厄米特自对偶广义里德-所罗门码

Chun'e Zhao[1],Wenping Ma[2]

1 中国石油大学理学院，山东青岛 266555，中国 2 西安电子科技大学通信工程学院，
中国西安 电子邮件：zhaochune1981@163.com；wp ma@mail.xidian.edu.cn；

arXiv:2602.06377v1 [cs.IT] 6 Feb 2026

摘要

最大距离可分（MDS）自对偶码在理论和实践中都具有重要意义。广义里德-所罗门码（GRS码）是最重要的 MDS 码。相应地，已有许多研究利用 GRS 码构造欧几里得自对偶 MDS 码。然而，关于厄米特自对偶 GRS 码的研究相对有限。由于当 $n > q+1$ 时厄米特自对偶 GRS 码不存在，本文致力于研究 $n \leq q+1$ 情形下的 GRS 码。首先，我们证明，当 $n \leq q+1$ 时，厄米特自对偶 GRS 码只有两类，同时验证了 [13] 中的猜想并给出了证明。其次，我们提出两种显式构造方法。因此，厄米特自对偶 GRS 码的存在性与构造问题均已得到彻底解决。

索引术语

MDS码，广义里德-所罗门码，厄米特自对偶码

I. 引言

设 Et $\mathbb{F}_q$ 是一个大小为 q的有限域，其中 q是素数幂且 $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$。一个 $[n,k,d]$ 线性码 C是 $\mathbb{F}_q$上线性空间 $\mathbb{F}_q^n$的子空间，维数为 k，最小汉明距离为 d。众所周知， C的参数满足 $d \leq n-k+1$。若 $d = n-k+1$，则称 C为最大距离可分（MDS）码。

对于线性码 C，我们分别用 $C^{\perp_E}$ 和 $C^{\perp_H}$ 表示 C 的欧几里得对偶码和 C的厄米对偶码。若 $C = C^{\perp_E}$，则称线性码 C 为欧几里得自对偶。若 $C = C^{\perp_H}$，则称 C 为厄米自对偶。

MDS码和自对偶码在众多研究和工程领域都有广泛而重要的应用。由于具备最大的纠错能力，MDS码被广泛用于各种数据存储系统，例如分布式存储系统的编码设计 [1]。与此同时，MDS码还与组合设计、有限几何等数学分支密切相关 [2]。另一方面，自对偶码在密码学 [3] [4] 和格理论 [5] [6] 等领域具有重要价值。若一个线性码同时是 MDS 码和自对偶码，则称其为 MDS 自对偶码。

近年来，MDS 自对偶码的研究已成为代数编码理论中的热点课题。人们对欧几里得自对偶 MDS 码或厄米自对偶 MDS 码进行了大量研究。Kim 和 Lee 提出了一种关于欧几里得内积或厄米内积的自对偶码的高效构造方法，并构造了许多相应的自对偶 MDS 码 [7]。Guenda 通过扩展循环二元陪集码或负循环码，建立了欧几里得自对偶 MDS 码和厄米自对偶 MDS 码的系统构造方法 [8]。

GRS 码是最重要的 MDS 码。通过 GRS 码构造 MDS 自对偶码具有重要意义。Jin 和 Xing 首次在[9]提出了利用 GRS 码构造欧几里得自对偶 MDS 码的系统方法。此后，GRS 码成为构造 MDS 自对偶码最常用、最有效的工具之一。Yan 在 [10]中建立了 GRS 码成为欧几里得自对偶 MDS 码的充要条件。Labad 等人在 [11]中构造了更多类欧几里得自对偶 MDS 码。Fang W. 等人 [12] 利用 GRS 码和扩展GRS码构造了另外六类 q 元 MDS 欧几里得自对偶码。Fang X. 等人 [14] 构造了若干类

通过（扩展）GRS 码构造的欧几里得自对偶 MDS 码。Ning Y. 等人 [18] 着重研究了由（扩展）GRS 码构造 MDS 欧几里得自对偶码的方法，并扩展了连续范围。Fang W. 等人在 [19] 提出了一种利用灵活求值点构造欧氏自对偶GRS码的系统方法。Zhang and Feng 在 [15]提出了一种关于 MDS 欧几里得自对偶码存在性的统一方法。因此，关于欧氏自对偶GRS码的研究日益丰富。然而，关于厄米特自对偶广义里德-所罗门码的研究相对较少。2019年，Niu and Yue 等人在 [13] 给出了两类埃尔米特自对偶MDS GRS码，并证明厄米特自对偶MDS GRS码必属于上述两类（当 $n = 4$ 时），还猜想该结果对每个偶数长度 n、$4 \leq n \leq q+1$也成立。2021，Guo and Li [16] 修订并改进了 [13] 中的结果，并通过 Magma 编程猜想当 $n > q+1$ 时不存在厄米特自对偶GRS码。2025年，Wan and Zhu 在 [17]从理论上证明了这一点。除此之外，没有其他关于厄米特自对偶GRS码的相关介绍。

为阐述这一主题的内容，本文聚焦于 $n \leq q+1$ 的厄米自对偶 MDS 码和 GRS 码。具体而言，我们证明了对于 $n \leq q+1$，厄米特自对偶广义里德-所罗门码仅存在两类；这一结果不仅验证了 [13] 提出的猜想的正确性，也完成了该猜想的严格证明。此外，本文还给出了这类厄米特自对偶广义里德-所罗门码的两种具体构造。因此，关于厄米特自对偶广义里德-所罗门码的存在性与构造问题已得到彻底解决。

本文其余部分的组织结构如下。第 2 节将介绍有关 GRS 码和厄米特自对偶码的一些基础知识与辅助结果。第 3 节将给出关于厄米特自对偶广义里德-所罗门码的主要结果。第 4 节将利用 GRS 码给出两种 MDS 厄米自对偶码的具体构造。

II. Preliminaries

本节将介绍厄米自对偶码和 GRS 码的基本定义，以供后续讨论使用。

A. 厄米自对偶码

设 q为素数幂，$\mathbb{F}_{q^2}$为含有 q^2 个元素的有限域。设 $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ 和 $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$ 是 $\mathbb{F}_{q^2}^n$中的两个向量。以下定义两种内积。

$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的欧几里得内积定义如下:

$$< \boldsymbol{x}, \boldsymbol{y} >_E = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的厄米内积定义如下:

$$< \boldsymbol{x}, \boldsymbol{y} >_H = x_1y_1^q + x_2y_2^q + \cdots + x_ny_n^q.$$

设 C 是一个长度为 n 、定义在 $\mathbb{F}_{q^2}$上的线性码。 C的欧几里得对偶记为 $C^{\perp E}$，其定义为 as

$$C^{\perp E} = \{\boldsymbol{x} \in \mathbb{F}_{q^2}^n | < \boldsymbol{x}, \boldsymbol{y} >_E = 0, \text{ for all } \boldsymbol{y} \in C\}.$$

类似地， C的厄米对偶码记为 $C^{\perp H}$，其定义为

$$C^{\perp H} = \{\boldsymbol{x} \in \mathbb{F}_{q^2}^n | < \boldsymbol{x}, \boldsymbol{y} >_H = 0, \text{ for all } \boldsymbol{y} \in C\}.$$

若 $C = C^{\perp H}$，则称 C 为厄米自对偶码。

B. GRS 码

设 k, n 为正整数，且满足 $k \leq n$。定义集合

$$\mathbb{F}_{q^2}[x]_k = \{f(x) \in \mathbb{F}_{q^2}[x] | deg(f(x)) \leq k-1\}.$$

容易验证， $\mathbb{F}_{q^2}[x]_k$ 是 $\mathbb{F}_{q^2}$ 上的 $k-$ 维线性空间。设 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in(\mathbb{F}_{q^2})^n$，其中$\alpha_1$、$\alpha_2$、$\cdots$、$\alpha_n$ 是 $\mathbb{F}_{q^2}$ 中的 n 个互异元素，且 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)\in(\mathbb{F}_{q^2}^*)^n$。则与 $\boldsymbol{\alpha}$ 和 $\boldsymbol{v}$ 相关联的广义 Reed-Solomon 码 GRS_n，$_k(\boldsymbol{\alpha},\boldsymbol{v})$，定义为

$$GRS_{n,k}(\boldsymbol{\alpha},\boldsymbol{v})=\{(v_1f(\alpha_1),v_2f(\alpha_2),\cdots,v_nf(\alpha_n))|\text{ for all } f(x)\in\mathbb{F}_{q^2}[x]_k\}.$$

事实上，$GRS_{n,\ k}(\boldsymbol{\alpha},\ \boldsymbol{v})$也可以视为具有如下生成矩阵的线性码：

$$G=[I_k,0]V_n(\boldsymbol{\alpha})diag(\boldsymbol{v}),$$

其中

$$I_k=\begin{pmatrix}1&&&\\&1&&\\&&\ddots&\\&&&1\end{pmatrix},V_n(\boldsymbol{\alpha})=\begin{pmatrix}1&1&\cdots&1\\\alpha_1&\alpha_2&\cdots&\alpha_n\\\vdots&\vdots&\ddots&\vdots\\\alpha_1^{n-1}&\alpha_2^{n-1}&\cdots&\alpha_n^{n-1}\end{pmatrix},\mathrm{diag}(\boldsymbol{v})=\begin{pmatrix}v_1&&&\\&v_2&&\\&&\ddots&\\&&&v_n\end{pmatrix}.\tag{1}$$

III. 厄米特自对偶广义里德-所罗门码

本节中，我们运用矩阵理论和线性反馈移位寄存器序列理论，开始研究厄米特自对偶广义里德-所罗门码。首先介绍一些相关记号，以供后续讨论使用。

(1) 对任意向量 $\boldsymbol{\xi}\in\mathbb{F}_{q^2}^n$，$\boldsymbol{\xi}^T$ 表示 $\boldsymbol{\xi}$的转置。

(2) For any sequence $S=(s_0,s_1,s_2,\cdots)$, $L^{(i)}(S)=(s_i,s_{i+1},s_{i+2},\cdots)$, $L^{(i)}(S)_{[j]}=(s_i,s_{i+1},s_{i+2},\cdots,s_{i+j-1})$.

(3) 对任意矩阵 $A_{m\times n}$，$A[i_1,i_2,\cdots,i_t;\ j_1,\ j_2,\ \cdots,\ j_s]$ 表示由 i_1，i_2，$\cdots$，i_t 这些行以及j_1，j_2，$\cdots$，j_s 这些列从 A中构成的子矩阵，其中 $0\le i_k\le m-1$ 和 $0\le j_k\le n-1$。

$_n$**定理 1.** 设 α_1、α_2、$\cdots$、α_n 为有限域 $\mathbb{F}_{q^2}$ 中的互异元素，其中 q 为素数幂。设 $G(x)=\prod(x-\alpha_i)=_{i=1}$

$_{n-1}x^n-\sum c_ix^i$，则矩阵

$_{i=0}$

$$T=\begin{pmatrix}0&1&&&\\&0&1&&\\&&0&\ddots&\\&&&\ddots&1\\c_0&c_1&c_2&\cdots&c_{n-1}\end{pmatrix}\tag{2}$$

以 α_1、α_2、$\cdots$、α_n 为其特征值，且对应于每个 α_i 的特征向量为 $(1,\alpha_i,\alpha_i^2,\cdots,\alpha_i^{n-1})^T$，其中 i =1、2、$\cdots$、n。

证明. 矩阵 T 的特征多项式为

$$|xI_n-T|=\begin{vmatrix}x&-1&&&\\&x&-1&&\\&&\ddots&\ddots&\\&&&x&-1\\-c_0&-c_1&-c_2&\cdots&x-c_{n-1}\end{vmatrix}=x^n-c_{n-1}x^{n-1}-\cdots-c_1x-c_0=G(x),$$

其中，I_n的定义如公式 (1) 所示。因此，T的特征值为 α_1、α_2、$\cdots$、α_n。此外，$\alpha_i^n=c_{n-1}\alpha_i^{n-1}+\cdots+c_1\alpha_i+c_0$，因此

$$T\begin{pmatrix}1\\ \alpha_i\\ \alpha_i^2\\ \vdots\\ \alpha_i^{n-1}\end{pmatrix}=\begin{pmatrix}0&1&&&\\ &0&1&&\\ &&0&\ddots&\\ &&&\ddots&1\\ c_0&c_1&c_2&\cdots&c_{n-1}\end{pmatrix}\begin{pmatrix}1\\ \alpha_i\\ \alpha_i^2\\ \vdots\\ \alpha_i^{n-1}\end{pmatrix}=\begin{pmatrix}\alpha_i\\ \alpha_i^2\\ \vdots\\ \alpha_i^{n-1}\\ \alpha_i^n\end{pmatrix}=\alpha_i\begin{pmatrix}1\\ \alpha_i\\ \alpha_i^2\\ \vdots\\ \alpha_i^{n-1}\end{pmatrix}$$

对于 $i=1$、2、$\cdots$、n。 □

定理 2. 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是有限域 $\mathbb{F}_{q^2}$ 中互不相同的元素。设 $x_1,x_2,\cdots,x_n\in\mathbb{F}_{q^2}$，并定义 $\Delta_i=\sum\alpha_l^i x_{l=1}$，其中 $i=0$、1、$\cdots$。若 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 $x^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0=0$ 的根，则

$$\Delta_{m+i}+a_{m-1}\Delta_{m-1+i}+\cdots+a_1\Delta_{1+i}+a_0\Delta_i=0$$

对于任意非负整数 i。

证明。 由于 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 $x^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0=0$ 的根，因此

$$\alpha_j^m+a_{m-1}\alpha_j^{m-1}+\cdots+a_1\alpha_j+a_0=0,j=1,2,\cdots,n.$$

即 $\alpha_j^i\left(\alpha_j^m+a_{m-1}\alpha_j^{m-1}+\cdots+a_1\alpha_j+a_0\right)=\alpha_j^{m+i}+a_{m-1}\alpha_j^{m-1+i}+\cdots+a_1\alpha_j^{1+i}+a_0\alpha_j^i=0$，其中 $j=1,2,\cdots,n$，即。

$$(a_0,a_1,\cdots,a_{m-1},1)\begin{pmatrix}\alpha_1^i&\alpha_2^i&\cdots&\alpha_n^i\\ \alpha_1^{i+1}&\alpha_2^{i+1}&\cdots&\alpha_n^{i+1}\\ \vdots&\vdots&&\vdots\\ \alpha_1^{m-1+i}&\alpha_2^{m-1+i}&\cdots&\alpha_n^{m-1+i}\\ \alpha_1^{m+i}&\alpha_2^{m+i}&\cdots&\alpha_n^{m+i}\end{pmatrix}=0.$$

Then $\Delta_{m+i}+a_{m-1}\Delta_{m-1+i}+\cdots+a_1\Delta_{1+i}+a_0\Delta_i=(a_0,a_1,\cdots,a_{m-1},1)\begin{pmatrix}\Delta_i\\ \Delta_{1+i}\\ \vdots\\ \Delta_{m-1+i}\\ \Delta_{m+i}\end{pmatrix}$

$$=(a_0,a_1,\cdots,a_{m-1},1)\begin{pmatrix}\alpha_1^i&\alpha_2^i&\cdots&\alpha_n^i\\ \alpha_1^{1+i}&\alpha_2^{1+i}&\cdots&\alpha_n^{1+i}\\ \vdots&\vdots&&\vdots\\ \alpha_1^{m-1+i}&\alpha_2^{m-1+i}&\cdots&\alpha_n^{m-1+i}\\ \alpha_1^{m+i}&\alpha_2^{m+i}&\cdots&\alpha_n^{m+i}\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ \vdots\\ x_{n-1}\\ x_n\end{pmatrix}=0.$$

□

根据定理 1 和定理 2，我们立即得到以下结果。

n $n-1$**推论 1**。 设 α_1、α_2、$\cdots$、α_n 是有限域 $\mathbb{F}_{q^2}$ 中互不相同的元素。设 $G(x)=\prod(x-\alpha_i)$ $=x^n-\sum c_ix^i$，并设 $i=1$ $i=0n$$x_1$、$x_2$、$\cdots$、$x_n\in\mathbb{F}_{q^2}$。定义 $\Delta_i=\sum\alpha_l^ix_l$、$i=0$、1、$\cdots$。令矩阵 T 如公式 *(2)* 所定义。则 $l=1$

$$T\begin{pmatrix}\Delta_i\\ \Delta_{i+1}\\ \vdots\\ \Delta_{i+n-1}\end{pmatrix}=\begin{pmatrix}\Delta_{i+1}\\ \Delta_{i+2}\\ \vdots\\ \Delta_{i+n}\end{pmatrix}.$$

证明。显然， α_1、α_2、$\cdots$、α_n 是 $G(x)=0$ 的根。因此

$$\alpha_j^n - c_{n-1}\alpha_j^{n-1} - \cdots - c_1\alpha_j - c_0 = 0, j = 1, 2, \cdots, n.$$

根据定理 2，我们有如下表达式

$$\Delta_{n+i} - c_{n-1}\Delta_{n-1+i} - \cdots - c_1\Delta_{1+i} - c_0\Delta_i = 0.$$

□

引理 *1.* 设 $n=2k$ 为偶数，并设 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in(\mathbb{F}_{q^2})^n$，其中 α_1、α_2、$\cdots$、α_n 为互异元素。则存在向量 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)\in(\mathbb{F}_{q^2}^*)^n$，使得$GRS_{n,k}(\boldsymbol{\alpha},\boldsymbol{v})$是 q^2元厄米自对偶，当且仅当方程组 $\sum_{l=1}^{n}\alpha_l^{i+jq}x_l=0$、$0\le i$、$j\le k-1$ 有解 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in(\mathbb{F}_q^*)^n$。

证明。码$GRS_{n,k}(\boldsymbol{\alpha},\boldsymbol{v})$是 q^2元厄米自对偶GRS码，当且仅当

$$\sum_{l=1}^{n}(\alpha_l^i v_l)(\alpha_l^j v_l)^q = \sum_{l=1}^{n}\alpha_l^{i+jq}v_l^{1+q} = 0, 0\le i,j\le k-1.$$

这等价于

$$\sum_{l=1}^{n}\alpha_l^{i+jq}x_l = 0, 0\le i,j\le k-1$$

有解 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in(\mathbb{F}_q^*)^n$，其中 $x_i=v_i^{1+q}, 1\le i\le n$。 □

注 1： 当 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in(\mathbb{F}_{q^2}^*)^n$ 时，引理 1 与 [13] 中的命题 1 重合。事实上，当 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in(\mathbb{F}_{q^2})^n$ 时，该结果同样成立。为方便读者，现将其重述如下。

定理 3。 设 $\mathbb{F}_{q^2}$ 是一个含有 q^2 个元素的有限域，其中 q 是一个素数幂。设 $n=2k$ 满足 $n\le q+k$。设 n 个 α_1、α_2、$\cdots$、α_n 是 $\mathbb{F}_{q^2}$ 中互不相同的元素，并设 x_1、x_2、$\cdots$、$x_n\in\mathbb{F}_{q^2}^*$。定义 $\Delta_i=\sum_{l=1}^{n}\alpha_l^i x_l$、$i=0$、1、$\cdots$。如果对于 $0\le i$、$j\le k-1$，$\Delta_{i+jq}=0$，则这些向量

$$\beta_0,\beta_1,\cdots,\beta_{k-1}$$

are 线性无关，其中 $\beta_l=(\Delta_{lq+k},\Delta_{lq+k+1},\cdots,\Delta_{lq+n-1})$ 对 $l=0$，$1,\cdots,k-1$。

证明。令 $\Delta_i=\sum_{l=1}^{n}\alpha_l^i x_l, i=0,1,\cdots$。则 $\Delta_{i+jq}=0$ 对 $0\le i,j\le k-1$。令 $G(x)=\prod_{l=1}^{n}(x-\alpha_i)=x^n-\sum_{i=1}^{n-1}c_i x^i$，且 T 按式 (2) 定义。根据推论 1，序列 $S=(\Delta_0,\Delta_1,\Delta_2,\cdots)$ 可视为线性反馈移位寄存器序列，其初始状态为 $(\Delta_0,\Delta_1,\cdots,\Delta_{n-1})$，状态转移矩阵为 T。令$\sim\beta_l=(\Delta_{lq},\Delta_{lq+1}\cdots,\Delta_{lq+k-1},\Delta_{lq+k},\Delta_{lq+k+1},\cdots,\Delta_{lq+n-1})$ 对 $l=0$，$1,\cdots,k-1$。如果存在 $b_0,b_1,\cdots,b_{k-1}\in\mathbb{F}_{q^2}$ 使得

$$\sum_{i=0}^{k-1}b_i\widetilde{\beta}_i = 0. \tag{3}$$

根据推论 1，我们知道对于 $i=0,1,\cdots,k-1$，$\widetilde{\beta}_i^T=T^{iq}\widetilde{\beta}_0^T$。接下来

$$\sum_{i=0}^{k-1}b_i\widetilde{\beta}_i^T = \sum_{i=0}^{k-1}b_i(T^q)^i\widetilde{\beta}_0^T = 0.$$

由定理 1 可知，$f(x)=b_{k-1}x^{k-1}+\cdots+b_1x+b_0$，那么 $f(\alpha_i^q)$ $i=1$、2、$\cdots$、n 都是 $\sum_{i=0}^{k-1}b_i(T^q)^i=f(T^q)$ 的特征值。并且，对于 $i=1$、2、$\cdots$、n，$(1,\alpha_i,\alpha_i^2,\cdots,\alpha_i^{n-1})^T$ 是矩阵 $f(T^q)$ 关于特征值 $f(\alpha_i^q)$ 的特征向量。

Then

$$\sum_{i=0}^{k-1} b_i (T^q)^i \widetilde{\beta}_0^T = f(T^q) \begin{pmatrix} \Delta_0 \\ \Delta_1 \\ \vdots \\ \Delta_{n-1} \end{pmatrix}$$

$$= f(T^q) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} f(\alpha_1^q) & & & \\ & f(\alpha_2^q) & & \\ & & \ddots & \\ & & & f(\alpha_n^q) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} f(\alpha_1^q)x_1 \\ f(\alpha_2^q)x_2 \\ \vdots \\ f(\alpha_n^q)x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

因此 $f(\alpha_i^q)x_i = 0$和 $x_i \neq 0$，那么对于 $i = 1$、2、$\cdots$、n， $f(\alpha_i^q) = 0$。因此，多项式 $f(x) = b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$有 n 个互不相同的根 α_1^q、α_2^q、$\cdots$、α_n^q，其中 $k < n$。由于一个非零的 $k-1$ 次多项式至多有 $k-1$个互不相同的根，因此可得 $f(x) = 0$，进而有 $b_0 = b_1 = \cdots = b_{k-1} = 0$。结合式 (3)，我们得出 $\widetilde{\beta}_0^T$、$\widetilde{\beta}_1^T$、$\cdots$、$\widetilde{\beta}_{k-1}^T$向量线性无关。此外，由于每个 β_l的前 k 个分量均为零，因此 β_0、β_1、$\cdots$、β_{k-1}也线性无关。 □

定理 4。设 $\mathbb{F}_{q^2}$ 是具有 q^2 个元素的有限域，其中 q 是素数幂。设 $n = 2k$，并设 α_1、α_2、$\cdots$、α_n 为 $\mathbb{F}_{q^2}$ 中的互异元素。设 $\boldsymbol{v} = (v_1, v_2, \cdots, v_n) \in (\mathbb{F}_{q^2}^*)^n$。若广义 *Reed-Solomon* 码 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 是厄米自对偶的，则 $k \leq q-1$。

证明。由于 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 是厄米自对偶的，由引理 1，存在向量 $\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in (\mathbb{F}_q^*)^n$，使得 $\sum_{l=1}^{n} \alpha_l^{i+jq} x_l = 0, 0 \leq i, j \leq k-1$。定义 $\Delta_i = \sum_{l=1}^{n} \alpha_l^i x_l, i = 0, 1, \cdots$。则对所有 $0 \leq i, j \leq k-1$，有 $\Delta_{i+jq} = 0$。

假设 $k \geq q$。那么对于任意 $0 \leq i_0 \leq n-1$，存在指标 $0 \leq l_{i_0} \leq k-1, 0 \leq l_0 \leq k-1$，使得 $\Delta_{i_0} = \Delta_{l_{i_0} q + l_0}$。由此可得 $(\Delta_0, \Delta_1, \cdots, \Delta_{n-1}) = (0, 0, \cdots, 0)$，这与

$$\begin{pmatrix} \Delta_0 \\ \Delta_1 \\ \vdots \\ \Delta_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

其中 $\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in (\mathbb{F}_q^*)^n$。因此 $k \leq q-1$。

□

以下结论已得到证明。为使本文内容连贯、易于阅读，我们在此重述该结论，并提供一种新的证明方法。

定理5。设 $\mathbb{F}_{q^2}$ 是一个含有 q^2 个元素的有限域，其中 q 是一个素数幂。设 $n = 2k$，且 α_1、α_2、$\cdots$、α_n 是 $\mathbb{F}_{q^2}$中的互不相同的元素。设 $\boldsymbol{v} = (v_1, v_2, \cdots, v_n) \in (\mathbb{F}_{q^2}^*)^n$。如果广义 *Reed-Solomon* 码 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 是厄米自对偶的，那么 $n \leq q+1$。

证明。 根据定理 4，可得 $n \le q+k$。根据定理 3，我们知道下列矩阵的行向量

$$A(\Delta)=\begin{pmatrix} \Delta_k & \Delta_{k+1} & \cdots & \Delta_{n-1} \\ \Delta_{q+k} & \Delta_{q+k+1} & \cdots & \Delta_{q+n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots & \Delta_{(k-2)q+n-1} \end{pmatrix}$$

are linearly independent. Let $\widetilde{A}(\Delta)=\begin{pmatrix} \Delta_k & \Delta_{k+1} & \cdots & \Delta_{q-1} \\ \Delta_{q+k} & \Delta_{q+k+1} & \cdots & \Delta_{q+q-1} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots & \Delta_{(k-2)q+q-1} \end{pmatrix}$. We prove that the row vectors 哦，$\widetilde{A}(\Delta)$ 如此接近，却彼此独立。 d t

(1) 如果 $n \le q$，那么

$$\widetilde{A}(\Delta)=\begin{pmatrix} \Delta_k & \Delta_{k+1} & \cdots & \Delta_{n-1} & \cdots & \Delta_{q-1} \\ \Delta_{q+k} & \Delta_{q+k+1} & \cdots & \Delta_{q+n-1} & \cdots & \Delta_{2q-1} \\ \vdots & \vdots & \ddots & \vdots & & \\ \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots & \Delta_{(k-2)q+n-1} & \cdots & \Delta_{(k-1)q-1} \end{pmatrix}.$$

~因此，矩阵 $A(\Delta)$ 的行向量也线性无关。

(2) 如果 $n > q$，那么根据定理 4，我们有 $q < n \le q+k-1$。因此

$$(\Delta_{lq+k}, \Delta_{lq+k+1}, \cdots, \Delta_{lq+n-1}) = (\Delta_{lq+k}, \Delta_{lq+k+1}, \cdots, \Delta_{lq+q-1}, 0, \cdots, 0)$$

对于 $l=0$，1，$\cdots$，$k-2$。因此矩阵

$$\begin{aligned} A(\Delta) &= \begin{pmatrix} \Delta_k & \Delta_{k+1} & \cdots & \Delta_{n-1} \\ \Delta_{q+k} & \Delta_{q+k+1} & \cdots & \Delta_{q+n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots & \Delta_{(k-2)q+n-1} \end{pmatrix} \\ &= \begin{pmatrix} \Delta_k & \Delta_{k+1} & \cdots & \Delta_{q-1} & 0 & \cdots & 0 \\ \Delta_{q+k} & \Delta_{q+k+1} & \cdots & \Delta_{2q-1} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots & \Delta_{(k-1)q-1} & 0 & \cdots & 0 \end{pmatrix} \\ &= \begin{pmatrix} \widetilde{A}(\Delta) & O \end{pmatrix}. \end{aligned}$$

~ ~ ~因此， $A(\Delta)$ 的行向量也线性无关。因此， $A(\Delta)$ 的秩满足 $R(A(\Delta)) = k-1$，其值不能超过列数，即 $k-1 \le q-k$。由此可得 $2k \le q+1$，这意味着 $n \le q+1$。 □

注记2： 该结果表明，当 $n > q+1$ 时，不存在长度为 n 的 q^2 元厄米特自对偶 GRS 码。该结果通过 [16] 中的 Magma 编程得到，并在 [17] 中作为 $e=\frac{m}{2}$ 上 $e-$ 伽罗瓦自对偶的一个特例得到了理论证明。本文提出了一种新的证明方法，且易于理解。

定理6。 设 $\mathbb{F}_{q^2}$ 是一个含有 q^2 个元素的有限域，其中 q 是素数幂。设 $n=2k$ 为偶数，且 α_1、α_2、$\cdots$、α_n 是 $\mathbb{F}_{q^2}$ 中互不相同的元素。设 $\boldsymbol{v}=(v_1, v_2, \cdots, v_n) \in (\mathbb{F}_{q^2}^*)^n$。若广义 *Reed-Solomon* 码 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 是厄米特自对偶的，则以下情形之一成立：

(i) $n=q+1$，并且存在 $a \in \mathbb{F}_{q^2}$ 和 $b \in \mathbb{F}_q^*$，使得 α_1、α_2、$\cdots$、α_n 是 $(x+a)^{q+1}=b$ 的根。

(ii) $n \le q$，并且存在 $a \in \mathbb{F}_{q^2}$ 和 $b \in \mathbb{F}_q^*$，使得 α_1、α_2、$\cdots$、α_n 是 $(x+a)^{q+1}=b$ 或 $x^q = ax+b$ 的根。

证明。由于 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 是厄米自对偶的，根据引理 1，存在 $\boldsymbol{x}=(x_1, x_2, \cdots, x_n) \in (\mathbb{F}_q^*)^n$，使得 $\sum_{l=1}^{n} \alpha_l^{i+jq} x_l = 0$，$0 \le i, j \le k-1$。令 $\Delta_i = \sum_{l=1}^{n} \alpha_l^i x_l, i = 0, 1, \cdots$。则对于 $0 \le i, j \le k-1$，有 $\Delta_{i+jq} = 0$。令 $G(x) = \prod_{l=1}^{n}(x-\alpha_i) = x^n - \sum_{i=0}^{n-1} c_i x^i$，且 T 如式（2）所定义。根据推论 1，序列 $S=(\Delta_0, \Delta_1, \Delta_2, \cdots)^T$ 可视为一个线性反馈移位寄存器序列，其初始状态为 $(\Delta_0, \Delta_1, \cdots, \Delta_{n-1})^T$，状态转移矩阵为 T。对任意正整数 $i, j \ge 1$，记 $L^{(i)}(S) = (\Delta_i, \Delta_{i+1}, \Delta_{i+2}, \cdots)^T$，以及 $L^{(i)}(S)_{[j]} = (\Delta_i, \Delta_{i+1}, \Delta_{i+2}, \cdots \Delta_{i+j-1})^T$。对于 $\mathbb{F}_{q^2}$ 上的线性空间 $(\mathbb{F}_{q^2})^n$，向量 $(1, 1, \cdots, 1)$，$(\alpha_1, \alpha_2, \cdots, \alpha_n)$ $\cdots$，$\left(\alpha_1^{n-1}, \alpha_2^{n-1}, \cdots, \alpha_n^{n-1}\right)$ 可视为一组基。

(i) 若 $n = q+1$，则对于向量 $(\alpha_1^n, \alpha_2^n, \cdots, \alpha_n^n) \in (\mathbb{F}_{q^2})^n$，存在 k_0，k_1，$\cdots$，$k_{n-1} \in \mathbb{F}_{q^2}$ 使得 t

$$\alpha_j^n = \sum_{i=0}^{n-1} k_i \alpha_j^i, j = 1, 2, \cdots, n.$$

因此，α_1，α_2，$\cdots$，α_n 是 $-x^n + k_{n-1}x^{n-1} + \cdots + k_1 x + k_0 = 0$ 的根。根据定理 2，我们有

$$-\Delta_{n+i} + k_{n-1}\Delta_{n-1+i} + \cdots + k_1 \Delta_{1+i} + k_0 \Delta_i = 0$$

对于任意非负整数 i。因此 $k_0 S + k_1 L^{(1)}(S) + \cdots + k_{n-1} L^{(n-1)}(S) - L^{(n)}(S) = \mathbf{0}$，此外

$$\left(k_0 S + k_1 L^{(1)}(S) + \cdots + k_{n-1} L^{(n-1)}(S) - L^{(n)}(S)\right)_{[(k-1)q]} = \mathbf{0}$$

al因此成立。将该序列视为列向量，我们得到以下矩阵乘积 :

$$\left(S_{[(k-1)q]}, L^{(1)}(S)_{[(k-1)q]}, \cdots, L^{(n)}(S)_{[(k-1)q]}\right) \begin{pmatrix} k_0 \\ k_1 \\ \vdots \\ k_{n-1} \\ -1 \end{pmatrix} = \mathbf{0}.$$

定义矩阵 M as $M = \left(S_{[(k-1)q]}, L^{(1)}(S)_{[(k-1)q]}, \cdots, L^{(n)}(S)_{[(k-1)q]}\right) = \begin{pmatrix} A_0 \\ B_0 \\ A_1 \\ B_1 \\ \vdots \\ A_{k-2} \\ B_{k-2} \end{pmatrix}$, where

$$A_l = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \Delta_{lq+k} & \Delta_{lq+k+1} & \cdots \Delta_{(l+1)q-1} & 0 & 0 \\ 0 & 0 & \cdots & 0 & \Delta_{lq+k} & \Delta_{lq+k+1} & \cdots \Delta_{(l+1)q-1} & 0 & 0 & 0 \\ \vdots & \vdots & & & & & & & & \vdots \\ 0 & 0 & \Delta_{lq+k} & \Delta_{lq+k+1} & \cdots \Delta_{(l+1)q-1} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \Delta_{lq+k} & \Delta_{lq+k+1} & \cdots \Delta_{(l+1)q-1} & 0 & \cdots & \cdots & \cdots & 0 & \Delta_{(l+1)q+k} \end{pmatrix}$$

是一个 $k \times (n+1)$ 矩阵，其中 $l = 0$，1，$\cdots$，$k-2$。

则对于 $l = 0$、1、$\cdots$、$k-2$，其中 $\boldsymbol{X} = (k_0$、k_1、$\cdots$、k_{n-1}、$-1)^T$。

由每个 $A_l\boldsymbol{X}=0$ 的前 $k-1$ 个方程组成的方程组可写为 $A\boldsymbol{Y}=0$，即

$$\begin{pmatrix} A_0[0,1,\cdots,k-2;2,3,\cdots,n-2] \\ A_1[0,1,\cdots,k-2;2,3,\cdots,n-2] \\ \vdots \\ A_{k-2}[0,1,\cdots,k-2;2,3,\cdots,n-2] \end{pmatrix} \begin{pmatrix} k_2 \\ k_3 \\ \vdots \\ k_{n-2} \end{pmatrix} = \mathbf{0}.$$

根据定理 3，行向量 $A_0[0;2,3,\cdots,n-2], A_1[0;2,3,\cdots,n-2],\cdots,A_{k-2}[0;2,3,\cdots,n-2]$ 也线性无关。因为每个 $A_l[0;2,3,\cdots,n-2]=(0,\cdots,0,\Delta_k,\Delta_{k+1},\cdots,\Delta_{q-1})$，$l=0,1,\cdots,k-2$。因此，该图

$$\begin{vmatrix} \Delta_k & \Delta_{k+1} & \cdots & \Delta_{q-1} \\ \Delta_{q+k} & \Delta_{q+k+1} & \cdots & \Delta_{2q-1} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots & \Delta_{(k-1)q-1} \end{vmatrix} \neq 0.$$

因此，Δ_k，Δ_{q+k}，$\cdots$，$\Delta_{(k-2)q+k}$ 并非全为零。假设 $\Delta_{l_0q+k}\neq 0$，对于某个 $0\leq l_0\leq k-2$，则

$$A_{l_0}[0,\cdots,k-2;2,\cdots,n-2]=\begin{pmatrix} 0 & \cdots & 0 & \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots\Delta_{(l_0+1)q-1} \\ 0 & \cdots & \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots\Delta_{(l_0+1)q-1} & 0 \\ \vdots & & & & & \vdots \\ \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots\Delta_{(l_0+1)q-1} & 0 & \cdots & 0 \end{pmatrix}$$

其行秩为 $k-1$。因此，$A_{l_0}[0,1,\cdots,k-2$ 的 $k-1$ 个行向量；2，3，$\cdots$，$n-2]$ 在 $\mathbb{F}_{q^2}$ 上线性无关。设

$$B=\begin{pmatrix} A_0[0;2,3,\cdots,n-2] \\ A_1[0;2,3,\cdots,n-2] \\ \vdots \\ A_{k-2}[0;2,3,\cdots,n-2] \\ A_{l_0}[1,2,\cdots,k-2;2,3,\cdots,n-2] \end{pmatrix}$$

$$=\begin{pmatrix} 0 & \cdots & 0 & \Delta_k & \Delta_{k+1} & \cdots\Delta_{q-1} \\ 0 & \cdots & 0 & \Delta_{q+k} & \Delta_{q+k+1} & \cdots\Delta_{2q-1} \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots\Delta_{(k-1)q-1} \\ 0 & \cdots & \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots\Delta_{(l_0+1)q-1} & 0 \\ \vdots & & & & & \vdots \\ \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots\Delta_{(l_0+1)q-1} & 0 & \cdots & 0 \end{pmatrix},$$

then B satisfies $B\begin{pmatrix} k_2 \\ k_3 \\ \vdots \\ k_{n-2} \end{pmatrix}=0$ and

$$|B|=\pm\begin{vmatrix} \Delta_k & \Delta_{k+1} & \cdots & \Delta_{q-1} \\ \Delta_{q+k} & \Delta_{q+k+1} & \cdots & \Delta_{2q-1} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots & \Delta_{(k-1)q-1} \end{vmatrix}\begin{vmatrix} 0 & \cdots & 0 & \Delta_{l_0q+k} \\ 0 & \cdots & \Delta_{l_0q+k} & \Delta_{l_0q+k+1} \\ \vdots & & \vdots & \\ \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots & \Delta_{(l_0+1)q-1} \end{vmatrix}\neq 0.$$

由此可得 $k_2 = k_3 = \cdots = k_{n-2} = 0$。因此，

$$\alpha_j^n = \sum_{i=0}^{n-1} k_i \alpha_j^i = k_{n-1}\alpha_j^{n-1} + k_1\alpha_j + k_0$$

对于 $j = 1, 2, \cdots, n.$

对于 $n = q+1$，我们有 $\alpha_j^{q+1} - k_{n-1}\alpha_j^q - k_1\alpha_j - k_0 = 0$，这等价于 $\alpha_j^{q+1} - k_{n-1}^q\alpha_j - k_1^q\alpha_j^q - k_0^q = 0$。因此，$\alpha_1, \alpha_2, \cdots, \alpha_n$是 $x^{q+1} - k_{n-1}x^q - k_1x - k_0 = 0$ 和 $x^{q+1} - k_{n-1}^q x - k_1^q x^q - k_0^q = 0$ 的根。通过比较系数，我们得到 $k_1^q = k_{n-1}$ 和 $k_0^q = k_0$，这意味着 $k_0 \in \mathbb{F}_q$。令 $-k_1 = a \in \mathbb{F}_{q^2}$ 和 $k_1^{q+1} + k_0 = b$。那么$\alpha_1, \alpha_2, \cdots, \alpha_n$是方程的根

$$(x+a)^{q+1} = b.$$

由此可得 $b \in \mathbb{F}_q^*$。

（ii）若 $n \le q$，则对向量 $\left(\alpha_1^{q+t}, \alpha_2^{q+t}, \cdots, \alpha_n^{q+t}\right) \in (\mathbb{F}_{q^2})^n$，其中 $t = 0, 1$，（且在下文中，t始终满足 $t = 0$或 $t = 1$），存在系数 $k_{t,0}, k_{t,1}, \cdots, k_{t,n-1} \in \mathbb{F}_{q^2}$ 使得

$$\alpha_j^{q+t} = \sum_{i=0}^{n-1} k_{t,i}\alpha_j^i, j = 1, 2, \cdots, n.$$

因此，$\alpha_1, \alpha_2, \cdots, \alpha_n$是 $-x^{q+t} + k_{t,n-1}x^{n-1} + \cdots + k_{t,1}x + k_{t,0} = 0$ 的根。由定理 2，我们有

$$-\Delta_{q+t+i} + k_{t,n-1}\Delta_{n-1+i} + \cdots + k_{t,1}\Delta_{1+i} + k_{t,0}\Delta_i = 0$$

对任意非负整数 i。由此可得 $k_{t,0}S + k_{t,1}L^{(1)}(S) + \cdots + k_{t,n-1}L^{(n-1)}(S) - L^{(q+t)}(S) = \mathbf{0}$ 从而

$$\left(k_{t,0}S + k_{t,1}L^{(1)}(S) + \cdots + k_{t,n-1}L^{(n-1)}(S) - L^{(q+t)}(S)\right)_{[(k-1)q]} = 0.$$

将这些序列视为列向量，我们得到以下矩阵乘积:

$$\left(S_{[(k-1)q]}, L^{(1)}(S)_{[(k-1)q]}, \cdots, L^{(q+t)}(S)_{[(k-1)q]}\right) \begin{pmatrix} k_{t,0} \\ k_{t,1} \\ \vdots \\ k_{t,n-1} \\ 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix} = \mathbf{0}.$$

Define the matrix $M(t)$ by $M(t)=\left(S_{[(k-1)q]},L^{(1)}(S)_{[(k-1)q]},\cdots,L^{(q+t)}(S)_{[(k-1)q]}\right)=\begin{pmatrix}A_{t,0}\\B_{t,0}\\A_{t,1}\\B_{t,1}\\\vdots\\A_{t,k-2}\\B_{t,k-2}\end{pmatrix}$, where

$$A_{1,l}=\begin{pmatrix}0&0&\cdots&0&0&\Delta_{lq+k}&\Delta_{lq+k+1}&\cdots\Delta_{(l+1)q-1}&0&0\\0&0&\cdots&0&\Delta_{lq+k}&\Delta_{lq+k+1}&\cdots\Delta_{(l+1)q-1}&0&0&0\\\vdots&\vdots&&&&&&&\vdots&\vdots\\0&0&\Delta_{lq+k}&\Delta_{lq+k+1}&\cdots\Delta_{(l+1)q-1}&0&\cdots&\cdots&0&0\\0&\Delta_{lq+k}&\Delta_{lq+k+1}&\cdots\Delta_{(l+1)q-1}&0&\cdots&\cdots&\cdots&0&*\end{pmatrix}$$

是一个 $k\times(q+2)$ 矩阵，且 $A_{0,l}=A_{1,l}[0,1,\cdots,k-1;\ 0,\ 1,\ \cdots,q]$ 是一个 $k\times(q+1)$ 矩阵，其中 $l=0,\ 1,\ \cdots,k-2$。然后 $A_{t,l}\boldsymbol{X(t)}=\mathbf{0}$，其中 $l=0,\ 1,\ \cdots,k-2$，这里 $\boldsymbol{X(t)}=(k_t,0,k_t,1,\cdots,k_{t,n-1},0,\cdots,0,-1)^T$。由每个 $A_{t,l}\boldsymbol{X(t)}=\mathbf{0}$ 的前 $k-1$ 个方程构成的方程组可写为 $A(t)\boldsymbol{Y(t)}=\mathbf{0}$，即 .

$$\begin{pmatrix}A_{t,0}[0,1,\cdots,k-2;2,3,\cdots,n-1]\\A_{t,1}[0,1,\cdots,k-2;2,3,\cdots,n-1]\\\vdots\\A_{t,k-2}[0,1,\cdots,k-2;2,3,\cdots,n-1]\end{pmatrix}\begin{pmatrix}k_{t,2}\\k_{t,3}\\\vdots\\k_{t,n-1}\end{pmatrix}=\mathbf{0}. \tag{4}$$

根据定理 3，则矩阵 $A(t)$ 的 $k-1$ 行:

$$A_{t,0}[0;2,3,\cdots,n-1],A_{t,1}[0;2,3,\cdots,n-1],\cdots,A_{t,k-2}[0;2,3,\cdots,n-1] \tag{5}$$

是线性无关的。因为每个 $A_{t,l}[0;2,3,\cdots,n-1]=(0,\cdots,0,\Delta_{lq+k},\Delta_{lq+k+1},\cdots,\Delta_{lq+n-1}),\ l=0,1,\cdots,k-2$。因此下列矩阵的行向量

$$M=\begin{pmatrix}\Delta_k&\Delta_{k+1}&\cdots&\Delta_{n-1}\\\Delta_{q+k}&\Delta_{q+k+1}&\cdots&\Delta_{q+n-1}\\\vdots&\vdots&\ddots&\vdots\\\Delta_{(k-2)q+k}&\Delta_{(k-2)q+k+1}&\cdots&\Delta_{(k-2)q+n-1}\end{pmatrix}$$

也都是线性无关的。因此，M 的秩为 $R(M)=k-1$，M 的列数为 k。如果 M 的第一列不恒为零，设对于某个 $0\le l_0\le k-2$，有 $\Delta_{l_0q+k}\neq 0$。那么

$$A_{t,l_0}[0,1,2,\cdots,k-2;2,3,\cdots,n-1]$$

$$=\begin{pmatrix}0&\cdots&0&\Delta_{l_0q+k}&\Delta_{l_0q+k+1}&\cdots\Delta_{l_0q+n-1}\\0&\cdots&\Delta_{l_0q+k}&\Delta_{l_0q+k+1}&\cdots\Delta_{l_0q+n-1}&0\\\vdots&&&&&\vdots\\\Delta_{l_0q+k}&\Delta_{l_0q+k+1}&\cdots\Delta_{l_0q+n-1}&0&\cdots&0\end{pmatrix}$$

的行秩为 $k-1$。因此，A_t的 $k-1$ 行向量、$_{l_0}[0,1,\cdots,k-2;$ 2、3、 $\cdots$、 $n-1]$ 在 $\mathbb{F}_{q^2}$上线性无关。

$$B(t)=\begin{pmatrix} A_{t,0}[0;2,3,\cdots,n-1] \\ A_{t,1}[0;2,3,\cdots,n-1] \\ \vdots \\ A_{t,k-2}[0;2,3,\cdots,n-1] \\ A_{t,l_0}[1,2,\cdots,k-2;2,3,\cdots,n-1] \end{pmatrix}$$

$$=\begin{pmatrix} 0 & \cdots & 0 & \Delta_k & \Delta_{k+1} & \cdots\Delta_{n-1} \\ 0 & \cdots & 0 & \Delta_{q+k} & \Delta_{q+k+1} & \cdots\Delta_{q+n-1} \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \Delta_{(k-2)q+k} & \Delta_{(k-2)q+k+1} & \cdots\Delta_{(k-2)q+n-1} \\ 0 & \cdots & \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots\Delta_{l_0q+n-1} & 0 \\ \vdots & & & & & \vdots \\ \Delta_{l_0q+k} & \Delta_{l_0q+k+1} & \cdots\Delta_{l_0q+n-1} & 0 & & 0 \end{pmatrix}.$$

因此 $B(0)=B(1)$。将这个公共矩阵记为 B。于是 B 满足 $B\begin{pmatrix} k_t & {}^{3} \\ {}_{2} & \cdots\vdots \\ {}_{,}k_t & {}_{,}k_t \quad {}_{,}{}_{n-1} \end{pmatrix}=\mathbf{0}$。因此，这两个向量

$(k_{0,}2,k_{0,}3,\cdots,k_{0,n-1})^T$和 $(k_{1,}2,k_{1,}3,\cdots,k_{1,n-1})^T$都是 $B\boldsymbol{X}=\mathbf{0}$的解。由于 B的秩为 $R(B)=k-1+k-2=n-3$，可知 $(k_{0,}2,k_{0,}3,\cdots,k_{0,n-1})^T$和 $(k_{1,}2,k_{1,}3,\cdots,k_{1,n-1})^T$线性相关。如果 M 的第一列恒为零，则该图

$$\begin{vmatrix} \Delta_{k+1} & \Delta_{k+2} & \cdots & \Delta_{n-1} \\ \Delta_{q+k+1} & \Delta_{q+k+2} & \cdots & \Delta_{q+n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{(k-2)q+k+1} & \Delta_{(k-2)q+k+2} & \cdots & \Delta_{(k-2)q+n-1} \end{vmatrix}\neq 0.$$

因此，对于某个 $0\le j_0\le k-2$，存在某个 $\Delta_{j_0q+k+1}\neq 0$。

取

$$B_1(t)=\begin{pmatrix} A_{t,0}[0;2,3,\cdots,n-1] \\ A_{t,1}[0;2,3,\cdots,n-1] \\ \vdots \\ A_{t,k-2}[0;2,3,\cdots,n-1] \\ A_{t,j_0}[1,2,\cdots,k-2;2,3,\cdots,n-1] \end{pmatrix}$$

$$=\begin{pmatrix} 0 & 0 & \cdots & 0 & \Delta_{k+1} & \Delta_{k+2} & \cdots\Delta_{n-1} \\ 0 & 0 & \cdots & 0 & \Delta_{q+k+1} & \Delta_{q+k+2} & \cdots\Delta_{q+n-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \Delta_{(k-2)q+k+1} & \Delta_{(k-2)q+k+2} & \cdots\Delta_{(k-2)q+n-1} \\ 0 & 0 & \cdots & \Delta_{j_0q+k+1} & \Delta_{j_0q+k+2} & \cdots\Delta_{j_0q+n-1} & 0 \\ \vdots & \vdots & & & & & \vdots \\ 0 & \Delta_{j_0q+k+1} & \Delta_{j_0q+k+2} & \cdots\Delta_{j_0q+n-1} & 0 & \cdots & 0 \end{pmatrix}.$$

因此，我们还有 $B_1(0) = B_1(1)$。我们将这个公共矩阵记为 B_1。那么 B_1 满足 $B_1 \begin{pmatrix} k_t & & & 3 \\ & 2 & \vdots & \\ , k_t & , k_t & , n-1 & \end{pmatrix} = \mathbf{0}$ 13 。

因此，向量 $(k_0,2, k_0,3, \cdots, k_{0,n-1})^T$ 和 $(k_1,2, k_1,3, \cdots, k_{1,n-1})^T$ 都是 $B_1\boldsymbol{X} = \mathbf{0}$ 的解。由于 B_1 的秩为 $R(B_1) = k-1+k-2 = n-3$，因此 $(k_0,2, k_0,3, \cdots, k_{0,n-1})^T$ 和 $(k_1,2, k_1,3, \cdots, k_{1,n-1})^T$ 线性相关。

因此，存在 λ_0，$\lambda_1 \in \mathbb{F}_{q^2}$，且二者不全为零，使得

$$\lambda_0(k_{0,2}, k_{0,3}, \cdots, k_{0,n-1}) + \lambda_1(k_{1,2}, k_{1,3}, \cdots, k_{1,n-1}) = \mathbf{0}. \tag{6}$$

定义 $(\alpha_1^i, \alpha_2^i, \cdots, \alpha_n^i) = \boldsymbol{\alpha}^i$，其中 $i = 0$、1、$\cdots$，$\boldsymbol{\alpha}^0$ 表示 $(1, 1, \cdots, 1)$。那么这些向量满足 $\boldsymbol{\alpha}^q = k_{0,0}\boldsymbol{\alpha}^0 + k_{0,1}\boldsymbol{\alpha}^1 + k_{0,2}\boldsymbol{\alpha}^2 + \cdots + k_{0,n-1}\boldsymbol{\alpha}^{n-1}$ 以及 $\boldsymbol{\alpha}^{q+1} = k_{1,0}\boldsymbol{\alpha}^0 + k_{1,1}\boldsymbol{\alpha}^1 + k_{1,2}\boldsymbol{\alpha}^2 + \cdots + k_{1,n-1}\boldsymbol{\alpha}^{n-1}$. 结合式 (6)，可得

$$\begin{aligned} \lambda_0\boldsymbol{\alpha}^q + \lambda_1\boldsymbol{\alpha}^{q+1} &= \lambda_0(k_{0,0}\boldsymbol{\alpha}^0 + k_{0,1}\boldsymbol{\alpha}^1) + \lambda_1(k_{1,0}\boldsymbol{\alpha}^0 + k_{1,1}\boldsymbol{\alpha}^1) \\ &= (\lambda_0 k_{0,0} + \lambda_1 k_{1,0})\boldsymbol{\alpha}^0 + (\lambda_0 k_{0,1} + \lambda_1 k_{1,1})\boldsymbol{\alpha}^1. \end{aligned}$$

定义 $\lambda_0 k_{0,0} + \lambda_1 k_{1,0} = c_0, \lambda_0 k_{0,1} + \lambda_1 k_{1,1} = c_1$。那么

$$\lambda_0\boldsymbol{\alpha}^q + \lambda_1\boldsymbol{\alpha}^{q+1} = c_0\boldsymbol{\alpha}^0 + c_1\boldsymbol{\alpha}^1. \tag{7}$$

由式（7），我们分析以下几种情况:

（1）若 $\lambda_1 = 0$，则 $\lambda_0 \neq 0$ 和 $\boldsymbol{\alpha}^q = \frac{c_1}{\lambda_0}\boldsymbol{\alpha} + \frac{c_0}{\lambda_0}\boldsymbol{\alpha}^0$。设 $a = \frac{c_1}{\lambda_0} \in \mathbb{F}_{q^2}$ 和 $b = \frac{c_0}{\lambda_0} \in \mathbb{F}_{q^2}$。那么每个 α_i 都是方程 $x^q = ax + b$ 的一个根。

（2）若 $\lambda_1 \neq 0$ 和 $\lambda_1 + \lambda_1^q \neq 0$，则每个 α_i 都是 $\lambda_1 x^{q+1} + \lambda_0 x^q - c_1 x - c_0 = 0$ 的一个根，也都是 $\lambda_1^q x^{q+1} + \lambda_0^q x - c_1^q x^q - c_0^q = 0$ 的一个根。将这两个方程相加，得到 $(\lambda_1 + \lambda_1^q)\, x^{q+1} + (\lambda_0 - c_1^q)\, x^q + (\lambda_0^q - c_1)\, x - (c_0 + c_0^q) = 0$。定义 $a = \frac{\lambda_0 - c_1^q}{\lambda_1 + \lambda_1^q}$ 和 $b = \frac{c_0 + c_0^q}{\lambda_1 + \lambda_1^q} + a^{q+1} \in \mathbb{F}_q^*$。那么每个 α_i 都是 $(x + a)^{q+1} = b$ 的一个根。

(3) 若 $\lambda_1 \neq 0$ 和 $\lambda_1 + \lambda_1^q = 0$，则 $\lambda_0 - c_1^q \neq 0$。定义 $a = -\frac{\lambda_0^q - c_1}{\lambda_0 - c_1^q}$ 和 $b = \frac{c_0 + c_0^q}{\lambda_0 - c_1^q} \in \mathbb{F}_{q^2}$。那么，每个 α_i 都是 $x^q = ax + b$ 的根。

□

注 3: 该结果表明，当 $n \leq q + 1$ 时，厄米特自对偶广义里德-所罗门码恰有两类。因此，[13]中的猜想是正确的，现已得到证明。

IV. 构造

事实上，GRS码 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 可视为由求值点 $\boldsymbol{\alpha}$ 和列向量 $\boldsymbol{v}$ 确定的一类线性码。在前几节中，我们刻画了使 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 成为厄米自对偶码的求值点 $\boldsymbol{\alpha}$。接下来，我们将确定给定 $\boldsymbol{\alpha}$ 时 $\boldsymbol{v}$ 的取值，并进一步给出厄米自对偶GRS码的显式构造。

在本节中，我们将用 $G'(x)$ 表示多项式 $G(x)$ 的形式导数).

定理 7. 设 $\mathbb{F}_{q^2}$ 是一个含有 q^2 个元素的有限域，其中 q 是一个素数幂。设 $n = 2k$, $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 $\mathbb{F}_{q^2}^*$ 中的互不相同的元素。广义 *Reed-Solomon* 码 $GRS_{n,k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 是厄米自对偶的，当且仅当

$$deg(f(x)m^i(x)) \mod G(x)) \leq k-1, i = 0, 1, \cdots, k-1,$$

where $G(x)=\prod_{i=1}^{n}(x-\alpha_i)$, $f(x)=\sum_{i=1}^{n}\frac{v_i^{q+1}}{u_i}f_i(x)$, $m(x)=\sum_{i=1}^{n}\alpha_i^q f_i(x)$, $f_i(x)=\prod_{j=1,j\neq i}^{n}\frac{x-\alpha_j}{\alpha_i-\alpha_j}$,$u_i=\frac{1}{G'(\alpha_i)}$, $i=1,2,\cdots,n$.

证明。设 $C=GRS_{n,k}(\boldsymbol{\alpha},\boldsymbol{v})$ 是与求值点 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 和列向量 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$ 相关联的广义 Reed-Solomon 码。当且仅当 $C=C^{\perp H}$ 时，码 C 是厄米自对偶的；这等价于 $C^{\perp E}=C^q$，其中 $C^q=\{c^q|c\in C\}$，且对于 $c=(c_1,c_2,\cdots,c_n)$，有 $c^q=(c_1^q,c_2^q,\cdots,c_n^q)$。众所周知，$C^q$ 的生成矩阵是 $G^q=[I_k,0]V_n(\boldsymbol{\alpha})^q diag(\boldsymbol{v}^q)$，而 C 的校验矩阵是 $H=[I_k,0]V_n(\boldsymbol{\alpha})diag(\frac{\boldsymbol{u}}{\boldsymbol{v}})$，它同时也是 $C^{\perp E}$ 的生成矩阵。由于 $dimC^q=dimC^{\perp E}$，条件 $C=C^{\perp H}$ 等价于 $C^q\subseteq C^{\perp E}$。进而，这等价于要求 $[I_k,0]V_n(\boldsymbol{\alpha})^q diag(\boldsymbol{v}^{q+1})$ 的行向量可以表示为 $[I_k,0]V_n(\boldsymbol{\alpha})$ 的行向量的线性组合。

那么，对于向量 $(\underbrace{\frac{v_1^{q+1}}{u_1}\alpha_1^{iq}}, \underbrace{\frac{v_2^{q+1}}{u_2}\alpha_2^{iq}}, \cdots, \underbrace{\frac{v_n^{q+1}}{u_n}\alpha_n^{iq}})$，存在多项式 $g_i(x)\in\mathbb{F}_{q^2}[x]_{k-1}$ 使得

$$(\frac{v_1^{q+1}}{u_1}\alpha_1^{iq},\frac{v_2^{q+1}}{u_2}\alpha_1^{iq},\cdots,\frac{v_n^{q+1}}{u_n}\alpha_1^{iq})=(g_i(\alpha_1),g_i(\alpha_2),\cdots,g_i(\alpha_n)),$$

for $0\leq i\leq k-1$. Indeed, since

$(\alpha_1^q,\alpha_2^q,\cdots,\alpha_n^q)=(m(\alpha_1),m(\alpha_2),\cdots,m(\alpha_n))$ and $(\frac{v_1^{q+1}}{u_1},\frac{v_2^{q+1}}{u_2},\cdots,\frac{v_n^{q+1}}{u_n})=(f(\alpha_1),f(\alpha_2),\cdots,f(\alpha_n))$, we have

$$(\frac{v_1^{q+1}}{u_1}\alpha_1^{iq},\frac{v_2^{q+1}}{u_2}\alpha_1^{iq},\cdots,\frac{v_n^{q+1}}{u_n}\alpha_1^{iq})=(f(\alpha_1)m^i(\alpha_1),f(\alpha_2)m^i(\alpha_2),\cdots,f(\alpha_n)m^i(\alpha_n))$$

对于 $0\leq i\leq k-1$，此结论也成立。因此，$g_i(x)\equiv f(x)m^i(x) \bmod G(x)$，并且 C 是厄米自对偶的当且仅当

$$deg(f(x)m^i(x) \mod G(x))\leq k-1,$$

对于 $i=0,1,2,\cdots,k-1$. □

A. 第一类厄米特自对偶*GRS*码

引理 2. 设 q 为 一个素数幂，设 $\mathbb{F}_{q^2}$ 为含有 q^2 个元素的有限域，并设 $a,b\in\mathbb{F}_{q^2}$。定义 *se* *t*

$$S=\{\alpha\in\mathbb{F}_{q^2}|\alpha^q=a\alpha+b\}.$$

那么，基数 $|S|>1$ 当且仅当 $a^{q+1}=1,b^q+a^qb=0$。

证明。(1) 若 $a=0$ 且 $b=0$，则显然 $S=\{0\}$，因此 $|S|=1$。
(2) 若 $b=0$ 且 $a\neq 0$，则方程 $\alpha^q=a\alpha+b$ 化简为 $\alpha(\alpha^{q-1}-a)=0$。因此，$|S|>1$ 当且仅当 $a^{q+1}=1$。
(3) 若 $b\neq 0$，则由 $\alpha^q=a\alpha+b$，对等式两边取 $q-$次幂，得到 $\alpha=(a\alpha+b)^q=a^q\alpha^q+b^q=a^q(a\alpha+b)+b^q=a^{q+1}\alpha+a^qb+b^q$。

若 $a^{q+1}\neq 1$，则此方程关于 α 有唯一解，因此 $|S|=1$。

I对于 $a^{q+1}=1$，方程简化为 $0=a^qb+b^q$，因此 $|S|>1$ 当且仅当 $a^qb+b^q=0$。

综合情形 (1)、(2) 和 (3)，我们得出 $|S|>1$ 当且仅当 $a^{q+1}=1$，$b^q+a^qb=0$。 □

$$S_1=\{\alpha\in\mathbb{F}_{q^2}|\alpha^q=a\alpha+b\} \text{ for } a^{q+1}=1,b^q+a^qb=0.$$

当 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}\subseteq S_1$ 时，定理 7 中的多项式 $m(x)$ 为 $m(x)=ax+b$。根据定理 7 和引理 2，我们可知，对于 $GRS_{n,k}(\boldsymbol{\alpha},\boldsymbol{v})$ 是厄米自对偶的，定理 7 中的多项式 $f(x)$ 必须满足 $degf(x)=0$，即对于某个 $\lambda\in\mathbb{F}_{q^2}^*$，$f(x)=\lambda$。结合引理 2，我们得到如下厄米特自对偶广义里德-所罗门码的构造。

构造 1. 设 $\mathbb{F}_{q^2}$ 是一个含有 q^2 个元素的有限域，其中 q 是一个素数幂，并令 a、$b\in\mathbb{F}_{q^2}$ 满足 $a^{q+1}=1$ 和 $b^q+a^qb=0$。令 $n=2k$，并设 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}\subseteq S_1$ 为一组互不相同的元素。那么，广义 *Reed-Solomon* 码 $GRS_{n,k}(\boldsymbol{\alpha},\boldsymbol{v})$ 是厄米特自对偶的，当且仅当存在 $\lambda\in\mathbb{F}_{q^2}^*$ 使得

$$\frac{v_i^{q+1}}{u_i}=\lambda,$$

where $u_i = \frac{1}{G'(\alpha_i)}$, $G(x) = \prod_{i=1}^{n}(x-\alpha_i)$ *for* $i = 1, 2, \cdots, n$.

B. 第二类厄米自对偶 *GRS* 码

$$S_2 = \{\alpha \in \mathbb{F}_{q^2} | (\alpha + a)^{q+1} = b\}.$$

当 α_1、α_2、$\cdots$、α_n 是 $x^{q+1} = 1$ 的根时，可得，对于 $i = 1$、2、$\cdots$、n，$\alpha_i^q = \alpha_i^{-1}$。因此，定理 7 中的多项式 $m(x)$ 可表示为 $m(x) = x^{-1}$ 模 $G(x)$。根据定理 7，该定理中的多项式 $f(x)$ 为 $f(x) = x^{k-1}$。由此得到以下厄米特自对偶广义里德-所罗门码的构造。

构造2。设 $\mathbb{F}_{q^2}$ 是一个含有 q^2 个元素的有限域，其中 q 是一个素数幂，令 $n = 2k$，且令 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\} \subseteq S_2$。那么，广义 *Reed-Solomon* 码 $GRS_{n,\ k}(\boldsymbol{\alpha}, \boldsymbol{v})$ 是厄米特自对偶的，当且仅当存在一个多项式$g(x) = (x+a)^{k-1} \in \mathbb{F}_{q^2}[x]_k$，使得

$$\frac{v_i^{q+1}}{u_i} = g(\alpha_i),$$

其中 $u_i = \frac{1}{G'(\alpha_i)}$ 以及 $G(x) = \prod_{i=1}^{n}(x-\alpha_i)$ 对于 $i = 1$、2、$\cdots$、n。

V. Conclusion

本文全面而严谨地解决了一个长期悬而未决的问题：刻画厄米特自对偶广义里德-所罗门（GRS）码。我们的主要贡献如下：

(1) 存在性判据： 当码长为 $n > q+1$ 时，厄米特自对偶 GRS 码不存在。对于 $n \leq q+1$，我们证明此类码恰好存在两个不同的类，从而完整证明了 [13] 中的猜想。

(2) 显式构造： 我们为厄米特自对偶 GRS 码推导出两种显式构造方法，分别对应所确定的两个类。这些构造具体且可直接实现，解决了此类码的存在性和显式构造问题。

本研究解决了厄米特自对偶广义里德-所罗门码存在性与分类的基础问题，而我们提出的显式构造为其在编码理论及相关应用中的使用提供了切实可行的途径。

致谢

参考文献

[1] S. Balaji, M. Krishnan, M. Vajha, V. Ramkumar, B. Sasidharan, P. Kumar，“分布式存储的擦除编码”，综述。《中国科学：信息科学》，61，100301，2018年。[2] F. J. MacWilliams 和 N. J. A. Sloane，《纠错码理论》，荷兰阿姆斯特丹：North Holland，1977年。[3] R. Cramer, V. Daza, I. Gracia, J.J. Urroz, G. Leander, J. Marti-Farre, C. Padro，“关于线性秘密共享方案中的码、拟阵和安全多方计算”，*IEEE*信息论汇刊，54(6)，第2647–2657页，2008年。[4] S.T. Dougherty, S. Mesnager, P. Sole，“基于自对偶码的秘密共享方案”，信息论研讨会论文集，第338–342页，2008年。[5] J.H. Conway, N.J.A. Sloane，《球堆积、格与群》，第*3*版。*Springer*，纽约，1999年。[6] W.C. Huffman, V. Pless，《纠错码基础》，剑桥大学出版社，英国，2003年。[7] J.-L. Kim, Y. Lee，“大有限域上的欧几里得与厄米自对偶MDS码”，《组合理论杂志》，A，105(1)，第79–95页，2004年。[8] K. Guenda，“有限域上的新MDS自对偶码”，设计、编码与密码学，62(1)，第31–42页，2012年。[9] L. Jin, C. Xing，“基于广义里德-所罗门码的新MDS自对偶码”，*IEEE*信息论汇刊，63(3)，第1434–1438页，2017年。[10] H. Yan，“关于MDS自对偶码构造的注记”，《密码学与通信》，11(2)，第259–268页，2018年。[11] K. Labad,H. Liu, and J. Luo，“有限域上的MDS自对偶码构造”，《有限域及其应用》，第59卷，第199–207页，2019年。[12] W. Fang, F. Fu，“基于GRS码和扩展GRS码的MDS欧几里得自对偶码新构造”，*IEEE*信息论汇刊，65(9)，第5574–5579页，2019年。[13] Y. Niu, Q. Yue, Y. Wu, L. Hu，“厄米自对偶、MDS和广义里德-所罗门码”，*IEEE*通信快报，23(5)，第781–784页，2019年。[14] X. Fang, K. Labad, H. Liu, and J. Luo，“奇特征有限域上的新MDS自对偶码”，设计、编码与密码学，88(6)，第1127–1138页，2020年。

[15] A. Zhang, K. Feng, “通过 Reed-Solomon 码构造MDS自对偶码的统一方法”，*IEEE*信息论汇刊，66(6)，第3650–3656页，2020。[16] G. Guo, R. Li，“厄米自对偶GRS码和扩展GRS码”，*IEEE*通信快报，25(4)，第1221–1225页，2021。[17] R. Wan, S. Zhu，“关于伽罗瓦自对偶GRS码和TGRS码的存在性”，《有限域及其应用》，105，102608，第1–25页，2025。[18] Y. Ning, Z. Ye, G. Ge, F. Miao, Y. Xiong, X. Zhang，“自对偶广义Reed-Solomon码的新结果”，*IEEE*信息论汇刊，67(11)，第7240–7252页，2021。[19] W. Fang, J. Zhang,S. Xia, F. Fu，“自对偶广义Reed-Solomon码的新构造”，密码学与通信，14，第677–690页，2022。[20] R. Wan, Y. Li, S. Zhu，“有限域上的新MDS自对偶码 F_{r^2}”，*IEEE*信息论汇刊，69(8)，第5009–5016页，2023。