Advances in Applied Mathematics 应用数学进展, 2026, 15(1), 133-141
Published Online January 2026 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2026.151014

Hans汉斯

由EGRS码构造的量子MDS码

吴莲铭

西北师范大学数学与统计学院，甘肃 兰州

收稿日期：2025年12月7日；录用日期：2026年1月1日；发布日期：2026年1月12日

摘　要

本文针对量子纠错领域中量子最大距离可分(MDS)码的构造问题展开研究，量子MDS码是一类达到量子Singleton界的最优码，在量子计算与通信中具有重要应用价值。为了突破现有构造方法在码长和参数灵活性上的限制，本文提出了一种创新性的构造：利用两个已知的埃尔米特(Hermitian)自正交扩展广义里德－所罗门(EGRS)码，通过特定的条件组合，来构造一个新的Hermitian自正交EGRS码。利用这一关键结论，我们获得了若干类新的q元量子MDS码。我们构造的量子MDS码的码长与以往的码有很大不同，且参数灵活。本研究不仅为量子MDS码的构造理论提供了新的思路和工具，也为实际量子信息系统中纠错码的设计提供了更多可能性。

关键词

量子MDS码，EGRS码，Hermitian自正交

Quantum MDS Codes Constructed by EGRS Codes

Lianming Wu

School of Mathematics and Statistics, Northwest Normal University, Lanzhou Gansu

Received: December 7, 2025; accepted: January 1, 2026; published: January 12, 2026

Abstract

This article focuses on the construction of quantum Maximum Distance Separable (MDS) codes in the field of quantum error correction. MDS codes are a class of optimal codes that reach the quantum Singleton boundary and have important application value in quantum computing and communication. In order to overcome the limitations of existing construction methods in terms of code length and parameter flexibility, this paper proposes an innovative construction method: using two known Hermitian self-orthogonal Extended Generalized Reed Solomon (EGRS) codes, a new

文章引用: 吴莲铭. 由 EGRS 码构造的量子 MDS 码[J]. 应用数学进展, 2026, 15(1): 133-141.
DOI: 10.12677/aam.2026.151014

Hermitian self-orthogonal EGRS code is constructed through specific condition combinations. By utilizing this key conclusion, we have obtained several new classes of *q*-ary quantum MDS codes. The code length of the quantum MDS code we constructed is significantly different from previous codes, and the parameters are flexible. This study not only provides new ideas and tools for the construction theory of quantum MDS codes, but also offers more possibilities for the design of error correction codes in practical quantum information systems.

Keywords

Quantum MDS Codes, EGRS Code, Hermitian Self-Orthogonal

1. 引言

近几十年来，量子信息与计算已迅速发展为前沿科学技术的核心领域之一，其理论框架与技术路径对未来信息处理范式具有革命性潜在影响。在这一背景下，量子纠错码(QECCs)作为保障量子信息传输的核心技术，一直受到学术界的高度关注与深入研究。由于量子系统极易受到环境干扰而产生退相干现象，量子态的脆弱性成为实现大规模量子信息处理的主要障碍之一。量子纠错码通过编码逻辑量子信息到多个物理量子比特上，并利用特定的测量与复原机制，能够检测并纠正一定范围内的错误，从而有效对抗退相干与操作误差，为量子计算机和量子通信系统的实用化奠定基础。因此，构建具有优良纠错性能、较高编码效率及可实现的量子纠错码，一直是量子信息科学中的一个关键课题。

令 q 为素数幂，一个长度为 n 的 q 元 QECC 码是希尔伯特空间 $(Cq)\otimes n$ 的一个 q^k 维子空间，记为 $[\![n,k,d]\!]_q$，它能够将 k 个逻辑量子位编码到 n 个物理量子位中，并纠正所有不超过 $\left\lfloor \frac{d-1}{2} \right\rfloor$ 的错误。众所周知，QECC 码的参数受限于量子 Singleton 界：$2d \le n-k+2$。当等式成立时，我们称这个码为量子最大距离可分(MDS)码。在所有量子码中，量子最大距离可分(MDS)码由于达到量子 Singleton 界而在纠错能力与编码效率之间实现了最优平衡，成为研究者重点关注的码类。构造量子 MDS 码在文献中已被广泛研究。所有长度 $n \le q+1$ 的 q 元量子 MDS 码已在文献[1] [2]中被构造出来。文献[3]-[5]中使用了负循环码、常循环码和伪循环码来构造长度为 n 满足 $q+1<n\le q^2+1$ 且具有较大最小距离的量子 MDS 码。广义 Reed-Solomon (GRS)码因其优良的代数结构与灵活的码长选择，成为构造量子 MDS 码的主力。Li[6]等人首次提出了通过 GRS 码构造量子 MDS 码的统一框架。Jin 和 Xing [7] [8]推广和发展了文献[6]中的方法，并构造了多类具有灵活参数的量子 MDS 码。Fang 和 Fu [4]利用经典的 Hermitian 自正交 GRS 码和扩展 GRS (EGRS)码提出了两类新的量子 MDS 码。此后，GRS 和 EGRS 码近年来被广泛用于构造最小距离大于 $\frac{q}{2}+1$ 的量子 MDS 码(见[9]-[11])。

量子 MDS 码在量子计算与通信系统中具有重要的理论与应用价值。然而，现有构造方法在码长范围与参数灵活性方面仍存在一定局限，制约了量子 MDS 码在实际量子信息系统中的进一步应用。本文正是在此背景下，聚焦于量子 MDS 码的构造问题，旨在通过新的代数编码方法，进一步拓展其参数范围。据此，本文提出一种基于两个已知的 Hermitian 自正交 EGRS 码，通过特定条件组合构造新的 Hermitian 自正交 EGRS 码的创新方法。基于这一核心结论，我们成功构造出若干类新的 q 元量子 MDS 码。

本文其余部分的结构安排如下。在第 2 节中，我们将回顾线性码的基本概念及相关结论，为后续讨论奠定理论基础。第 3 节聚焦于 Hermitian 自正交 EGRS 码，总结已有重要结果，并给出本文构造 Hermitian 自正交 EGRS 码的关键引理。在第 4 节中，我们基于前述理论提出的一种构造量子 MDS 码的通用方法，推导出若干类具有新参数的量子 MDS 码。最后，在第 5 节中对本文的研究内容进行总结。

2. 预备知识

设 $\mathbb{F}_{q^2}$ 为包含 q^2 个元素的有限域，q 是奇素数幂，n 是一个正整数，$\mathbb{F}_{q^2}^n$ 是 $\mathbb{F}_{q^2}$ 向量空间中的 n 元组。一个长度为 n 的线性码 C 是 $\mathbb{F}_{q^2}^n$ 的一个 $\mathbb{F}_{q^2}$ 子空间。如果其维数为 k，最小 Hamming 距离为 d，则称 $\mathbb{F}_{q^2}$ 上的一个长度为 n 的线性码 C 参数为 $[n,k,d]$。

设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n), \boldsymbol{y}=(y_1,y_2,\cdots,y_n)\in\mathbb{F}_{q^2}^n$，向量 $\boldsymbol{x},\boldsymbol{y}$ 的欧几里得内积和 Hermitian 内积分别定义为 $\langle \boldsymbol{x},\boldsymbol{y}\rangle_E=\sum_{i=1}^{n}x_iy_i$ 和 $\langle \boldsymbol{x},\boldsymbol{y}\rangle_H=\sum_{i=1}^{n}x_iy_i^q$。据此，线性码 C 的欧几里得对偶码和 Hermitian 对偶码分别定义为：

$$C^{\perp E}=\left\{\boldsymbol{x}\mid \boldsymbol{x}\in\mathbb{F}_{q^2}^n, \langle \boldsymbol{x},\boldsymbol{y}\rangle_E=0, \text{对所有 } \boldsymbol{y}\in C\right\},$$

和

$$C^{\perp H}=\left\{\boldsymbol{x}\mid \boldsymbol{x}\in\mathbb{F}_{q^2}^n, \langle \boldsymbol{x},\boldsymbol{y}\rangle_H=0, \text{对所有 } \boldsymbol{y}\in C\right\}.$$

换句话说，$C^{\perp H}$ ($C^{\perp E}$)是关于 Hermitian(欧几里得)内积与码 C 正交的子空间。如果 $C\subseteq C^{\perp H}$，则称码 C 为 Hermitian 自正交码。特别地，如果 $C^{\perp H}=C$，称码 C 是 Hermitian 自对偶码。取向量 $v=(v_1,\cdots,v_n)\in\mathbb{F}_{q^2}^n$，令 $v^q=\left(v_1^q,\cdots,v_n^q\right)$。容易看出，对于一个 q^2 元线性码 C，我们有 $C^{\perp H}=\left(C^q\right)^{\perp E}$。因此，$C$ 是 Hermitian 自对偶码当且仅当 $C=\left(C^q\right)^{\perp E}$，即 $C^q=C^{\perp H}$，其中 $C^q=\left\{c^q\mid c\in C\right\}$。

接下来，设 $A=\{a_1,a_2,\cdots,a_n\}$ 是 $\mathbb{F}_{q^2}$ 的一个大小为 n 的子集。固定 $\mathbb{F}_{q^2}^*$ 中的 n 个非零元素 $v_{a_1},v_{a_2},\cdots,v_{a_n}$，其中 $\mathbb{F}_{q^2}^*=\mathbb{F}_{q^2}\setminus\{0\}$。对于 $1\le k\le n$，与 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$ 和 $\boldsymbol{v}_A=\left(v_{a_1},v_{a_2},\cdots,v_{a_n}\right)$ 关联的长度为 n 的 k 维广义 Reed-Solomon(GRS)码定义为：

$$GRS_k(\boldsymbol{a},\boldsymbol{v}_A)=\left\{\left(v_{a_1}f(a_1),v_{a_2}f(a_2),\cdots,v_{a_n}f(a_n)\right): f(x)\in\mathbb{F}_{q^2}[x], deg\left(f(x)\le k-1\right)\right\}.$$

其中 $a_1,a_2,\cdots,a_n$ 被称为 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A)$ 的码定位器，$v_{a_1},v_{a_2},\cdots,v_{a_n}$ 被称为列乘子。众所周知，$GRS_k(\boldsymbol{a},\boldsymbol{v}_A)$ 是参数为 $[n,k,n-k+1]$ 的 MDS 码，且其对偶码也是一个 MDS 码，其参数为 $[n,n-k,k+1]$。此外，可知 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A)$ 的生成矩阵为：

$$G_k(\boldsymbol{a},\boldsymbol{v}_A)=\begin{pmatrix} v_{a_1} & v_{a_2} & \cdots & v_{a_n} \\ v_{a_1}a_1 & v_{a_2}a_2 & \cdots & v_{a_n}a_n \\ \vdots & \vdots & \ddots & \vdots \\ v_{a_1}a_1^{k-2} & v_{a_2}a_2^{k-2} & \cdots & v_{a_n}a_n^{k-2} \\ v_{a_1}a_1^{k-1} & v_{a_2}a_2^{k-1} & \cdots & v_{a_n}a_n^{k-1} \end{pmatrix}.$$

进一步，我们考虑扩展 GRS (EGRS)码 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)$，定义如下：

$$GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)=\left\{\left(v_{a_1}f(a_1),v_{a_2}f(a_2),\cdots,v_{a_n}f(a_n),f_{k-1}\right): f(x)\in\mathbb{F}_{q^2}[x], deg\left(f(x)\le k-1\right)\right\}.$$

其中 f_{k-1} 表示 $f(x)$ 中 x^{k-1} 的系数。显然知 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 是 $\mathbb{F}_{q^2}$ 上的一个 $[n+1,k,n-k+2]$ MDS 码，其对偶码也是一个 MDS 码。其中，可知 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 的生成矩阵为：

$$G_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)=\begin{pmatrix} v_{a_1} & v_{a_2} & \cdots & v_{a_n} & 0 \\ v_{a_1}a_1 & v_{a_2}a_2 & \cdots & v_n a_n & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_{a_1}a_1^{k-2} & v_{a_2}a_2^{k-2} & \cdots & v_{a_n}a_n^{k-2} & 0 \\ v_{a_1}a_1^{k-1} & v_{a_2}a_2^{k-1} & \cdots & v_{a_n}a_n^{k-1} & 1 \end{pmatrix}=\begin{pmatrix} \boldsymbol{g}_0 \\ \boldsymbol{g}_1 \\ \vdots \\ \boldsymbol{g}_{k-2} \\ \boldsymbol{g}_{k-1} \end{pmatrix},$$

其中 $\boldsymbol{g}_i=\left(v_{a_1}a_1^i,v_{a_2}a_2^i,\cdots,v_{a_n}a_n^i,A_i\right)$，且 $A_i=\begin{cases}0, & \text{if } 0\le i<k-1\\ 1, & \text{if } i=k-1\end{cases}$。

3. Hermitian 自正交 EGRS 码

命题 1. 设 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$ 和 $\boldsymbol{v}_A=\left(v_{a_1},v_{a_2},\cdots,v_{a_n}\right)$，则 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 是一个 Hermitian 自正交码当且仅当

$$\left\langle \boldsymbol{a}^{qj+i},\boldsymbol{v}_A^{q+1}\right\rangle_E=\begin{cases}0, & \text{if } i+j\ne 2k-2,\\ -1, & \text{if } i+j=2k-2.\end{cases}$$

对所有 $0\le i,j\le k-1$ 成立。

证明： 注意到 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)\subseteq GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)^{\perp H}$ 当且仅当 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)^q\subseteq GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)^{\perp E}$。显然，$GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 有一个基 $\{\boldsymbol{g}_0,\boldsymbol{g}_1,\cdots,\boldsymbol{g}_{k-2},\boldsymbol{g}_{k-1}\}$，则 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)^q$ 也有一个基 $\left\{\boldsymbol{g}_0^q,\boldsymbol{g}_1^q,\cdots,\boldsymbol{g}_{k-2}^q,\boldsymbol{g}_{k-1}^q\right\}$。所以 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)^q\subseteq GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)^{\perp E}$ 当且仅当 $\left\langle \boldsymbol{g}_i,\boldsymbol{g}_j^q\right\rangle_E=0$ 对所有 $0\le i,j\le k-1$ 成立，于是得到 $\sum_{k=1}^{n}v_{a_k}^{q+1}a_k^{qj+i}+A_iA_j=\left\langle \boldsymbol{a}^{qj+i},\boldsymbol{v}_{\boldsymbol{a}}^{q+1}\right\rangle_E+A_iA_j=0$。

引理 2. 从命题 1 容易看出，如果 $GRS_k(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 是一个 Hermitian 自正交码，那么对任意 $k'\le k$，$GRS_{k'}(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 也是一个 Hermitian 自正交码。

现在，我们给出本文的关键结果，它确保我们可以从两个给定的 Hermitian 自正交 EGRS 码中获得新的 Hermitian 自正交 EGRS 码。

定理 3. 假设 $A,B\subseteq\mathbb{F}_{q^2},\boldsymbol{a}\in\mathbb{F}_{q^2}^{|A|}$，以及 $\boldsymbol{b}\in\mathbb{F}_{q^2}^{|B|}$。令 $GRS_{k_1}(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 和 $GRS_{k_2}(\boldsymbol{b},\boldsymbol{w}_B,\infty)$ 是两个 Hermitian 自正交码，其中 $\boldsymbol{v}_A=(v_a)_{a\in A}\in\left(\mathbb{F}_{q^2}^*\right)^{|A|}$，同时 $\boldsymbol{w}_B=(w_b)_{b\in B}\in\left(\mathbb{F}_{q^2}^*\right)^{|B|}$。如果

$$\left|\left\{\frac{v_d^{q+1}}{w_d^{q+1}}:d\in A\cap B\right\}\right|<q-1, \tag{1}$$

那么对于 $\boldsymbol{c}\in\mathbb{F}_{q^2}^{|A\cup B|}$，存在 $\boldsymbol{r}_{A\cup B}\in\left(\mathbb{F}_{q^2}^*\right)^{|A\cup B|}$，使得 $GRS_k(\boldsymbol{c},\boldsymbol{r}_{A\cup B},\infty)$ 也是一个 Hermitian 自正交码，其中 $k=\min\{k_1,k_2\}$。

证明： 由命题 1 和 $k=\min\{k_1,k_2\}$，显然可以得到对任意 $0\le i,j\le k-1$，有

$$\left\langle \boldsymbol{a}^{qj+i},\boldsymbol{v}_A^{q+1}\right\rangle_E+A_iA_j=0,$$

和

$$\left\langle \boldsymbol{b}^{qj+i},\boldsymbol{w}_B^{q+1}\right\rangle_E+A_iA_j=0.$$

其中 $A_i=\begin{cases}0, & \text{若 } 0\le i<k-1\\ 1, & \text{若 } i=k-1\end{cases}$。

对于任意 $x^{q+1}\in\mathbb{F}_q^*$，有 $x\in\mathbb{F}_{q^2}^*$。由(1)，我们可以选择

$$\lambda\in\mathbb{F}_q^*\setminus\left\{\frac{v_a^{q+1}}{w_a^{q+1}}:a\in A\cap B\right\}.$$

记 $d\in A\cap B$，则有 $\boldsymbol{v}_{A\cap B}=\left(v_d\right)_{d\in A\cap B}$ 和 $\boldsymbol{w}_{A\cap B}=\left(w_d\right)_{d\in A\cap B}$，因此

$$\left(1+\lambda\right)\boldsymbol{v}_{A\cap B}^{q+1}-\lambda\boldsymbol{w}_{A\cap B}^{q+1}\in\left(\mathbb{F}_q^*\right)^{|A\cap B|}.$$

注意到 $A\cup B=\left(A\setminus B\right)\cup\left(A\cap B\right)\cup\left(B\setminus A\right)$。设 $\boldsymbol{r}_{A\cup B}\in\left(\mathbb{F}_{q^2}^*\right)^{|A\cup B|}$ 使得

$$\boldsymbol{r}_{A\cup B}^{q+1}=\left(\left(1+\lambda\right)\boldsymbol{v}_{A\setminus B}^{q+1},\left(1+\lambda\right)\boldsymbol{v}_{A\cap B}^{q+1}-\lambda\boldsymbol{w}_{A\cap B}^{q+1},-\lambda\boldsymbol{w}_{B\setminus A}^{q+1}\right)\in\left(\mathbb{F}_q^*\right)^{|A\cup B|}.$$

因此对于 $\boldsymbol{c}\in\mathbb{F}_{q^2}^{|A\cup B|}$，我们有

$$\begin{aligned}
&\left\langle\boldsymbol{c}^{qj+i},\boldsymbol{r}_{A\cup B}^{q+1}\right\rangle_E\\
&=\left\langle\boldsymbol{a}^{qj+i},\left(1+\lambda\right)\boldsymbol{v}_{A\setminus B}^{q+1}\right\rangle_E+\left\langle\boldsymbol{d}^{qj+i},\left(1+\lambda\right)\boldsymbol{v}_{A\cap B}^{q+1}-\lambda\boldsymbol{w}_{A\cap B}^{q+1}\right\rangle_E+\left\langle\boldsymbol{b}^{qj+i},-\lambda\boldsymbol{w}_{B\setminus A}^{q+1}\right\rangle_E\\
&=\left(1+\lambda\right)\left\langle\boldsymbol{a}^{qj+i},\boldsymbol{v}_{A\setminus B}^{q+1}\right\rangle_E+\left(1+\lambda\right)\left\langle\boldsymbol{d}^{qj+i},\boldsymbol{v}_{A\cap B}^{q+1}\right\rangle_E-\lambda\left\langle\boldsymbol{d}^{qj+i},\boldsymbol{w}_{A\cap B}^{q+1}\right\rangle_E-\lambda\left\langle\boldsymbol{b}^{qj+i},\boldsymbol{w}_{B\setminus A}^{q+1}\right\rangle_E\\
&=\left(1+\lambda\right)\left\langle\boldsymbol{a}^{qj+i},\boldsymbol{v}_A^{q+1}\right\rangle_E-\lambda\left\langle\boldsymbol{b}^{qj+i},\boldsymbol{w}_B^{q+1}\right\rangle_E.
\end{aligned}$$

如果 $i+j=2k-2$，我们有 $\left\langle\boldsymbol{a}^{qj+i},\boldsymbol{v}_A^{q+1}\right\rangle_E=-1$，和 $\left\langle\boldsymbol{b}^{qj+i},\boldsymbol{w}_B^{q+1}\right\rangle_E=-1$。那么显然有 $\left\langle\boldsymbol{c}^{qj+i},\boldsymbol{r}_{A\cup B}^{q+1}\right\rangle_E=-1$。
如果 $i+j\neq 2k-2$，我们有 $\left\langle\boldsymbol{a}^{qj+i},\boldsymbol{v}_{\boldsymbol{a}}^{q+1}\right\rangle_E=0$，和 $\left\langle\boldsymbol{b}^{qj+i},\boldsymbol{w}_{\boldsymbol{b}}^{q+1}\right\rangle_E=0$。那么显然有 $\left\langle\boldsymbol{c}^{qj+i},\boldsymbol{r}_{A\cup B}^{q+1}\right\rangle_E=0$。
由命题 1，证得 $GRS_k\left(\boldsymbol{c},\boldsymbol{r}_{A\cup B},\infty\right)$ 是一个 Hermitian 自正交码。

定理 3 的关键点在于条件(1)。注意到

$$\left|\left\{\frac{v_d^{q+1}}{w_d^{q+1}}:d\in A\cap B\right\}\right|\le\left|A\cap B\right|,$$

和

$$\left|\left\{\frac{v_d^{q+1}}{w_d^{q+1}}:d\in A\cap B\right\}\right|\le\left|v_d^{q+1}:d\in A\cap B\right|\cdot\left|w_d^{q+1}:d\in A\cap B\right|,$$

则我们可以直接得到以下推论。

推论 4. 假设 $A,B\subseteq\mathbb{F}_{q^2},\boldsymbol{a}\in\mathbb{F}_{q^2}^{|A|}$ 和 $\boldsymbol{b}\in\mathbb{F}_{q^2}^{|B|}$。令 $GRS_{k_1}\left(\boldsymbol{a},\boldsymbol{v}_A,\infty\right)$ 和 $GRS_{k_2}\left(\boldsymbol{b},\boldsymbol{w}_B,\infty\right)$ 是两个 Hermitian 自正交码，其中 $\boldsymbol{v}_A=\left(v_a\right)_{a\in A}\in\left(\mathbb{F}_{q^2}^*\right)^{|A|}$ 和 $\boldsymbol{w}_B=\left(w_b\right)_{b\in B}\in\left(\mathbb{F}_{q^2}^*\right)^{|B|}$。如果下列任一条件成立：

(1) $\left|A\cap B\right|<q-1$，

(2) $\left|v_d^{q+1}:d\in A\cap B\right|\cdot\left|w_d^{q+1}:d\in A\cap B\right|<q-1$。

那么对于 $\boldsymbol{c}\in\mathbb{F}_{q^2}^{|A\cup B|}$，存在 $\boldsymbol{r}_{A\cup B}\in\left(\mathbb{F}_{q^2}^*\right)^{|A\cup B|}$，使得 $GRS_k\left(\boldsymbol{c},\boldsymbol{r}_{A\cup B},\infty\right)$ 也是一个 Hermitian 自正交码，其中 $k=\min\left\{k_1,k_2\right\}$。

注 5. 定理 3.1 成功构造新线性码的关键在于(1)，其核心思想源于有限域 $\mathbb{F}_q$ 的乘法群结构。

1. 条件的来源与意义：由于 $v^{q+1},w^{q+1}\in\mathbb{F}_q^*$，其比值也属于 $\mathbb{F}_q^*$。$\mathbb{F}_q^*$ 是一个 $q-1$ 阶循环群。条件要求这些比值所构成的集合的个数小于 $q-1$。这意味着在 $\mathbb{F}_q^*$ 中，存在至少一个元素不在这个比值集合里。这正是我们能够选取合适的 λ 的充分必要条件，该条件在实践中是比较容易满足的。例如，推论 4 给出了两

个更宽松的充分条件：(1) 当交集$|A\cap B|$本身小于$q-1$时，比值集合的大小就不可能超过$q-1$，条件自然满足。(2) 只要v^{q+1}或w^{q+1}的取值有限，其比值集合的大小也会被限制。这为构造提供了很大的灵活性。

2. λ的选取：λ的作用是将两个已知码的列乘子v^{q+1}和w^{q+1}融合成一个适用于并集$A\cup B$的新列乘子r^{q+1}。其存在性由上述条件直接保证：既然比值集合未能占满整个$\mathbb{F}_q^*$，我们总可以从中选取一个元素作为λ。选取方式是非构造性的，即存在这样一个λ，在实际操作中只需遍历$\mathbb{F}_q^*$中有限的$q-1$个元素即可找到。公式$(1+\lambda)\boldsymbol{v}_{A\cap B}^{q+1}-\lambda\boldsymbol{w}_{A\cap B}^{q+1}\in\left(\mathbb{F}_q^*\right)^{|A\cap B|}$的设计确保了在交集部分，新列乘子的构造满足线性组合关系，最终得出新线性码的自正交性。

4. 量子 MDS 码的构造

从现在开始直到本文结束，我们始终假设ω是$\mathbb{F}_{q^2}$的一个本原元，即$\mathbb{F}_{q^2}^*=\langle\omega\rangle$。此外，我们总是将$\mathbb{F}_q$中的元素记为$\mathbb{F}_q=\{\alpha_1,\alpha_2,\cdots,\alpha_q\}$。假设$1\le s,t\le q$。

(1) 固定$\beta\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$。对于$1\le i\le s$，记

$$A_i=\alpha_i\beta+\mathbb{F}_q:=\{\alpha_i\beta+x:x\in\mathbb{F}_q\}. \tag{2}$$

(2) 令$\beta_m=\omega^m,1\le m\le q$，则$\beta_m\in\{\omega,\omega^2,\cdots,\omega^q\}$。对于$1\le j\le t$，记

$$B_{j,m}=\alpha_j+\mathbb{F}_q\beta_m:=\{\alpha_j+\beta_m x:x\in\mathbb{F}_q\}. \tag{3}$$

那么容易验证，对于任意$1\le i_1\ne i_2\le s$和$1\le j_1\ne j_2\le t$，有$|A_i|=|B_{j,m}|=q$，$A_{i_1}\cap A_{i_2}=\varnothing$和$B_{j_1,m}\cap B_{j_2,m}=\varnothing$。

引理 6. 保持上述记号。对于任意$1\le i\le s$和$1\le j\le t$，我们有

$$|A_i\cap B_{j,m}|=1.$$

证明：假设$z\in A_i\cap B_{j,m}$。则存在$x,y\in\mathbb{F}_q$，使得$z=\alpha_j+\beta_m y=\alpha_i\beta+x$。因此

$$\alpha_i\beta-\beta_m y=\alpha_j-x. \tag{4}$$

显然$\alpha_j-x\in\mathbb{F}_q$，我们也有$\alpha_i\beta-\beta_m y\in\mathbb{F}_q$。因此，我们得到$(\alpha_i\beta-\beta_m y)^q=\alpha_i\beta-\beta_m y$，

$$y=\frac{\alpha_i(\beta-\beta^q)}{\beta_m-\beta_m^q}.$$

注意到$\beta-\beta^q=\left(\omega^{\frac{q+1}{2}}\right)^{k_1}$和$\beta_m-\beta_m^q=\left(\omega^{\frac{q+1}{2}}\right)^{k_2}$，其中$k_1,k_2$均为奇数。所以，我们有唯一的$y=\alpha_i\left(\omega^{q+1}\right)^{\frac{k_1-k_2}{2}}$，$x=\alpha_j-\alpha_i\left(\beta-\beta_m\left(\omega^{q+1}\right)^{\frac{k_1-k_2}{2}}\right)$，使得(4)成立。

引理 7. [5] (1) 设$n=2k_1-1,n\le q$，$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)\in A_i^n$，其中$a_1,a_2,\cdots,a_n$是互不相同的元素。则存在向量$\boldsymbol{v}_A=(v_{a_1},v_{a_2},\cdots,v_{a_n})\in\left(\mathbb{F}_{q^2}^*\right)^n$使得$GRS_{k_1}(\boldsymbol{a},\boldsymbol{v}_A,\infty)$是$\mathbb{F}_{q^2}$上参数为$\left[n+1,\frac{n+1}{2},\frac{n+1}{2}+1\right]$的一个 Hermitian 自对偶 EGRS 码。

(2) 设$m=2k_2-1$，$m\le q$，$\boldsymbol{b}=(b_1,b_2,\cdots,b_n)\in B_{j,m}^m$，其中$b_1,b_2,\cdots,b_n$是互不相同的元素。则存在向量$\boldsymbol{w}_B=(w_{b_1},w_{b_2},\cdots,w_{b_n})\in\left(\mathbb{F}_{q^2}^*\right)^m$使得$GRS_{k_2}(\boldsymbol{b},\boldsymbol{w}_B,\infty)$是$\mathbb{F}_{q^2}$上参数为$\left[m+1,\frac{m+1}{2},\frac{m+1}{2}+1\right]$的一个 Hermitian 自对偶 EGRS 码。

在[13]中，Ashikhmin 和 Knill 提供了一种从 $\mathbb{F}_{q^2}$ 上的经典 Hermitian 自正交 MDS 码构造 q 元量子 MDS 码的方法，如下所示。

引理 8. [12] (量子 MDS 码的 Hermitian 构造)如果存在一个 $[n,k,n-k+1]_{q^2}$ Hermitian 自正交 MDS 码 C，即 $C\subseteq C^{\perp H}$，那么存在一个 $[\![n,n-2k,k+1]\!]_q$ 量子 MDS 码。

引理 9. [13]假设存在一个量子 MDS 码 $[\![n,n+2-2d,d]\!]_q$。那么对所有 $0\le s<d$，也存在量子 MDS 码 $[\![n-s,n+s+2-2d,d-s]\!]_q$。

现在，我们提出我们关于量子 MDS 码的构造。

定理 10. 假设 $n=2q-1$。令 A_i 和 $B_{j,m}$ 分别由方程(2)和(3)定义。如果有

$$\left|\left\{\frac{v_d^{q+1}}{w_d^{q+1}}: d\in A_i\cap B_{j,m}\right\}\right|<q-1,$$

那么对于 $k=\dfrac{q+1}{2}$，存在一个 $[\![n+1,n-2k+1,k+1]\!]_q$ 量子 MDS 码。

证明：由引理 6 得，

$$\left|A_i\cup B_{j,m}\right|=\left|A_i\right|+\left|B_{j,m}\right|-\left|A_i\cap B_{j,m}\right|=2q-1=n.$$

由引理 7 知，$GRS_{k_1}(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 和 $GRS_{k_2}(\boldsymbol{b},\boldsymbol{w}_B,\infty)$ 都是 Hermitian 自对偶 MDS 码，其中 $\boldsymbol{v}_A^{q+1}=\left(v_{a_i}^{q+1}\right)$ 和 $\boldsymbol{w}_B^{q+1}=\left(w_{b_j}^{q+1}\right)$，且 $1\le i\le n, 1\le j\le m$。因此有

$$\left|\left\{\frac{v_d^{q+1}}{w_d^{q+1}}: d\in A_i\cap B_{j,m}\right\}\right|<q-1,$$

由定理 3，对于任意 $k=\dfrac{q+1}{2}$ 和 $\boldsymbol{c}\in\mathbb{F}_{q^2}^{\left|A_i\cup B_{j,m}\right|}$，存在 $\boldsymbol{r}_{A_i\cup B_{j,m}}\in\left(\mathbb{F}_{q^2}^*\right)^{\left|A_i\cup B_{j,m}\right|}$，使得 $GRS_k\left(\boldsymbol{c},\boldsymbol{r}_{A_i\cup B_{j,m}},\infty\right)$ 是一个长度为 $n+1$ 的 Hermitian 自正交码。随后，结论可由引理 8 直接推出。

推论 11. 假设 $n=2q-1$。令 A_i 和 $B_{j,m}$ 分别由方程(2)和(3)定义。如果

$$\left|\left\{\frac{v_d^{q+1}}{w_d^{q+1}}: d\in A_i\cap B_{j,m}\right\}\right|<q-1,$$

那么对于 $k=\dfrac{q+1}{2}$ 和 $0\le s<\dfrac{q+1}{2}+1$，存在一个 $[\![n-s+1,n+s-2k+1,k-s+1]\!]_q$ 量子 MDS 码。

证明：结论由定理 10 与引理 9 直接得到。

为使定理 10 的构造过程具体化，我们选取一个较小的参数，逐步演示如何构造一个新的量子 MDS 码。

例 12. 取 $q=5$，设 ω 为 $\mathbb{F}_{q^2}$ 的一个本原元。首先选取 $\mathbb{F}_5$ 的元素，记 $\mathbb{F}_5=\{0,1,2,3,4\}=\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5\}$。简便起见，取 $\alpha_1=1$。固定 $\beta=\omega\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$，同时取 $m=1$，得到 $\beta_m=\omega^1=\omega$，由方程(2)和(3)，可构造两个集合(取 $i=j=1$)：

$$A_1=\alpha_1\beta+\mathbb{F}_q=\{\omega,\omega+1,\omega+2,\omega+3,\omega+4\},$$

$$B_{1,1}=\alpha_1+\mathbb{F}_q\beta_1:=\{1,1+\omega,1+2\omega,1+3\omega,1+4\omega\}.$$

显然，$\left|A_1\right|=\left|B_{1,1}\right|=5$，且由引理 6，知 $\left|A_1\cap B_{1,1}\right|=1$，且通过解方程可得唯一交为 $d=\omega+1$。

根据引理 7，对于集合 A_1，存在向量 $\boldsymbol{a}=(a_1,a_2,a_3,a_4,a_5)\in A_1^5$ 和 $\boldsymbol{v}_A=\left(v_{a_1},v_{a_2},v_{a_3},v_{a_4},v_{a_5}\right)\in\left(\mathbb{F}_{25}^*\right)^5$，使得 $GRS_{k_1}(\boldsymbol{a},\boldsymbol{v}_A,\infty)$ 是一个 $[6,3,4]_{25}$ Hermitian 自对偶码，其中 $k_1=3$。同理，对于集合 $B_{1,1}$，存在向量

$\boldsymbol{b}=(b_1,b_2,b_3,b_4,b_5)\in B_{1,1}^5$ 和 $\boldsymbol{w}_B=\left(w_{b_1},w_{b_2},w_{b_3},w_{b_4},w_{b_5}\right)\in\left(\mathbb{F}_{25}^*\right)^5$，使得 $\mathrm{GRS}_{k_2}(\boldsymbol{b},\boldsymbol{w}_B,\infty)$ 是一个 $[6,3,4]_{25}$ Hermitian 自对偶码，其中 $k_2=3$。

现在，考虑交集 $A_1\cap B_{1,1}=\{d\}$，我们需要检查定理 3 的条件：

$$\left|\left\{\frac{v_d^{q+1}}{w_d^{q+1}}:d\in A_1\cap B_{1,1}\right\}\right|<q-1.$$

因为交集只有一个元素 d，所以上述集合的大小至多为 1。而 $q-1=4$，故条件 $1<4$ 成立。因此，满足定理 3 的运用条件。

令 $k=\min\{k_1,k_2\}=3$，集合 $C=A_1\cup B_{1,1}$，其大小为 $|C|=|A_1|+|B_{1,1}|-|A_1\cap B_{1,1}|=5+5-1=9=n$。在 $\mathbb{F}_5^*=\{1,2,3,4\}$ 中选取一个 λ，使得 $\lambda\neq\frac{v_d^{q+1}}{w_d^{q+1}}$（由于比值集合只有一个元素，而 $\mathbb{F}_5^*$ 有 4 个元素，这样的 λ 必然存在，例如可取 $\lambda=1$，只要确保它不等于具体比值即可）。根据定理 3 的证明，我们可以构造向量 $\boldsymbol{r}_C\in\left(\mathbb{F}_{25}^*\right)^9$，使 $GRS_k(\boldsymbol{c},\boldsymbol{r}_C,\infty)$ 为 $[10,3,8]_{25}$ Hermitian 自正交 MDS 码。

应用引理 8，由上述 $[10,3,8]_{25}$ Hermitian 自正交 MDS 码 C，我们可以得到一个量子 MDS 码，其参数为：$[\![n,n-2k,k+1]\!]_5=[\![10,4,4]\!]_5$。验证量子 Singleton 界：$2d=8=n-k+2=10-4+2=8$，等号成立，因此该码是量子 MDS 码。

通过上述步骤，我们成功地从两个已知的 Hermitian 自对偶 EGRS 码出发，构造出了一个参数为 $[\![10,4,4]\!]_5$ 的新量子 MDS 码。此示例清晰地展示了定理 10 从集合构造、条件验证到最终码生成的完整流程，验证了所述方法的可行性与具体操作过程。

5. 总结

本文中，我们提出了一种新方法，利用两个已知的 Hermitian 自正交 EGRS 码来构造一个新的 Hermitian 自正交 EGRS 码。通过将两个满足特定条件的 Hermitian 自正交 EGRS 码进行组合，证明了在所给条件下，所构造的码仍保持 Hermitian 自正交性。基于这一关键结论，我们进一步构建了若干类新的量子 MDS 码。与已有结果相比，本文所构造的量子 MDS 码不仅码长具有显著差异性，参数选择也更为灵活。此外，本文构造的所有 q 元量子 MDS 码的最小距离均可大于 $\frac{q}{2}+1$，从而在纠错能力上实现了进一步提升。本研究为量子 MDS 码的构造提供了新的思路，扩展了可用参数的覆盖范围。

参考文献

[1] Grassl, M., Rötteler, M. and Beth, T. (2003) Efficient Quantum Circuits for Non-Qubit Quantum Error-Correcting Codes. *International Journal of Foundations of Computer Science*, **14**, 757-775. https://doi.org/10.1142/s0129054103002011

[2] Jin, L.F. and Xing, C.P. (2014) A Construction of New Quantum MDS Codes. *IEEE Transactions on Information Theory*, **60**, 2921-2925. https://doi.org/10.1109/tit.2014.2299800

[3] Chen, B., Ling, S. and Zhang, G. (2015) Application of Constacyclic Codes to Quantum MDS Codes. *IEEE Transactions on Information Theory*, **61**, 1474-1484. https://doi.org/10.1109/tit.2015.2388576

[4] Fang, W. and Fu, F. (2018) Two New Classes of Quantum MDS Codes. *Finite Fields and Their Applications*, **53**, 85-98. https://doi.org/10.1016/j.ffa.2018.06.003

[5] Guo, G. and Li, R. (2020) Hermitian Self-Dual GRS and Extended GRS Codes. *IEEE Communications Letters*, **25**, 1062-1065. https://doi.org/10.1109/lcomm.2020.3044893

[6] Rotteler, M., Grassl, M. and Beth, T. (2004) On Quantum MDS Codes. 2004 *International Symposium on Information Theory*, Chicago, 27 June-2 July 2004, 356. https://doi.org/10.1109/isit.2004.1365393

[7] Kai, X. and Zhu, S. (2012) New Quantum MDS Codes from Negacyclic Codes. *IEEE Transactions on Information*

Theory, **59**, 1193-1197. https://doi.org/10.1109/tit.2012.2220519

[8] Li, Z., Xing, L.J. and Wang, X.M. (2008) Quantum Generalized Reed-Solomon Codes: Unified Framework for Quantum Maximum-Distance-Separable Codes. *Physical Review A*, **77**, Article 012308. https://doi.org/10.1103/physreva.77.012308

[9] Ball, S. (2021) Some Constructions of Quantum MDS Codes. *Designs*, *Codes and Cryptography*, **89**, 811-821. https://doi.org/10.1007/s10623-021-00846-y

[10] Fang, W. and Fu, F. (2019) Some New Constructions of Quantum MDS Codes. *IEEE Transactions on Information Theory*, **65**, 7840-7847. https://doi.org/10.1109/tit.2019.2939114

[11] Guo, G., Li, R. and Liu, Y. (2021) Application of Hermitian Self-Orthogonal GRS Codes to Some Quantum MDS Codes. *Finite Fields and Their Applications*, **76**, Article 101901. https://doi.org/10.1016/j.ffa.2021.101901

[12] Ashikhmin, A. and Knill, E. (2002) Nonbinary Quantum Stabilizer Codes. *IEEE Transactions on Information Theory*, **47**, 3065-3072. https://doi.org/10.1109/18.959288

[13] Grassl, M. and Rotteler, M. (2015) Quantum MDS Codes over Small Fields. 2015 *IEEE International Symposium on Information Theory* (*ISIT*), Hong Kong, 14-19 June 2015, 1104-1108. https://doi.org/10.1109/isit.2015.7282626