arXiv:2303.03079v1 [cs.IT] 6 Mar 2023

纠缠辅助量子纠错码的 Steane 扩张

CARLOS GALINDO、FERNANDO HERNANDO 和 RYUTAROH MATSUMOTO

Abstract. 我们介绍一种通过考虑欧几里得内积而获得的、针对纠缠辅助量子纠错码（纠缠辅助量子纠错码）的 Steane 类扩展过程。我们给出了这些扩张码的参数公式，并将所得结果应用于显式计算由某些 BCH 码得到的扩张纠缠辅助量子纠错码的参数。

1. Introduction

量子纠错码（量子纠错码）是量子计算中的重要工具，因为它们能够保护量子信息免受量子噪声，尤其是退相干的影响。能够改善经典处理器性能的量子处理器的存在 [2] 说明了获得优良量子纠错码的重要性。长度为 n 的 q 元量子纠错码（其中 q 是素数的幂 p）是希尔伯特空间 $\mathbb{C}^{q^n}$ 的一个子空间，其中 $\mathbb{C}$ 表示复数。它们的参数写作 $((n, K, d))_q$，其中 K 是维数， d 是距离。最常见的量子纠错码是稳定子码 [30]。许多此类码满足 $K = q^k$，其中 k 为某个非负整数；此时，它们的参数表示为 $[[n, k, d]]_q$；滥用记号，我们称 k 为这些码的维数。量子纠错码最初在二元情形下被引入 [10, 22, 9, 4, 5]，随后推广到一般情形 [7, 3, 30, 1, 32, 11, 17, 18], ，这里我们仅引用了该领域浩瀚文献中的部分参考文献。非二元情形下的量子纠错码便于实现容错量子计算 [43, 31, 23, 36]。

稳定子量子码与自正交加法码密切相关，其中对偶性由迹辛形式 [3, 30]给出。作为上述构造的特例，稳定子量子码可由关于 Hermitian 内积或欧几里得内积的自正交线性码获得。欧几里得情形对应于所谓的 CSS 构造，该构造由 Calderbank 和 Shor [10] 以及 Steane [44]给出。接下来我们回顾这一结果 [30, 引理 20], ，其中 $\perp_e$ 表示欧几里得对偶，wt 表示汉明重量。

定理 1. 设有两个 q 元线性码 C_i, $i = 1, 2$，其参数分别为$[n, k_i, d_i]_q$，并假设 $C_2^{\perp_e} \subseteq C_1$。那么，存在一个参数为 $[[n, k_1 + k_2 - n, d]]_q$、最小距离为

$$d = \min\left\{\mathrm{wt}(\boldsymbol{c}) \mid \boldsymbol{c} \in \left(C_1 \setminus C_2^{\perp_e}\right) \cup \left(C_2 \setminus C_1^{\perp_e}\right)\right\}.$$

Key words and phrases. EAQECC；纠缠辅助量子纠错码；Steane 扩展；BCH 码。前两位作者获得了 MCIN/AEI/10.13039/501100011033、“ERDF：建设欧洲之路”以及“欧盟 NextGenerationEU/PRTR”的部分资助，项目编号为 PGC2018-096446-B-C22 和 TED2021-130358B-I00；此外还获得了海梅一世大学的资助，项目编号为 UJI-B2021-02。

通过 CSS过程获得的量子码具有若干优点。事实上，它们可用于量子密码学的隐私放大 [42] 以及构造非对称量子码 [29, 41], ，但它们的优点主要体现在计算方面，其中包括支撑字母表规模较小 [24]。

CSS 码的另一个优良性质是，可以使用 Steane扩展过程对其进行改进。该过程最初由 Steane 在二元情形 [45] 中提出，随后推广到一般情形 [27, 33] （另见 [20]）。记 $\mathbb{F}_q$ 为含有 q 个元素的有限域，具体结果如下：

定理 2。设 C 是定义在 $\mathbb{F}_q$ 上的长度为 n、维数为 k的线性码。假设 $C^{\perp_e} \subseteq C$ 和 C 可以扩张为长度为 n 、维数为 $k' \geq k+2$的 q-元线性码 C' 。那么，存在一个参数为 $[[n, k+k'-n, d]]_q$的稳定子量子码，其中 $d \geq \min\{d_1, \lceil \frac{q+1}{q} d_2 \rceil\}$， $d_1 = \mathsf{wt}\left(C \setminus (C')^{\perp_e}\right)$ 以及 $d_2 = \mathsf{wt}\left(C' \setminus (C')^{\perp_e}\right)$。

如前所述，为构造稳定子量子码，必须考虑自正交码（或包含其对偶码的码），这一事实决定了所得码的参数。然而，只要编码器和解码器共享纠缠，就可以使用任意线性码而不受任何限制，从而提高通信容量 [8]。这类码称为纠缠辅助量子纠错码（EAQECC）。除了量子码所用的长度 n、维数 k 和最小距离 d等参数外，纠缠辅助量子纠错码还包含一个新参数 c，它表示所需最大纠缠量子态（对）的最小数量。因此，这些码的参数表示为 $[[n, k, d;\ c]]_q$。

对于 CSS 构造 [28]，最早给出了计算二元纠缠辅助量子纠错码 c 参数的公式。之后，仍在二元情形下，Wilde 和 Brun [46]研究了更一般的构造。在一般情形下，可在 [19]中找到用于求取 q元纠缠辅助量子纠错码参数的公式，这些公式推广了 [28, 46] 中的公式。近期，利用这些公式，人们给出了许多特定纠缠辅助量子纠错码构造的参数 [37, 40, 13, 38, 26, 34, 15, 21]。

接下来，我们回顾本文将用到的关于纠缠辅助量子纠错码的两个主要结果。首先，考虑向量空间 $\mathbb{F}_q^{2n}$，其中 n 是一个正整数。$\mathbb{F}_q^{2n}$ 中两个向量 $(\boldsymbol{x}|\boldsymbol{y})$ 和 $(\boldsymbol{z}|\boldsymbol{t})$ 的辛积定义为

$$(\boldsymbol{x}|\boldsymbol{y}) \cdot_s (\boldsymbol{z}|\boldsymbol{t}) := \boldsymbol{x} \cdot_e \boldsymbol{t} - \boldsymbol{z} \cdot_e \boldsymbol{y},$$

其中 $\cdot_e$ 表示欧几里得内积。关于辛积 $\cdot_s$，向量子空间 $C \subseteq \mathbb{F}_q^{2n}$ 的对偶空间记作 $C^{\perp_s}$。

$\mathbb{F}_q^{2n}$ 中向量 $(\boldsymbol{x}|\boldsymbol{y})$ 的辛重量为

$$\mathrm{swt}(\boldsymbol{x}|\boldsymbol{y}) := \#\{j \mid (x_j, y_j) \neq (0,0), 1 \leq j \leq n\},$$

表示基数，x_j （分别为 y_j）是向量 $\boldsymbol{x}$（分别为 $\boldsymbol{y}$）的第 j 个坐标。我们将子集 $S \subseteq \mathbb{F}_q^{2n}$ 的最小辛距离定义为

$$d_s(S) := \min\{\mathrm{swt}(\boldsymbol{x}|\boldsymbol{y}) \mid (\boldsymbol{x}|\boldsymbol{y}) \in S \setminus \{(\mathbf{0}|\mathbf{0})\}\}.$$

我们的第一个结果见于 [19, 定理 2], ，它确定了由 $C \subseteq \mathbb{F}_q^{2n}$上的线性码所得到的纠缠辅助量子纠错码的参数。假设 C的维数为 $n-k$。我们希望得到一个辛自正交的 $\mathbb{F}_q$-向量空间$\tilde{C} \subseteq \mathbb{F}_q^{2n+2c}$，其投影为 C ，并且 c 是最大纠缠˜量子态的最小数量。 C 给出了量子电路，该电路借助 c 个最大纠缠对，将 $k+c$ 个逻辑量子位编码为 n 个物理量子位。

定理 3. 设 $C \subseteq \mathbb{F}_q^{2n}$为一个线性码，其由大小为（$n-k$） $\times 2n$的矩阵（$H_X|H_Z$）的各行生成。那么， C 产生一个参数为$[[n, k+c, d;\ c]]_q$的纠缠辅助量子纠错码，其中

$$2c = \operatorname{rank}\left(H_X H_Z^T - H_Z H_X^T\right) = \dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}\left(C \cap C^{\perp_s}\right)$$

以及 $d = d_s\left(C^{\perp_s} \setminus (C \cap C^{\perp_s})\right)$。

关于纠缠辅助量子纠错码的第二个所述结果 [19, 定理 4] 是定理 3 的一个特例，它展示了如何利用 CSS 构造来提供 q 元纠缠辅助量子纠错码。为陈述该结果，考虑两个维数分别为 k_1 和 k_2 的 $\mathbb{F}_q$ 线性码 C_1、$C_2 \subseteq \mathbb{F}_q^n$，以及它们的生成矩阵 H_1 和 H_2。具体结果如下，其中d_H 表示汉明距离， $\perp_e$ 表示欧几里得对偶，而对于矩阵 M， M^T 表示其转置。

定理 4. 在上述记号下，码 $C_1 \times C_2 \subseteq \mathbb{F}_q^{2n}$ 确定了一个参数为 $[[n, n-k_1-k_2+c, d$ 的纠缠辅助量子纠错码；$c]]_q$，其中

$$c = \operatorname{rank}\left(H_1 H_2^T\right) = \dim_{\mathbb{F}_q} C_1 - \dim_{\mathbb{F}_q}\left(C_1 \cap C_2^{\perp_e}\right),$$

and

$$d = \min\left\{d_H\left(C_1^{\perp_e} \setminus (C_2 \cap C_1^{\perp_e})\right), d_H\left(C_2^{\perp_e} \setminus (C_1 \cap C_2^{\perp_e})\right)\right\}.$$

在本文第 2 节中，我们证明，采用与 Steane 所提出的方法类似的步骤，只要定理 4 中涉及的线性码 C_1 和 C_2 相同，就可以扩展定理 4 给出的纠缠辅助量子纠错码。令 $C = C_1 = C_2$，并将 C 表示为两个线性空间 $\langle B_r\rangle$ 和 $\langle B_t\rangle$的直和，定理 6 给出了如何计算相应扩展后的纠缠辅助量子纠错码的参数。该扩展码使用一个可逆的 $t \times t$矩阵 A，其中 t 是空间 $\langle B_t\rangle$的维数。在附加假设 A 在基域中没有特征值且 $\langle B_t\rangle \subseteq C^{\perp_e}$成立时，定理 7 确定了扩展后的纠缠辅助量子纠错码的参数。特别地，定理 7 证明，扩展码保持相同的参数 c，且其维数相较于原始纠缠辅助量子纠错码有所增加。定理 10、推论 12 和注 13 研究并展示了当空间 $\langle B_r\rangle$ 和 $\langle B_t\rangle$ 欧几里得正交时，对纠缠辅助量子纠错码进行 Steane 扩张所带来的优势。

如前所述，我们的方法适用于线性码的任意分解。作为一个具体案例，第 3 节说明如何通过某些 BCH 码将我们的结果付诸实践。将 BCH 码视为子域子码，并应用定理 7 及前述结果，定理 17 和定理 20 明确给出了由适当 BCH 码构造的纠缠辅助量子纠错码的 Steane 扩张参数。最后，在定理 21 和定理 22 以及注 23 中，通过考察另一类 BCH 码，我们确定了根据定理 10、推论 12 和注 13 推导出的纠缠辅助量子纠错码的相应参数。

本节简要介绍了量子纠错码和纠缠辅助量子纠错码，并回顾了一些后文将用到的主要已知结果。本文旨在阐明如何对纠缠辅助量子纠错码进行 Steane 扩张。我们还将这一构造专门应用于某些 BCH 码，并由此得到具有显著计算优势的新纠缠辅助量子纠错码（见定理 1 后段的最后部分）。第 2 节介绍纠缠辅助量子纠错码的 Steane 扩张，并证明若干关于其参数的结果；第 3 节则运用第 2 节的结果，计算与 BCH 码相关的扩张纠缠辅助量子纠错码的参数。本节末尾还介绍了由我们的方法推导出的一些优良码。

2. Steane enlargement of EAQECCs

本节旨在证明，定理 2 中展示的类似 Steane 扩张的过程也可用于纠缠辅助量子纠错码的框架。首先，我们将考察该方法如何应用于定理 4 所述的码；随后将说明，在特定条件下，我们能够确定扩张后的纠缠辅助量子纠错码的参数，以及它们如何优于原码。

设 $C \subseteq \mathbb{F}_q^n$ 是一个参数为 $[n,k,\delta]_q$ 的 $\mathbb{F}_q$-线性码。设 B 是一个元素属于 $\mathbb{F}_q$ 的矩阵，其行是 $\mathbb{F}_q^n$ 中线性无关的向量。在本文中，为方便起见，我们用 $\langle B\rangle$ 表示由 B 的行生成的 $\mathbb{F}_q^n$ 的向量子空间。假设 $C = \langle B_r\rangle \oplus \langle B_t\rangle$，其中 B_r（分别为 B_t）是 C 的 $\mathbb{F}_q$-线性子码 $\langle B_r\rangle$（分别为 $\langle B_t\rangle$）的生成矩阵，且 $r = \dim_{\mathbb{F}_q}\langle B_r\rangle$ 和 $t = \dim_{\mathbb{F}_q}\langle B_t\rangle$。将定理 4 应用于 $C_1 = C_2 = C$，可得到一个 ˜ 纠缠辅助量子纠错码 C，其参数为

$$[[n, n-2k+c, d; c]]_q, \tag{1}$$

其中 $k = r+t$, $d = d_H(C^{\perp_e} \setminus C)$ 且

$$c = \operatorname{rank}\left[\begin{pmatrix} B_r \\ B_t \end{pmatrix}(B_r^T B_t^T)\right] = \operatorname{rank}\left[\begin{pmatrix} B_r B_r^T & B_r B_t^T \\ B_t B_r^T & B_t B_t^T \end{pmatrix}\right]. \tag{2}$$

接下来，我们引入所需的线性码 D_A，以对 C进行 Steane˜扩张。

定义 5. 给定上述码 $C = \langle B_r\rangle \oplus \langle B_t\rangle$，且满足 $\dim_{\mathbb{F}_q}\langle B_t\rangle \geq 2$，我们将码 D_A 定义为 $\mathbb{F}_q$-线性码 $D_A \subseteq \mathbb{F}_q^{2n}$，其生成矩阵为

$$\begin{pmatrix} B_t & AB_t \\ Br & 0 \\ 0 & B_r \end{pmatrix}, \tag{3}$$

其中 A 是 $\mathbb{F}_q$上的一个 $t \times t$ 可逆矩阵。

关于 Steane 扩张的一般结果如下：

定理 6. 设 $C = \langle B_r\rangle \oplus \langle B_t\rangle \subseteq \mathbb{F}_q^n$是一个 $\mathbb{F}_q$-线性码，满足 $\dim_{\mathbb{F}_q}\langle B_t\rangle \geq 2$。假设 A 是 $\mathbb{F}_q$ 上的一个 $t \times t$ 可逆矩阵，且在 $\mathbb{F}_q$中没有特征值。那么 ˜ ˜ D_A 可导出一个参数为下述数值的纠缠辅助量子纠错码 D_A；该码是纠缠辅助量子纠错码 C的 Steane 扩张

$$[[n, n-2r-t+c', d', c']]_q,$$

$$where\ d' \geq \min\left\{\delta_1, \left\lceil\left(1+\tfrac{1}{q}\right)\delta_2\right\rceil\right\},\ \delta_1 = d_H(C^{\perp_e})\ and\ \delta_2 = d_H\left(\langle B_r\rangle^{\perp_e}\right),\ and$$

$$c' = \frac{1}{2}\operatorname{rank}\begin{pmatrix} B_t B_t^T A^T - AB_t B_t^T & -AB_t B_r^T & B_t B_r^T \\ B_r B_t^T A^T & 0 & B_r B_r^T \\ -B_r B_t^T & -B_r B_r^T & 0 \end{pmatrix}. \tag{4}$$

证明。将定理 3 应用于线性码 $D_A \subseteq \mathbb{F}_q^{2n}$ 即可得出证明。其生成矩阵的大小为 $(n-(n-2r-t))\times 2n$。根据定理 3，所得纠缠辅助量子纠错码的维数为 $n-2r-t+c'$，最大纠缠对的数量 c' 由以下公式给出

$$2c' = \operatorname{rank}\left[\begin{pmatrix} B_t \\ B_r \\ 0 \end{pmatrix}\begin{pmatrix} B_t^T A^T & 0 & B_r^T \end{pmatrix} - \begin{pmatrix} AB_t \\ 0 \\ B_r \end{pmatrix}\begin{pmatrix} B_t^T & B_r^T & 0 \end{pmatrix}\right].$$

因此，我们已经证明，除最小距离外，纠缠辅助量子纠错码 C 的 Steane 扩张的参数与陈述中的一致。

关于最小距离 d'，我们将证明

$$d_s\left(D_A^{\perp_s}\setminus D_A\cap D_A^{\perp_s}\right)\geq\min\left\{\delta_1,\left\lceil\left(1+\frac{1}{q}\right)\delta_2\right\rceil\right\},$$

根据定理 3，这再次完成了我们的证明。

记 G 为欧几里得对偶 $C^{\perp_e}$ 的一个生成矩阵，其大小为 $(n-(r+t))\times n$，并令 $(G'\mid G)^T$ 为对偶向量空间 $\langle B_r\rangle^{\perp_e}$ 的一个生成矩阵。于是，根据 [33] 中定理 2.6 的证明（另见 [27]），D_A 的辛对偶 $D_A^{\perp_s}$ 具有

$$\begin{pmatrix}\bar{A}G' & G'\\ G & 0\\ 0 & G\end{pmatrix},$$

作为生成矩阵，其中 $\bar{A}:=G'B_t^T\left(A^T\right)^{-1}\left(G'B_t^T\right)^{-1}$。

Now, $\bar{A}$ 在 $\mathbb{F}_q$ 中没有特征值，因为 A 在 $\mathbb{F}_q$ 中没有特征值；如果一个元素属于 $\mathbb{F}_q$ 的可逆矩阵 M 具有特征值 $\lambda\in\mathbb{F}_q$，那么 M^T、M^{-1} 和 PMQ（其中 P 和 Q 是元素属于 $\mathbb{F}_q$ 的可逆矩阵）也会在 $\mathbb{F}_q$ 中具有特征值。最后，根据 [33], 中定理 2.6 的证明

$$d_s\left(D_A^{\perp_s}\setminus D_A\cap D_A^{\perp_s}\right)\geq\min\left\{d_H\left(\langle G\rangle\right),d_H\left(\langle B_r\rangle^{\perp_e}\right)\right\},$$

证明陈述中的 d' 下界。 □

下面的小节将研究一些具体情形，在这些情形中，可以更详细地说明使用纠缠辅助量子纠错码的 Steane 扩张所带来的优势。第 3 节将通过考虑 BCH 码给出这些结果的一项应用。

2.1. $\langle B_t\rangle$ 与 C 欧几里得正交的情形。本小节中，我们考虑由 $\mathbb{F}_q$-线性码$C=\langle B_r\rangle\oplus\langle B_t\rangle$ 定义的纠缠辅助量子纠错码 D_A 的 Steane 扩张 C，其中满足 $\langle B_t\rangle\subseteq C^{\perp_e}$。沿用上述记号，结果如下。

定理 7. 设 $C=\langle B_r\rangle\oplus\langle B_t\rangle\subseteq\mathbb{F}_q^n$ 为一个 $\mathbb{F}_q$-线性码，满足 $\langle B_t\rangle\subseteq C^{\perp_e}$ 且 $\mathbf{dim}_{\mathbb{F}_q}\langle B_t\rangle\geq 2$。令 $t=\mathbf{dim}_{\mathbb{F}_q}\langle B_t\rangle$，并假设 A 是一个在 $\mathbb{F}_q$ 上没有属于 $\mathbb{F}_q$ 的特征值的 $t\times t$ 可逆矩阵。记 c 为由 C 确定的纠缠辅助量子纠错码 C 所需的最大纠缠态的最少数量。则定义 5 中引入的线性码 D_A，intro-duced，可导出一个纠缠辅助量子纠错码 D_A，它是 C 的 Steane 扩张，其参数为

$$[[n,n-2r-t+c,d',c]]_q,$$

where $d'\geq\min\left\{\delta_1,\left\lceil\left(1+\frac{1}{q}\right)\delta_2\right\rceil\right\}$, $\delta_1=d_H\left(C^{\perp_e}\right)$ *and* $\delta_2=d_H\left(\langle B_r\rangle^{\perp_e}\right)$.

证明。定理 6 确定了定理陈述中给出的纠缠辅助量子纠错码 D_A 参数，但有一点除外：$\tilde{D}_A$ 中所需的最少最大纠缠态 c' 数量等于 c。现在，$\langle B_t\rangle\subseteq C^{\perp_e}$，于是 $B_tB_t^T=0$ 且 $B_rB_t^T=0$。然后，由（2）可得，

$$c=\operatorname{rank}\begin{pmatrix}B_rB_r^T & 0\\ 0 & 0\end{pmatrix}=\operatorname{rank}\left(B_rB_r^T\right).$$

最后，由（4）以及上述等式可得

$$c' = \frac{1}{2}\mathrm{rank}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & B_r B_r^T \\ 0 & -B_r B_r^T & 0 \end{pmatrix} = \mathrm{rank}\left(B_r B_r^T\right) = c,$$

由此完成证明。 □

上述结果表明，适当选择线性码 C，便可得到对由 C 给出的纠缠辅助量子纠错码进行 Steane 扩张，使其维数增加（增加量为 t），同时保持所需最大纠缠态的数量 c 不变。

为结束本小节，我们引入一类矩阵，它们可用于构造定理 6 和定理 7 所需的矩阵A 。这类矩阵也将在后续的第 2.2 小节中使用。设 $j \geq 2$ 为一个整数，考虑首一多项式

$$h_{\boldsymbol{a}}(X) := X^j + a_{j-1}X^{j-1} + \cdots + a_1 X + a_0 \in \mathbb{F}_q[X] \tag{5}$$

以及其对应的、元素属于 $\mathbb{F}_q$的 $j \times j$ （伴随）矩阵：

$$L_j(h_{\boldsymbol{a}}) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{j-2} & -a_{j-1} \end{pmatrix}.$$

于是有以下命题。

命题 8. $h_{\boldsymbol{a}}(X)$ 是矩阵 $L_j(h_{\boldsymbol{a}})$ 的特征多项式。

证明。证明见 [27, 引理 7] 或 [33, 引理 2.5]。 □

注 9. 设 $t \geq 2$ 是一个正整数。考虑多项式 $\bar{h}_t := X^t + X^{t-1} \in \mathbb{F}_q[X]$，它诱导出映射 $\varphi_{\bar{h}_t} : \mathbb{F}_q \to \mathbb{F}_q$, $\varphi_{\bar{h}_t}(x) = h_t(x)$。显然，$\varphi_{\bar{h}_t}$ 不是单射，因此存在一个不属于 $\varphi_{\bar{h}_t}$像集的 $0 \neq \xi \in \mathbb{F}_q$。那么，多项式$h_t := h_t - \xi \in \mathbb{F}_q[X]$ 在 $\mathbb{F}_q$中没有根。因此， $L_t(h_t)$ 是定理 7 中矩阵 A 的合适选择。

2.2. $\langle B_r \rangle$ 与 $\langle B_t \rangle$ 欧几里得正交的情形。本小节研˜究由满足码 $C = \langle B_r \rangle \oplus \langle B_t \rangle \subseteq \mathbb{F}_q^n$ 的纠缠辅助量子纠错码 C 的 Steane 扩张，其中码 $\langle B_r \rangle$ 和 $\langle B_t \rangle$ 欧几里得正交。注意，小节 2.1 研究的是本小节的一种特殊情形；本小节将给出 Steane 扩张 D_A的参数˜。在这种情形下，对矩阵 A还需要附加条件。

令 $\langle B_t \rangle = \langle B_{t_\ell} \rangle \oplus \langle B_{t_Q} \rangle$，其中 $\langle B_{t_Q} \rangle \subseteq \langle B_t \rangle^{\perp_e}$。我们用 t_ℓ 表示线性码 $\langle B_{t_\ell} \rangle$ 的维数。不失一般性，假设 B_{t_ℓ} 的各行与 $\mathbb{F}_q^n$ 的几何分解相容（见 [39]），根据第 2 节的 [19, 。4], $Z := B_{t_\ell} B_{t_\ell}^T$ 是一个矩阵，除形如.....的对角块外，其所有元素均为零

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

或（z_i）， $z_i \neq 0$，在特征 2 中可能包含如下方框：

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

也就是说,

$$Z = \begin{pmatrix} \boxed{\begin{matrix}0&1\\1&0\end{matrix}} & & & & & & & \\ & \ddots & & & & & & \\ & & \boxed{\begin{matrix}0&1\\1&0\end{matrix}} & & & & & \\ & & & z_1 & & & & \\ & & & & \ddots & & & \\ & & & & & z_s & & \\ & & & & & & \boxed{\begin{matrix}0&1\\1&1\end{matrix}} \end{pmatrix},$$

其中最后一个方框仅可能出现在特征 2 的情况下。

现在考虑一个可逆矩阵

$$A = \begin{pmatrix} A_0 Z^{-1} & 0 \\ 0 & A_1 \end{pmatrix},$$

其中 A_0（分别为 A_1）是元素属于 $\mathbb{F}_q$ 的 $t_\ell \times t_\ell$（分别为 $(t-t_\ell)\times(t-t_\ell)$）矩阵。我们还假设 A 在有限域 $\mathbb{F}_q$ 中没有特征值。于是，我们可以陈述本小节的主要结果。

定理 10. 设 $C = \langle B_r \rangle \oplus \langle B_t \rangle \subseteq \mathbb{F}_q^n$ 是如前所述的 $\mathbb{F}_q$-线性码。用 c 表示由 $\mathcal{C}$ 确定的 EAQECC C 所需的最大纠缠态的最小数量 ~。那么，线性码 D_A 可导出一个 EAQECC D_A，它是 C 的 Steane 扩张~，其参数为

$$[[n, n-2r-t+c', d', c']]_q,$$

其中

$$c' = (c - t_\ell) + \frac{1}{2}\mathrm{rank}\left(A_0 - A_0^T\right) = c - \mathrm{rank}\left(B_t B_t^T\right) + \frac{1}{2}\mathrm{rank}\left(A_0 - A_0^T\right)$$

$and\ d' \geq \min\left\{\delta_1, \left\lceil\left(1+\frac{1}{q}\right)\delta_2\right\rceil\right\},\ \delta_1 = d_H\left(C^{\perp_e}\right)\ and\ \delta_2 = d_H\left(\langle B_r\rangle^{\perp_e}\right).$

证明。定理 6 给出了陈述中的参数，但 c' 的公式除外。最大纠缠态的数量 c' 取决于式 (4) 中矩阵的秩。我们假设码 $\langle B_r \rangle$ 和 $\langle B_t \rangle$ 欧几里得正交，因此 $B_r B_t^T = 0$，且式 (4) 中矩阵位置 (1, 2)、(1, 3)、(2, 1) 和 (3, 1) 处的元素均为零。此外，回顾一下，$Z = B_{t_\ell} B_{t_\ell}^T$ 是一个大小为 t_ℓ 的可逆方阵，因此有

$$B_t B_t^T = \begin{pmatrix} Z & 0 \\ 0 & 0 \end{pmatrix}$$

于是，式 (4) 中矩阵位置 (1, 1) 处的元素，即 $B_t B_t^T A^T - A B_t B_t^T$，等于

$$\begin{pmatrix} Z & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} (Z^{-1})^T A_0^T & 0 \\ 0 & A_1^T \end{pmatrix} - \begin{pmatrix} A_0 Z^{-1} & 0 \\ 0 & A_1 \end{pmatrix}\begin{pmatrix} Z & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} A_0^T - A_0 & 0 \\ 0 & 0 \end{pmatrix}.$$

因此，有

$$c' = \frac{1}{2}\left(\mathrm{rank}\left(A_0 - A_0^T\right)\right) + \mathrm{rank}\left(B_r B_r^T\right). \tag{6}$$

现在，考虑到 $\langle B_r \rangle$ 和 $\langle B_t \rangle$ 欧几里得正交，由等式 (2) 可得

$$c = \operatorname{rank}\left(B_r B_r^T\right) + \operatorname{rank}\left(B_t B_t^T\right) = \operatorname{rank}\left(B_r B_r^T\right) + t_\ell. \tag{7}$$

结合等式（6）和（7），陈述中关于 c' 的等式得以证明 . □

我们通过说明一个由上述矩阵 L_j 表示的矩阵 A 适用于我们的目的，来结束本小节。

引理 11. 设 $h_{\boldsymbol{a}}(X)$ 是如（5）所示的多项式，并考虑伴随矩阵 $L_j := L_j(h_{\boldsymbol{a}})$。那么

$$\operatorname{rank}(L_j - L_j^T) \geq j - 2.$$

Mo此外，若 j 为奇数，则秩$(L_j - L_j^T) = j - 1$；否则，秩$(L_j - L_j^T) = j$ 当且仅 if

$$1 + a_0 + a_2 + a_4 + \cdots + a_{j-2} \neq 0.$$

证明. 首先，有

$$L_j - L_j^T$$

$$= \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & a_0 \\ -1 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & a_1 \\ 0 & -1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & -1 & 0 & 1 & a_{j-3} \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 0 & 1 + a_{j-2} \\ -a_0 & -a_1 & -a_2 & -a_3 & -a_4 & \cdots & -a_{j-4} & -a_{j-3} & -1 - a_{j-2} & 0 \end{pmatrix}.$$

矩阵 $L_j - L_j^T$是斜对称的。由于其对角线上的元素均为零，即使在特征为 2 时，该矩阵也是交错矩阵。因此，其秩为偶数 [14]。此外，删去最后两行以及第一列和最后一列后，可得到一个对角线上全为 1 的三角矩阵。因此，rank$(L_j - L_j^T) \geq j - 2$，由此我们证明了第一个结论。由于秩为偶数，当 j为奇数时，rank$(L_j - L_j^T) = j - 1$ 这一结论显然成立。

最后，假设 j 为偶数。那么，rank$(L_j - L_j^T)$ 等于 j 或 $j - 2$。我们将证明，当且仅当 det$(L_j - L_j^T) \neq 0$、当且仅当 $(1 + a_0 + a_2 + a_4 + \cdots + a_{j-2})^2 \neq 0$、当且仅当 ($1 + a_0 + a_2 + a_4 + \cdots + a_{j-2}) \neq 0$时，该秩为 j，由此完成证明。因此，需要证明的是，对于偶数 j，

$$\det(L_j - L_j^T) = (1 + a_0 + a_2 + a_4 + \cdots + a_{j-2})^2.$$

确实，将奇数行加到第（$j - 1$）行后，我们得到一个新矩阵，其行列式不变，除第（$j - 1$）行外，其余各行也都不变；第（$j - 1$）行的所有元素均为零，只有最后一个元素例外，它是

$$1 + a_0 + a_2 + a_4 + \cdots + a_{j-2}.$$

现在沿第 ($j - 1$) 行进行拉普拉斯展开，得到唯一一个非零加项。接下来，我们再次依次沿那些恰有一个元素为 1 的行进行拉普拉斯展开（这些 1 位于初始矩阵的奇数列中）。然后，

剩下的工作是计算由该矩阵的行列式给出的子式

$$\begin{pmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 1 \\ -a_0 & -a_2 & -a_4 & -a_6 & \cdots & -a_{j-6} & -a_{j-4} & -1-a_{j-2} \end{pmatrix}.$$

最后，将上面矩阵的所有列加到最后一列，得到下列矩阵（行列式相同）：

$$\begin{pmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 0 \\ -a_0 & -a_2 & -a_4 & -a_6 & \cdots & -a_{j-6} & -a_{j-4} & -(1+a_0+a_2+\cdots+a_{j-2}) \end{pmatrix}.$$

这证明了 $\det(L_j - L_j^T) = (1 + a_0 + a_2 + a_4 + \cdots + a_{j-2})^2,$，并完成了证明。□

沿用注 9 中的记号。可以将矩阵 L_{t-t_ℓ} (h_{t-t_ℓ}) 用作定理 10 所考虑的矩阵 A 中的方框 A_1。

我们寻找形如 L_j 的矩阵 A_0，以保证 A 在 $\mathbb{F}_q$ 中没有特征值。下面的方法可以得到所述类型的矩阵，使得 $\operatorname{rank}(A_0 - A_0^T)$ 达到最大。注意，根据定理 10，这一事实不仅增加了纠缠，也增加了所得码的维数。

首先，假设域 $\mathbb{F}_q$ 的特征为奇数，或者为偶数且 $t_\ell > 2$。然后，令 $\tilde{\phi}_{t_\ell}$: $= X^{t_\ell} - X^{t_\ell - 2} \in \mathbb{F}_q[X]$。相应的映射

$$\varphi_{\tilde{\phi}_{t_\ell}} : \mathbb{F}_q \to \mathbb{F}_q$$

~是 $\varphi_{\tilde{\phi}_{t_\ell}}(x) = \phi_{t_\ell}(x)$。与注 9 中一样，$\varphi_{\tilde{\phi}_{t_\ell}}$不是双射，因此可以在 $\mathbb{F}_q$ 中找到一个非零的~元素 ξ_1，使得多项式 $\phi_{t_\ell} := \phi_{t_\ell} - \xi_1 \in \mathbb{F}_q[X]$ 在 $\mathbb{F}_q$中没有根。在这种情况下，$L_{t_\ell}(\phi_{t_\ell})$是一个合适的矩阵，可作为 A的方框 (1, 1) 中涉及的矩阵 A_0。

当 $q \neq 2$时，域 $\mathbb{F}_q$ 的特征为二且 $t_\ell = 2$，只需考虑由 $\phi_2 = h_2$定义的矩阵 $L_{t_2}(\phi_2)$，其中 h_2 是注 9 中给出的多项式；再考虑 $\phi_2 = \phi_2 - \xi$，其中 $\xi \neq 0$，1 是 $\mathbb{F}_q$中的一个合适取值。注意，在这种情况下，多项式 $X^2 + X - \varsigma, \varsigma \in \mathbb{F}_q$要么有两个不同的根，要么不可约。

推论 12。设 A_0 和 A_1 为上文所述的矩阵。那么，该矩阵

$$A = \begin{pmatrix} A_0 Z^{-1} & 0 \\ 0 & A_1 \end{pmatrix}$$

~~可用于对定理 10 中给出的纠缠辅助量子纠错码 C 进行 Steane 扩张 D_A。此外，矩阵 $A_0 - A_0^T$的秩达到最大。也就是说，当 t_ℓ 为偶数（分别为奇数）时，它为t_ℓ （分别为 $t_\ell - 1$）。

证明。证明基于以下事实：我们对 A_0 和 A_1 的选择意味着它们在 $\mathbb{F}_q$ 中没有特征值，因此 A也如此。最后，根据引理 11，若 t_ℓ 为偶数，则与 ϕ_{t_ℓ}对应的值 $1+a_0+a_2+a_4+\cdots+a_{j-2}$为 $-\xi_1\neq 0$，且其秩达到最大。□

注 13. 当 t_ℓ 为奇数时，若考虑 L_j 类型的矩阵 A_0，则秩$(A_0-A_0^T)=t_\ell-1$ 是唯一的可能性。

现在假设 t_ℓ 为偶数。若 $t_\ell\geq q$ 且 $\mathbb{F}_q$ 的特征为二，我们考虑多项式 η_{t_ℓ}：$=X^{t_\ell}-X^{t_\ell-q+1}-1$。假设 q 为奇数。很快我们将证明存在 $0\neq a\in\mathbb{F}_q$，使得多项式 $X^2+aX-1\in\mathbb{F}_q[X]$ 在 $\mathbb{F}_q$ 中没有根。因此，多项式 $\eta_{2w}=X^{2w}+aX^w-1$ 在 w 为奇正整数时，在 $\mathbb{F}_q$ 中没有根。因此，若特征为二时 $t_\ell\geq q$，否则当 $t_\ell=2w$ 时，多项式 η_{t_ℓ} 可构造出矩阵 $A_0:=L_{t_\ell}(\eta_{t_\ell})$，这些矩阵适用于我们的目的，且满足秩$(A_0-A_0^T)=t_\ell-2$。对于其余情况，我们没有适用于 A_0 且满足秩$(A_0-A_0^T)=t_\ell-2$ 的通用候选；不过，对于特定情况以及适中的 q 和 t_ℓ 值，不难找到合适的多项式 η_{t_ℓ} 及其对应矩阵 A_0，使其具有上述秩。还要注意，这里所述的传播规则 [35] 在此处不适用，因为我们的码并非来自厄米构造。

接下来要证明，对于某个 $a\neq 0$，X^2+aX-1 是不可约的。当且仅当存在 $0\neq a\in\mathbb{F}_q$，使得对于所有 $b\in\mathbb{F}_q$，$a^2+4\neq b^2$ 成立。考虑附带的方程 (1)：$x^2+4=y^2, x,y\in\mathbb{F}_q$，以及新变量 $x_1=(x+y)/2$ 和 $y_1=(y-x)/2$，它们满足 $x=x_1-y_1$ 和 $y=x_1+y_1$。由此可知，(x,y) 是 (1) 的解，当且仅当 (x_1,y_1) 是方程 (2)：$x_1y_1=1$ 的解。因此，映射 $\zeta:\mathbb{F}_q^*\to\mathbb{F}_q$ 定义为 $\zeta(x_1)=x_1-x_1^{-1}=x_1^{-1}(x_1^2-1)$，会将 (2) 的解映射为 (1) 的解；而且，$x_1=1$ 和 $x_1=-1$ 给出满足 $x=0$ 的 (1) 的解。这证明了在 $\mathbb{F}_q$ 中存在某个值 $a\neq 0$，使得 $a^2+4=y^2$ 在 $\mathbb{F}_q$ 中无解，从而完成证明。

3. Steane enlargement of EAQECCs given by BCH codes

在最后这一节中，我们研究由某些 BCH 码给出的纠缠辅助量子纠错码的 Steane 扩张。我们将其分为两个小节。第一小节展示我们的结果，第二小节给出一些例子。

3.1. 结果。

BCH 码是循环码，但我们更倾向于将其视为某些求值码的子域子码 [6, 12]。事实上，我们的 BCH 码是单变量的 J-仿射簇码，其中 $J=\{1\}$，其定义见 [16],，我们将使用该文献中的一些结果。

设 $q=p^m$、$m\geq 1$ 和 $n=p^m-1$。我们考虑求值映射

$$\mathrm{ev}:\frac{\mathbb{F}_q[X]}{\langle X^n-1\rangle}\to\mathbb{F}_q^n,$$

由 ev$(h)=(h(R_1)\ldots,h(R_n))$ 给出，其中 $\{R_i\}_{i=1}^n$ 是有限域 $\mathbb{F}_q$中 n次单位根的集合。现在定义 $H:=\{0,1,\ldots,n-1\}$，对于集合 $\emptyset\neq\Delta\subseteq H$，用 C_Δ表示由 $\{\mathrm{ev}(X^i):i\in\Delta\}$生成的 $\mathbb{F}_q$ 上线性码。再考虑一个正整数 s，使得 $s\neq m$ 整除 m，此时，$\mathbb{F}_{p^s}$ 上的 BCH 码是码C_Δ的子域子码，即形如 $\mathbb{F}_{p^s}^n\cap C_\Delta$的码。给定 $a\in H$，最小分圆陪集（相对于 n 和 s）是元素集合 $\mathcal{I}_a:=\{ap^{\ell s}:\ell\geq 0\}$，其中乘积均模 n 计算（也就是说，a 和 $\mathcal{I}_a$ 中的元素都是同余环 $\mathbb{Z}_n$ 中各等价类在 H 中的代表元）。用 i_a 表示 $\mathcal{I}_a$ 的基数，并令 $\mathcal{I}_a^R=\mathcal{I}_{n-a}$，我们

将其称为 $\mathcal{I}_a$的倒数陪集。此外，当 $\mathcal{I}_a = \mathcal{I}_a^R$时， $\mathcal{I}_a$ 称为对称；否则称为非对称。

在每个最小分圆陪集中，我们取其在自然顺序下的最小元素，并用 $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_z\}$ 表示这些最小代表元的集合。于是，$\{\mathcal{I}_{a_\nu}\}_{\nu=0}^{z}$ 是最小分圆陪集的集合（相对于 n 和 s）。我们将使用以下结果，该结果可见于 [21, 命题 1 和 2]。

命题 14。沿用上述记号。

（1）设 $\Delta = \cup_{\nu=\ell_1}^{\ell_2}\mathcal{I}_{a_\nu}$，其中 $\ell_1 < \ell_2$ 属于 $\{0, 1, \ldots, z\}$。则子域子码 $\mathbb{F}_{p^s}^n \cap C_\Delta$ 的维数等于 $\sum_{\nu=\ell_1}^{\ell_2} i_{a_\nu}$。当 Δ 是非连续最小分圆陪集的并集时，同样的结果也成立。

（2）现在设 $\ell_1 = 0$，并令 δ 表示 $\mathbb{F}_{p^s}^n \cap C_\Delta$ 的欧几里得对偶码的最小距离，则 $\delta \geq a_{\ell_2+1} + 1$。

对于 $0 \leq \ell < z$，记 $\Delta(\ell) = \cup_{\nu=0}^{\ell}\mathcal{I}_{a_\nu}$和 $\Delta(\ell)^{\perp_e} = H \setminus \cup_{\nu=0}^{\ell}\mathcal{I}_{a_\nu}^R$。于是，根据 [21, 第5], 页， $\mathbb{F}_{p^s}^n \cap C_{\Delta(\ell)}$的欧几里得对偶与子域子码 $\mathbb{F}_{p^s}^n \cap C_{\Delta(\ell)^{\perp_e}}$相同。我们将 $\Delta(\ell) = \Delta_r \sqcup \Delta_L$分解，其中 Δ_r 由 $\Delta(\ell)$ 中倒数陪集不属于 $\Delta(\ell)$的非对称陪集组成，而 Δ_L 是其余非对称陪集与对称陪集的并集。显然， $\Delta(\ell) = \Delta_r \cup \Delta_L$ 且 $\Delta_r \cap \Delta_L = \emptyset$。

以下结果可由应用定理 4（其中考虑 $C_1 = C_2 = \mathbb{F}_{p^s}^n \cap C_{\Delta(\ell)}$）以及 [21, 第 7] 页中的第一个显示公式得出。

定理 15。在上述记号下，存在一个参数为

$$\left[\left[n, n - 2\sum_{\nu=0}^{\ell} i_{a_\nu} + c, \geq a_{\ell+1} + 1; c\right]\right]_{p^s},$$

其中 $c = \#\Delta_L$，# 表示基数。

本节旨在计算由定理 15 给出的某些纠缠辅助量子纠错码的 Steane 扩张的参数，或通过与该定理相同的过程、但关联到另一组码 C_Δ 所得到的参数。给定一个素数 p 以及如上所述的互异正整数m和 s，我们将正整数 $B(p, m, s)$ 定义为

$$B(p, m, s) := \begin{cases} (p^s)^{\frac{m}{2s}} - 1 & \text{if } \frac{m}{s} \text{ is even}, \\ (p^s)^{\lceil \frac{m}{2s} \rceil} - p^s + 1 & \text{otherwise.} \end{cases}$$

我们将频繁使用这个整数。

以下结果由 [1] 中的定理 3 和引理 8 推出。

命题 16。设 p、m 和 s 为上述整数，并考虑另一个整数 b，使得 $0 < b < B(p, m, s)$。那么，

a): $\mathcal{I}_b \subseteq \mathcal{I}_b^{\perp_e} := H \setminus \mathcal{I}_b^R$。 b): $\#\mathcal{I}_b = \frac{m}{s}$，当 $b = B(p, m, s)$ 时，

这个等式也成立。

现在可以陈述本节中的第一个新结果了。它属于小节 2.1 所述的情形。我们先陈述该结果，随后给出两个推论。

定理 17. 设 p 为素数， m 和 s 为上述不同的正整数。令 $n = p^m - 1$ 和 $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_z\}$ 为关于 n 和 s 的最小分圆陪集族的最小代表元集合。选取指标 $\ell_1 < \ell_2 < z$

使得 $a_{\ell_2} < B(p,m,s)$。那么，存在一个定理 15 中所述的纠缠辅助量子纠错码的 Steane 扩张，其参数为

$$\left[\left[n, n-\frac{m}{s}(\ell_1+\ell_2)-1, d'; 1\right]\right]_{p^s},$$

where $d' \geq \min\left\{a_{\ell_2+1}+1, \left\lceil\left(\frac{p^s+1}{p^s}\right)(a_{\ell_1+1}+1)\right\rceil\right\}$.

证明。采用定理 7 中的记号，令 $C := \mathbb{F}_{p^s} \cap C_{\Delta(\ell_2)}$ 以及 B_r（分别为 B_t）为码 $\mathbb{F}_{p^s} \cap C_{\Delta(\ell_1)}$（分别为 $\mathbb{F}_{p^s} \cap C_{\Delta'}$）的生成矩阵，其中 $\Delta' = \cup_{\nu=\ell_1+1}^{\ell_2} \mathcal{I}_{a_\nu}$）。然后，注意到单项式 X^a 的求值与X^b 的求值正交，除非 $a+b \equiv 0$ 模 n（见 [16, 命题 2.2]），由命题 16 可推出，在定理 15 之前给出的分解 $\Delta(\ell_2) = \Delta_r \sqcup \Delta_L$ 中，$\Delta_L = \mathcal{I}_0$。因此，由 C 给出的纠缠辅助量子纠错码的 c 值为 $c = 1$。最后，应用定理 7 并考虑命题 14 和 16，可得到由 C 给出的纠缠辅助量子纠错码的 Steane 扩张，其参数为

$$\left[\left[n, n-2\left(\frac{m\ell_1}{s}+1\right)-\left(\frac{m(\ell_2-\ell_1)}{s}\right)+1, d'; 1\right]\right]_{p^s},$$

其中 $d' \geq \min\left\{a_{\ell_2+1}+1, \left\lceil\left(\frac{p^s+1}{p^s}\right)(a_{\ell_1+1}+1)\right\rceil\right\}$。证明至此结束。□

在上述定理中取 $\ell_1 = 0$ 和 $\ell_2 = 1$，可得到以下结果。

推论 18。设 p 为素数，且正整数 $n = p^m - 1$ 由$m > 0$给出。令 $s \neq m$ 为一个正整数，使得 s 整除 m。那么，存在一个如定理 15 所述的纠缠辅助量子纠错码的 Steane 扩张，其参数为 $\left[\left[n, n-\frac{m}{s}-1, 3;\ 1\right]\right]_{p^s}$。

以下结果比定理 17 稍弱，但只依赖于 $\mathcal{A}$中的一个元素。

推论 19。沿用定理 17 中的记号，并选取 $a_\ell \in \mathcal{A}$ 使得 $a_\ell < B(p,m,s)$。那么，存在一个如定理 15 所述的纠缠辅助量子纠错码的 Steane 扩张，其参数为

$$\left[\left[n, n-\frac{m}{s}(2\ell-1)-1, a_{\ell+1}; 1\right]\right]_{p^s}.$$

证明。对 $\ell_1 = \ell - 1$ 和 $\ell_2 = \ell$应用定理 17。证明基于以下事实：当 $a_\ell + 1$是 p^s的倍数时，$a_{\ell+1} = a_\ell + 2$；否则，$a_{\ell+1} = a_\ell + 1$。事实上，显然，当 $i < p^s$时，$a_i = i$；而当 $a_\ell + 1$是 p^s的倍数时，则有 $a_{\ell+1} > a_\ell + 1$。因此，当 m/s为偶数时，只需证明形如 $b + \lambda p^s < p^{m/2} - 1$、$b$、$\lambda$正整数且 $0 \neq b < p^s$ 的元素是 $\mathcal{A}$中的最小代表元。这是因为 b 是 $b + \lambda p^s$ 的 p^s进制展开中的首项；将一个整数的 p^s进制展开$a_0 + a_1 p^s + \cdots + a_{\lfloor \frac{n}{s} \rfloor} p^{\lfloor \frac{n}{s} \rfloor s}$ 写成 $(a_0, a_1, \ldots, a_{\lfloor \frac{n}{s} \rfloor})$ 后，陪集 $\mathcal{I}_{b+\lambda p^s}$ 中各元素的 p^s进制展开可通过依次移位 $b + \lambda p^s$的 p^s进制展开得到。在一段时间内，这些移位后的展开在首位为零；当首位出现非零项时，相应的数值大于 $p^{m/2} - 1$。用类似的推理可证明 $m/2$ 为奇数时的结果。□

以下结果也基于定理 7。我们沿用定理 17 中的相同条件。也就是说，考虑一个素数 p，以及 m 和 s 两个不同的正整数，使得 s 整除 m。令 $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_z\}$ 为最小分圆陪集的集合（相对于 $n = p^m - 1$ 和 s）。

定理 20. 设 $\ell_1 < \ell_2 < z$为两个指标，使得 $a_{\ell_2} < B(p,m,s)$。那么，存在一个由码 C_Δ 确定的 EAQECC 的 Steane 扩张，其参数为：

$$\left[\left[n, n-\frac{m}{s}(\ell_1+\ell_2)-1, d'; c\right]\right]_{p^s},$$

其中 $d' \geq \min\left\{a_{\ell_1+1}+a_{\ell_2+1}, \left\lceil 2\left(\frac{p^s+1}{p^s}\right)a_{\ell_1+1}\right\rceil\right\}$ and $c = 1+2\frac{m}{s}\ell_1$。

证明。对于非负整数 ℓ，定义 $\Delta(\ell, R) := \cup_{\nu=0}^{\ell}\mathcal{I}_{a_\nu} \bigcup \cup_{\nu=1}^{\ell}\mathcal{I}_{a_\nu}^{R}$。现在，采用定理 7 中的记号，令 $C := \mathbb{F}_{p^s} \cap C_{\Delta(\ell_1,R)\cup\Delta'}$，其中 $\Delta' = \cup_{\nu=\ell_1+1}^{\ell_2}\mathcal{I}_{a_\nu}$。固定 B_r（分别为 B_t）作为码 $\mathbb{F}_{p^s} \cap C_{\Delta(\ell_1,R)}$（分别为 $\mathbb{F}_{p^s} \cap C_{\Delta'}$）的生成矩阵。

为计算 c，我们采用定理 17 证明中的推理，并且 $c = 1+2\frac{m}{s}\ell_1$，因为定理 15 之前给出的分解 $\Delta(\ell_1, R) \cup \Delta' = \Delta_r \sqcup \Delta_L$ 中的集合 Δ_L 是 $\Delta(\ell_1, R)$。关于距离，我们注意到 $\Delta(\ell, R)$ 中的值包含从 0 到 $a_{\ell+1}-1$ 的所有连续整数，以及它们模 n 的相反数。然后，使用 $*$ 由 $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n)$ 定义的乘积，我们推得存在一个与 $C_{\Delta(\ell, R)}$ 等距的码，其中包含X连续幂的求值。这证明了 $\langle B_r\rangle^{\perp_e}$ 的最小汉明距离大于或等于$2a_{\ell_1+1}$。类似的论证表明，$d_H(C^{\perp_e}) \geq a_{\ell_1+1}+a_{\ell_2+1}$，从而证明完毕。□

我们的最后结果与第 2.2 小节所述的情形相吻合。我们从下面的结果开始。

定理 21。设 p为素数，且 m 和 s 为正整数，满足 s 整除m、$s \neq m$。假设 m 和 m/s 为偶数。令 $n = p^m-1$ 和 $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_z\}$ 关于 n 和 s，最小分圆陪集族的最小代表元集合。令 $0 < \ell_2 < z$ 为满足 $a_{\ell_2} = p^{\frac{m}{2}}-1$ 的指标。考虑指标 $0 \leq \ell_1 < \ell_2$。那么，存在一个如定理 15 所示的纠缠辅助量子纠错码的 Steane 扩张，其参数为

$$\left[\left[n, n-\frac{m}{s}(\ell_1+\ell_2)-1+\frac{m}{2s}, d'; \frac{m}{2s}+1\right]\right]_{p^s},$$

$where\ d' \geq \min\left\{a_{\ell_2+1}+1, \left\lceil\left(\frac{p^s+1}{p^s}\right)(a_{\ell_1+1}+1)\right\rceil\right\}.$

证明。我们希望使用定理 10。考虑 $C := \mathbb{F}_{p^s} \cap C_{\Delta(\ell_2)}$ 以及子域码 $\mathbb{F}_{p^s} \cap C_{\Delta(\ell_1)}$（分别为 $\mathbb{F}_{p^s} \cap C_{\Delta'}$，其中$\Delta' = \cup_{\nu=\ell_1+1}^{\ell_2}\mathcal{I}_{a_\nu}$）的一个合适生成矩阵 B_r（分别为 B_t）。采用命题 14 之后使用的记号，并根据 [16, 注 3，4],有 $\Delta_L = \mathcal{I}_0 \cup \mathcal{I}_{a_{\ell_2}}$，且在分解 $\Delta(\ell_2) = \Delta_r \sqcup \Delta_L$ 中有 $\Delta_r = \cup_{\nu=1}^{\ell_2-1}\mathcal{I}_{a_\nu}$。定理 15 和命题 16 表明，由 C 给出的纠缠辅助量子纠错码的值 c 为$c = 1 + \#\mathcal{I}_{a_{\ell_2}} = 1 + (m/s)$。

最后，注意到 m/s 是第 2.2 小节中引入的某个适当矩阵 $A_0 - A_0^T$ 的秩，且 rank($B_rB_r^T$) $= 1$，应用定理 10 和推论 12 即可得到证明。因此，我们已证明存在由 C 给出的纠缠辅助量子纠错码的 Steane 扩张，其参数如命题所述。

□

与定理 20 的证明相同，我们可以添加互反陪集，所得结果如下。

定理 22. 以下陈述成立。

i)：沿用定理 20 中相同的记号和要求，则存在一个由码 C_Δ 确定的纠缠辅助量子纠错码的 Steane 扩张，其参数为：

$$\left[\left[n, n-\frac{m}{s}(\ell_1+\ell_2)-1, d'; c'\right]\right]_{p^s},$$

where $d' \geq \min\left\{2a_{\ell_2+1}, \left\lceil 2\left(\frac{p^s+1}{p^s}\right)a_{\ell_1+1}\right\rceil\right\}$ *and* $c' = 1+\frac{m}{s}(\ell_1+\ell_2)$.

ii) 在定理的记号和条件下，存在一个 Steane 扩张，其对应的纠缠辅助量子纠错码参数为

$$\left[\left[n, n-\frac{m}{s}\left(\ell_1+\ell_2-\frac{1}{2}\right)-1, d'; c'\right]\right]_{p^s},$$

where

$$d' \geq \min\left\{a_{\ell_2+1}+a_{\ell_2}-1, \left\lceil 2\left(\frac{p^s+1}{p^s}\right)a_{\ell_1+1}\right\rceil\right\}$$

and $c' = 1+\frac{m}{s}(\ell_1+\ell_2-\frac{1}{2})$.

证明。为证明第一个结论，只需考虑 $C := \mathbb{F}_{p^s} \cap C_{\Delta(\ell_2,R)}$ 以及适当的矩阵 B_r 和 B_t，其中 B_r 生成子域码 $\mathbb{F}_{p^s} \cap C_{\Delta(\ell_1,R)}$，然后采用与定理 21 的证明相同的步骤。考虑到陪集 $\mathcal{I}_{a_{\ell_2}}$ 是对称的，第二个结论的证明类似。回顾一下，在这种情况下 $a_{\ell_2} = p^{\frac{m}{2}}-1$。□

注 23。在注 13 第二段所述条件下，我们也可以得到纠缠辅助量子纠错码的 Steane 扩张，其参数与定理 21 和定理 22 中给出的参数相同，但纠缠 c' 和维数各少一个单位。为此，只需考虑由多项式 η_{t_ℓ} 定义的矩阵 A_0，如上述注 13 所述。

3.2. 示例。我们以给出由第 3.1 小节中的一些结果得到的纠缠辅助量子纠错码参数，作为本节及本文的结尾。请注意，Steane 扩展码具有定理 1 后所述的有趣计算优势。我们给出了一些在文献中未曾发现、且无法通过传播规则从现有码得到的纠缠辅助量子纠错码及其参数。

我们给出三张关于 $q = 2,4,9$ 元纠缠辅助量子纠错码的表格，其中 q。表格展示了这些码的参数以及用于推导这些参数的相关结果。表格还列出了我们在计算中使用的值 m、s、a_{ℓ_1} 和 a_{ℓ_1}。

表 1 展示了二元情形中的一些示例。为加深理解，我们详细解释其中三个情形。采用相同的步骤即可获得我们所有表格中的参数。表中的第一个二元码具有参数 $[[15,4,6;\ 3]]_2$，其参数由定理 21 中的公式得到，其中 $m=4$、$s=1$、$\ell_1=1$、$a_{\ell_1}=1$、$\ell_2=2$、$a_{\ell_2}=3$ 和 $a_3=5$。如果对 $m=5$、$s=1$、$\ell_1=1$、$a_{\ell_1}=1$、$\ell_2=2$、$a_{\ell_2}=3$ 和 $a_3=5$ 应用定理 17，则可得到一个参数为 $[[31,15,6;\ 1]]_2$ 的码，如表中的第二行所示。最后，表中第八行的二元码 $[[63,32,14;\ 31]]_2$ 可根据定理 22 构造，注意到 $m=6$、$s=1$、$\ell_1=2$、$a_{\ell_1}=3$、$\ell_2=3$、$a_{\ell_2}=5$ 和 $a_4=7$。据我们所知，表 1 中的纠缠辅助量子纠错码除标有 * 的码之外，均为新码。我们认为它们表现良好，因为在某些情况下，它们与文献中的其他码相比具有优势。事实上，我们的码 $[[15,4,6;\ 3]]_2$（分别为 $[[63,44,8;\ 13]]_2$）优于文献 [25] 中出现的 $[[15,4,6;\ 5]]_2$（分别为 $[[63,42,8;\ 14]]_2$）。该文献还包含标有 * 的码，这些码是具有相应参数的已知最佳码。我们将它们加入其中，以说明我们能够获得性能良好的码。

n	k	$d \geq$	c	结果	(m, s)	a_{ℓ_1}	a_{ℓ_2}
15	4	6	3	定理 21	(4,1)	1	3
31	15	6	1^*	定理 17	(5,1)	1	3
31	15	8	11	定理 20	(5,1)	1	3
63	44	8	13	定理 20	(6,1)	1	3
63	32	8	1^*	定理 17	(6,1)	3	5
63	44	9	19	定理 22	(6,1)	1	3
63	38	9	13	定理 20	(6,1)	1	5
63	32	14	31	定理 22	(6,1)	3	5
127	70	12	1	定理 17	(7,1)	5	9
127	84	14	29	定理 20	(7,1)	3	7
127	70	18	43	定理 20	(7,1)	5	7
255	214	12	33	定理 20	(8,1)	3	5
255	214	14	41	定理 22	(8,1)	3	5
255	190	18	49	定理 20	(8,1)	5	9

TABLE 1. 二元纠缠辅助量子纠错码的参数

n	k	$d \geq$	c	结果	(m, s)	a_{ℓ_1}	a_{ℓ_2}
63	59	3	1	定理 17	(6,2)	0	1
63	26	17	31	定理 20	(6,2)	6	9
63	23	19	37	定理 20	(6,2)	7	9
63	23	20	40	定理 22	(6,2)	7	9
63	14	23	43	定理 20	(6,2)	9	11
63	11	26	52	定理 22	(6,2)	10	11
1023	1017	3	1	定理 17	(10,2)	0	1
1023	1007	4	1	定理 17	(10,2)	1	2
1023	892	36	121	定理 20	(10,2)	15	18
1023	887	37	131	定理 20	(10,2)	17	18
1023	887	38	136	定理 22	(10,2)	17	18
1023	877	40	141	定理 20	(10,2)	18	19
1023	877	42	146	定理 22	(10,2)	18	19
1023	847	50	176	定理 22	(10,2)	22	23
1023	602	113	411	定理 20	(10,2)	54	57
1023	597	115	421	定理 20	(10,2)	55	57

TABLE 2. 四元 EAQECC 的参数

表 2（分别为表 3）给出了利用我们的结果获得的一些新的四元（分别为九元）纠缠辅助量子纠错码示例。此外，根据注 23，在应用定理 21 和定理 22 时，k和 c 的值均可减少一个单位。事实上，在注意到表 3 中相应情况下的 $t_\ell = 6$ 后，可以使用注 13 中给出的多项式 η_{t_ℓ}。

CONFLICT OF INTEREST

作者声明不存在利益冲突。

n	k	$d \geq$	c	结果	(m, s)	a_{ℓ_1}	a_{ℓ_2}
728	724	3	1	定理 17	(6,2)	0	1
728	526	78	202	定理 22	(6,2)	37	38
728	517	80	205	定理 20	(6,2)	38	40
728	514	81	211	定理 20	(6,2)	39	40
728	511	82	211	定理 20	(6,2)	39	41
728	508	83	217	定理 20	(6,2)	40	41
728	496	88	232	定理 22	(6,2)	42	43
728	490	90	235	定理 20	(6,2)	43	44
728	490	92	238	定理 22	(6,2)	43	44

TABLE 3. 9元纠缠辅助量子纠错码的参数

REFERENCES

[1] S.A. Aly、A. Klappenecker 和 P. K. Sarvepalli。关于量子和经典 BCH 码。 *IEEE Trans.*，(): –。 *Inform. Theory* 53 3 1183 1188, 2007

[2] F. Arute 等。利用可编程超导处理器实现量子霸权。 *Nature*，574 505 510，2019：–。[3] A. Ashikhmin 和 E. Knill。非二元量子稳定子码。 *IEEE Trans. Inform. Theory*，47 7 3065 3072，2001 ()：–。[4] A.E. Ashikhmin、A.M. Barg、E. Knill 和 S.N. Litsyn。量子错误检测 I：问题陈述。 *IEEE Trans. Inform. Theory*，46(3):778–788，2000。[5] A.E. Ashikhmin、A.M. Barg、E. Knill 和 S. N. Litsyn。量子错误检测 II：界。 *IEEE Trans. Inform. Theory* 46 3 789 800, 2000 ，(): –。

[6] J. Bierbrauer。循环码理论及其向加性码的推广。 *Des. Codes Cryptogr.*，25 2 189 206，2002 ()：–。[7] J. Bierbrauer 和 Y. Edel。量子扭曲码。 *J. Comb. Designs*，8:174–188，2000。[8] T. Brun、I. Devetak 和 M. Hsieh。利用纠缠纠正量子错误。 *Science*，314 5798 436 439，2006 ()：–。[9] A. R. Calderbank、E. M. Rains、P. W. Shor 和 N. J. A. Sloane。通过 GF(4) 上的码实现量子纠错。 *IEEE Trans. Inform. Theory*，44(4):1369–1387，1998。[10] A. R. Calderbank 和 Peter W. Shor。良好的量子纠错码确实存在。 *Phys. Rev. A*，54 1098 1105，1996：–，8月。[11] M. Cao 和 J Cui。由自正交矩阵乘积码构造得到的新稳定子码。 *Finite Fields Appl.*，63:101643，2020。[12] I. Cascudo。关于循环码的平方。 *IEEE Trans. Inform. Theory*，65(2):1034–1047，2019。[13] X. Chen、S. Zhu 和 X. Kai。纠缠辅助量子负循环 BCH 码。 *Internat. J.*，(): –。 *Theoret. Phys.* 58 5 1509 1523, 2019

[14] P. Delsarte 和 J. M. Goethals。GF(q) 上的交替双线性形式。 *J. Comb. Th.*，19:26–50，1975。[15] Z. Du、C. Li 和 S. Mesnager。由 BCH 码的核构造自正交码及其参数。 *IEEE Trans. Inform. Theory*，第 6774–6785 页，2020。[16] C. Galindo、O. Geil、F. Hernando 和 D. Ruano。关于由 J 仿射簇码得到的稳定子量子码的距离。 *Quantum Inf. Process.*，16(4):第 111 条，32 页，2017。[17] C. Galindo 和 F. Hernando。关于从 Hermithian 自正交码构造量子码方法的推广。 *Des. Codes Cryptogr.*，90:1103–1112，2022。[18] C. Galindo、F. Hernando、H. Mart´ín-Cruz 和 D. Ruano。由依赖迹的多项式定义的稳定子量子码。 *Finite Fields Appl.*，87:102138，2023。[19] 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。 *Quantum Inf. Process.*，18(4):第 116 条，18 页，2019。[20] C. Galindo、F. Hernando 和 D. Ruano。由 J 仿射簇码构造稳定子量子码及一种新的 Steane 类扩张。 *Quantum Inf. Process.*，14(9):3211–3231，2015。[21] C. Galindo、F. Hernando 和 D. Ruano。由 RS 码和扩张次数为 2 的 BCH 码构造纠缠辅助量子纠错码。 *Quantum Inf. Process.*，20:158，2021。

[22] D. Gottesman。达到量子汉明界的量子纠错码类。*Phys. Rev. A*，54(3):1862–1868，1996。[23] D. Gottesman。利用高维系统实现容错量子计算。载于 Colin P. Williams 编，*Quantum Computing and Quantum Communications*，第 302–313 页，柏林、海德堡，1999。施普林格·柏林·海德堡。[24] M. Grassl。由 CSS 码得到的新量子码。 *Quantum Inf. Process.*，22:86，2023。[25] M. Grassl。线性码最小距离的界。 *www.codetables.de*，访问日期：2022 年 11 月 22 日。[26] G. Guo 和 R. Li。由广义 Reed-Solomon 码导出的新型纠缠辅助量子 MDS 码。 *Internat. J. Theoret. Phys.*，59(4):1241–1254，2020。[27] M. Hamada。可在多项式时间内构造的级联量子码：高效译码与纠错。*IEEE Trans. Inform. Theory*，54(12):5689–5704，2008。[28] M. H. Hsieh、I. Devetak 和 T. Brun。一般的纠缠辅助量子纠错码。*Phys. Rev. A*，76:062313，2007 年 12 月。[29] L. Ioffe 和 M. M´ezard。非对称量子纠错码。 *Phys. Rev. A*，75:032345，2007 年 3 月。[30] A. Ketkar、A. Klappenecker、S. Kumar 和 P. K. Sarvepalli。有限域上的非二元稳定子码。 *IEEE Trans. Inform. Theory*，52(11):4892–4914，2006。[31] E. Knill、R. Laflamme 和 W.H. Zurek。弹性量子计算：错误模型与阈值。*Proc. Royal Soc. London A*，454:365–384，1998。[32] G. G. La Guardia。关于非二元量子 BCH 码的构造。 *IEEE Trans. Inform. Theory*，60 3 1528( )：–1535，2014。[33] S. Ling、J. Luo 和 C. Xing。Steane 量子码扩展构造的推广及其应用。*IEEE Trans. Inform. Theory*，56(8):4080–4084，2010。[34] G. Luo 和 X. Cao。由广义 Reed-Solomon 码构造的两个新系列纠缠辅助量子 MDS 码。 *Quantum Inf. Process.*，18(3):第 89 号论文，12 页，2019。[35] G. Luo、M.F. Ezerman 和 S. Ling。纠缠辅助量子码与子系统量子码：新的传播规则与构造。*arXiv:2206.09782*，2022。[36] L. Luo 和 Z. Ma。利用非二元系统实现容错量子计算。*Quantum Inf.*，：。*Process.* 18 188, 2019
[37] J. Qian 和 L. Zhang。关于 MDS 线性互补对偶码和纠缠辅助量子码。 *Des. Codes Cryptogr.*，86(7):1565–1572，2018。[38] J. Qian 和 L. Zhang。新型纠缠辅助量子 MDS 码和近似 MDS 码的构造。*Quantum Inf. Process.*，18(3):第 71 号论文，12 页，2019。[39] D. Ruano。线性码的度量结构。载于 *Singularities algebraic geometry commutative*，，，，*algebra and related topics* 537 561 2018
第 – 页。施普林格，查姆，。[40] M. Sari 和 E. Kolotoglu。常循环码在纠缠辅助量子 MDS 码中的应用。*Comput. Appl. Math.*，38(2):第 75 号论文，13 页，2019。[41] P. K. Sarpevalli、A. Klappenecker 和 M. Rotteler。非对称量子码：构造、界与性能。 *Proc. Roy. Soc. A*，465:1645–1672，2000。[42] P. W. Shor 和 J. Preskill。BB84 量子密钥分发协议安全性的简单证明。*Phys. Rev. Lett.*，85:441–444，2000 年 7 月。[43] P.W. Shor。容错量子计算。*Proc. 37th ann. symp. found. comp. sc. IEEE Comp.*，，*Soc. Press* 56 65, 1996
第 – 页。[44] A. Steane。简单量子纠错码。 *Phys. Rev. Lett.*，77:2551–2577，1996。[45] A.M. Steane。Calderbank-Shor-Steane 量子码的扩张。 *IEEE Trans. Inform. Theory*，45 7 2492 2495，1999 ( )：–。[46] M. M. Wilde 和 T. A. Brun。纠缠辅助量子编码的最优纠缠公式。 *Phys. Rev. A*，77:064302，2008 年 6 月。*Current address*：Carlos Galindo 和 Fernando Hernando：卡斯特利翁数学与应用研究所及海梅一世大学数学系，里乌塞克校区。

12071 卡斯特利翁（西班牙），Ryutaroh Matsumoto：信息与通信工程系，东京工业大学，日本；奥尔堡大学数学科学系，
9220 奥尔堡 Ø，丹麦。
Email address: Galindo: galindo@uji.es; Hernando: carrillf@uji.es; Matsumoto: ryutaroh@ict.e.titech.ac.jp