arXiv:2603.03182v1 [quant-ph] 3 Mar 2026

稳定子框架之外的纠缠辅助码

JASZMINE DEFRANCO* 与ANDREW NEME C†

我们表明，通过将任意量子码与面向擦除信道的量子码相关联，可以由任意量子码构造纠缠辅助码。若某一子集的物理量子比特对擦除错误是可纠正的，则它自然构成一个双部态中接收方的份额，该双部态可用于纠缠辅助通信，这在无噪声与有噪声纠缠比特错误模型中均成立。对于简并码，我们表明双部态中接收方的份额有时可以被压缩，代价是在有噪声纠缠比特错误模型中纠错能力可能降低。我们还给出置换不变纠缠辅助码与XP稳定子纠缠辅助码的例子，这是稳定子框架与码字稳定框架之外的首批此类编码。

1. Introduction

量子纠错码 [1, 2, 3, 4, 5] 对于经由噪声信道忠实传输量子信息是必要的，从而使可靠的量子通信与量子计算成为可能。自Shor [1], 演示首个量子码以来，量子编码理论进展迅速，尤其是在引入稳定子形式体系 [4, 5]之后。该框架利用自正交经典码构造量子码，使量子编码理论研究者能够借助经典编码理论中已有的大量研究成果。

量子通信中的一个重要信道是 Grassl 等人提出的量子擦除信道 [6], ，在该信道中，任意错误会影响一组已知的量子比特。最小距离为 d 的量子码能够纠正 $d-1$ 个擦除，相较之下，它可以纠正作用于未知量子比特集合的 $\lfloor (d-1)/2 \rfloor$ 个任意错误。利用这种更强纠错能力的可能性，促使近年来有关擦除转换的大量研究蓬勃发展 [7, 8, 9], ： 通过以特定方式选择物理量子比特，使物理噪声导致可检测到的量子比特子空间外泄漏；擦除转换已在各种平台上实现 [10, 11, 12, 13]。此外，量子擦除编码自然出现在量子密码学中，尤其是量子秘密共享方案 [14, 15],；它们也出现在黑洞理论中，相关研究探讨了反德西特/共形场论对应、量子纠错与量子秘密共享之间的联系 [16, 17, 18, 19, 20]。

在量子世界中，发送方通过有噪声信道向接收方传输量子比特，并不是最一般的协议类型。一些早期的量子通信协议，例如超密编码 [21]和量子隐形传态 [22], 属于“纠缠辅助”（EA）协议，即在协议开始之前，发送方和接收方共享一定数量的无噪声纠缠量子比特（纠缠比特）。Bowen 首先

提出了纠缠辅助量子纠错（EAQEC），展示了这样一种可能性：假设发送方和接收方预先共享两个纠缠比特 [23]，便可以使用三个物理量子比特发送一个逻辑量子比特，并纠正作用于一个量子比特的任意错误。

Brun 等人 [24, 25]将 Bowen 码完全纳入一种新的纠缠辅助稳定子框架，从而取消了所用经典码必须自正交的限制。这大大增加了可用于构造量子码的经典码类型，只要参与者拥有一定量预先共享、并能作为资源使用的纠缠。此后，围绕纠缠辅助量子纠错涌现了大量工作，包括纠缠辅助量子卷积码 [26, 27, 28], 纠缠辅助经典码 [29, 30], 纠缠辅助码界 [31, 32, 33, 34],以及对码字稳定框架的推广 [35, 36] ，以及与子系统和量子-经典混合码的整合 [37, 38, 39, 40]。通常使用两种不同的错误模型：无噪声纠缠比特错误模型 [24], ，其中双部态中接收方的份额不经历噪声；以及有噪声纠缠比特错误模型 [41], ，其中接收方的份额可能经历噪声。关于纠缠辅助量子纠错的介绍，见 [42]。

利用现有量子码构造纠缠辅助码已得到广泛研究 [41, 43, 44, 45, 46]；然而，这些研究主要局限于非简并稳定子码，且通常通过对大小小于 d 的子集进行类似穿孔的过程来实现。本文将通过考察在擦除信道下可纠正的子集，说明任何量子码都可以轻松转换为纠缠辅助码。具体而言，我们表明，Chitambar 等人最近给出的替换码结构定理 [47] 能够自然地确定发送方和接收方共享的双部态，以及发送方的编码酉算子，从而使我们得以构造首批不属于稳定子框架或码字稳定框架的纠缠辅助码。我们还表明，退化可纠正集合可能产生一种接收方共享部分经过压缩的纠缠辅助码，但代价是，在有噪声纠缠比特错误模型下，接收方的量子比特无法得到错误保护。

本文的结构如下。第 2 节简要回顾擦除信道的量子码以及本文后续内容所需的纠缠辅助量子纠错基础。第 3 节展示 [47] 的结构定理如何导出纠缠辅助量子码的构造，并给出置换不变框架和 XP 稳定子框架中的若干纠缠辅助码新例子。第 4 节说明，原始码的简并性可能使接收方所需共享的纠缠更少，但在有噪声纠缠比特错误模型中，也可能因此丧失对接收方量子比特的纠错保护。最后，第 5 节给出一些总结性评论，并探讨未来可能的研究方向。

2. 背景

下面回顾本文所需的量子纠错领域相关成果。本文始终仅讨论量子比特码。

2.1. 量子纠错。 量子纠错码 $\mathcal{C}$ 是一个 n量子比特希尔伯特空间 $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$中的 K维子空间。我们将$\{|\widetilde{i}\rangle\}_{i=0}^{K-1}$ 记作该编码 $\mathcal{C}$的一组标准正交基。如果存在一个恢复算子 ，使得

存在一个恢复算子 $\mathcal{R}$，使得

$$\mathcal{R}\left(E|\widetilde{\psi}\rangle\langle\widetilde{\psi}|E^{\dagger}\right) \propto |\widetilde{\psi}\rangle\langle\widetilde{\psi}| \tag{1}$$

$\widetilde{}$对所有 $|\psi\rangle \in \mathcal{C}$ 都成立。Knill 和 Laflamme 在 [48] 中给出了一个关于投影到编码子空间上的正交投影算子 P 的等价条件：

定理 1（量子子空间码的纠错条件）。设 $\mathcal{C} \subseteq \mathcal{H}$ 是一个投影算子为 P 的量子码。那么，当且仅当满足以下条件时，$\mathcal{C}$ 能纠正错误集合 $\mathcal{E} \subseteq \mathcal{L}$（$\mathcal{H}$）

$$P\left(E_i^{\dagger}E_j\right)P = \lambda_{ij}P, \tag{2}$$

对所有 E_i、$E_j \in \mathcal{E}$ 均成立，其中 $\lambda_{ij} \in \mathbb{C}$。

算子 $\cdot$ 的汉明重量 wt(·) 是其非平凡作用的物理量子比特数量。纠错能力最常用的度量是编码 [1] 的最小距离 d：最小距离为 d 的编码可以纠正任何满足 wt(E) $\leq \lfloor (d-1)/2 \rfloor$、且对编码有非平凡作用的错误 E，可以检测任何满足 wt(E) $\leq d-1$ 的错误 E，并可以纠正对 $d-1$ 个或更少物理量子比特的任何擦除。若量子码 $\mathcal{C}$ 是希尔伯特空间中一个 K 维子空间，该空间包含 n 个物理量子比特且最小距离为 d，则称其参数为 $((n, K, d))_2$。本文后续将省略表示局部维数的下标，因为我们将讨论范围限定在量子比特码。

一类重要的量子码是稳定子码 [4, 5], ，它们是根据 n 量子比特泡利群 $\mathcal{P}_n$ 定义的。令 $\mathcal{S}$ 为 $\mathcal{P}_n$ 的一个不包含 $-I$ 的阿贝尔子群。稳定子码 $\mathcal{C}$ 是由 $\mathcal{S}$ 稳定的子空间（我们将其称为该编码的稳定子群）：

$$\mathcal{C} = \operatorname{span}\{|\psi\rangle \mid S|\psi\rangle = |\psi\rangle,\ \forall S \in \mathcal{S}\}. \tag{3}$$

如果 $\mathcal{S}$ 有 $n-k$ 个独立生成元，那么 $\mathcal{C}$ 可以编码 k 个逻辑量子比特，即 dim($\mathcal{C}$) $= K = 2^k$。因此，我们通常将稳定子码的参数写作 $[\![n, k, d]\!]$，以便将其与非加性（即非稳定子）量子码的参数区分开来。

对于稳定子群，在 $\mathcal{P}_n$ 中的正规化子 $N(\mathcal{S})$ 与中心化子 $C(\mathcal{S})$ 等价，它们包含所有与 $\mathcal{S}$ 的每个元素都对易的 Pauli 算子。因此，由于 $\mathcal{S}$ 是阿贝尔的，必有 $\mathcal{S} \leq N(\mathcal{S})$。该群的元素在码空间上充当逻辑泡利算子。对于稳定子框架中的编码，我们可以将编码的最小距离提取为

$$d = \min \operatorname{wt}(N(\mathcal{S}) - \langle \mathcal{S}, iI\rangle), \tag{4}$$

也就是说，d是最小非平凡逻辑算符的权重。

2.2. 擦除信道与替换信道。量子信道是两个希尔伯特空间 $\mathcal{H}$ 和 $\mathcal{K}$上的算子之间的完全正且保迹映射 $\mathcal{E}: \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$。对于 $\mathcal{H} = B \otimes B$的任意量子比特子集 M，存在一族定义在 $\mathcal{H}$ 上的量子替换信道，定义如下：

$$\mathcal{E}_B : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}),\ \rho \mapsto \rho_{\overline{B}} \otimes \sigma_B, \tag{5}$$

[1]通常更容易通过 Knill-Laflamme 错误检测条件来定义最小距离：$d = \min\{\text{wt}(E) \mid PEP \neq \lambda_E P,\ E \in \mathcal{L}(\mathcal{H})\}$。

其中，ρ_B=Tr$_B(\rho)$ 是 B 上的约化态， σ_B 是一个固定的“替换态”，对所有输入都相同。替换信道可以看作是在子集 B上施加擦除信道，随后将丢失的量子比特重置为已知状态 σ_B。

最近，Chitambar 等人 [47] 提出了量子替换码的结构定理，综合了此前关于可通过酉变换恢复的码 [49, 50]的研究成果。这些码能够从作用于 b 个量子比特子集 B上的量子替换信道 $\mathcal{E}_B$ 中恢复；该信道会将 B 上的所有状态映射到某个固定状态 σ_B。下文中，我们将错误信道限定为在 B上完全退极化的信道，这等价于具有最大混合态 $\sigma_B = I_B/2^b$（B上的最大混合态）的替换信道。众所周知，对一组量子比特进行完全退极化的信道，可以建模为一个量子信道，其 Kraus 算子是该空间上的 Pauli 算子；此外，只要 Kraus 算子构成算子 [51, 的标准正交基，同样的结论也成立。引理 4.1]:

$$\frac{1}{\dim(\mathcal{H})^2}\sum_{E\in\mathcal{E}} E\rho E^\dagger = \frac{I_{\mathcal{H}}}{\dim(\mathcal{H})}, \tag{6}$$

对于任意密度矩阵 $\rho \in \mathcal{L}(\mathcal{H})$，其中 $\mathcal{E}$ 构成了 $\mathcal{L}(\mathcal{H})$的标准正交基。若已知量子比特子集 B 能够从作用于 B上的完全退极化信道中恢复，或者等价地，该编码的可纠正错误 $\mathcal{E}$ 集合包含 $\mathcal{L}(B)$的一个标准正交基，则称该子集是可纠正的。

我们仅给出与本文相关的结构定理部分：

定理 2 ([47, 结构定理])**.** 设 $\mathcal{C}$ 是一个量子码，其标准正交基为 $\{|\tilde{i}\rangle\}$，且 B 是 b 个物理量子比特的已知子集。则以下条件等价：

(1) 量子比特集合 B 对于编码 $\mathcal{C}$是可纠正的。(2) 存在一个参考系统 R =张成 $\{|i\rangle\} \cong \mathcal{C}$、一个辅助系统 A，满足(维数 A)(维数 $\mathcal{C}$) $\leq$维数 B，一个等距映射 U_B: $RA \to B$，以及一个密度算符 $\tilde{\ }$ $\tilde{\ }$*tor* σ_{AB}，使得对于所有支撑在 $\mathcal{C}$上的 $\tilde{\rho} = \sum_{ij}\alpha_{ij}|i\rangle\langle j|$，都有

$$\mathcal{E}_B(\tilde{\rho}) = \left(\mathcal{U}_{\overline{B}} \otimes I_B\right)\left(\rho_R \otimes \sigma_{AB}\right),$$

其中 $\rho_R = \sum_{ij}\alpha_{ij}|i\rangle\langle j|_R$ 和 $\mathcal{U}_B(\underline{\cdot}) = U_B(\underline{\cdot})U_B^\dagger$。此外，我们有

$$\sigma_{AB} = \Gamma_A \otimes I_B/2^b,$$

对于某个密度算子 Γ_A。

(3) 存在一个参考系统 R =span$\{|i\rangle\} \cong \mathcal{C}$、一个辅助系统 A，其维数为(dim A)(dim $\mathcal{C}$) $\leq$dim B，一个等距映射 U_B: $RA \to B$，以及一个态 $|\tilde{\psi}\rangle_{AB}$，它们均由 B 和 $\mathcal{C}$ 决定，使得对于所有 $|i\rangle \in \mathcal{C}$，我们有

$$|\tilde{i}\rangle = \left(U_{\overline{B}} \otimes I_B\right)\left(|i\rangle_R \otimes |\psi\rangle_{AB}\right).$$

Bravyi 和 Terhal 的清除引理 [52], 对稳定子码中的可纠正集合给出了一个有用的刻画。该引理指出，对于一个稳定子群为 $\mathcal{S}$ 的稳定子码中的量子比特集合 B，以下两者必有其一：

（1）存在一个非平凡逻辑算符 $L \in N(\mathcal{S}) - \langle\mathcal{S},\ iI\rangle$ 使得 supp$(L) \subseteq B$；或者（2）对于任意逻辑算符 $L \in N(\mathcal{S})$，都存在一个稳定子 $S \in \mathcal{S}$ 使得 supp$(LS) \subseteq B$。—

第二种情况称为“清除”子系统 B，是 B 可纠正的等价条件。[2] 作为定理 2的推论，我们得到了清除引理情形（2）的一种推广，尽管只在一个方向上成立：

推论3。设 $\mathcal{C}$ 是一个投影算子为 P的量子码。如果 B 是 $\mathcal{C}$的可纠正子集，那么码空间上不存在非平凡的逻辑算子 L，使得 $\operatorname{supp}(L) \subseteq B$。此外，任何作用于参考系统 R上的逻辑酉算子 V，都有一个等效的物理酉算子 $\widetilde{V}$作用于 $\mathcal{C}$，使得 $\operatorname{supp}\left(\widetilde{V}\right) \subseteq B$。

证明。第一个结论由 [47, 推论 4.8]得出。第二个结论可由定理 2 推得，其中令 $V = \mathcal{U}_B(V_R \otimes I_A)$。□

2.3. 纠缠辅助量子纠错。量子码的设计仅假设发送方和接收方之间共享一条量子信道。然而，如果考虑双方共享一定量纠缠的情形，就会得到更一般的纠缠辅助（EA）量子码。这类量子码最初由 Bowen [23]提出，随后由 Brun 等人 [24, 25] 纳入稳定子框架。下面我们回顾纠缠辅助稳定子码的构造。

与稳定子码的情形一样，我们取一个不包含 $-I$ 的泡利子群 $\mathcal{S} \leq \mathcal{P}_n$ 作为稳定子群，但在这里允许 $\mathcal{S}$ 是非阿贝尔的。我们总能找到一组生成元 $\mathcal{S} = \langle Z_1, \ldots, Z_{c+s}, X_1, \ldots, X_c \rangle$，使其满足标准的泡利对易关系：

$$\left[\widetilde{Z}_i, \widetilde{Z}_j\right] = 0 \qquad \forall\, i, j, \tag{7}$$

$$\left[\widetilde{X}_i, \widetilde{X}_j\right] = 0 \qquad \forall\, i, j, \tag{8}$$

$$\left[\widetilde{X}_i, \widetilde{Z}_j\right] = 0 \qquad \forall\, i \neq j, \tag{9}$$

$$\left\{\widetilde{X}_i, \widetilde{Z}_i\right\} = 0 \qquad \forall\, i, \tag{10}$$

其中，$[M, N]$ 是两个矩阵 M 和 N 的对易子，$\{M, N\}$ 是它们的反对易子。迷向子群为 $\mathcal{S}_I = \langle Z_{c+1}, \ldots, Z_{c+s} \rangle$，而辛（或纠缠）子群为 $\mathcal{S}_S = \langle Z_1, \ldots, Z_c, X_1, \ldots, X_c \rangle$。$s$ 和 c 的值分别表示编码所需的辅助量子比特数和纠缠比特数。我们将纠缠辅助稳定子码的参数记为 $[\![n, k, d; c]\!]$。

由于稳定子群 $\mathcal{S}$ 是非阿贝尔的，因此它不会稳定任何子空间。不过，存在一个酉映射 U，使得 $U\widetilde{Z}_i U^\dagger = Z_i$（即仅作用于第 i 个量子比特的 Pauli-Z 算符）以及 $U\widetilde{X}_i U^\dagger = X_i$，从而得到 c 对反对易的 X 和 Z，以及 s 个额外的未配对 Z 算符。为了得到一组对易算符，我们可以扩展辛子群生成元：在每个反对易配对中的 Z_i（分别为 X_i）末尾追加一个 Z（分别为 X）算符，从而得到一对新的对易稳定子生成元。请注意，每个反对易配对都必须添加一个新的物理量子比特。我们

[2]这似乎是一个众所周知的结果；我们能够找到的文献中首次给出证明的是 Ashikhmin，时间相对较近，见 [53, 定理 1]。不过，我们注意到，该结果可直接由 Rains 关于量子码的酉枚举子的早期结果推出（参见 [54, 定理 10]之后的讨论）。

随后可以对原始量子比特应用 $U^\dagger$，从而得到一个纠缠辅助码。所得编码中的编码向量将具有以下形式

$$\left(U_B^\dagger \otimes I_B\right)\left(|\psi\rangle_R |0\rangle_S^{\otimes s} |\Phi\rangle_{AB}^{\otimes c}\right), \tag{11}$$

其中，$U_B^\dagger$：$RSA \to B$ 和 $|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 是最大纠缠贝尔态，我们将其称为纠缠比特。如果发送方和接收方共享 c 个纠缠比特，那么发送方就可以借助 s 个辅助态以及自己持有的纠缠比特，将状态 $|\psi\rangle$编码到编码中。

例4. 这里我们展示如何将 *Bowen* 的原始 $[\![3,1,3;2]\!]$ 纠缠辅助码纳入稳定子框架。我们从一个非阿贝尔稳定子群 $\mathcal{S} = \langle XZZ, ZYY, ZZX, YYZ\rangle$开始，它可以划分为两对反对易对。由此，存在一个酉算子 U，可将稳定子生成元变换为单量子比特泡利算符，随后还可对其进行扩展。这两对扩展生成元稳定两个纠缠比特，它们可以在发送方和接收方之间分配。之后，发送方可以对消息及自己持有的纠缠比特半部施加编码酉算子 $U^\dagger$，将其编码到码空间中：

$$\begin{array}{rcccc}
\widetilde{X}_1 & = & X & Z & Z \\
\widetilde{Z}_1 & = & Z & Y & Y \\
\widetilde{X}_2 & = & Z & Z & X \\
\widetilde{Z}_2 & = & Y & Y & Z
\end{array}
\overset{U}{\longmapsto}
\begin{array}{ccc}
X & I & I \\
Z & I & I \\
I & X & I \\
I & Z & I
\end{array}$$

$$\overset{extend}{\longmapsto}
\left[\begin{array}{ccc|cc}
X & I & I & X & I \\
Z & I & I & Z & I \\
I & X & I & I & X \\
I & Z & I & I & Z
\end{array}\right]$$

$$\overset{U^\dagger \otimes I_4}{\longmapsto}
\left[\begin{array}{ccc|cc}
X & Z & Z & X & I \\
Z & Y & Y & Z & I \\
Z & Z & X & I & X \\
Y & Y & Z & I & Z
\end{array}\right]$$

这些扩展稳定子稳定的码空间，与完美的 $[\![5,1,3]\!]$ 稳定子码 [55, 56], 的码空间相同，但分布在发送方和接收方两处。

如果假设预共享纠缠比特不受噪声影响，那么系统中的任何噪声都必定作用于通过发送方与接收方之间的量子信道传输的量子比特。与非纠缠辅助情形类似，我们可以根据稳定子群计算纠缠辅助稳定子码的最小距离：

$$d = \min \mathrm{wt}(N(\mathcal{S}) - \langle \mathcal{S}_I, iI\rangle), \tag{12}$$

也就是说，d 是发送方量子比特上最小非平凡逻辑算符的权重。

本文最关注的问题是如何利用已有的量子码构造纠缠辅助码。虽然已有多项相关成果（参见 [41, 43, 44, 45, 46]），但这些成果主要局限于非简并稳定子码，并通过对大小小于 d 的子集执行删位过程来实现。其中最完整的是 Grassl 等人 [45] 提出的以下结果：

定理5 ([45, 定理 10])。设 $\mathcal{C}$ 是一个纯 $[\![n,k,d]\!]$ 量子码。则对于所有 $c < d$，都存在参数为 $[\![n-c,k,d;\ c]\!]$ 的纠缠辅助码。

注 6。 *Grassl* 等人在 [45, 定理 10] 中给出的构造与该主题的其他结果不同之处在于，它适用于一般的纯量子码，包括稳定子框架之外的量子码。然而，由于他们对所得纠缠辅助码使用了稳定子式参数，并且没有给出任何非加性纠缠辅助码的示例，这一点可能被忽视了。

在本文后续部分，我们通过在例 *12*、*13* 和 *17* 中给出稳定子框架与码字稳定框架之外的首批纠缠辅助码示例来弥补这一不足。此外，我们在定理 *10* 和 *16* 中将其结果推广到任意量子码，所依据的是更一般的可纠正子集概念，该概念涵盖了规模小于最小距离的集合。

3. Entanglement-Assisted Subspace Codes

在构造纠缠辅助码时，可能存在两种错误模型：无噪声纠缠比特 [24] 和有噪声纠缠比特 [41]。在无噪声纠缠比特错误模型中，我们假定纠缠比特不受任何噪声影响，因此任何错误都必须发生在 B 的量子比特上，即它们通过量子信道传输之时。在有噪声纠缠比特错误模型中，我们不作此假定，既允许纠缠比特在开始之前存在不完美，也允许在等待B 传输期间可能发生在 B 上的错误。

由于此前关于纠缠辅助码的研究主要局限于稳定子框架，纠缠辅助纠错条件也以同一语言加以表述。我们通过给出 Knill-Laflamme 式纠错条件，开始对非加性纠缠辅助码的研究。

定理 7（无噪声纠缠比特的纠错条件）**.** 设 $\mathcal{C} \subseteq B \otimes B$ 为具有投影算子 $\overline{P}$的量子码。则 $\mathcal{C}$ 能够纠正错误集 $\mathcal{E} \subseteq \mathcal{L}\big(B\big)$，当且仅当

$$P\left(E_i^\dagger E_j \otimes I_B\right) P = \lambda_{ij} P, \tag{13}$$

对所有 E_i、$E_j \in \mathcal{E}$，其中 $\lambda_{ij} \in \mathbb{C}$。

定理 8（有噪声纠缠比特的纠错条件）**.** 设 $\mathcal{C} \subseteq B \otimes B$ 为具有投影算子 $\overline{P}$的量子码。则 $\mathcal{C}$ 能够纠正错误集 $\mathcal{E} \subseteq \mathcal{L}\big(B \otimes B\big)$，当且仅当

$$P\left(E_i^\dagger E_j\right) P = \lambda_{ij} P, \tag{14}$$

对所有 E_i、$E_j \in \mathcal{E}$，其中 $\lambda_{ij} \in \mathbb{C}$。

请注意，前一个结果是定理 1 中标准纠错条件的一个特例，而后一个结果则与之等价。本节余下部分的结果通常对无噪声和有噪声纠缠比特错误模型均成立，而第 4 节中的结果通常仅适用于无噪声纠缠比特错误模型。

从量子码构造纠缠辅助码的关键在于确定信息传输之前接收方可以持有哪些子集。推论3是清除引理的一个部分推广 [52],，它指出，如果一组量子比特 B 是可纠正的，也就是说，编码可以从对 B的擦除中恢复，那么没有非平凡逻辑算符的支撑集会落在 B上；此外， B 拥有一组完备的 $\overline{}$

支撑在其上的逻辑算符。本质上，编码时发送方无需访问 B，因为她总能构造一个~ _ ~ ~ ~V，其作用仅限于 B，并将 $|0\rangle \mapsto |\psi\rangle$映射到她打算发送的编码态 $|\psi\rangle$。

定理 9. 假设 $\mathcal{C}$是一个$((n, K, d))$量子码，其可纠正集合 B包含 b个量子比特。那么，通过预先向接收方发送 B， $\mathcal{C}$也是一个 $\big((n-b, K, d; 2^b)\big)$纠缠辅助码。

证明。 由推论3及前述讨论可得。 □

在此，我们用 C 表示接收方所持子系统的维数，并将一般纠缠辅助码的参数记为$\mathbf{((}n, K, d\mathbf{;}\ C\mathbf{))}$，以类比非加性码的参数。这使得双体态可以超出纠缠辅助稳定子情形中的 m个共享贝尔对，也包括发送方与接收方之间并非最大纠缠的双体态。对于 $[\![n, k, d; c]\!]$纠缠辅助稳定子码，我们有 $C = 2^c$。

定理 2《 [47]》的结构定理提出了另一种策略。对于码空间上的密度算子 $\widetilde{\rho}$，偏迹掉可纠正子集 B 后得到的约化态具有如下形式

$$\mathrm{Tr}_B(\widetilde{\rho}) = \widetilde{\rho}_{\overline{B}} = U_{\overline{B}} \left(\rho_R \otimes \Gamma_A\right) U_{\overline{B}}^\dagger, \tag{15}$$

其中U_B ÷$RA \to B$ 是一个等距映射，而 Γ_A 是某个密度矩阵。于是存在 $|\psi\rangle_{AB}$ 的一个纯化 Γ_A，使得

$$|\widetilde{i}\rangle = \left(U_{\overline{B}} \otimes I_B\right)\left(|i\rangle_R \otimes |\psi\rangle_{AB}\right) \tag{16}$$

对于 $\mathcal{C}$的所有基态 $|i\rangle$，均有~。

定理 10。 设 $\mathcal{C}$是一个 $((n, K, d))$ 量子码，其具有一个包含 b 个量子比特的可纠正集合 B。则存在一个双部态 $|\psi\rangle_{AB}$ 和一个编码等距算子 U_B，发送方和接收方可以使用它们，使 $\mathcal{C}$成为一个 $\big((n-b, K, d;\ 2^b)\big)$ 纠缠辅助编码。

证明。 由定理 2 及前文讨论可得。 □

采用这两种策略构造的任何纠缠辅助码都与原始码相同，因此能够纠正相同的一组错误。本文余下部分将重点讨论采用后一种方法构造的编码，因为这种方法推广了 [23, 24, 41] 中已有的成熟纠缠辅助方案。下文将展示如何应用结构定理来构造一些已有的和新的纠缠辅助码。

例 11. 在 [47, 例4.7]，中，作者将结构定理应用于完美的 $[\![5, 1, 3]\!]$ 稳定子码，得到一个编码酉算子和一个由两个纠缠比特组成的纠缠态。它们与 ***Bowen*** [23] 利用 $[\![5, 1, 3]\!]$ 编码构造的原始 $[\![3, 1, 3; 2]\!]$ 纠缠辅助码的编码酉算子和共享纠缠完全相同（见例*4*）。

迄今为止，所有纠缠辅助码的示例都来自稳定子形式体系 [24], 、其推广——码字稳定（CWS）形式体系 [35, 36],，或隐形传态式方案 [32]。定理 10 允许从任意量子码构造纠缠辅助码，包括稳定子框架和码字稳定框架之外的量子码。正如注 6 所述，这一构造

推广了 Grassl 等人在 [45, 定理 10], 中给出的构造，该构造同样适用于稳定子框架之外的纯码。然而，我们的构造也适用于非纯码（第 4 节将对此作进一步阐述），并且适用于任意可纠错集合，而不仅仅是大小小于最小距离的集合 d。下面我们将给出置换不变 [57] 码和 XP 稳定子码 [58, 59], 的纠缠辅助码示例，这两类码都不属于通常的稳定子框架和 CWS 框架。

例 12. 置换不变（*PI*）编码在物理量子比特的任意置换下保持不变。因此，它们是 n 量子比特对称子空间的子空间，该对称子空间以 ***Dicke*** 态 $\{|D_i^n\rangle\}_{i=0}^n$ 为基，其中

$$|D_i^n\rangle = \frac{1}{\sqrt{\binom{n}{i}}} \sum_{\mathrm{wt}(x)=i} |x\rangle$$

是汉明重量为 i 的计算基态的均匀叠加。***Aydin*** 等人 [60] 定义了一个 $((4,\ 2,\ 2))$ ***PI*** 码，其逻辑基态为

$$|\tilde{0}\rangle = \frac{\sqrt{3}}{3}|D_0^4\rangle + \frac{\sqrt{6}}{3}|D_3^4\rangle,$$
$$|\tilde{1}\rangle = \frac{\sqrt{6}}{3}|D_1^4\rangle - \frac{\sqrt{3}}{3}|D_4^4\rangle.$$

对于擦除一个物理量子比特，我们遵循定理 *2*（不失一般性，选择˜ ˜量子比特 *4*）。选择 $\tilde{\rho} = |0\rangle\langle 0|$，我们得到

$$\mathrm{Tr}_4(\tilde{\rho}) = \frac{1}{2}\left(|c_0\rangle\langle c_0| + |c_1\rangle\langle c_1|\right),$$

其中

$$|c_0\rangle = \frac{\sqrt{6}}{3}|D_0^3\rangle + \frac{\sqrt{3}}{3}|D_3^3\rangle,$$
$$|c_1\rangle = |D_2^3\rangle.$$

因此 $A = \mathbb{C}^2$ 和 $\Gamma_A = \frac{1}{2}I_2$，所以我们可以通过其对基态的作用定义等距映射 U_B：

$$\begin{array}{cccc} R & A & U_{\overline{B}} & \overline{B} \\ \hline |0\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} \frac{\sqrt{6}}{3}|D_0^3\rangle + \frac{\sqrt{3}}{3}|D_3^3\rangle \\ |D_2^3\rangle \end{cases} \\ |1\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} |D_1^3\rangle \\ \frac{\sqrt{3}}{3}|D_0^3\rangle - \frac{\sqrt{6}}{3}|D_3^3\rangle \end{cases} \end{array}$$

那么，对于 $i = 0,1$ 我们有

$$|\tilde{i}\rangle = \left(U_{\overline{B}} \otimes I_B\right)\left(|i\rangle_R \otimes |\psi\rangle_{AB}\right),$$

其中 $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 是 Γ_A 的纯化。

假设发送方和接收方分别持有子系统 A 和 B，发送方能够使用等距映射U_B将消息与她持有的纠缠比特的另一半一起编码。因此，我们得到一个 $((3,\ 2,2;\ 2))$ 纠缠辅助*PI*码。

例 13. ***XP*** 稳定子形式体系是标准稳定子形式体系的推广，因为稳定子生成元取自群 $\langle \omega I,$ $X, P\rangle^{\otimes n}$，其中 $\omega = e^{i\pi/N}$, $P = \mathrm{diag}\left(1, \omega^2\right)$，而 N 是一个固定的正整数，称为

精度。*Webster* 等人 $[59, \text{例 } 6.3]$ 给出了一个精度为 $N=8$ 的 $((7,8,2))$ *XP* 稳定子码，其编码基态为

$$
\begin{aligned}
|\widetilde{0}\rangle &= \frac{1}{\sqrt{2}}\left(|0000000\rangle + \omega^{12}|1111111\rangle\right)\\
|\widetilde{1}\rangle &= \frac{1}{\sqrt{2}}\left(|0000111\rangle + |1111000\rangle\right)\\
|\widetilde{2}\rangle &= \frac{1}{\sqrt{2}}\left(|0001011\rangle + \omega^{14}|1110100\rangle\right)\\
|\widetilde{3}\rangle &= \frac{1}{\sqrt{2}}\left(|0001101\rangle + \omega^{12}|1110010\rangle\right)\\
|\widetilde{4}\rangle &= \frac{1}{\sqrt{2}}\left(|0011110\rangle + |1100001\rangle\right)\\
|\widetilde{5}\rangle &= \frac{1}{\sqrt{2}}\left(|0011001\rangle + \omega^{8}|1100110\rangle\right)\\
|\widetilde{6}\rangle &= \frac{1}{\sqrt{2}}\left(|0010101\rangle + \omega^{10}|1101010\rangle\right)\\
|\widetilde{7}\rangle &= \frac{1}{\sqrt{2}}\left(|0010011\rangle + \omega^{12}|1101100\rangle\right)
\end{aligned}
$$

令可纠正集合 B 为量子比特 *7*。根据定理 *2*，我们取逻辑 $\widetilde{}$ 态 $|0\rangle$，并对 B 求偏迹，计算约化密度矩阵：

$$
\rho_B = \mathrm{Tr}_{\overline{B}}\Big(|\widetilde{0}\rangle\langle\widetilde{0}|\Big) = \frac{1}{2}(|000000\rangle\langle 000000| + |111111\rangle\langle 111111|), \tag{17}
$$

这意味着我们可以取 $\Gamma_A = \frac{1}{2}I_2$ 和 $A \cong \mathbb{C}^2$。我们可以构造一个等距映射U_B：$RA \to B$，使得

$$
|\tilde{i}\rangle = (U_{\overline{B}} \otimes I_B)(|i\rangle_R \otimes |\psi\rangle_{AB}), \tag{18}
$$

其中，$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 是 Γ_A 的纯化。具体而言，U_B 的作用如下：

$$
\begin{array}{ccccc}
R & A & U_{\overline{B}} & \overline{B} \\
\hline
|0\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} |000000\rangle \\ \omega^{12}|111111\rangle \end{cases} \\
|1\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} |111100\rangle \\ |000011\rangle \end{cases} \\
|2\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} \omega^{14}|111010\rangle \\ |000101\rangle \end{cases} \\
|3\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} \omega^{12}|111001\rangle \\ |000110\rangle \end{cases} \\
|4\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} |001111\rangle \\ |110000\rangle \end{cases} \\
|5\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} \omega^{8}|110011\rangle \\ |001100\rangle \end{cases} \\
|6\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} \omega^{10}|110101\rangle \\ |001010\rangle \end{cases} \\
|7\rangle & \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \longmapsto & \begin{cases} \omega^{12}|001001\rangle \\ |110110\rangle \end{cases}
\end{array}
$$

假设发送方持有 A，接收方持有 B，发送方使用U_B进行编码，并将 B 的 6个量子比特传送给接收方，我们得到一个 $((6、8、2;2))$ 纠缠辅助 *XP* 码。

4. Receiver Share Compression via Degeneracy

使用定理 10 构造的纠缠辅助码适用于有噪声和无噪声的纠缠比特错误模型。然而，特别是在无噪声纠缠比特错误模型中，如果接收方的量子比特需要多于必要数量，那么对这些量子比特的额外保护可能会被视为不必要，甚至造成浪费。一个自然的问题是，能否减少接收方所持份额的大小？本节将表明，只有当相关编码在可纠正子集 B 上针对擦除信道是简并的，才有可能减少接收方所持份额的大小。

为了对辅助系统上的密度矩阵 Γ_A 及其纯化进行分类，我们需要借鉴编码理论文献中的两组二分概念：一组是简并性与非简并性，另一组是纯性与混合性。设 $\mathcal{C}$ 为一个能够纠正线性无关错误集合 $\mathcal{E}$ 的量子码。根据 Knill-Laflamme 条件，对于所有 E_i， $E_j \in \mathcal{E}$，我们有 $PE_i^\dagger E_j P = \lambda_{ij} P$。众所周知，由系数组成的矩阵 λ 是厄米矩阵，因此可对角化。如果 $\mathrm{rank}(\lambda) = |\mathcal{E}|$，我们称该编码为非简并；如果 $\mathrm{rank}(\lambda) < |\mathcal{E}|$，则称其为简并。

如果对于所有无迹错误算符 $E \in \mathcal{E}$，编码均为 $PEP = 0$，则称其为纯编码；否则称为非纯编码。对于影响 B 的替换信道，这等价于：对 $\mathcal{C}$ 中的每个编码态，在将 B 迹出后，其约化密度算符均为秩为 2^b 的最大混合态。对于任意量子码，纯性意味着非简并性，因此得到以下三分法：

定理 14。设 $\mathcal{C}$ 为量子码， B 为 b 个量子比特的可纠正子集。则以下情况之一成立：

（1） $\mathcal{C}$ 相对于擦除 B 是纯的，且 ρ_B 为秩为 2^b的最大混合态。（2） $\mathcal{C}$ 相对于擦除 B 是非纯且非简并的，且 ρ_B 不是最大混合态，但其秩为 2^b。（3） $\mathcal{C}$ 相对于擦除 B 是简并的，且 ρ_B 的秩小于 2^b。

证明。对于情形（1），众所周知，编码是纯的，等价于相应擦除的边缘态为最大混合态（见 [45]）。

对于情形（3），我们首先对 Knill-Laflamme 矩阵 λ 进行对角化，方法是找到错误算符 $\{F_i\}$ 的标准正交基，使得 $\lambda_{ij} = 0$ 当且仅当 $i \neq j$。注意，如果$\varrho = P/K$ 是码空间的最大混合态，那么

$$\lambda_{ij} = \mathrm{Tr}\Big(\varrho \left(I \otimes F_i^\dagger\right)(I \otimes F_j)\Big) = \mathrm{Tr}\Big(\varrho_B F_i^\dagger F_j\Big), \tag{19}$$

对于对角项，我们有

$$\lambda_{ii} = \left\| \varrho_B^{1/2} F_i^\dagger \right\|^2. \tag{20}$$

假设 ϱ_B 是满秩的。那么 $\varrho_B^{1/2}$ 是可逆的，并且 $\varrho_B^{1/2} F_i^\dagger = 0$ 蕴含$F_i^\dagger = 0$。然而，这不可能发生，因为 $\{F_i\}$ 被选为标准正交基。因此 λ 也是满秩的。

现在假设秩$(\varrho_B) = r < 2^b$。我们可以选择基，使得

$$\varrho_B^{1/2} = \begin{pmatrix} \varrho_B^{1/2} & 0 \\ 0 & 0 \end{pmatrix}, \tag{21}$$

那么，任何形如

$$F_i = \begin{pmatrix} 0 & 0 \\ F & 0 \end{pmatrix} \tag{22}$$

满足 $\varrho_B^{1/2} F_i^\dagger = 0$，因此 $\lambda_{ii} = 0$。由于存在 $r\left(2^b - r\right)$ 个这样的线性无关算符，因此 λ 不是满秩的。

情形（2）包含了所有尚未涵盖的情况。 □

对于稳定子码这一特殊情形，纯性与非简并性等价，因此不会出现情形（2）。这给出了基于共享双体态对纯/非简并稳定子码的一种简洁刻画：

推论15. 设 $\mathcal{C}$ 是一个稳定子码， B 是 b 个量子比特的一个可纠正子集。那么，当且仅当 $\mathcal{C}$ 没有支撑在 B 上的稳定子时，我们可以选择 $|\psi\rangle_{AB}$ 为 b 个纠缠比特。

定理 14 完全确定了接收方的份额 B 何时可以被压缩：恰好当原始码对于 B 的擦除是简并的。利用这一认识，我们可以修改定理 10，从而允许更小的接收方份额规模。

定理 16. 假设 $\mathcal{C}$ 是一个具有由 b 个量子比特组成的可纠正集合 B 的 $((n, K, d))$ 量子码，并设 Γ_A 具有施密特秩为 C 的纯化 $|\psi'\rangle_{AB}$ 。如果态 $|\psi'\rangle_{AB}$ 在发送方与接收方之间被划分，则存在一个针对无噪声纠缠比特错误模型的 $((n-b, K, d; C))$ 纠缠辅助码。此外， $C < 2^b$ 当且仅当编码 $\mathcal{C}$ 对于 B 的擦除是简并的。

证明. 根据结构定理，存在一个等距映射 U_B ： $RA \to B$ ，使得

$$|\tilde{i}\rangle = \left(U_{\overline{B}} \otimes I_B\right)\left(|i\rangle_R \otimes |\psi\rangle_{AB}\right). \tag{23}$$

由于 Γ_A 的所有纯化在纯化系统上的等距映射意义下都是等价的，因此存在纯化 $|\psi'\rangle_{AB'}$ 与等距映射 V： $B' \to B$ ，使得 $\dim(B') = C$ 且 $|\psi\rangle_{AB} = (I_A \otimes V_{B'})$ $|\psi'\rangle_{AB'}$。因此，在从发送方接收到 B 后，接收方可以将 V 作用于其份额 B' ，然后使用编码 $\mathcal{C}$ 的标准解码器进行恢复。□

一种特殊的边界情形是，码空间由 B 与 B之间的乘积态构成，从而编码态 $|\phi\rangle \in \mathcal{C}$ 具有如下形式

$$|\widetilde{\phi}\rangle = |\widetilde{\phi}'\rangle_{\overline{B}} \otimes |\varphi\rangle_B, \tag{24}$$

其中 $|\varphi\rangle_B$ 与所编码的信息无关。此类编码经常出现在码传播规则 [5, 定理 6], 中，并且对 B的擦除总是简并的。在这种情况下，定理 16 中的共享双体态 $|\psi'\rangle$同样是一个乘积态，所得的纠缠辅助码现在实际上是一个已移除其无用子系统 B 的标准量子码。

利用定理 16 中的构造，我们考察两个例子：对于擦除各自可纠正子集的信道，这些编码是简并的。

例 17. *Kubischta* 和 *Teixeira* [61] 定义了一个$((7,\ 2,\ 3))$ *PI*码，其逻辑基态为

$$|\tilde{0}\rangle = \frac{\sqrt{15}}{8}|D_0^7\rangle + \frac{\sqrt{7}}{8}|D_2^7\rangle + \frac{\sqrt{21}}{8}|D_4^7\rangle - \frac{\sqrt{21}}{8}|D_6^7\rangle,$$
$$|\tilde{1}\rangle = -\frac{\sqrt{21}}{8}|D_1^7\rangle + \frac{\sqrt{21}}{8}|D_3^7\rangle + \frac{\sqrt{7}}{8}|D_5^7\rangle + \frac{\sqrt{15}}{8}|D_7^7\rangle.$$

对于两个物理量子比特的擦除，我们遵循结构定理（不失一般性˜ ˜，我们选取量子比特 *6* 和 *7*）。选择 $\tilde{\rho} = |0\rangle\langle 0|$ 后，我们看到

$$\mathrm{Tr}_{6,7}(\tilde{\rho}) = \frac{1}{3}\left(|c_0\rangle\langle c_0| + |c_1\rangle\langle c_1| + |c_2\rangle\langle c_2|\right),$$

其中

$$|c_0\rangle = -\frac{\sqrt{10}}{8}|D_1^5\rangle - \frac{3}{4}|D_3^5\rangle + \frac{3\sqrt{2}}{8}|D_5^5\rangle,$$
$$|c_1\rangle = \frac{\sqrt{70}}{14}|D_0^5\rangle + \frac{3\sqrt{14}}{14}|D_4^5\rangle,$$
$$|c_2\rangle = \frac{\sqrt{6}}{3}|D_0^5\rangle + \frac{\sqrt{3}}{3}|D_2^5\rangle.$$

因此，$A = \mathbb{C}^3$ 和 $\Gamma_A = \frac{1}{3}I_3$，所以我们可以通过其对基态的作用来定义等距映射 U_B：

R	A	$U_{\overline{B}}$	$\overline{B}$
$\|0\rangle$	$\begin{cases}\|D_0^2\rangle\\ \|D_1^2\rangle\\ \|D_2^2\rangle\end{cases}$	$\longmapsto$	$\begin{cases}\frac{3\sqrt{5}}{8}\|D_0^5\rangle + \frac{\sqrt{10}}{8}\|D_2^5\rangle + \frac{3}{8}\|D_4^5\rangle\\ \frac{\sqrt{10}}{8}\|D_1^5\rangle + \frac{3}{4}\|D_3^5\rangle - \frac{3\sqrt{2}}{4}\|D_5^5\rangle\\ \frac{1}{8}\|D_0^5\rangle + \frac{3\sqrt{2}}{8}\|D_2^3\rangle - \frac{3\sqrt{5}}{8}\|D_4^5\rangle\end{cases}$
$\|1\rangle$	$\begin{cases}\|D_0^2\rangle\\ \|D_1^2\rangle\\ \|D_2^2\rangle\end{cases}$	$\longmapsto$	$\begin{cases}-\frac{3\sqrt{5}}{8}\|D_1^5\rangle + \frac{3\sqrt{2}}{8}\|D_3^5\rangle + \frac{1}{8}\|D_5^5\rangle\\ -\frac{3\sqrt{2}}{8}\|D_0^5\rangle + \frac{3}{4}\|D_2^5\rangle + \frac{\sqrt{10}}{8}\|D_4^5\rangle\\ \frac{3}{8}\|D_1^5\rangle + \frac{\sqrt{10}}{8}\|D_3^5\rangle + \frac{3\sqrt{5}}{8}\|D_5^5\rangle\end{cases}$

那么对于 $i = 0,\ 1$ 我们有

$$|\tilde{i}\rangle = \left(U_{\overline{B}} \otimes I_B\right)\left(|i\rangle_R \otimes |\psi\rangle_{AB}\right),$$

其中 $|\psi\rangle_{AB} = \frac{1}{\sqrt{3}}\left(|D_0^2\rangle_A|D_0^2\rangle_B + |D_1^2\rangle_A|D_1^2\rangle_B + |D_2^2\rangle_A|D_2^2\rangle_B\right)$ 是 Γ_A的纯化。这给出了一个共享双体态，它并非两个纠缠比特，而是两个量子比特上的两个对称子空间之间的最大纠缠态。

假设发送方和接收方分别持有子系统 A 和 B，发送方能够使用等距映射 U_B 将消息与她持有的那一半纠缠对一起编码。因此，我们有一个 $((5、2、3;3))$ 纠缠辅助*PI*码。

—

一般而言，距离为 $d > 2$ 的任何 PI 编码对于擦除 2 至 $d-1$ 个量子比特的情况都是简并的。设 B 是一个可纠正集合，且有一个支撑于其上的 SWAP 算子；设 $\mathcal{E}$ 是擦除 B时的线性可纠正错误集合，并设 $F = \mathrm{SWAP} - I = \sum_j f_j E_j$，其中 $E_j \in \mathcal{E}$。那么，由于码空间在 SWAP 算子作用下保持不变，我们有 $FP = 0$。对于任意 E_i，我们有

$$0 = PE_i^\dagger FP = \sum_j f_j P E_i^\dagger E_j P = \left(\sum_j f_j \lambda_{ij}\right) P, \tag{25}$$

从而对于任意 i都会导致 $\sum_j f_j \lambda_{ij} = 0$ 。因此 λ 不是满秩的。这意味着，只要接收方愿意放弃其所持部分的置换不变性，压缩总是一种可行选择。

备注 18. 请注意，即使发送方和接收方没有共享其特定编码所需的施密特秩为 C 的二分态 $|\psi\rangle_{AB}$ ，仍然存在一种局域操作与经典通信变换，可以将发送方和接收方共享的 $\lceil \log_2 C \rceil$ 个纠缠比特转换为 $|\psi\rangle_{AB}$。这是尼尔森主序定理 [62, 定理 1]，的结果，因为 $\lceil \log_2 C \rceil$ 个最大纠缠态被任何施密特秩为 C 的态所主序。

将定理 16 限定于稳定子码时，我们可以用稳定子群的子群来刻画：

推论 19. 设 $\mathcal{C}$ 是一个 $[\![n, k, d]\!]$ 稳定子码。设 B 是 $\mathcal{C}$ 上一个可纠正的量子比特集合，并设 $\mathcal{S}_B$ 是 $\mathcal{S}$ 中支撑在 B 上的子群，即

$$\mathcal{S}_B = \{S \in \mathcal{S} \mid \mathrm{supp}(S) \subseteq B\}.$$

设 $|B| = b$ 和 $|\mathcal{S}_B| = 2^s$。那么存在一个参数为 $[\![n-b, k, d;\ b-s]\!]$ 的纠缠辅助码。

例 20. $[\![7, 1, 3]\!]$ *Steane* 码 [2] 的稳定子生成元如下：

$$\begin{array}{ccccccc} I & I & I & X & X & X & X \\ X & I & X & I & X & I & X \\ I & X & X & I & I & X & X \\ I & I & I & Z & Z & Z & Z \\ Z & I & Z & I & Z & I & Z \\ I & Z & Z & I & I & Z & Z \end{array}$$

该编码有多个可纠正的 *4* 量子比特子集，例如 $B = \{4, 5, 6, 7\}$；这些子集上都支撑着一对稳定子生成元，因此该编码对擦除 B 是简并的。由于 $|\mathcal{S}_B| = 2^2$，根据推论 *19*，我们应该能够将该编码转换为一个 $[\![3, 1, 3;\ 2]\!]$ 纠缠辅助码。

这可以通过选取 Γ_A 的一个纯化来实现，使接收方持有的量子比特数量最少。按照 *Fattal* 等人 [63]，，在 B 上具有部分支撑的稳定子生成元可以配对成与 X_i 和 Z_i 同构的反对易对，而完全支撑在 $\mathcal{S}_B$ 上的生成元则映射为其他 Z_i 算子。因此，与例*4*类似，我们可以选取一个仅作用于 B 的酉算子 V，只对该部分进行解码：

$$\left.\begin{array}{ccc|cccc} I & I & I & I & I & Z & I \\ X & I & X & X & I & I & I \\ I & X & X & I & X & I & I \\ I & I & I & I & I & I & Z \\ Z & I & Z & I & Z & I & I \\ I & Z & Z & Z & I & I & I \end{array}\right. \overset{punc}{\longmapsto} \left.\begin{array}{ccc|cc} X & I & X & X & I \\ I & X & X & I & X \\ Z & I & Z & I & Z \\ I & Z & Z & Z & I \end{array}\right.$$

由于最后两个量子比特现在已与码字的其余部分解纠缠，我们可以将它们“穿孔”并丢弃。

如前所述，这可以看作是去除接收方量子比特上的纠错保护。因此，从某种意义上说，这可以视为 Lai 和 Brun [41], 提出方案的逆向操作；在该方案中，接收方未编码的量子比特被编码进另一种量子码。

5. Conclusion

纠缠辅助码是量子子空间码的一种自然扩展，使发送方和接收方能够利用共享纠缠。此前，已知的纠缠辅助码仅通过稳定子框架及其直接推广——CWS框架构造。本文的主要结果表明，任何量子码都可以转化为纠缠辅助码：可以让接收方预先持有该编码的一个可纠正子集，也可以根据 [47] 的结构定理选择共享双体态和局部编码酉算子。此外，我们还揭示了码简并性与能否缩减接收方份额大小之间的直接联系。

将纠缠辅助码推广到稳定子框架之外，为其他推广开辟了道路。尽管本文仅限于量子比特码，但我们的主要工具—— [47], 的结构定理并不受此限制，这表明推广到量子位码应当是直接的。一个更有趣的推广是将纠缠辅助码纳入OAQEC框架 [64, 65, 66], ，把共享纠缠与子系统 [67, 68] 以及量子-经典混合码 [69, 70, 71, 72]结合起来。Nadkarni等人 [40]已在稳定子框架中沿这一方向开展了近期工作。

尽管本文的结果相当一般，局部酉算子的定义却相当繁琐。一个自然的问题是，特定类别的纠缠辅助码是否允许更紧凑的描述，类似于纠缠辅助稳定子码，后者可用稳定子群的生成集来描述。一个显而易见的首选是纠缠辅助XP稳定子码 [59], ，它们同样具有稳定子群，但结构更为复杂。另一种选择是纠缠辅助PI码，因为Aydin 等人 [60] 已用描述Dicke 态叠加态的系数向量，对二维PI码给出了简洁描述。

这些结果还可能有助于推广 Grassl 的隐形传态方案 [32] 、Wilde 和 Fattal 的双部稳定子码 [73], ，以及与网络量子码 [74, 75]建立联系。另一个有趣的方向，是根据先前关于量子数据压缩的研究，特别是通过 Koashi-Imoto分解 [76, 77], ，重新诠释第 4 节中的结果；该分解的形式与 [47]的结构定理中给出的形式相似。由于这项工作为使用除贝尔态之外的双部态构造纠缠辅助码提供了可能，因此，能否发展出关于 $C \neq 2^c$ 的编码的新上界，从而利用 Munn´e 等人的技术，扩展 Lai等人 [33] 关于纠缠辅助CWS码半定规划界的工作，仍有待研究 [78]。

最后，在本文中，我们一直将擦除原本供接收方使用的量子比特这一操作，与经典编码理论中的删余构造作非正式类比（见 [79, 第 1.5] 节）。近期，Cao 等人 [80]利用量子反码，将稳定子码的删余与缩短和清除引理之间的联系形式化。虽然目前这些反码仅限于稳定子框架，但如果能利用更一般的版本，将本文中非正式使用的删余概念形式化，将会很有意义；此外，这是否有助于更深入地理解稳定子框架之外的纠缠辅助码，也值得探究。

Acknowledgments

作者谨此感谢 Eric Chitambar、Markus Grassl 和 Felix Huber 提供的宝贵意见。

References

[1] P. W. Shor, 《减少量子计算机存储器中退相干的方案》, *Phys. Rev. A* 52, 2493 2496, 1995, 第[2] 卷, 第R–R页。 *Phys. Rev. Lett.*A. M. Steane, 《量子理论中的纠错码》, [3] , 第77卷, 第793–797页, 1996年。*Phys. Rev. A* 54, 1098 1105, 1996, A. R. Calderbank和P. W. Shor, 《优良量子纠错码的存在》, [4] , 第-卷, 第–页。]D. Gottesman, 《稳定子码与量子纠错》, 博士论文, 加州理工学院, 1997年。[5] 9705052 在线 *IEEE Trans. Inf. Theory*。可访问：https://arxiv.org/abs/quant- ph/[6] A. R. Calderbank、E. M. Rains、P. M. Shor和N. J. A. Sloane, 《通过GF(4)上的编码进行量子纠错》, *Phys. Rev. A* 56, 33 38, 1997, 第44卷, 第4期, 第1369–1387页, 1998年。[7] M. Grassl、T. Beth和T. Pellizzari, 《量子擦除信道的编码》, *Nat. Commun.*, 第[8] 卷, 第–页。¯Y. Wu、S. Kolkowitz、S. Puri和J. D. Thompson, 《碱土金属里德堡原子阵列中容错量子计算的擦除转换》, T_1 , 第13卷, 第1期, 第4657页, 2022年。 *Phys. Rev. X*A. Kubica、A. Haim、Y. Vaknin、H. Levine、F. Brand[9] ao和A. Retzker, 《擦除量子比特：突破超导电路中的 *PRX Quantum*极限》, [10] , 第13卷, 第041022页, 2023年。 *Nature* 622, 273 278, M. Kang、2023 W. C. Campbell和K. R. Brown, 《利用擦除转换和囚禁离子的亚稳态实现量子纠错》, [11] , 第4卷, 第020358页, 2023年。 *Nature*P. Scholl、A. L. Shaw、R. B.-S. Tsai、R. Finkelstein、J. Choi和M. Endres, 《高保真里德堡量子模拟器中的擦除转换》, [12] , 第 *et al.*卷, 第–页。 *Phys. Rev. X*S. Ma、G. Liu、P. Peng、B. Zhang、S. Jandura、J. Claes、A. P. Burgers、G. Pupillo、S. Puri和J. D. Thompson, 《原子量子比特中的高保真门与电路中途擦除转换》, [13] , 第622卷, 第279–284页, 2023年。 *PRX Quantum* H. Levine [14] , 《利用可调谐跨蒙特演示长相干时间双轨擦除量子比特》, *Phys. Rev. Lett.*, 第14卷, 第011051页, 2024年。[15] S. Gu、Y. Vaknin、A. Retzker和A. Kubica, 《利用擦除量子比特优化量子纠错方 *Phys. Rev. A*案》, [16] , 第6卷, 第040354页, 2025年。 *J. High Energy Phys.*R. Cleve、D. Gottesman和H.-K. Lo, 《如何共享量子秘密》, [17] , 第83卷, 第648–651页, 1999年。 *Commun. Math. Phys.* 354, 3, 865 912, 2017, D. Gottesman, 《量子秘密共享理论》, [18] , 第61卷, 第042311页, 2000年。 *J. High Energy Phys.*A. Almheiri、X. Dong和D. Harlow, 《反德西特/共形场论中的体局域性与量子纠错》, [19] , 第2015卷, 第4期, 2015年。 *Journal of High Energy Physics* 2019, 5, 52, 2019, D. Harlow, 《从量子纠错推导Ryu–Takayanagi公式》, [20] , 第*SciPost Phys.*卷, 第–页。[21] P. Hayden和G. Penington, 《学习黑洞的Alpha比特》, *Phys. Rev. Lett.*, 第2019卷, 第12期, 第7页, 2019年。[22] C. Akers和P. Rath, 《通过量子纠错得到全息Rényi熵》, ´, 第*Phys. Rev. Lett.*卷, 第[23] 页。*Phys. Rev. A*C. Akers和G. Penington, 《通过量子纠错得到量子极小曲面》, , 第12卷, 第157页, 2022年。C. H. Bennett和S. J. Wiesner, 《通过作用于爱因斯坦-波多尔斯基-罗森态的单粒子和双粒子算符进行通信》, , 第69卷, 第2881–2884页, 1992年。C. H. Bennett、G. Brassard、C. Crepeau、R. Jozsa、A. Peres和W. K. Wootters, 《通过经典信道与爱因斯坦-波多尔斯基-罗森信道传送未知量子态》, , 第70卷, 第1895–1899页, 1993年。G. Bowen, 《实现纠缠辅助信道容量所需的纠缠》, , 第66卷, 第052313页, 2002年。

[24] T. Brun、I. Devetak和M.-H. Hsieh，《利用纠缠纠正量子错误》，*Science*，第314卷，第5798期，第436–439页，2006年。[25] T. A. Brun、I. Devetak和M.-H. Hsieh，《催化量子纠错》，*IEEE Trans. Inf. Theory* 60, 6, 3073 3089, 2014 ，第

[26] 卷，第–页。 *Phys. Rev. A*M. M. Wilde和T. A. Brun，《额外的共享纠缠可降低量子卷积编码的存储需求》，[27] ，第79卷，第032313页，2009年。 *Phys. Rev. A*——，《纠缠辅助量子卷积编码》，[28] ，第81卷，第042333页，2010年。 *Quantum Inf. Process.* 9, 5, 509 540, 2010 ——，

《共享纠缠的量子卷积编码：一般结构》，[29] ，第 *New J. Phys.*卷，第–页。[30] Z. Shadman、H. Kampermann、C. Macchiavello和D. Bruß，《噪声量子信道上的最优超密编码》，*npj Quantum Inf.* 11, 1, 2025 ，第

12卷，第7期，第073042页，2010年。[31] T. Prasad和M. Grassl，《用于纠缠辅助经典通信的编码》，*IEEE Trans. Inf. Theory*，第[32] 卷。 *Phys. Rev. A*C.-Y. Lai和A. Ashikhmin，《利用分裂重量枚举求纠缠辅助量子纠错码的线性规划界》，[33] ，第64卷，第1期，第622–639页，2018年。 *IEEE Trans. Inf. Theory*M. Grassl，《纠缠辅助量子通信突破量子Singleton界》，[34] ，第103卷，第L020601页，2021年。 *Phys. Rev. A*C.-Y. Lai、P.-C. Tseng和W.-H. Yu，《纠缠辅助码字稳定量子码规模的半定规划界》，[35] ，第70卷，第11期，第7867–7881页，2024年。*Phys. Rev. A*N. R. Dash、S. Dutta、R. Srikanth和S. Banerjee，《级联纠缠辅助量子纠错码的界》，[36] ，第112卷，第052419页，2025年。 *ICT Express*J. Shin、J. Heo和T. A. Brun，《纠缠辅助码字稳定量子码》，[37] ，第84卷，第062321页，2011年。 *Phys. Rev. A*B. Ahn、J. Shin和J. Heo，《采用不完美纠缠比特的纠缠辅助码字稳定量子码》，[38] ，第2卷，第2期，第47–52页，2016年。 *Phys. Rev. A*M.-H. Hsieh、I. Devetak和T. Brun，《一般的纠缠辅助量子纠错码》，[39] ，第76卷，第062313页，2007年。 [I. Kremsky、M.-H. Hsieh和T. A. Brun，《量子纠错码的经典增强》，]，第78卷，第012341页，2008年。 1311 1533 J. Shin、J. Heo和T. A. Brun，《基于码字稳定量子码的通用量子纠错码》，2013年。 [在线]。可访问：https://arxiv.org/abs/ 2411 14389 。P. J. Nadkarni、S. Adonsou、G. Dauphinais、D. W. Kribs和M. Vasmer，《纠缠辅助量子纠错的统一推广方法》，2024年。 *Phys. Rev. A*在线[42] 。可访问：https://arxiv.org/abs/*Quantum Error Correction*。C.-Y. Lai和T. A. Brun，《采用不完美纠缠比特的纠缠辅助量子纠错码》，[43] ，第86卷，第032319页，2012年。 *Quantum Inf. Process.*T. A. Brun和M.-H. Hsieh，《纠缠辅助量子纠错码》，载于[44] ，D. A. Lidar和T. A. Brun编。剑桥大学出版社，2013年，第181–200页。 *Quantum Inf. Process.*C. Galindo、F. Hernando、R. Matsumoto和D. Ruano，《任意有限域上的纠缠辅助量子纠错码》，[45] ，第18卷，第4期，2019年。 *IEEE Trans. Inf. Theory*——，《更正：任意有限域上的纠缠辅助量子纠错码》，[46] ，第20卷，第6期，2021年。 2022 [ ] 2205 13732 M. Grassl、F. Huber和A. Winter，《量子纠错码Singleton界的熵证明》， *J. Math. Phys.*，第68卷，第6期，第3942–3950页，2022年。[48] D. Ueno和R. Matsumoto，《从稳定子量子纠错码构造缩短稳定子纠缠辅助量子纠错码的显式方法》， *Phys. Rev. A*。在线。可访问：https://arxiv.org/abs/。E. Chitambar、S. Hagen、D. W. Kribs、M. I. Nelson和A. Nemec，《量子替换码的结构定理》，[49] ，第66卷，第12期，2025年。 *Quantum Info. Comput.*E. Knill和R. Laflamme，《量子纠错码理论》，，第55卷，第900–911页，1997年。A. Nayak和P. Sen，《可逆量子操作与量子态的完美加密》，，第7卷，第1期，第103–110页，2007年。

[50] D. W. Kribs 和 R. W. Spekkens，“量子纠错子系统是可通过酉变换恢复的子系统”， *Phys. Rev. A*，第 74 卷，第 042329 页，2006年。[51] M. Junge 和 P. Wu，“开放系统量子跳跃算符的稳定性”，
2022 [ ] 2211 07527 。在线。可访问:
[52]
https://arxiv.org/abs/。S. Bravyi 和 B. Terhal，“基于稳定子码的二维自纠错量子存储器的不可能性定理”， *New J. Phys.*，第 11 卷，第 4 期，第 043029 页，2009年。[53] A. Ashikhmin，“量子比特擦除信道中有限长度量子码的保真度”，载于 *2020 IEEE Int. Symp. Inf. Theory (ISIT)* 2020, 1880 1885 ，美
国加利福尼亚州洛杉矶，6月，第 – 页。[54] E. M. Rains，“量子重量枚举式”，
IEEE Trans. Inf. Theory，第 44 卷，第 4 期，第 1388–1394 页，1998年。[55] R. Laflamme、C. Miquel、J. P. Paz 和 W. H. Zurek，“完美量子纠错码”， *Phys. Rev. Lett.*，第 77 卷，第 198–201 页，1996年。[56] C. H. Bennett、D. P. DiVincenzo、J. A. Smolin 和 W. K. Wootters，“混合态纠缠与量子纠错”， *Phys. Rev. A*，第 54 卷，第 3824–3851 页，1996年。[57] H. Pollatsek 和 M. B. Ruskai，“用于量子纠错的置换不变码”， *Linear Algebra Appl.*，第 392 卷，第 255–288 页，2004年。[58] X. Ni、O. Buerschaper 和 M. Van den Nest，“非对易稳定子形式体系”，
J. ，第
Math. Phys. 56, 5, 2015
卷，第 期。[59] M. A. Webster 、 B. J. Brown 和 S. D. Bartlett，“XP 稳定子形式：具有任意相位的泡利稳定子形式的推广”， *Quantum*，第 6 卷，第 815 页，2022年。[60] A. Aydin、M. A. Alekseyev 和 A. Barg，“置换不变量子码族”， *Quantum*，第 8 卷，第 1321 页，2024年。[61] E. Kubischta 和 I. Teixeira，“具有特殊横向门的量子码族”，*Phys. Rev. Lett.*，第 131 卷，第 240601 页，2023年。[62] M. A. Nielsen，“一类纠缠变换的条件”， *Phys. Rev. Lett.*，第 83 卷，第 436–439 页，1999年。[63] D. Fattal、T. S. Cubitt、Y. Yamamoto、S. Bravyi 和 I. L. Chuang，“稳定子形式体系中的纠缠”，
2004 [ ] 0406168 。
[64] ´
在线。可访问：https://arxiv.org/abs/quant-ph/。C. Beny、A. Kempf 和 D. W. Kribs，“通过海森堡绘景推广量子纠错”， *Phys. Rev. Lett.*，第 98 卷，第 100502 页，2007年。[65] ——，“可观测量的量子纠错”， *Phys. Rev. A*，第 76 卷，第 042303 页，2007年。[66] G. Dauphinais、D. W. Kribs 和 M. Vasmer，“算子代数量子纠错的稳定子形式体系”， *Quantum*，第 8 卷，第 1261 页，2024年。[67] D. Kribs、R. Laflamme 和 D. Poulin，“量子纠错的统一推广方法”， *Phys. Rev. Lett.*，第 94 卷，第 180501 页，2005年。[68] D. Poulin，“算子量子纠错的稳定子形式体系”， *Phys. Rev. Lett.*，第 95 卷，第 230504 页，2005年。[69] M. Grassl、S. Lu 和 B. Zeng，“同时传输量子和经典信息的编码”，载于 *2017 IEEE Int. Symp. Inf. Theory (ISIT)*，德国亚琛，2017年6月，第 1718–1722 页。[70] A. NEMEC 和 A. Klappenecker，“混合码”，载于
2018 IEEE Int. Symp. Inf. Theory ，美
(ISIT) 2018, 796 800
国科罗拉多州韦尔，第 – 页。[71] ——，“量子-经典混合码的无限族”， *IEEE Trans. Inf. Theory*，第 67 卷，第 5 期，第 2847–2856 页，2021年。[72] ——，“在量子码的规范子系统中编码经典信息”，
Int. J. Quan- ，第
tum Inf. 20, 02, 2150041, 2022
卷，第 页。[73] M. M. Wilde 和 D. Fattal，“ 双分量子纠错中的非局域量子信息 ”，
Quantum Inf. Process.，第 9 卷，第 591–610 页，2010年。[74] H. Yamasaki 和 M. Murao，“通过网络分布式编码与解码量子信息”， *Adv. Quantum Tech.*，第 2 卷，第 1–2 期，2018年。[75] K. Shiraishi、H. Yamasaki 和 M. Murao，“通过高效局域操作和经典通信提取稳定子码中编码的量子信息”， *Phys. Rev. A*，第 110 卷，第 052617 页，2024年。[76] M. Koashi 和 N. Imoto，“不会扰动部分已知量子态的操作”，*Phys. Rev. A*，第 66 卷，第 022318 页，2002年。

[77] P. Hayden、R. Jozsa、D. Petz 和 A. Winter，“满足量子熵强次可加性等号条件的态的结构”，*Comm. Math. Phys.*，第 246 卷，第 359–374 页，2004年。[78] G. A. Munn´e、A. Nemec 和 F. Huber，“量子码的半正定规划界”，2024年。 [在线]。可访问：https://arxiv.org/abs/2408 10323 。W. C. Huffman 和 V. Pless,
[79] *Fundamentals of Error-Correcting Codes*。剑桥大学出版社，2003年。[80] C. Cao、G. Cotardo 和 B. Lackey，“量子反码”，2025年。 [在线]。可访问：https://arxiv.org/abs/2512.13891

Department of Computer Science、 University of Texas at Dallas、890 FranklynJenifer Drive、 Richardson、 TX 75080 USA*Email address*: *jaszmine.defranco@utdallas.edu*Email address*: †andrew.nemec@utdallas.edu