays of strength three[J]. Scientia Sinica Mathematica, 2017, 47(23): 545-564.

[136] SHI F. A construction for a 3-uniform state of 1 qutrit and 256 qubits (IrMOA(1728,$3^1 2^{256}$,3))[EB/OL]. http://home.ustc.edu.cn/~shifei/.

[137] NGUYEN M V. Some new constructions of strength 3 mixed orthogonal arrays[J]. Journal of Statistical Planning and Inference, 2008, 138(1): 220-233.

[138] WANG J, YUE R X, PANG S Q. Construction of asymmetric orthogonal arrays of high strength by juxtaposition[J]. Communications in Statistics-Theory and Methods, 2019: 1-11.

[139] NEBE G, RAINS E M, SLOANE N J A. Self-dual codes and invariant theory: volume 17 [M]. Springer, 2006.

[140] GOUR G, WALLACH N R. Entanglement of subspaces and error-correcting codes[J]. Physical Review A, 2007, 76(4): 042309.

致　谢

不知不觉，科大五年时光即将接近尾声。科大给予了很多美好的回忆。

在这里，我要感谢我的导师张先得老师。张老师把我引领到量子信息理论这个方向，教会了我很多科研方法和写作技巧，并给予了我很多支持与鼓励。每次有量子信息理论方向上的会议，她都会让我积极参加。每次帮我修改论文时，她都是一遍又一遍地修改。即使在寒暑假，都能看到张老师的身影。张老师对科研严谨的态度让我非常钦佩。在生活上，张老师也给予了我们很多关心和照顾。非常感谢张老师的细心栽培。

感谢首都师范大学的葛根年老师。去北京交流的时候葛老师给我提供了一个舒适的科研环境与住宿条件，平时给我发了很多量子信息理论方向上的论文，开阔了我的视野。葛老师的团队有很多优秀的老师和同学，加入他的团队，是我的荣幸。

感谢北京航空航天大学的陈霖老师。陈老师知识渊博，在量子信息理论方向上给予了我很多指导。当我决定要申请去国外交流的时候，陈老师帮我找了很多国外的导师，给我写推荐信。陈老师待我就像待他自己的学生一样，也给我了很多关于职业发展上的建议和规划。非常感谢陈老师一直以来的帮助。

感谢华南理工大学的李茂生老师。李茂生老师一直以来都是我学习的榜样，他是一个很纯粹的科研人，基础非常扎实，为人也很谦和。我和李老师有过很多次合作，和他讨论问题，让我对问题会有一个新的理解，也让我学到了很多知识。非常感谢李老师一直以来的合作。

感谢首都师范大学的费少明老师，费老师善于指导，思维敏捷，有幸能去他那里交流了一段时间。感谢山西大同大学的郭钰老师，有幸和他有过合作与交流。感谢山东大学的张一炜师兄，他带我一起研究了不可扩充乘积基的问题。

感谢一起学习的同学：陈婷婷、叶左、余文俊、邓治、马一鸣、魏歆、李言智、章宛晨、于克凡、张树亮、何奕昀、任年新、王飞、王国平、吴荣胜、王运韬、朱玮奇、王琛、杨倩倩、高俊、杨天驰、火清羿、祖春蕾、谢天颖、何家林、邱榆、刘西之、曹梦月、严炜、邵文炳、黄炳儒、唐文强、王镇、姚金翔、古艳东、张煜明、张裕烽、胡梦瑶、沈毅、臧亚娟、孔祥梁、兰昭君。

感谢我的父母，对我一直以来的支持、理解与包容。感谢我的爱人及其家人，对我一直以来的陪伴与鼓励。

石飞

2022 年 3 月

在读期间发表的学术论文与取得的研究成果

已发表论文

1. **Fei Shi**, Yi Shen, Lin Chen, and Xiande Zhang, "k-Uniform states in heterogeneous systems", *IEEE Transactions on Information Theory*, 68(5), 3115-3129 (2022).
2. **Fei Shi**, Zuo Ye, Lin Chen, and Xiande Zhang, "Strong quantum nonlocality in N-partite systems", *Physical Review A*, 105, 022209 (2022).
3. **Fei Shi***, Mao-Sheng Li*, Mengyao Hu, Lin Chen, Man-Hong Yung, Yan-Ling Wang, and Xiande Zhang, "Strongly nonlocal unextendible product bases do exist", *Quantum*, 6, 619 (2022). ("$*$" 为共同一作)
4. **Fei Shi**, Mao-Sheng Li, Lin Chen, and Xiande Zhang, "k-uniform quantum information masking", *Physical Review A*, 104, 032601 (2021).
5. **Fei Shi**, Mao-Sheng Li, Lin Chen, and Xiande Zhang, "Strong quantum nonlocality for unextendible product bases in heterogeneous systems", *Journal of Physics A: Mathematical and Theoretical*, 55, 015305 (2021).
6. **Fei Shi**, Mengyao Hu, Lin Chen, and Xiande Zhang, "Strong quantum nonlocality with entanglement", *Physical Review A*, 102, 042202 (2020).
7. **Fei Shi**, Xiande Zhang, and Lin Chen, "Unextendible product bases from tile structures and their local entanglement-assisted distinguishability", *Physical Review A*, 101, 062329 (2020).
8. **Fei Shi**, Yi Shen, Lin Chen, and Xiande Zhang, "Bounds on the number of mutually unbiased entangled bases", *Quantum Information Processing*, 19(10), 383 (2020).
9. **Fei Shi**, Xiande Zhang, and Yu Guo, "Constructions of unextendible entangled bases", *Quantum Information Processing*, 18(10), 324 (2019).

---

10. Mao-Sheng Li, **Fei Shi**, Yan-Ling Wang, "Local discrimination of generalized Bell states via commutativity", *Physical Review A*, 105, 032455 (2022).
11. Yiwei Zhang, **Fei Shi**, Xiande Zhang, Yiting Yang, and Gennian Ge, "New results on unextendible product bases", *SCIENTIA SINICA Mathematica*, 51, 11 (2021).
12. Mao-Sheng Li, Yan-Ling Wang, **Fei Shi**, and Man-Hong Yung, "Local distinguishability based genuinely quantum nonlocality without entanglement", *Journal of Physics A: Mathematical and Theoretical*, 54, 445301, (2021).

待发表论文

1. Yiyun He, **Fei Shi**, and Xiande Zhang, "Strong quantum nonlocality and unextendibility without entanglement in N-partite systems with odd N", *arXiv:2203.14503* (2022).
2. **Fei Shi***, Mao-Sheng Li*, Mengyao Hu, Lin Chen, Man-Hong Yung, Yan-Ling Wang, and Xiande Zhang, "Strong quantum nonlocality from hypercubes", *arXiv:2110.08461* (2021). ("∗" 为共同一作)
3. Mengyao Hu, Lin Chen, **Fei Shi**, and Xiande Zhang, "Unextendible product operator basis", *arXiv:2109.13537* (2021).

荣誉奖项

1. 博士生国家奖学金，2021 年
2. 王小谟网络空间科技英才优秀学生奖学金，2020 年
3. 信息学院优秀共产党员，2020 年