LCD MDS 码的几类构造方法

献给冯克勤教授 80 华诞

金玲飞^{1*}, 孙中华², 滕佳明¹

1. 复旦大学计算机科学技术学院, 上海 201203;

2. 合肥工业大学数学学院, 合肥 230601

E-mail: lfjin@fudan.edu.cn, sunzhonghuas@163.com, mingyutjm@icloud.com

收稿日期: 2020-12-30; 接受日期: 2021-01-11; 网络出版日期: 2021-02-10; * 通信作者

国家自然科学基金 (批准号: 11501117 和 62002093) 和上海市科委启明星计划 (批准号: 20QA1401100) 资助项目

摘要 线性互补对偶 (linear complementary dual, LCD) 码因其在数据存储和密码学方面的显著作用而受到广泛研究. 线性互补对偶极大距离可分 (LCD MDS (maximum distance separable)) 码具有最大的纠错能力, 因而, 构造 LCD MDS 码是 LCD 码理论研究的一个热点. Carlet 等利用线性码的生成矩阵给出了 LCD MDS 码的存在性结果. 最近, 编码学者们基于广义 Reed-Solomon 码、代数几何码和常循环码等给出了 LCD MDS 码的显式构造. 本文将介绍构造 LCD MDS 码的主要方法、结果以及最新进展.

关键词 线性互补对偶码 MDS 码 Reed-Solomon 码

MSC (2020) 主题分类 81P45, 11B75, 11T71

1 引言

线性互补对偶 (linear complementary dual, LCD) 码是一类重要的纠错码, 已广泛应用于数据存储、通信系统和密码等领域. 1964 年, Massey^[1] 首次研究了有限域上的 LCD 循环码, 当时称为可逆码 (reversible codes). 1992 年, Massey^[2] 提出了 LCD 码的概念, 证明了 LCD 码为双用户二元加法器信道提供了一种最佳的线性编码方案. 2015 年前后, Carlet 和 Guilley^[3,4] 证明了二元 LCD 码在抗侧信道攻击 (side-channel attacks) 和故障注入攻击 (fault injection attacks) 方面具有重要应用, 他们提出了几类针对这些攻击的 LCD 码的构造, 并且证明 2^m 元 $[n, k, d]$ LCD 码可以扩展为二元 $[nm, mk, \geq d]$ LCD 码. 随后, 大批学者围绕 LCD 码开展了深入和系统的研究工作.

1992 年, Massey^[2] 基于线性码的生成矩阵通过扩展的方法构造了 LCD 码. 1994 年, Yang 和 Massey^[5] 给出了循环码是 LCD 码的充要条件. 随后, 循环 LCD 码的构造受到了广泛的研究. Li 等^[6-9] 构造了有限域上几类 LCD BCH (Bose-Chaudhuri-Hocquenghem) 码并研究了它们的参数. Rao 等^[10]

英文引用格式: Jin L F, Sun Z H, Teng J M. Several constructions of LCD MDS codes (in Chinese). Sci Sin Math, 2021, 51: 1463-1484, doi: 10.1360/SSM-2020-0351

研究了短码长二元 LCD 码的最优性. Pang 等^[11] 给出了重根循环码是 LCD 码的充要条件并研究了它们的参数. Liu 等^[12] 和 Liu 等^[13] 研究了 q 元码长为 q^m+1 的 LCD BCH 码的参数. Huang 等^[14] 研究了几类具有较大设计距离的二元 LCD BCH 码的参数. Li 等^[15] 研究了具有较大设计距离的本原 LCD BCH 码的参数. 与此同时, 准循环 LCD 码和常循环 LCD 码的构造也得到了广泛的关注, 可参见文献 [16–20]. 最近, Carlet 等^[21] 利用线性码的生成矩阵构造了 LCD 码, 证明了当 $q > 3$ 时, 一个 q 元线性码等同于一个 q 元 LCD 码, 即 q 元 $[n, k, d]$ 线性码存在, 则存在 q 元 $[n, k, d]$ LCD 码. 随后, Zhou 等^[22] 通过矩阵的方法, 构造了参数优的二元 LCD 码. Galindo 等^[23] 利用 J - 仿射变种码的子域子码构造了参数好的二元和三元 LCD 码. 在此期间, Kandasamy 等^[24] 证明了由迹正交生成矩阵构造的最大秩距离码 (maximum rank distance codes) 是 LCD 码. Liu 和 Liu^[25] 研究了线性互补矩阵积码. Mesnager 等^[26] 研究了代数几何 LCD 码. Roy 和 Bagchi^[27] 研究了极大距离可分 LCD 群码. López 等^[28] 研究了广义仿射 Cartesian LCD 码. 除此之外, 学者们还研究了 Hermite LCD 码, 如 Güneri 等^[16]、Carlet 等^[21]、Boonniyom 和 Jitman^[29] 以及 Li^[30].

除了构造方面, 人们还研究了 LCD 码的界. Massey^[2] 指出存在渐近良好的 LCD 码. Tzeng 和 Hartmann^[31] 证明了一类 LCD 码的最小距离大于 BCH 界. 随后, Sendrier^[32] 利用线性码的 Hull 维谱, 证明了 LCD 码可以达到渐近的 Gilbert-Varshamov 界. Dougherty 等^[33] 研究了给定码长和最小距离的 LCD 码的线性规划界 (linear programming bound). Jin 和 Xing^[34] 证明了偶特征有限域上的代数几何码等同于 LCD 码, 因而构造了一系列超过了渐近 Gilbert-Varshamov 界的 LCD 码. 最近, 文献 [35, 36] 研究了二元 LCD 码相关的界.

众所周知, 极大距离可分 (maximum distance separable, MDS) 码是编码理论中非常重要的一类纠错码, 它在理论研究和实际应用中都有重要的地位. 近年来, MDS 码在分布式存储中得到了广泛的应用, 从而引起了大量的研究. 一些特定性质的 MDS 码具有重要的应用价值, 例如, 自正交 MDS 码在量子码的构造中有关键性作用 (详见文献 [37] 及其引用). 另一个极端情形即是线性互补 MDS 码 (LCD MDS 码). LCD MDS 码研究的一个核心问题是 LCD MDS 码的存在性. 2018 年, Carlet 等^[38] 解决了 LCD MDS 码的存在性问题. 因而, 给出 LCD MDS 码的显式构造是一个有趣的问题.

目前编码理论研究证明, Reed-Solomon (RS) 码和广义 Reed-Solomon (generalized Reed-Solomon, GRS) 码是构造 LCD MDS 码的重要经典码之一. Jin^[39] 给出了 GRS 码和扩展 GRS 码是 LCD 码的充分条件, 完全解决了偶特征有限域上 LCD MDS 码显式构造的存在性问题, 并给出了奇特征有限域上特定参数的 LCD MDS 码的显式构造. 随后, Beelen 和 Jin^[40] 利用代数几何码进一步研究了奇特征有限域上的 LCD MDS 码, 构造了几类代数几何 LCD MDS 码. Chen 和 Liu^[41] 拓展了文献 [39] 的结果, 利用 GRS 码给出了奇特征有限域上特定参数的 LCD MDS 码的显式构造. 最近, Shi 等^[42] 利用 GRS 码构造了奇特征有限域上新参数的 LCD MDS 码. 常循环码是构造 LCD MDS 码的另一类重要的经典码之一. Dinh^[43] 证明了, 当 $\lambda \notin \{1, -1\}$ 时, q 元 λ -常循环码是 LCD 码. 因而, 由非循环和负循环 MDS 码, 可以构造一系列 LCD MDS 码. Pang 等^[18] 利用负循环码构造了奇特征有限域上的两类 LCD MDS 码. Koroglu 和 Sari^[44] 进一步研究了奇特征有限域上的负循环 LCD MDS 码. Qian 和 Zhang^[45] 利用常循环码构造了 LCD MDS 码, 并将其应用于构造纠缠辅助量子码. Fu 等^[46] 利用循环码给出了 LCD MDS 码的显式构造. 最近, Liu 和 Liu^[47] 将广义扭曲 Reed-Solomon (generalized twisted Reed-Solomon, GTRS) 码应用于构造 LCD MDS 码, 构造了一类 LCD MDS 码.

本文主要介绍 LCD MDS 码的几类构造方法和研究结果. 第 2 节给出本文所需的线性码相关基本概念和性质, 第 3 节给出本文所需的 RS 码的相关结论, 第 4 节介绍 LCD MDS 码的几类主要构造方法和结果, 最后是全文的总结.

2 线性码基本概念

设 p 是一个素数, m 是一个正整数且 $q = p^m$. 设 $\mathbb{F}_q$ 是阶为 q 的有限域, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, $\mathbb{F}_q^n$ 是 $\mathbb{F}_q$ 上 n 维行向量空间, 其中 n 是一个正整数. $\mathbb{F}_q^n$ 的每个 k 维子空间 C 都称作一个 q 元 $[n, k]$ 线性码. 设

$$\mathbf{u} = (u_1, u_2, \dots, u_n) \in \mathbb{F}_q^n, \quad \mathbf{v} = (v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n,$$

$\mathbf{u}$ 和 $\mathbf{v}$ 的 (Hamming) 距离定义为

$$\text{dist}(\mathbf{u}, \mathbf{v}) := \sharp\{i : u_i \neq v_i, 1 \leq i \leq n\},$$

其中 $\sharp S$ 表示集合 S 的阶. 设 C 是一个 q 元 $[n, k]$ 线性码, 码 C 的最小距离定义为

$$d(C) := \min\{\text{dist}(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}.$$

如果 $d(C) = d$, 则称 C 是参数为 $[n, k, d]$ 的 q 元线性码. 在 $\mathbb{F}_q^n$ 上, $\mathbf{u}$ 和 $\mathbf{v}$ 的 (Euclid) 内积定义为

$$(\mathbf{u}, \mathbf{v}) := u_1 v_1 + u_2 v_2 + \dots + u_n v_n.$$

一个 q 元 $[n, k]$ 线性码的 (Euclid) 对偶码定义为

$$C^\perp := \{\mathbf{u} \in \mathbb{F}_q^n : (\mathbf{u}, \mathbf{w}) = 0, \mathbf{w} \in C\}.$$

容易验证, $C^\perp$ 是一个 q 元 $[n, n-k]$ 线性码.

定义 2.1 ^[2] 设 C 是一个 q 元 $[n, k]$ 线性码, 若 $C \cap C^\perp = \{\mathbf{0}\}$, 则称 C 是一个 q 元 $[n, k]$ LCD 码.

显然, 如果 C 是一个 q 元 $[n, k]$ LCD 码, 则 $C^\perp$ 是一个 q 元 $[n, n-k]$ LCD 码. 由 LCD 码的定义知, C 是一个 q 元码长为 n 的 LCD 码当且仅当 $\mathbb{F}_q^n = C \oplus C^\perp$, 即 $\mathbb{F}_q^n$ 是 C 和 $C^\perp$ 的直和. 下面的性质给出了一个线性码是 LCD 码的充要条件.

性质 2.1 ^[2] 设 C 是由 $\mathbf{G}$ 生成的 q 元 $[n, k]$ 线性码, 则 C 是 LCD 码当且仅当 $\mathbf{G}\mathbf{G}^\top$ 是 k 阶可逆矩阵.

如果 $C \subseteq C^\perp$, 则称 C 是一个 q 元码长为 n 的自正交码. 下面的性质给出了一个自正交码与 LCD 码的关系.

性质 2.2 ^[38] 设 C 是由 $(\mathbf{I}_k \mathbf{P})$ 生成的 q 元 $[n, k, d]$ 自正交码, 则对任意 $\lambda \in \mathbb{F}_q \setminus \{0, 1, -1\}$, 由 $(\mathbf{I}_k \lambda \mathbf{P})$ 生成的 q 元线性码 C_λ 是一个 q 元 $[n, k, d]$ LCD 码.

一个 q 元 $[n, k, d]$ 线性码的 3 个参数满足 Singleton 界: $d \leq n + 1 - k$. 若一个线性码的参数达到 Singleton 界, 则称它为极大距离可分码 (MDS 码). 可以证明, 如果 C 是一个 q 元 $[n, k]$ MDS 码, 则 $C^\perp$ 是一个 q 元 $[n, n-k]$ MDS 码. 对于 MDS 码, 存在如下 MDS 猜想: 设 $m(k, q)$ 是 q 元 $[n, k]$ MDS 码的最大码长, 则

- 当 $q = 2^m$ 时, $m(2, q) = m(q-1, q) = q+2$;
- 对于其他情形,

$$m(k, q) = \begin{cases} q+1, & 2 \leq k \leq q, \\ k+1, & q < k. \end{cases}$$

Ball ^[48] 证明了 MDS 猜想在素域上成立.

3 RS 码的相关结果

MDS 码是一类达到 Singleton 界的最优码, 它在存储开销和修复性能上达到了最佳权衡, 即给定码长 n 和维度 k , MDS 码拥有最大的错误修复能力.

1960 年, Reed 和 Solomon^[49] 提出了 RS 码. RS 码是一类 MDS 码, 它在数据存储和数据传输中有极其广泛的应用. 下面给出 RS 码相关的基本概念和性质, 更详细的内容可参见文献 [50, 51].

定义 3.1 对任意的向量 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n$ ($\alpha_i \neq \alpha_j$, 对 $i \neq j$)、 $\mathbf{v} = (v_1, v_2, \dots, v_n) \in (\mathbb{F}_q^*)^n$ 和非负整数 k , GRS 码定义为

$$\text{GRS}(\alpha, (k-1)\infty, \mathbf{v}) := \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\}. \quad (3.1)$$

可以验证, 当 $0 \leq k \leq n$ 时, $\text{GRS}(\alpha, (k-1)\infty, \mathbf{v})$ 是一个 q 元 $[n, k]$ MDS 码, 且它的生成矩阵为

$$\mathbf{G} = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1 \alpha_1 & v_2 \alpha_2 & \cdots & v_n \alpha_n \\ v_1 \alpha_1^2 & v_2 \alpha_2^2 & \cdots & v_n \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \cdots & v_n \alpha_n^{k-1} \end{pmatrix}.$$

对于满足 $\gcd(P(x), \prod_{i=1}^n (x - \alpha_i)) = 1$ 的任一多项式 $P(x) \in \mathbb{F}_q[x]$, 定义

$$\text{GRS}(\alpha, P(x), \mathbf{v}) := \left\{ \left(\frac{v_1 f(\alpha_1)}{P(\alpha_1)}, \frac{v_2 f(\alpha_2)}{P(\alpha_2)}, \dots, \frac{v_n f(\alpha_n)}{P(\alpha_n)} \right) : f \in \mathbb{F}_q[x], \deg(f) < \deg(P) \right\}. \quad (3.2)$$

注 3.1 定义 (3.1) 和 (3.2) 关系如下: 如果 $k = \deg(P)$ 且 $0 \leq k \leq n$, 则

$$\text{GRS}(\alpha, P(x), \mathbf{v}) = \text{GRS}(\alpha, (k-1)\infty, \mathbf{u}),$$

其中 $\mathbf{u} = (u_1, u_2, \dots, u_n)$, $u_i = \frac{v_i}{P(\alpha_i)}$.

上述 GRS 码不包括无穷点, 为了包括无穷点, 对于 $\mathbb{F}_q(x)$ 上的有理函数

$$r(x) = \frac{a(x)}{b(x)} = \frac{a_0 + a_1 x + \cdots + a_t x^t}{b_0 + b_1 x + \cdots + b_t x^t}, \quad b_t \neq 0,$$

定义 $r(\infty)$ 为 $\frac{a_t}{b_t}$. 因此, $r(\infty) = 0$ 当且仅当 $\deg(r) \leq -1$, 其中 $\deg(r) := \deg(a) - \deg(b)$. 对于任意向量 $\beta = (\beta_1, \beta_2, \dots, \beta_{n-1}) \in \mathbb{F}_q^n$ ($\beta_i \neq \beta_j$, 对 $i \neq j$) 和 $\mathbf{v} = (v_1, v_2, \dots, v_n) \in (\mathbb{F}_q^*)^n$, 定义扩展 GRS 码

$$\begin{aligned} & \text{GRS}_\infty(\beta, (k-1)\infty, \mathbf{v}) \\ &:= \left\{ \left(v_1 f(\beta_1), v_2 f(\beta_2), \dots, v_{n-1} f(\beta_{n-1}), v_n \left(\frac{f}{x^{k-1}} \right)(\infty) \right) : f \in \mathbb{F}_q[x], \deg(f) < k \right\}. \end{aligned}$$

容易验证, $(\frac{f}{x^{k-1}})(\infty)$ 是 $f(x)$ 的 x^{k-1} 项的系数. 因此, $(\frac{f}{x^{k-1}})(\infty) = 0$ 当且仅当 $\deg(f) < k-1$. 同理, 对于满足 $\gcd(P(x), \prod_{i=1}^{n-1} (x - \beta_i)) = 1$ 的多项式 $P(x) \in \mathbb{F}_q[x]$, 定义

$$\begin{aligned} & \text{GRS}_\infty(\beta, P(x), \mathbf{v}) \\ &:= \left\{ \left(\frac{v_1 f(\beta_1)}{P(\beta_1)}, \frac{v_2 f(\beta_2)}{P(\beta_2)}, \dots, \frac{v_{n-1} f(\beta_{n-1})}{P(\beta_{n-1})}, v_n \left(\frac{x f}{P} \right)(\infty) \right) : f \in \mathbb{F}_q[x], \deg(f) < \deg(P) \right\}. \end{aligned}$$

容易证明, $\text{GRS}_\infty(\beta, (k-1)\infty, \mathbf{v})$ 和 $\text{GRS}_\infty(\beta, P(x), \mathbf{v})$ 都是 q 元线性码.

注 3.2 如果 $k = \deg(P)$, $0 \leq k \leq n$, 且 α 是 $P(x)$ 的首项系数, 则

$$\text{GRS}_{\infty}(\beta, P(x), \mathbf{v}) = \text{GRS}_{\infty}(\beta, (k-1)\infty, \mathbf{u}),$$

其中 $\mathbf{u} = (u_1, u_2, \dots, u_n)$, $u_i = \frac{v_i}{P(\beta_i)}$, $i = 1, 2, \dots, n-1$, 且 $u_n = \frac{v_n}{\alpha}$.

引理 3.1 设 $k = \deg(P)$. 如果 $0 \leq k \leq n$, 则扩展码 $\text{GRS}_{\infty}(\beta, (k-1)\infty, \mathbf{v})$ 和 $\text{GRS}_{\infty}(\beta, P(x), \mathbf{v})$ 都是 q 元 $[n, k]$ MDS 码.

GRS 码和扩展 GRS 码都可以在代数几何码的框架中定义. 为了明确定义 GRS 码的对偶码, 我们可以避免使用代数几何码. 但是, 使用代数几何码来描述扩展 GRS 码的对偶码更为方便. 文献 [39] 给出了 GRS 码的对偶码的刻画.

对于某些 $r(x) \in \mathbb{F}_q(x)$, 有理函数域 $\mathbb{F}_q(x)$ 的微分 η 具有形式 $\eta = rdx$. 对于 $\alpha \in \mathbb{F}_q$, 有理函数 $r(x) := a(x)/b(x)$, 其中 $a(x), b(x) \in \mathbb{F}_q[x]$ 且 $(x-\alpha)^2 \nmid b(x)$, 定义微分 $\eta = rdx$ 在 α 处的余数为 $((x-\alpha)r)(\alpha)$. 此外, 若 $\deg(a) \leq \deg(b) - 1$, 则微分 $\eta = rdx$ 在 ∞ 处的余数 $\text{res}_{\infty}(\eta) := -a_{k-1}/b_k$, 其中

$$a(x) = a_{k-1}x^{k-1} + \dots + a_1x + a_0, \quad b(x) = b_kx^k + \dots + b_1x + b_0, \quad b_k \neq 0.$$

引理 3.2 对于 $0 \leq k \leq n$, $\text{GRS}(\alpha, (k-1)\infty, \mathbf{1})$ 的对偶码为 $\text{GRS}(\alpha, (n-k-1)\infty, \mathbf{u})$, 其中 $\mathbf{1}$ 表示全 1 向量, $\mathbf{u} = (u_1, u_2, \dots, u_n)$, $u_j = \prod_{1 \leq i \leq n, i \neq j} (\alpha_j - \alpha_i)^{-1}$, $j = 1, 2, \dots, n$.

由引理 3.2 知, $\text{GRS}(\alpha, P(x), \mathbf{v})$ 的对偶码有如下结论.

推论 3.1 设 $k = \deg(P)$ 且 $0 \leq k \leq n$, 则 $\text{GRS}(\alpha, P(x), \mathbf{v})$ 的对偶码为 $\text{GRS}(\alpha, (n-k-1)\infty, \mathbf{u})$, 其中 $\mathbf{u} = (u_1, u_2, \dots, u_n)$, $u_j = \frac{P(\alpha_j)}{v_j} \times \prod_{1 \leq i \leq n-1, i \neq j} (\alpha_j - \alpha_i)^{-1}$, $j = 1, 2, \dots, n$.

证明 注意到

$$\begin{aligned} & \text{GRS}(\alpha, P(x), \mathbf{v}) \\ &= \left\{ \left(\frac{v_1}{P(\alpha_1)} c_1, \frac{v_2}{P(\alpha_2)} c_2, \dots, \frac{v_n}{P(\alpha_n)} c_n \right) : (c_1, c_2, \dots, c_n) \in \text{GRS}(\alpha, (n-k-1)\infty, \mathbf{1}) \right\}, \end{aligned}$$

由引理 3.2 知, 结论成立. □

扩展 GRS 码的对偶码有如下结论.

引理 3.3 对于 $0 \leq k \leq n$, $\text{GRS}_{\infty}(\beta, (k-1)\infty, \mathbf{1})$ 的对偶码为 $\text{GRS}_{\infty}(\beta, (n-k-1)\infty, \mathbf{u})$, 其中 $\mathbf{u} = (u_1, u_2, \dots, u_n)$, 这里 $u_j = \prod_{1 \leq i \leq n-1, i \neq j} (\beta_j - \beta_i)^{-1}$, $j = 1, 2, \dots, n-1$; $u_n = -1$.

证明 设 $R(x)$ 是一个 $k-1$ 次的首一多项式且 $\gcd(R, \prod_{i=1}^{n-1} (x - \beta_i)) = 1$. 设

$$C := \left\{ \left(\left(\frac{f}{R} \right) (\beta_1), \dots, \left(\frac{f}{R} \right) (\beta_{n-1}), \left(\frac{f}{R} \right) (\infty) \right) : f(x) \in \mathbb{F}_q[x]; \deg(f) \leq k-1 \right\}.$$

由代数几何的理论 (参见文献 [52, 定理 II.2.8]) 知, C 的对偶码为

$$\begin{aligned} & \left\{ (\text{res}_{\beta_1}(hdx), \dots, \text{res}_{\beta_{n-1}}(hdx), \text{res}_{\infty}(hdx)) \right. \\ & \left. : h(x) = \frac{g(x)R(x)}{\prod_{i=1}^{n-1} (x - \beta_i)}; g(x) \in \mathbb{F}_q[x]; \deg(g) \leq n-k-1 \right\}. \end{aligned}$$

对于 $h(x) = \frac{g(x)R(x)}{\prod_{i=1}^{n-1}(x-\beta_i)}$,

$$\text{res}_{\beta_j}(hdx) = ((x - \beta_j)f)(\beta_j) = \frac{g(\beta_j)R(\beta_j)}{\prod_{1 \leq i \leq n-1, i \neq j}(\beta_j - \beta_i)} = u_j g(\beta_j) R(\beta_j),$$

其中 $1 \leq j \leq n-1$, $\text{res}_{\infty}(hdx) = -g_{n-k-1}$. 由此推导出, 对于任意 $f(x), g(x) \in \mathbb{F}_q[x]$, $\deg(f) \leq k-1$ 且 $\deg(g) \leq n-k-1$, 有

$$0 = \sum_{j=1}^{n-1} \frac{f(\beta_j)}{R(\beta_j)} \times u_j g(\beta_j) R(\beta_j) - f_{k-1} g_{n-k-1} = \sum_{j=1}^{n-1} f(\beta_j) u_j g(\beta_j) + f_{k-1} u_n g_{n-k-1}.$$

结论成立. $\square$

由以上结果, 可以得到如下结论.

推论 3.2 设 $\deg(P) = k$ 且 $0 \leq k \leq n-1$, 则 $\text{GRS}_{\infty}(\beta, P(x), \mathbf{v})$ 的对偶码为 $\text{GRS}_{\infty}(\beta, (n-k-1)\infty, \mathbf{u})$, 其中 $\mathbf{u} = (u_1, u_2, \dots, u_n)$, 这里 $u_j = \frac{P(\beta_j)}{v_j} \times \prod_{1 \leq i \leq n-1, i \neq j} (\beta_j - \beta_i)^{-1}$, $j = 1, 2, \dots, n-1$; $u_n = -\frac{\alpha}{v_n}$, 这里 α 为 $P(x)$ 的首项系数.

4 LCD MDS 码的构造

限于篇幅, 下文介绍 LCD MDS 码的几类主要构造方法.

4.1 基于线性码的 LCD MDS 码的构造

Carlet 等^[38] 完全确定了 q 元 $[n, k]$ LCD MDS 码的存在性, 其中 $0 \leq k \leq q+1$. 本小节将介绍这一结果. 对于偶数 q , 令 $\epsilon_q = 1$; 对于奇数 q , 令 $\epsilon_q = 0$. 则关于 LCD 码的存在性有如下结论.

定理 4.1 如果 q 元 $[n, k, d]$ 线性码存在, 其中 $0 \leq k \leq \lfloor \frac{q-2}{2} \rfloor (1 + \epsilon_q)$ 或 $0 \leq n-k \leq \lfloor \frac{q-2}{2} \rfloor (1 + \epsilon_q)$, 则存在 q 元 $[n, k, d]$ LCD 码.

众所周知, $\text{GRS}_{\infty}(\beta, (k-1)\infty, \mathbf{1})$ 是一个 q 元 $[n, k]$ MDS 码. 由定理 4.1 知, 存在如下参数的 LCD MDS 码.

推论 4.1 对于 $0 \leq k \leq n \leq q+1$ 且 $0 \leq k \leq \lfloor \frac{q-2}{2} \rfloor (1 + \epsilon_q)$, 存在 q 元 $[n, k]$ LCD MDS 码.

下面利用线性码的生成矩阵构造 LCD MDS 码.

引理 4.1 设 $m \geq 2$ 且 $q = 2^m$, 则存在 q 元 $[q+2, 3]$ 和 q 元 $[q+2, q-1]$ LCD MDS 码.

证明 当 $m > 2$ 时, 设 $\mathbb{F}_q^* = \{\omega_1, \omega_2, \dots, \omega_{q-1}\}$, 其中 $\omega_1 = 1$. 设

$$\mathbf{G} = \begin{pmatrix} 1 & \cdots & 1 & \omega_2 & 0 & 0 \\ \omega_1 & \cdots & \omega_q & 0 & 1 & 0 \\ \omega_1^2 & \cdots & \omega_{q-1}^2 & 0 & 0 & 1 \end{pmatrix}.$$

当 $m = 2$ 时, 设

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & \omega & 0 & 0 \\ 1 & \omega & \omega^2 & 0 & 1 & 0 \\ 1 & \omega^2 & \omega & 0 & 0 & \omega \end{pmatrix},$$

其中 $\omega \in \mathbb{F}_4$ 且 $\omega^2 + \omega + 1 = 0$.

容易验证, $\mathbf{G}\mathbf{G}^\top$ 是 3 阶可逆矩阵. 由命题 2.1 知, 由 $\mathbf{G}$ 生成的 q 元线性码是一个参数为 $[q+2, 3]$ 的 LCD MDS 码. 同时, LCD MDS 码的对偶码也是 LCD MDS 码, 因此, 结论成立. $\square$

设 γ 是 $\mathbb{F}_q$ 中的一个本原元, $k \mid (q-1)$ 且 $k < q-1$ 为正整数. 设 $\langle \gamma^{\frac{q-1}{k}} \rangle = \{\omega_0, \dots, \omega_{k-1}\}$, 其中 $\omega_i = \gamma^{\frac{q-1}{k}i}$. 对于 $\beta \in \mathbb{F}_q^*$, 设

$$\mathbf{A}_\beta = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta\omega_0 & \beta\omega_1 & \cdots & \beta\omega_{k-1} \\ (\beta\omega_0)^2 & (\beta\omega_1)^2 & \cdots & (\beta\omega_{k-1})^2 \\ \vdots & \vdots & \ddots & \vdots \\ (\beta\omega_0)^{k-1} & (\beta\omega_1)^{k-1} & \cdots & (\beta\omega_{k-1})^{k-1} \end{pmatrix}.$$

对任意整数 t , 有

$$\omega_0^t + \cdots + \omega_{k-1}^t = \begin{cases} k, & t \equiv 0 \pmod{k}, \\ 0, & \text{其他}. \end{cases}$$

由此推导出

$$\mathbf{A}_\beta \mathbf{A}_\beta^\top = \begin{pmatrix} k & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & \beta^k k \\ 0 & 0 & \cdots & \beta^k k & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \beta^k k & 0 & \cdots & 0 & 0 \end{pmatrix}. \quad (4.1)$$

当 $k \neq \frac{q-1}{2}$ 时, 设 C 是由 $\mathbf{G} = (\mathbf{A}_1 \mathbf{A}_\gamma)$ 生成的 q 元线性码. 容易验证, $\mathbf{G}\mathbf{G}^\top = \mathbf{A}_1 \mathbf{A}_1^\top + \mathbf{A}_\gamma \mathbf{A}_\gamma^\top$. 由 (4.1) 知, $\det(\mathbf{G}\mathbf{G}^\top) = 2(1 + \gamma^k)^{k-1} k^k \neq 0$, 即 $\mathbf{G}\mathbf{G}^\top$ 是 k 阶可逆矩阵. 由命题 2.1 知, C 是 q 元 LCD 码. 又因为 $\mathbf{G}$ 的任一 $k \times k$ 子矩阵也是可逆矩阵, 所以, C 是 q 元 LCD MDS 码.

当 $q \neq 5$ 且 $k = \frac{q-1}{2}$ 时, 设 C 是由 $\mathbf{G} = (\mathbf{A}_1 \gamma \mathbf{A}_\gamma)$ 生成的 q 元线性码. 此时,

$$\mathbf{G}\mathbf{G}^\top = \mathbf{A}_1 \mathbf{A}_1^\top + \gamma^2 \mathbf{A}_\gamma \mathbf{A}_\gamma^\top.$$

由 (4.1) 知, $\det(\mathbf{G}\mathbf{G}^\top) = (1 + \gamma^2)(1 + \gamma^{k+2})^{k-1} k^k \neq 0$. 可以验证, $\mathbf{G}\mathbf{G}^\top$ 是 k 阶可逆矩阵. 由命题 2.1 知, C 是 q 元 LCD 码.

当 $q = 5$ 且 $k = \frac{q-1}{2} = 2$ 时, 可以验证, 由

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}$$

生成的 q 元线性码是一个 LCD MDS 码.

因此, 如下结论成立.

引理 4.2 设 k 为一个正整数, $k \mid (q-1)$ 且 $k < q-1$, 则存在 q 元 $[2k, k]$ LCD MDS 码. 以上构造方法可以推广到构造参数为 $[2k+1, k]$ 的 LCD MDS 码. 设

$$\mathbf{e}_{k-1} = (\underbrace{0, \dots, 0}_{k-1}, 1)^\top,$$

且

$$\mathbf{G}_1 = \begin{cases} (\mathbf{A}_1 \mathbf{A}_\gamma \mathbf{e}_{k-1}), & k \neq \frac{q-1}{2}, \\ (\mathbf{A}_1 \gamma \mathbf{A}_\gamma \mathbf{e}_{k-1}), & k = \frac{q-1}{2}, \quad q \neq 5. \end{cases}$$

容易验证, 由 $\mathbf{G}_1$ 生成的 q 元线性码是一个参数为 $[2k+1, k]$ 的 LCD MDS 码.

当 $q=5$ 且 $k = \frac{q-1}{2} = 2$ 时, 可以验证, 由

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & -1 & 2 \end{pmatrix}$$

生成的 q 元线性码是一个 LCD MDS 码.

同理, 利用以上方法, 可以构造 q 元 $[2k+2, k]$ LCD MDS 码. 设 $\alpha, \beta \in \mathbb{F}_q^*$ 且

$$\mathbf{G}_2(\alpha, \beta) = (\mathbf{A}_1 \quad \alpha \mathbf{A}_\gamma \quad \beta \mathbf{e}_0 \quad \mathbf{e}_{k-1}),$$

其中

$$\mathbf{e}_0 = (\underbrace{1, 0, \dots, 0}_k)^\top.$$

容易验证, 由 $\mathbf{G}_2(\alpha, \beta)$ 生成的 q 元线性码 $C_{\alpha, \beta}$ 是 LCD MDS 码当且仅当

$$\begin{cases} (1 + \alpha^2)k + \beta^2 \neq 0, \\ 1 + \alpha^2 \gamma^k \neq 0. \end{cases} \quad (4.2)$$

当 $q > 3$ 且 $k \neq \frac{q-1}{2}$ 时, 令 $\alpha = 1, \beta \in \mathbb{F}_q^*$ 且 $\beta^2 \neq -2k$, 则 (4.2) 成立, 因此, $C_{1, \beta}$ 是一个 q 元 $[2k+2, k]$ LCD MDS 码.

当 $q > 3$ 且 $k = \frac{q-1}{2}$ 时, 令 $\alpha = \beta = \gamma$, 则 (4.2) 成立. 因此, $C_{\gamma, \gamma}$ 是一个 q 元 $[2k+2, k]$ LCD MDS 码.

当 $q=3$ 时, 由 $(1 \ 1 \ 1 \ 1)$ 生成的 q 元线性码是一个参数为 $[q+1, \frac{q-1}{2}]$ 的 LCD MDS 码.

总结以上结果, 有如下定理.

定理 4.2 设 $q > 3$ 是一个素数幂, k 和 n 是整数且 $0 \leq k \leq n$, 则当下列条件之一成立时, 存在 q 元 $[n, k]$ LCD MDS 码:

- (i) $n \leq q+1$;
- (ii) $q = 2^m$ (m 为正整数), $n = q+2, k=3$ 或者 $k = q-1$.

4.2 GRS 型 LCD MDS 码的构造

GRS 码是构造 LCD MDS 码的重要码源, 本小节着重介绍 GRS 型 LCD MDS 码.

4.2.1 构造 I

Jin^[39] 给出了 GRS 码的另一种定义, 并由此构造了 LCD MDS 码, 本小节将介绍这一结果. 首先给出两个必要的引理.

引理 4.3 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n$ ($\alpha_i \neq \alpha_j$, 对 $i \neq j$), 且 $\mathbf{v} \in (\mathbb{F}_q^*)^n$. 设 $P(x), Q(x) \in \mathbb{F}_q[x]$, 且满足

- (i) $\gcd(P(x), Q(x)) = 1$;
- (ii) $\gcd(P(x)Q(x), \prod_{i=1}^n (x - \alpha_i)) = 1$;
- (iii) $\deg(P) + \deg(Q) \leq n$,

则 $\text{GRS}(\alpha, P(x), \mathbf{v}) \cap \text{GRS}(\alpha, Q(x), \mathbf{v}) = \{\mathbf{0}\}$.

引理 4.4 设 $\beta = (\beta_1, \beta_2, \dots, \beta_{n-1}) \in \mathbb{F}_q^{n-1}$ ($\beta_i \neq \beta_j$, 对 $i \neq j$), 且 $\mathbf{v} \in (\mathbb{F}_q^*)^n$. 设 $P(x), Q(x) \in \mathbb{F}_q[x]$, 且满足

- (i) $\gcd(P(x), Q(x)) = 1$;
- (ii) $\gcd(P(x)Q(x), \prod_{i=1}^{n-1} (x - \beta_i)) = 1$;
- (iii) $\deg(P) + \deg(Q) \leq n$,

则 $\text{GRS}_\infty(\beta, P(x), \mathbf{v}) \cap \text{GRS}_\infty(\beta, Q(x), \mathbf{v}) = \{\mathbf{0}\}$.

基于以上引理, 下面给出 $\text{GRS}(\alpha, P(x), \mathbf{v})$ 和 $\text{GRS}_\infty(\beta, P(x), \mathbf{v})$ 是 LCD MDS 码的一个充分条件.

定理 4.3 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n$ ($\alpha_i \neq \alpha_j$, 对 $i \neq j$). 设 $P(x), Q(x) \in \mathbb{F}_q[x]$, 且满足

- (i) $\gcd(P(x), Q(x)) = 1$ 且 $\gcd(P(x)Q(x), \prod_{i=1}^n (x - \alpha_i)) = 1$;
- (ii) $\deg(P) + \deg(Q) = n$;
- (iii) 对任意的 $1 \leq j \leq n$, $\frac{P(\alpha_j)Q(\alpha_j)}{\prod_{1 \leq i \leq n, i \neq j} (\alpha_j - \alpha_i)}$ 是平方数, 记作 v_j^2 .

令 $\mathbf{v} = (v_1, v_2, \dots, v_n)$, 则 $\text{GRS}(\alpha, P(x), \mathbf{v})$ 是一个 q 元 $[n, \deg(P)]$ LCD MDS 码, 而且,

$$\text{GRS}(\alpha, P(x), \mathbf{v})^\perp = \text{GRS}(\alpha, Q(x), \mathbf{v}).$$

证明 由注 3.1 知, $\text{GRS}(\alpha, P(x), \mathbf{v})$ 是一个 q 元 $[n, \deg(P)]$ MDS 码. 由引理 4.3 知,

$$\text{GRS}(\alpha, P(x), \mathbf{v}) \cap \text{GRS}(\alpha, Q(x), \mathbf{v}) = \{\mathbf{0}\}.$$

下证 $\text{GRS}(\alpha, P(x), \mathbf{v})^\perp = \text{GRS}(\alpha, Q(x), \mathbf{v})$. 由注 3.1 知, $\text{GRS}(\alpha, Q(x), \mathbf{v}) = \text{GRS}(\alpha, (n-k-1)\infty, \mathbf{w})$, 其中 $\mathbf{w} = (w_1, w_2, \dots, w_n)$, $w_i = \frac{v_i}{Q(\alpha_i)}$. 由推论 3.1 知, $\text{GRS}(\alpha, P(x), \mathbf{v})$ 的对偶码是 $\text{GRS}(\alpha, (n-k-1)\infty, \mathbf{u})$, 其中 $\mathbf{u} = (u_1, u_2, \dots, u_n)$ 且 $u_j = \frac{P(\alpha_j)}{v_j} \times \prod_{1 \leq i \leq n, i \neq j} (\alpha_j - \alpha_i)^{-1}$, $j = 1, 2, \dots, n$. 由定理的条件 (iii) 知, $\mathbf{u} = \mathbf{w}$. □

接下来, 讨论扩展 GRS 码.

定理 4.4 设 $\beta = (\beta_1, \beta_2, \dots, \beta_{n-1}) \in \mathbb{F}_q^{n-1}$ ($\beta_i \neq \beta_j$, 对 $i \neq j$). 设 $P(x), Q(x) \in \mathbb{F}_q[x]$, 且满足

- (i) $\gcd(P(x), Q(x)) = 1$ 且 $\gcd(P(x)Q(x), \prod_{i=1}^{n-1} (x - \beta_i)) = 1$;
- (ii) $\deg(P) + \deg(Q) = n$;
- (iii) $\frac{P(\beta_j)Q(\beta_j)}{\prod_{1 \leq i \leq n-1, i \neq j} (\beta_j - \beta_i)}$ 是平方数, 记为 v_j^2 , 其中 $1 \leq j \leq n-1$;
- (iv) $-\alpha\beta$ 是平方数, 记为 v_n^2 , 其中 α 和 β 分别是 $P(x)$ 和 $Q(x)$ 的首项系数.

记 $\mathbf{v} = (v_1, v_2, \dots, v_n)$, 则 $\text{GRS}_\infty(\beta, P(x), \mathbf{v})$ 是一个 q 元 $[n, \deg(P)]$ LCD MDS 码, 而且,

$$\text{GRS}_\infty(\beta, P(x), \mathbf{v})^\perp = \text{GRS}_\infty(\beta, Q(x), \mathbf{v}).$$

证明 由引理 3.1 知, $\text{GRS}_\infty(\beta, P(x), \mathbf{v})$ 是一个 q 元 $[n, k]$ MDS 码. 由引理 4.4 知,

$$\text{GRS}_\infty(\beta, P(x), \mathbf{v}) \cap \text{GRS}_\infty(\beta, Q(x), \mathbf{v}) = \{\mathbf{0}\}.$$

下证 $\text{GRS}_\infty(\beta, P(x), \mathbf{v})^\perp = \text{GRS}_\infty(\beta, Q(x), \mathbf{v})$. 由注 3.2 知,

$$\text{GRS}_\infty(\beta, Q(x), \mathbf{v}) = \text{GRS}_\infty(\beta, (n-k-1)\infty, \mathbf{w}),$$

其中 $\mathbf{w} = (w_1, w_2, \dots, w_n)$, $w_i = \frac{v_i}{Q(\beta_i)}$, $1 \leq i \leq n-1$, $w_n = \frac{v_n}{\beta}$. 由推论 3.2 知, $\text{GRS}_\infty(\beta, P(x), \mathbf{v})$ 的对偶码是 $\text{GRS}(\beta, (n-k-1)\infty, \mathbf{u})$, 其中 $\mathbf{u} = (u_1, u_2, \dots, u_n)$, 这里 $u_j = \frac{P(\beta_j)}{v_j} \times \prod_{1 \leq i \leq n-1, i \neq j} (\beta_j - \beta_i)^{-1}$ ($j = 1, 2, \dots, n-1$), $u_n = -\frac{\alpha}{v_n}$. 由定理的条件 (iii) 和 (iv) 知, $\mathbf{u} = \mathbf{w}$. 证毕. $\square$

下面, 根据定理 4.3 和 4.4 的充分条件, 给出 LCD MDS 码的明确构造. 首先, 考虑维数为 0、1、 $n-1$ 和 n 情形.

引理 4.5 对于任意的 $n \geq 2$ 且 $k \in \{0, 1, n-1, n\}$, 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 对于 $k=0$ 或 $k=n$, 结论显然成立. 当 $k=1$ 时, 考虑 $\mathbb{F}_q$ 中的方程 $x^2 = 1-n$. 当 q 为偶数时, 方程最多有一个解; 当 q 为奇数时, 方程最多有两个解. 无论哪种情形, 一定存在 $\alpha \in \mathbb{F}_q$ 使得 $\alpha^2 \neq 1-n$. 考虑 q 元 $[n, 1]$ MDS 码 $C = \{\lambda(1, 1, \dots, 1, \alpha) : \lambda \in \mathbb{F}_q\}$. 此时, $C \cap C^\perp = \{\mathbf{0}\}$, 否则, $C \subseteq C^\perp$, 这意味着 $(1, 1, \dots, \alpha) \cdot (1, 1, \dots, 1, \alpha) = 0$, 即 $n-1+\alpha^2 = 0$, 矛盾. 由于 $C^\perp$ 是一个 q 元 $[n, n-1]$ MDS 码, 故结论对 $k=n-1$ 也成立. $\square$

对于一般的参数, 有如下结论.

定理 4.5 如果 q 为偶数且 $n \leq q+1$, 则对任意 $0 \leq k \leq n$, 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 由引理 4.5 知, 只需证明 $2 \leq k \leq n-2$ 情形. 设 $\beta_1, \dots, \beta_{n-1}$ 是 $\mathbb{F}_q$ 中 $n-1$ 个不同的元素. 我们选择两个次数分别是 k 和 $n-k$ 且互素的不可约多项式 $P(x)$ 和 $Q(x)$. 又由于 $\mathbb{F}_q$ 中所有元素都是平方数, 因此, 定理 4.4 的所有条件均成立. 证毕. $\square$

上述定理完全解决了偶特征有限域上 LCD MDS 码的显式构造问题. 接下来, 考虑奇特征有限域上 LCD MDS 码的构造问题.

定理 4.6 设 q 是一个奇平方数且 $n \leq \sqrt{q}+1$, 则对任意 $0 \leq k \leq n$, 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 由引理 4.5 知, 只需证明 $2 \leq k \leq n-2$ 的情形. 设 $q = \ell^2$ 且 $\beta_1, \dots, \beta_{n-1}$ 为 $\mathbb{F}_\ell$ 中 $n-1$ 个不同的元素. 在 $\mathbb{F}_\ell[x]$ 上选择两个次数分别是 k 和 $n-k$ 且互素的不可约多项式 $P(x)$ 和 $Q(x)$. 由于 $\mathbb{F}_\ell$ 中所有元素在 $\mathbb{F}_q$ 中都是平方数, 因此, 定理 4.4 的所有条件均成立. 证毕. $\square$

定理 4.7 设 q 为奇数且 $n = q+1$, 则对于偶数 k ($4 \leq k \leq n-4$), 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 在 $\mathbb{F}_q[x]$ 上, 分别选择两个不同的次数为 $\frac{k}{2}$ 和 $\frac{n-k}{2}$ 的首一不可约多项式 $R(x)$ 和 $T(x)$. 设 $P(x) = -R^2(x)$, $Q(x) = T^2(x)$, 设 $\mathbb{F}_q = \{\beta_1, \dots, \beta_{n-1}\}$, 则

$$\prod_{1 \leq i \leq n-1, i \neq j} (\beta_j - \beta_i) = \frac{d(x^q - x)}{dx} \Big|_{x=\beta_j} = -1.$$

因此, 定理 4.4 的所有条件均成立. 证毕. $\square$

引理 4.6 对于任意给定的 m 和素数幂 q , 若 $q \geq 4^m \times m^2$, 则存在子集 $S = \{\alpha_1, \alpha_2, \dots, \alpha_m\} \subset \mathbb{F}_q$, 使得对于所有 $1 \leq i < j \leq m$, $\alpha_j - \alpha_i$ 是非零平方数.

证明 如果 q 是偶数, 因为 $\mathbb{F}_q$ 的每个元素都是平方数, 所以结论成立.

如果 q 是奇数, 当 $m = 2$ 时, 令 $S = \{0, 1\}$, 结论成立. 假设结论对小于等于 $m - 1$ 的正整数成立, 即 $\mathbb{F}_q$ 上存在一个大小为 $m - 1$ 的子集 $T = \{\alpha_1, \alpha_2, \dots, \alpha_{m-1}\}$ 使得对于所有 $1 \leq i < j \leq m - 1$, $\alpha_j - \alpha_i$ 是非零平方数. 设 α 是 $\mathbb{F}_q$ 的本原元, 设 χ 是 $\mathbb{F}_q$ 上的二次特征, 即 $\chi(\alpha^i) = \alpha^{i(q-1)/2}$ ($0 \leq i \leq q - 2$) 且 $\chi(0) = 0$. 显然, i 是偶数当且仅当 $\chi(\alpha^i) = 1$. 令 N 是 $\chi(\beta - \alpha_i) = 1$ (对任意 $i = 1, 2, \dots, m - 1$) 在 $\mathbb{F}_q$ 上解的个数, 则由文献 [53, 习题 5.64], 得

$$\left| N - \frac{q}{2^{m-1}} \right| \leq \left(\frac{m-3}{2} + \frac{1}{2^{m-1}} \right) \sqrt{q} + \frac{m-1}{2}. \quad (4.3)$$

因此, 由 (4.3) 以及 m 和 q 的条件, 有

$$N \geq \frac{q}{2^{m-1}} - \left(\frac{m-3}{2} + \frac{1}{2^{m-1}} \right) \sqrt{q} - \frac{m-1}{2} > 0,$$

这意味着存在一个元素 α_m 使得对于所有 $i = 1, 2, \dots, m - 1$, $\alpha_m - \alpha_i$ 是 $\mathbb{F}_q$ 的非零平方数, 即结论对 m 也成立. 由数学归纳法知, 定理的结论对所有的正整数均成立. $\square$

定理 4.8 设 n 是一个正整数, $q \equiv 1 \pmod{4}$ 且 $q \geq 4^{2n} \times (2n)^2$, 则对于任意 $0 \leq k \leq n$, 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 由引理 4.6 知, 对任意 $1 \leq i < j \leq 2n$, 在 $\mathbb{F}_q$ 上存在 $\{\alpha_1, \alpha_2, \dots, \alpha_{2n}\}$ 使得 $\alpha_j - \alpha_i$ 是非零平方数. 因此, 对任意 $j = 1, 2, \dots, n$, $\prod_{1 \leq i \leq n, i \neq j} (\alpha_j - \alpha_i)^{-1}$ 是非零平方数. 令 $P(x) = \prod_{i=1}^k (x - \alpha_{n+i})$ 和 $Q(x) = \prod_{i=1}^{n-k} (x - \alpha_{n+k+i})$, 则对任意 $1 \leq j \leq n$, $P(\alpha_j)Q(\alpha_i)$ 是一个平方数. 因此, 定理 4.4 的所有条件均成立. 证毕. $\square$

4.2.2 构造 II

本小节继续研究奇特征有限域上 LCD MDS 码的构造. Chen 和 Liu^[41] 通过刻画 GRS 码与其对偶码之间的交集, 构造了几类 LCD MDS 码. 下面介绍他们的主要结论. 为此, 首先给出两个重要的引理.

引理 4.7 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n$, 其中 $\alpha_i \neq \alpha_j$ ($i \neq j$), 且 $\mathbf{v} = (v_1, v_2, \dots, v_n) \in (\mathbb{F}_q^*)^n$. 设

$$\mathbf{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) \in \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}),$$

则 $\mathbf{c} \in \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp$ 当且仅当存在次数小于等于 $n - k - 1$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$(v_1^2 f(\alpha_1), v_2^2 f(\alpha_2), \dots, v_n^2 f(\alpha_n)) = (u_1 g(\alpha_1), u_2 g(\alpha_2), \dots, u_n g(\alpha_n)),$$

其中 $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$, $1 \leq i \leq n$.

对引理 4.7 进行修正, 可以得到如下引理.

引理 4.8 设 $\mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_q\}$, $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_q)$ 且 $\mathbf{v} = (v_1, v_2, \dots, v_q, 1) \in (\mathbb{F}_q^*)^{q+1}$. 设

$$\mathbf{c} = \left(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_q f(\alpha_q), \left(\frac{f}{x^{k-1}} \right)(\infty) \right) \in \text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v}),$$

则 $\mathbf{c} \in \text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v})^\perp$ 当且仅当存在次数小于等于 $q - k$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$\left(v_1^2 f(\alpha_1), v_2^2 f(\alpha_2), \dots, v_q^2 f(\alpha_q), \left(\frac{f}{x^{k-1}} \right)(\infty) \right) = \left(g(\alpha_1), g(\alpha_2), \dots, g(\alpha_q), \left(\frac{g}{x^{q-k}} \right)(\infty) \right).$$

以上两个引理在 GRS LCD MDS 码 (扩展 GRS LCD MDS 码) 的构造中起着重要作用. 由引理 4.7 和 4.8 可以推导出 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})$ 是 LCD 码的充要条件是: 对于任意给定的次数小于等于 $k-1$ 的多项式 $f(x) \in \mathbb{F}_q[x]$, 如果存在一个次数小于等于 $n-k-1$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得 $v_i^2 f(\alpha_i) = u_i g(\alpha_i)$, $1 \leq i \leq n$, 则 $f(x)$ 一定为零多项式. 因此, 构造 GRS LCD MDS 码等价于选择适当的 α 和 $\mathbf{v}$ 使得 $f(x)$ 为零多项式.

首先, 利用引理 4.8 构造码长为 $q+1$ 的 GRS LCD MDS 码.

定理 4.9 设 $q > 3$ 是奇素数幂, 则对任意 $2 \leq k \leq q-1$, 存在一个 q 元 $[q+1, k]$ LCD MDS 码.

证明 设 $\mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_q\}$ 且 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_q)$. 设 γ 是 $\mathbb{F}_q$ 的 $q-1$ 次本原单位根. 因为 $q > 3$, 所以 $\gamma^2 \neq 1$. 证明分如下两种情形.

情形 1 当 $2 \leq k \leq \frac{q-1}{2}$ 时, 令

$$\mathbf{v} = (\underbrace{1, 1, \dots, 1}_{q-k+1}, \underbrace{\gamma, \dots, \gamma}_{k-1}).$$

考虑扩展 GRS 码 $\text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v})$. 下证 $\text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v})$ 是 LCD 码, 即

$$\text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v})^\perp = \{\mathbf{0}\}.$$

为此, 设

$$\mathbf{c} = \left(f(\alpha_1), f(\alpha_2), \dots, f(\alpha_{q-k+1}), \gamma f(\alpha_{q-k+2}), \dots, \gamma f(\alpha_q), \left(\frac{f}{x^{k-1}} \right)(\infty) \right)$$

是 $\text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v})^\perp$ 的任意一个码字, 其中 $f(x) \in \mathbb{F}_q[x]$ 且 $\deg(f) \leq k-1$. 由引理 4.8 知, 存在一个次数小于等于 $q-k$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$\begin{aligned} & \left(f(\alpha_1), \dots, f(\alpha_{q-k+1}), \gamma^2 f(\alpha_{q-k+2}), \dots, \gamma^2 f(\alpha_q), \left(\frac{f}{x^{k-1}} \right)(\infty) \right) \\ &= \left(g(\alpha_1), \dots, g(\alpha_{q-k+1}), g(\alpha_{q-k+2}), \dots, g(\alpha_q), \left(\frac{g}{x^{q-k}} \right)(\infty) \right). \end{aligned} \quad (4.4)$$

下证 $\mathbf{c} = \mathbf{0}$, 显然, 其等价于证明 $f(x) = 0$. 由 (4.4) 推导出 $f(\alpha_i) = g(\alpha_i)$, $1 \leq i \leq q-k+1$. 由于 $\deg(f) \leq k-1 \leq q-k$ 和 $\deg(g) \leq q-k$, 所以 $f(x) = g(x)$. 但是, 由 (4.4) 知, $(\frac{f}{x^{k-1}})(\infty) = (\frac{g}{x^{q-k}})(\infty)$. 由此推导出 $(\frac{f}{x^{k-1}})(\infty) = 0$, 否则, $k = \frac{q+1}{2}$, 矛盾. 因此, $\deg(f) \leq k-2$. 此时, 由 (4.4) 知, $\gamma^2 f(\alpha_j) = g(\alpha_j) = f(\alpha_j)$, $q-k+2 \leq j \leq q$, 其中最后一个等号成立是因为 $f(x) = g(x)$. 又因为 $\gamma^2 \neq 1$, 所以 $f(\alpha_j) = 0$, $q-k+2 \leq j \leq q$. 注意到 $f(x) \in \mathbb{F}_q[x]$ 且 $\deg(f) \leq k-2$, 所以 $f(x) = 0$, 即 $\mathbf{c} = \mathbf{0}$.

情形 2 当 $k = \frac{q+1}{2}$ 时, 令

$$\mathbf{v}' = (\underbrace{1, \dots, 1}_{k-1}, \underbrace{\gamma, \dots, \gamma}_{q-k+1}).$$

考虑扩展 GRS 码 $\text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v}')$. 设

$$\left(f(\alpha_1), f(\alpha_2), \dots, f(\alpha_{k-1}), \gamma f(\alpha_k), \dots, \gamma f(\alpha_q), \left(\frac{f}{x^{k-1}} \right)(\infty) \right)$$

是 $\text{GRS}_\infty(\alpha, (k-1)_\infty, \mathbf{v}')$ 的任意一个码字, 其中 $\deg(f) \leq k-1 = \frac{q-1}{2}$. 由引理 4.8 知, 存在一个次数小于等于 $q-k = \frac{q-1}{2}$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$\left(f(\alpha_1), \dots, f(\alpha_{k-1}), \gamma^2 f(\alpha_k), \dots, \gamma^2 f(\alpha_q), \left(\frac{f}{x^{k-1}} \right)(\infty) \right)$$

$$= \left(g(\alpha_1), \dots, g(\alpha_{k-1}), g(\alpha_k), \dots, g(\alpha_q), \left(\frac{g}{x^{q-k}} \right)(\infty) \right). \quad (4.5)$$

由 (4.5) 知, $(\frac{f}{x^{k-1}})(\infty) = (\frac{g}{x^{q-k}})(\infty)$, 这意味着 $\deg(f - g) \leq k - 2$. 与情形 1 类似, 可以证明 $f(x) = 0$.

综合情形 1 和 2, 对任意的 $2 \leq k \leq \frac{q+1}{2}$, 存在 q 元 $[q+1, k]$ GRS LCD MDS 码. 注意到 LCD MDS 码的对偶码也是 LCD MDS 码, 故结论成立. $\square$

下面, 利用码长 $2 \leq n \leq q$ 的 q 元 GRS 码构造 LCD MDS 码.

定理 4.10 设 $q > 3$ 是一个奇素数幂. 如果 $n \geq 2$ 是 $q-1$ 的因子, 则存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 因为 LCD MDS 码的对偶码也是 LCD MDS 码, 因此, 只需证明存在 q 元 $[n, k]$ LCD MDS 码, $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$. 因为 n 是 $q-1$ 的因子, 则 $\mathbb{F}_q$ 上存在一个 n 次本原单位元 ω . 设 $\alpha = (\omega^0, \omega^1, \dots, \omega^{n-1})$, 且

$$\mathbf{v} = (\underbrace{1, \dots, 1}_{n-k+1}, v_{n-k+2}, \dots, v_n),$$

其中 $v_i \notin \{-1, 0, 1\}$, $n-k+2 \leq i \leq n$. 考虑 GRS 码 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})$. 下证

$$\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp = \{\mathbf{0}\}.$$

设

$$(f(\omega^0), \dots, f(\omega^{n-k}), v_{n-k+2}f(\omega^{n-k+1}), \dots, v_nf(\omega^{n-1}))$$

是 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp$ 的任意一个码字, 则

$$\mathbf{G}_2(f(\omega^0), \dots, f(\omega^{n-k}), v_{n-k+2}^2f(\omega^{n-k+1}), \dots, v_n^2f(\omega^{n-1}))^\top = \mathbf{0},$$

其中 $\mathbf{G}_2$ 是 $k \times n$ 矩阵

$$\mathbf{G}_2 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{k-1} & \cdots & \omega^{(k-1)(n-1)} \end{pmatrix}.$$

注意到

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-2} & \cdots & \omega^{(n-2)(n-1)} \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \vdots \\ \omega^{n-1} \end{pmatrix} = \mathbf{0},$$

由此推导出, 存在一个次数小于等于 $n-k-1$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$(f(\omega^0), \dots, f(\omega^{n-k}), v_{n-k+2}^2f(\omega^{n-k+1}), \dots, v_n^2f(\omega^{n-1})) = (g(\omega^0), \omega g(\omega^1), \dots, \omega^{n-1}g(\omega^{n-1})). \quad (4.6)$$

由 (4.6) 的前 $n - k + 1$ 项知, $f(\omega^i) = \omega^i g(\omega^i)$, $0 \leq i \leq n - k$. 由于 $k \leq \lfloor \frac{n}{2} \rfloor$, $\deg(f) \leq k - 1 \leq n - k - 1$ 且 $\deg(g) \leq n - k - 1$, 因此, $f(x) = xg(x)$. 特别地, $\deg(g) \leq k - 2$. 由 (4.6) 的最后 $k - 1$ 项知, 对于任意的 $n - k + 2 \leq j \leq n$, 有

$$v_j^2 f(\omega^{j-1}) = v_j^2 \omega^{j-1} g(\omega^{j-1}) = \omega^{j-1} g(\omega^{j-1}).$$

因为 $v_j^2 \neq 1$, 所以由上式推导出 $g(\omega^{j-1}) = 0$, $n - k + 2 \leq j \leq n$, 即 $g(x)$ 有 $k - 1$ 个不同的根, 故 $g(x) = 0$. 于是, $f(x) = 0$. 证毕. $\square$

下面的定理指出, 对于任意的 $2 \leq k \leq q - 1$, 存在一个维数为 k 的 q 元 LCD MDS 码.

定理 4.11 设 p 是一个奇素数, $q = p^e > 3$ 且 $n = p^\ell$, 其中 e 和 ℓ 是正整数且 $\ell \leq e$, 则对任意的 $2 \leq k \leq n - 2$, 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 设 H 是 $\mathbb{F}_{p^e}$ 的阶为 n 的加法子群, 记 $H = \{\alpha_1, \dots, \alpha_n\}$. 令 h 为 H 所有非零元的乘积, 即

$$h = \prod_{z \in H \setminus \{0\}} z.$$

设 $\gamma \in \mathbb{F}_q^*$ 且 $\gamma^2 \neq 1$. 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ 且

$$\mathbf{v} = (\underbrace{1, \dots, 1}_{n-k}, \underbrace{\gamma, \dots, \gamma}_k).$$

考虑 GRS 码 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})$. 与上述定理类似, 可以证明

$$\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp = \{\mathbf{0}\}.$$

事实上, 设

$$\mathbf{c} = (f(\alpha_1), \dots, f(\alpha_{n-k}), \gamma f(\alpha_{n-k+1}), \gamma f(\alpha_n))$$

是 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp$ 的任意一个码字. 由引理 4.7 知, 存在一个次数小于等于 $n - k - 1$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$(f(\alpha_1), \dots, f(\alpha_{n-k}), \gamma^2 f(\alpha_{n-k+1}), \dots, \gamma^2 f(\alpha_n)) = (u_1 g(\alpha_1), u_2 g(\alpha_2), \dots, u_n g(\alpha_n)),$$

其中 $u_i = \prod_{1 \leq j \leq n, i \neq j} (\alpha_i - \alpha_j)^{-1}$, $1 \leq i \leq n$. 注意到, 对于任意 $1 \leq i \leq n$, 有

$$u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1} = h^{-1}.$$

因此,

$$(f(\alpha_1), \dots, f(\alpha_{n-k}), \gamma^2 f(\alpha_{n-k+1}), \dots, \gamma^2 f(\alpha_n)) = (h^{-1} g(\alpha_1), h^{-1} g(\alpha_2), \dots, h^{-1} g(\alpha_n)).$$

与定理 4.10 类似可证 $f(x) = 0$, 即 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp = \{\mathbf{0}\}$. 证毕. $\square$

下面的结果表明, 如果码长 n 接近字母表大小 q , 则存在 q 元码长 n 的 LCD MDS 码.

定理 4.12 设 $q > 3$ 是奇素数幂且 $2 \leq n \leq q - 1$ 是正整数, 则对任意的 $q + 1 - n \leq k \leq \lfloor \frac{n}{2} \rfloor$, 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n$, 其中 $\alpha_i \neq \alpha_j, i \neq j$. 令

$$\mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1}, \dots, \alpha_q\}, \quad \mathbf{v} = (\underbrace{1, \dots, 1}_{q-k}, v_{q-k+1}, \dots, v_n),$$

其中 v_i 满足 $-v_i^2 \prod_{j=n+1}^q (\alpha_i - \alpha_j) \neq u_i, q-k+1 \leq i \leq n$. 考虑 GRS 码 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})$. 下证

$$\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp = \{\mathbf{0}\}.$$

为此, 设

$$\mathbf{c} = (f(\alpha_1), \dots, f(\alpha_{q-k}), v_{q-k+1}f(\alpha_{q-k+1}), \dots, v_nf(\alpha_n))$$

是 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp$ 的任意一个码字. 由引理 4.7 知, 存在一个次数小于等于 $n-k-1$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$(f(\alpha_1), \dots, f(\alpha_{q-k}), v_{q-k+1}^2 f(\alpha_{q-k+1}), \dots, v_n^2 f(\alpha_n)) = (u_1 g(\alpha_1), u_2 g(\alpha_2), \dots, u_n g(\alpha_n)), \quad (4.7)$$

其中

$$u_i = \prod_{1 \leq j \leq n, i \neq j} (\alpha_i - \alpha_j)^{-1}, \quad 1 \leq i \leq n.$$

由 (4.7) 的前 $q-k$ 项推导出 $f(\alpha_i) = u_i g(\alpha_i), 1 \leq i \leq q-k$, 其等价于

$$f(\alpha_i) = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1} g(\alpha_i) = - \prod_{j=n+1}^q (\alpha_i - \alpha_j) g(\alpha_i),$$

其中最后一个等号成立是因为

$$\prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j) = -1,$$

这表明 $\alpha_1, \dots, \alpha_{q-k}$ 是 $f(x) + \prod_{j=n+1}^q (x - \alpha_j)g(x)$ 的 $q-k$ 个不同的根. 注意到

$$\begin{aligned} \deg(f) &\leq k-1 \leq n-k-1 \leq q-k-1, \\ \deg\left(\prod_{j=n+1}^q (x - \alpha_j)g(x)\right) &\leq (q-n) + (n-k-1) = q-k-1. \end{aligned}$$

即 $f(x) + \prod_{j=n+1}^q (x - \alpha_j)g(x)$ 的次数至多为 $q-k-1$. 因此,

$$f(x) = - \prod_{j=n+1}^q (x - \alpha_j)g(x).$$

特别地,

$$\deg(f) = q-n + \deg(g) \leq k-1,$$

于是, $\deg(g) \leq n+k-q-1$. 然而, 由 (4.7) 的最后 $n+k-q$ 项可以得到, 对任意 $q-k+1 \leq i \leq n$, 有

$$v_i^2 f(\alpha_i) = u_i g(\alpha_i) = -v_i^2 \prod_{j=n+1}^q (\alpha_i - \alpha_j) g(\alpha_i).$$

因为 $-v_i^2 \prod_{j=n+1}^q (\alpha_i - \alpha_j) \neq u_i$, 由上式可推导出

$$g(\alpha_i) = 0, \quad q - k + 1 \leq i \leq n,$$

即 $g(x)$ 有 $n + k - q$ 个不同的根, 因此, $g(x) = 0$. 从而, $f(x) = 0$. 证毕. $\square$

下面的结论说明, 若 $2 \leq k \leq \lfloor \frac{n}{2} \rfloor$ 且 $2n - k + 1 \leq q \leq 2n$, 则存在 q 元 $[n, k]$ LCD MDS 码.

定理 4.13 设 $q > 3$ 是奇素数幂且 $\frac{q+1}{2} \leq n \leq q-1$ 是正整数, 则对任意的 $2n - q + 1 \leq k \leq \lfloor \frac{n}{2} \rfloor$, 存在一个 q 元 $[n, k]$ LCD MDS 码.

证明 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n$, 其中 $\alpha_i \neq \alpha_j$ 对 $i \neq j$ 都成立. 令

$$\mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1}, \dots, \alpha_q\}.$$

由定理假设知, $q - n > n - k$. 令 $\mathbf{v} = (v_1, v_2, \dots, v_n)$, 其中 $v_i = \prod_{j=1}^{n-k} (\alpha_i - \alpha_{n+j})$. 考虑 GRS 码 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})$. 下证 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp = \{\mathbf{0}\}$. 设

$$\mathbf{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n))$$

是 $\text{GRS}(\alpha, (k-1)_\infty, \mathbf{v}) \cap \text{GRS}(\alpha, (k-1)_\infty, \mathbf{v})^\perp$ 的任意一个码字. 由引理 4.7 知, 存在一个次数小于等于 $n - k - 1$ 的多项式 $g(x) \in \mathbb{F}_q[x]$ 使得

$$(v_1^2 f(\alpha_1), v_2^2 f(\alpha_2), \dots, v_n^2 f(\alpha_n)) = (u_1 g(\alpha_1), u_2 g(\alpha_2), \dots, u_n g(\alpha_n)).$$

由此推导出 $v_i^2 f(\alpha_i) = u_i g(\alpha_i)$, $1 \leq i \leq n$. 一方面, 由 v_i 的定义, 得

$$v_i^2 f(\alpha_i) = \prod_{j=1}^{n-k} (\alpha_i - \alpha_{n+j})^2 f(\alpha_i).$$

另一方面,

$$u_i g(\alpha_i) = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1} g(\alpha_i) = - \prod_{j=n+1}^q (\alpha_i - \alpha_j) g(\alpha_i).$$

由此推导出

$$\prod_{j=1}^{n-k} (\alpha_i - \alpha_{n+j}) f(\alpha_i) = - \prod_{j=n+(n-k+1)}^q (\alpha_i - \alpha_j) g(\alpha_i), \quad 1 \leq i \leq n. \quad (4.8)$$

注意到

$$\deg \left(\left(\prod_{j=1}^{n-k} (x - \alpha_{n+j}) \right) f(x) \right) \leq (n - k) + (k - 1) = n - 1$$

且

$$\deg \left(\left(\prod_{j=n+(n-k+1)}^q (x - \alpha_j) \right) g(x) \right) \leq (q - n) - (n - k) + (n - k - 1) = q - n - 1 \leq n - 1,$$

因此,

$$\deg \left(\left(\prod_{j=1}^{n-k} (x - \alpha_{n+j}) \right) f(x) + \left(\prod_{j=n+(n-k+1)}^q (x - \alpha_j) \right) g(x) \right) \leq n-1.$$

于是, 由 (4.8), 得

$$\left(\prod_{j=1}^{n-k} (x - \alpha_{n+j}) \right) f(x) = - \left(\prod_{j=n+(n-k+1)}^q (x - \alpha_j) \right) g(x).$$

显然, $\prod_{j=1}^{n-k} (x - \alpha_{n+j})$ 是 $g(x)$ 的一个因子. 然而, $\deg(g) \leq n-k-1$, 故 $g(x) = 0$, 即 $f(x) = 0$. $\square$

4.3 其他 LCD MDS 码的构造

本小节介绍 LCD MDS 码的另外 3 种构造方法, 即以代数几何码、TRS (twisted RS) 码及其常循环码为载体的构造方法. 利用这 3 种方法, 可以给出奇特征有限域上特定参数的 LCD MDS 码的显式构造.

4.3.1 代数几何 LCD MDS 码

Beelen 和 Jin^[40] 利用函数域和代数几何码的框架, 重新描述和构造了 LCD MDS 码. 研究结果表明, 函数域的全部机制都可以用于研究 LCD MDS 码, 代数几何框架也有助于对 GRS 码进行更精细的分析. 限于篇幅, 本小节只介绍其主要结果, 更详细的内容, 可参见文献 [40].

定理 4.14 设 p 是一个奇素数, m 是一个正整数且 $q = p^m$, 则当 n 和 k 满足下列条件之一时, q 元 $[n, k]$ LCD MDS 码存在显式构造:

- (i) $n = p^t$, $1 \leq t \leq m-1$, $0 \leq k \leq p^t$.
- (ii) $n < q$ 是正整数, $p \mid n$ 且 $(n-1) \mid (q-1)$, $0 \leq k \leq n$.
- (iii) $n = p\ell$, ℓ 是 $q-1$ 的一个因子且 $p\ell < q$. 如果 ℓ 是偶数, 则 $k = 2\ell - 2r$, $0 \leq r \leq \ell-1$; 如果 ℓ 是奇数, 则 $k = 2\ell - 2r$, $0 \leq r \leq \ell$.
- (iv) $q \geq 5$ 是一个奇平方数, $n < q$ 且 $n-1$ 是 $q-1$ 的奇因子, $k = n - 2r$, $0 \leq r \leq n/2$.
- (v) n 是 $(q-1)/2$ 的因子. 如果 n 是偶数 (奇数), 则 $k = n - 2r$ ($k = n - 2r - 1$), $1 \leq r \leq n/2$.
- (vi) $m > 1$, $n = p(p^{m-1} - 1)/(p-1)$ 且 $0 \leq k \leq n$.
- (vii) $t < m$, $1 \leq d \leq p^{m-t}$ 且 $\gcd(d, p) = 1$. $n = dp^t$, $k = dp^t - 2r$, $2 \leq r \leq p^t/2$.

4.3.2 TRS LCD MDS 码

2017 年, Beelen 等^[54] 引入 TRS 码, 并构造了非 RS 型 MDS 码. 2018 年, Beelen 等^[55] 引入了 GTRS 码, 并研究了这类码的对偶码及其在密码上的应用. 最近, Liu 和 Liu^[47] 推广了 GTRS 码, 并基于 GTRS 码构造了非 GRS 型 LCD MDS 码, 下面介绍他们的主要结果.

定义 4.1 设 n 、 k 和 ℓ 是正整数且 $1 \leq \ell \leq k \leq n$. 设 $\mathbf{h} = (h_1, h_2, \dots, h_\ell)$, 其中 $0 \leq h_1 < h_2 < \dots < h_\ell \leq k-1$. 设 $\mathbf{t} = (t_1, t_2, \dots, t_\ell) \in \{1, 2, \dots, n-k\}^\ell$, 其中 $t_i \neq t_j$ (对任意 $i \neq j$). 设 $\boldsymbol{\eta} \in (\mathbb{F}_q^*)^\ell$, 则 $[\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]$ - 扭曲多项式类定义为

$$\mathcal{P}_{k,n}[\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}] := \left\{ f(x) = \sum_{i=0}^{k-1} f_i x^i + \sum_{j=1}^{\ell} \eta_j f_{h_j} x^{k-1+t_j} : f_i \in \mathbb{F}_q \right\}.$$

定义 4.2 设 n 和 k 是正整数且 $k \leq n$. 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n$, 其中 $\alpha_i \neq \alpha_j$ (对任意 $i \neq j$), 且 $\mathbf{v} = (v_1, v_2, \dots, v_n) \in (\mathbb{F}_q^*)^n$. 设 $\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}$ 和 $\mathcal{P}_{k,n}[\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]$ 定义如上, 则 q 元码长为 n 、维度为 k 定位子 (locators) 为 α 的 GTRS 码定义为

$$\text{GTRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}, \mathbf{v}] := \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) : f \in \mathcal{P}_{k,n}[\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]\}.$$

由 GTRS 码的定义知, $\text{GTRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}, \mathbf{v}]$ 的生成矩阵为

$$\mathbf{G} = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1 \alpha_1 & v_2 \alpha_2 & \cdots & v_n \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1 \alpha_1^{h_1-1} & v_2 \alpha_2^{h_1-1} & \cdots & v_n \alpha_n^{h_1-1} \\ v_1(\alpha_1^{h_1} + \eta_1 \alpha_1^{k-1+t_1}) & v_2(\alpha_2^{h_1} + \eta_1 \alpha_2^{k-1+t_1}) & \cdots & v_n(\alpha_n^{h_1} + \eta_1 \alpha_n^{k-1+t_1}) \\ v_1 \alpha_1^{h_1+1} & v_2 \alpha_2^{h_1+1} & \cdots & v_n \alpha_n^{h_1+1} \\ \vdots & \vdots & \ddots & \vdots \\ v_1 \alpha_1^{h_\ell-1} & v_2 \alpha_2^{h_\ell-1} & \cdots & v_n \alpha_n^{h_\ell-1} \\ v_1(\alpha_1^{h_\ell} + \eta_\ell \alpha_1^{k-1+t_\ell}) & v_2(\alpha_2^{h_\ell} + \eta_\ell \alpha_2^{k-1+t_\ell}) & \cdots & v_n(\alpha_n^{h_\ell} + \eta_\ell \alpha_n^{k-1+t_\ell}) \\ v_1 \alpha_1^{h_\ell+1} & v_2 \alpha_2^{h_\ell+1} & \cdots & v_n \alpha_n^{h_\ell+1} \\ \vdots & \vdots & \ddots & \vdots \\ v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \cdots & v_n \alpha_n^{k-1} \end{pmatrix}_{k \times n}.$$

当 $\mathbf{v} = \mathbf{1}$ 时, $\text{GTRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}, \mathbf{v}]$ 简记为 $\text{GTRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]$. 特别地, $\text{GTRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]$ 恰好是文献 [55] 中定义的 GTRS 码. 下面, 利用 GTRS 码构造 LCD MDS 码.

由性质 2.2, 有如下结论.

引理 4.9 设 n 和 k 是正整数且 $k \leq n$. 设 C 是一个由 $(\mathbf{A}_{k \times k} \mathbf{B}_{k \times (n-k)})$ 生成的 q 元 $[n, k]$ 自正交 MDS 码, 则对任意 $\lambda \in \mathbb{F}_q \setminus \{0, 1, -1\}$, 由 $(\mathbf{A}_{k \times k} \lambda \mathbf{B}_{k \times (n-k)})$ 生成的 q 元线性码 C_β 是一个 q 元 $[n, k]$ LCD MDS 码.

利用 GTRS 码的生成矩阵, 可以得到如下参数的自正交码.

定理 4.15 设 $\ell = t = 1$ 且 $\eta \in \mathbb{F}_q^*$. 设 n, k 和 h 是正整数且 $1 \leq k \leq \frac{n-2}{2}$, $0 \leq h \leq k-1$. 设 $\alpha_1, \alpha_2, \dots, \alpha_n$ 是 $\mathbb{F}_q$ 的 n 个不同的元素, 且 $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ 是平方数, 记作 v_i^2 , $i = 1, 2, \dots, n$. 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\mathbf{v} = (v_1, v_2, \dots, v_n)$, 则 $\text{GTRS}_{k,n}[\alpha, 1, h, \eta, \mathbf{v}]$ 是一个 q 元自正交码.

由引理 4.9 和定理 4.15 知, 存在如下参数的 LCD MDS 码.

推论 4.2 设 $m \geq 2$, V 是 $\mathbb{F}_{2^m}$ 加法群 $(\mathbb{F}_{2^m}, +)$ 的阶为 s 的真子群, $L = \{\overline{b_1}, \dots, \overline{b_{\frac{2^m-1}{s}}}\}$ 是商群 $\mathbb{F}_{2^m}/V$ 的阶为 $\frac{2^m-1}{s}$ 的真子群. 设 $\ell = 1$, $(t, h) = (1, k-1)$, $1 \leq k \leq \frac{n-2}{2}$, $\{\alpha_1, \dots, \alpha_n\}$ 是 $\bigcup_{j=1}^{\frac{2^m-1}{s}} (b_j + V)$ 的子集, 且 $\eta^{-1} \in \mathbb{F}_{2^m} \setminus \bigcup_{j=1}^{\frac{2^m-1}{s}} (b_j + V)$. 设 $\lambda \in \mathbb{F}_q \setminus \{0, 1, -1\}$, $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1} = v_i^2$ ($i = 1, 2, \dots, n$), $\alpha = (\alpha_1, \dots, \alpha_n)$, $\mathbf{v}' = (v_1, \dots, v_k, \lambda v_{k+1}, \dots, \lambda v_n)$, 则 $\text{GTRS}_{k,n}[\alpha, 1, k-1, \eta, \mathbf{v}']$ 是一个 q 元 LCD MDS 码.

注 4.1 在推论 4.2 中, 选取 $\{\alpha_1, \alpha_2, \dots, \alpha_n\} = L$, 则 $n = 2^m - 1$. 由推论 4.2 知, 对于任意 $1 \leq k \leq \frac{n-2}{2}$, 存在一个 2^m 元 $[n, k]$ LCD MDS 码.

注 4.2 如果 $3 \leq k \leq n-3$, $|\mathbb{F}_{2^m} \setminus L| > 6$, 即 $m \geq 4$, 则定理 4.15 可以构造一些非 RS 型 LCD MDS 码.

对于奇特征有限域上的 LCD MDS 码, 有如下结论.

定理 4.16 ^[55] 设 q_0 是素数幂, $1 = s_0 < \cdots < s_\ell$ 是非负整数且使得 $\mathbb{F}_{q_0^{s_0}} \subset \mathbb{F}_{q_0^{s_1}} \subset \cdots \subset \mathbb{F}_{q_0^{s_\ell}} = \mathbb{F}_q$. 设 k 和 n 是正整数且 $k < n \leq q_0$. 设 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_{q_0}^n$, 其中 $\alpha_i \neq \alpha_j$ (对 $i \neq j$). 设 $\mathbf{t}$, $\mathbf{h}$ 和 $\boldsymbol{\eta}$ 定义如定义 4.2, 且使得 $\eta_i \in \mathbb{F}_{q_0^{s_i}} \setminus \mathbb{F}_{q_0^{s_{i-1}}}$, $i = 1, \dots, \ell$, 则 $\text{TRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]$ 是 q 元 MDS 码.

定理 4.17 设 k 和 n 是正整数且 $k \leq \frac{n}{2}$. 设 $q = p^m$, $\{\alpha_1, \dots, \alpha_n\}$ 是 $\mathbb{F}_q$ 乘法群 $(\mathbb{F}_q^*, \cdot)$ 的子群. 设 $\mathbf{t} = (1, 2, \dots, k)$, $\mathbf{h} = (0, 1, \dots, k-1)$, $\boldsymbol{\eta} = (\eta_1, \eta_2, \dots, \eta_k) \in (\mathbb{F}_q^*)^k$. 如果 k 和 n 满足下列条件之一, 则 $\text{TRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]$ 是一个 q 元 LCD 码:

- (i) $k \geq 3$, $k = \frac{n+1}{3}$;
- (ii) $k \geq 3$, $k = \frac{n}{3}$;
- (iii) $k \geq 3$, $\frac{n+2}{3} \leq k < \frac{n}{2}$, 且 $(\eta_{n-2k+2}, \eta_{n-2k+3}, \dots, \eta_k) + (\eta_k, \eta_{k-1}, \dots, \eta_{n-2k+2})$ 的所有分量非零;
- (iv) $k \geq 3$, $k = \frac{n}{2}$, $1 + \eta_1^2$ 非零, 且 $(\eta_2, \eta_3, \dots, \eta_k) + (\eta_k, \eta_{k-1}, \dots, \eta_2)$ 的所有分量非零;
- (v) $k = 2$, $n = 4$, 且 $2(1 + \eta_1^2)$ 非零;
- (vi) $k = 2$, $n = 5$;
- (vii) $k = 2$, $n = 6$;
- (viii) $k = 1$, $n = 2$, 且 $1 + \eta_1^2$ 非零;
- (ix) $k = 1$, $n > 2$.

由定理 4.16 和 4.17 知, 存在如下参数的 LCD MDS 码.

推论 4.3 设 k 和 n 是正整数且 $k \leq \frac{n}{2}$. 设 q 是奇素数幂, $1 = s_0 < \cdots < s_\ell$ 是非负整数且使得 $\mathbb{F}_{q_0} = \mathbb{F}_{q_0^{s_0}} \subsetneq \mathbb{F}_{q_0^{s_1}} \subsetneq \cdots \subsetneq \mathbb{F}_{q_0^{s_\ell}} = \mathbb{F}_q$. 设 $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ 是 $\mathbb{F}_{q_0}^*$ 的子群, $\eta_i \in \mathbb{F}_{q_0^{s_i}} \setminus \mathbb{F}_{q_0^{s_{i-1}}}$ ($i = 1, 2, \dots, n$), 且 $1 + \eta_1^2 \neq 0$, $\eta_i \neq 0$, $i = 2, \dots, \ell$. 设 $\mathbf{t} = (1, 2, \dots, k)$, $\mathbf{h} = (0, 1, \dots, k-1)$, $\boldsymbol{\eta} = (\eta_1, \eta_2, \dots, \eta_k) \in (\mathbb{F}_q^*)^n$. 如果 k 和 n 满足下列条件之一, 则 $\text{TRS}_{k,n}[\alpha, \mathbf{t}, \mathbf{h}, \boldsymbol{\eta}]$ 是一个 q 元 LCD MDS 码:

- (i) $k \geq 3$, $k = \frac{n+1}{3}$;
- (ii) $k \geq 3$, $k = \frac{n}{3}$;
- (iii) $k \geq 3$, $\frac{n+2}{3} \leq k < \frac{n}{2}$;
- (iv) $k \geq 3$, $k = \frac{n}{2}$;
- (v) $k = 1$, $n > 2$.

注 4.3 对足够大的 q 和特殊的 n , 当 $\max\{3, \frac{n}{3}\} \leq k \leq \frac{n}{2}$ 时, 定理 4.17 可以构造 LCD MDS 码.

4.3.3 常循环码 LCD MDS 码

常循环码是包含循环码为子类的一类经典码, 因其丰富的代数结构受到广泛的关注. 设 $\lambda \in \mathbb{F}_q^*$, 一个 q 元码长为 n 的线性码 C 称作 λ -常循环码当且仅当 C 是商环 $\mathbb{F}_q[x]/(x^n - \lambda)$ 的理想. 容易验证, 当 $\lambda^2 \neq 1$ 时, q 元码长为 n 的 λ -常循环码一定是 LCD 码 ^[43]. Krishna 和 Sarwate ^[56] 分类了常循环 MDS 码, 有如下结论.

定理 4.18 设 $\lambda \in \mathbb{F}_q^*$. 设 n 是正整数且 $n \mid (q+1)$. 当下列条件之一成立时, 存在 q 元 $[n, k]$ λ -常循环 MDS 码:

- (i) n 是奇数;

- (ii) n 是偶数, q 是奇数, k 是奇数, 且 λ 是 $\mathbb{F}_q$ 的平方数;
- (iii) n 是偶数, q 是奇数, k 是偶数, 且 λ 是 $\mathbb{F}_q$ 的非平方数.

定理 4.19 设 $\lambda \in \mathbb{F}_q^*$. 设 n 是正整数且 $n \mid (q-1)$. 当 $\text{ord}(\lambda) \mid \frac{q-1}{n}$ 时, 存在 q 元 $[n, k]$ λ -常循环 MDS 码.

由以上两个定理知, 存在如下参数的常循环 LCD MDS 码.

推论 4.4 设 p 是素数且 $q = p^m$. 设 k 和 n 是正整数且 $k \leq n$. 当下列条件之一成立时, 存在 q 元 $[n, k]$ 常循环 LCD MDS 码:

- (i) 当 $p = 2$ 时, n 是 $q-1$ 的真因子; 当 $p \geq 3$ 时, $n \mid (q-1)$ 且 $n < (q-1)/2$;
- (ii) 当 $q > 5$ 时, $n \mid (q+1)$.

设 C 是一个 q 元码长为 n 的 λ -常循环码, 当 $\lambda = 1$ 时, C 称作循环码; 当 $\lambda = -1$ 时 (q 为奇素数幂), C 称作负循环码. 对任意非零多项式 $f(x) = x^r \sum_{i=0}^t f_i x^i \in \mathbb{F}_q[x]$, 其中 $f_0, f_t \in \mathbb{F}_q^*$, 引入互反多项式 $f(x)^* = f_0^{-1} \sum_{i=0}^t f_i x^{t-i}$. 如果 $f(x)^* = f(x)$, 则称 $f(x)$ 是自互反多项式. Yang 和 Massey^[5] 证明了生成多项式为 $g(x)$ 的循环码是 LCD 码当且仅当 $g(x)$ 是自互反多项式, 对此进行直接推广可得如下结论.

性质 4.1 设 C 是生成多项式为 $g(x)$ 的 q 元循环码或负循环码, 则 C 是 LCD 码当且仅当 $g(x)$ 是自互反多项式.

Pang 等^[18] 利用负循环码构造了几类 LCD MDS 码, 相关结果总结如下.

定理 4.20 设 q 是奇素数幂, n 是正整数, 则下列条件之一成立时, 存在 q 元 $[n, k]$ 负循环 LCD MDS 码:

- (i) n 是偶数, $n \mid (\frac{q-1}{2})$, 或 $n \mid (\frac{q+1}{2})$ 且 $2 \leq k \leq n-2$ 是偶数;
- (ii) n 是奇数, $n \mid (\frac{q-1}{2})$, 或 $n \mid (\frac{q+1}{2})$ 且 $2 \leq k \leq n-3$ 是偶数.

Fu 等^[46] 构造了几类循环码 LCD MDS 码, 相关结果总结如下.

定理 4.21 设 q 为奇素数幂, n 和 k 是正整数且 $k \leq n$, 则下列条件之一成立时, 存在 q 元 $[n, k]$ 循环 LCD MDS 码:

- (i) $n \mid (q+1)$, 且当 n 是偶数时, k 是奇数;
- (ii) $q > 4$, $n \mid (q-1)$, 且当 n 是偶数时, k 是奇数.

此外, 文献 [46] 利用循环 LCD MDS 码构造了如下参数的 LCD MDS 码.

定理 4.22 设 $q \geq 4$, $n \mid (q-1)$ 且 $n \geq 3$.

- (i) 如果 $N = n+1$ 且 $2 \leq k \leq n-1$, 则存在 q 元 $[N, k]$ LCD MDS 码;
- (ii) 如果 $N = n+1$ 为奇数且 $2 \leq k \leq n$, 则存在 q 元 $[N, k]$ LCD MDS 码; 如果 $N = n+1$ 为偶数, 则存在 q 元 $[N, k]$ LCD MDS 码, 其中 $k = 2$, 或 k 为奇数且 $3 \leq k \leq n-1$, 或 $k = n$.

5 结论

本文介绍了 LCD MDS 码的几类有效的构造方法, 并对 LCD MDS 码的研究结果和最新进展进行了梳理和总结. 尽管 LCD MDS 码的存在性问题已被完全解决, 但是 LCD MDS 码的显式构造仍值得进一步深入研究. 基于 GRS 码, 我们解决了偶特征有限域上 LCD MDS 码的显式构造问题. 然而, 奇特征有限域上的 LCD MDS 码的显式构造仍未彻底解决. 为此, 如何彻底解决奇特征有限域上 LCD MDS 码的显式构造是一个有趣的研究问题.

致谢 感谢审稿人的评阅和建议.

参考文献

- 1 Massey J L. Reversible codes. *Inform Control*, 1964, 7: 369–380
- 2 Massey J L. Linear codes with complementary duals. *Discrete Math*, 1992, 106–107: 337–342
- 3 Carlet C, Guilley S. Complementary dual codes for counter-measures to side-channel attacks. In: *Coding Theory and Applications*. Cham: Springer, 2015, 97–105
- 4 Carlet C, Guilley S. Complementary dual codes for counter-measures to side-channel attacks. *Adv Math Commun*, 2016, 10: 131–150
- 5 Yang X, Massey J L. The condition for a cyclic code to have a complementary dual. *Discrete Math*, 1994, 126: 391–393
- 6 Li C, Ding C, Li S. LCD cyclic codes over finite fields. *IEEE Trans Inform Theory*, 2017, 63: 4344–4356
- 7 Li S, Li C, Ding C, et al. Two families of LCD BCH codes. *IEEE Trans Inform Theory*, 2017, 63: 5699–5717
- 8 Li S, Ding C, Liu H. A family of reversible BCH codes. *arXiv:1608.02169*, 2016
- 9 Li S, Li C, Ding C, et al. Parameters of two classes of LCD BCH codes. *arXiv:1608.02670*, 2016
- 10 Rao Y, Li R, Lv L, et al. On binary LCD cyclic codes. *Procedia Comput Sci*, 2017, 107: 778–783
- 11 Pang B, Zhu S, Li J. On LCD repeated-root cyclic codes over finite fields. *J Appl Math Comput*, 2018, 56: 625–635
- 12 Liu Y, Li R, Fu Q, et al. Some binary BCH codes with length $n = 2^m + 1$. *Finite Fields Appl*, 2019, 55: 109–133
- 13 Liu Y, Li R, Guo L, et al. Dimensions of nonbinary antiprimitive BCH codes and some conjectures. *arXiv:1712.06842*, 2017
- 14 Huang X, Yue Q, Wu Y, et al. Binary primitive LCD BCH codes. *Des Codes Cryptogr*, 2020, 88: 2453–2473
- 15 Li F, Yue Q, Wu Y. Designed distances and parameters of new LCD BCH codes over finite fields. *Cryptogr Commun*, 2020, 12: 147–163
- 16 Güneri C, Özkaya B, Solé P. Quasi-cyclic complementary dual codes. *Finite Fields Appl*, 2016, 42: 67–80
- 17 Güneri C, Özbudak F, Özkaya B, et al. Structure and performance of generalized quasi-cyclic codes. *Finite Fields Appl*, 2017, 47: 183–202
- 18 Pang B, Zhu S, Sun Z. On LCD negacyclic codes over finite fields. *J Syst Sci Complex*, 2018, 31: 1065–1077
- 19 Wu Y, Yue Q. Factorizations of binomial polynomials and enumerations of LCD and self-dual constacyclic codes. *IEEE Trans Inform Theory*, 2018, 65: 1740–1751
- 20 Shi Z, Fu F W. The primitive idempotents of irreducible constacyclic codes and LCD cyclic codes. *Cryptogr Commun*, 2020, 12: 29–52
- 21 Carlet C, Mesnager S, Tang C, et al. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. *IEEE Trans Inform Theory*, 2018, 64: 3010–3017
- 22 Zhou Z, Li X, Tang C, et al. Binary LCD codes and self-orthogonal codes from a generic construction. *IEEE Trans Inform Theory*, 2019, 65: 16–27
- 23 Galindo C, Geil O, Hernando F, et al. New binary and ternary LCD codes. *IEEE Trans Inform Theory*, 2019, 65: 1008–1016
- 24 Kandasamy W V, Smarandache F, Sujatha R, et al. *Erasure Techniques in MRD Codes*. Ohio: Zip Publishing, 2012
- 25 Liu X, Liu H. Matrix-product complementary dual codes. *arXiv:1604.03774*, 2016
- 26 Mesnager S, Tang C, Qi Y. Complementary dual algebraic geometry codes. *IEEE Trans Inform Theory*, 2018, 64: 2390–2397
- 27 Roy S, Bagchi S. On maximum distance separable group codes with complementary duals. *arXiv:1801.00961*, 2018
- 28 López H H, Manganiello F, Matthews G L. Affine Cartesian codes with complementary duals. *Finite Fields Appl*, 2019, 57: 13–28
- 29 Boonniyom K, Jitman S. Complementary dual subfield linear codes over finite fields. *arXiv:1605.06827*, 2016
- 30 Li C. Hermitian LCD codes from cyclic codes. *Des Codes Cryptogr*, 2018, 86: 2261–2278
- 31 Tzeng K, Hartmann C. On the minimum distance of certain reversible cyclic codes (Corresp.). *IEEE Trans Inform Theory*, 1970, 16: 644–646
- 32 Sendrier N. Linear codes with complementary duals meet the Gilbert-Varshamov bound. *Discrete Math*, 2004, 285: 345–347
- 33 Dougherty S T, Kim J L, Ozkaya B, et al. The combinatorics of LCD codes: Linear programming bound and orthogonal matrices. *Internat J Inform Coding Theory*, 2017, 4: 116–128
- 34 Jin L, Xing C. Algebraic geometry codes with complementary duals exceed the asymptotic Gilbert-Varshamov bound. *IEEE Trans Inform Theory*, 2018, 64: 6277–6282
- 35 Galvez L, Kim J L, Lee N, et al. Some bounds on binary LCD codes. *Cryptogr Commun*, 2018, 10: 719–728
- 36 Pang B, Zhu S, Kai X. Some new bounds on LCD codes over finite fields. *Cryptogr Commun*, 2020, 12: 743–755

- 37 Jin L, Ling S, Luo J, et al. Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. *IEEE Trans Inform Theory*, 2010, 56: 4735–4740
- 38 Carlet C, Mesnager S, Tang C, et al. Euclidean and Hermitian LCD MDS codes. *Des Codes Cryptogr*, 2018, 86: 2605–2618
- 39 Jin L. Construction of MDS codes with complementary duals. *IEEE Trans Inform Theory*, 2016, 63: 2843–2847
- 40 Beelen P, Jin L. Explicit MDS codes with complementary duals. *IEEE Trans Inform Theory*, 2018, 64: 7188–7193
- 41 Chen B, Liu H. New constructions of MDS codes with complementary duals. *IEEE Trans Inform Theory*, 2018, 64: 5776–5782
- 42 Shi X, Yue Q, Yang S. New LCD MDS codes constructed from generalized Reed-Solomon codes. *J Algebra Appl*, 2019, 18: 1950150
- 43 Dinh H Q. Repeated-root cyclic and negacyclic codes of length $6p^s$. *Contemp Math*, 2014, 609: 69–87
- 44 Koroglu M, Sari M. On MDS negacyclic LCD codes. *Flomat*, 2019, 33: 1–12
- 45 Qian J, Zhang L. On MDS linear complementary dual codes and entanglement-assisted quantum codes. *Des Codes Cryptogr*, 2018, 86: 1565–1572
- 46 Fu Q, Li R H, Guo L B. LCD MDS codes from cyclic codes. *Procedia Comput Sci*, 2019, 154: 663–668
- 47 Liu H, Liu S. New constructions of MDS twisted Reed-Solomon codes and LCD MDS codes. *arXiv:2008.03708*, 2020
- 48 Ball S. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J Eur Math Soc (JEMS)*, 2012, 4: 733–748
- 49 Reed I S, Solomon G. Polynomial codes over certain finite fields. *J Soc Indust Appl Math*, 1960, 8: 300–304
- 50 Ling S, Xing C. *Coding Theory: A First Course*. Cambridge: Cambridge University Press, 2003
- 51 MacWilliams F J, Sloane N J A. *The Theory of Error-Correcting Codes*. Amsterdam: Elsevier, 1977
- 52 Stichtenoth H. *Algebraic Function Fields and Codes*. Graduate Texts in Mathematics, vol. 254. New York: Springer, 2009
- 53 Lidl R, Niederreiter H. *Finite Fields*. Cambridge: Cambridge University Press, 1993
- 54 Beelen P, Puchinger S, né Nielsen J R. Twisted Reed-Solomon codes. In: *2017 IEEE International Symposium on Information Theory (ISIT)*. Aachen: IEEE, 2017, 336–340
- 55 Beelen P, Bossert M, Puchinger S, et al. Structural properties of twisted Reed-Solomon codes with applications to cryptography. In: *2018 IEEE International Symposium on Information Theory (ISIT)*. Aachen: IEEE, 2018, 946–950
- 56 Krishna A, Sarwate D V. Pseudocyclic maximum-distance-separable codes. *IEEE Trans Inform Theory*, 1990, 36: 880–884

Several constructions of LCD MDS codes

Lingfei Jin, Zhonghua Sun & Jiaming Teng

Abstract Linear complementary dual codes (LCD codes) have been widely studied because of their significant role in data storage and cryptography. Maximum distance separable codes with complimentary duals (LCD MDS codes) have the greatest error correcting ability, and so the construction of LCD MDS codes is a hot topic. By using the generator matrix of linear codes, the existence results of LCD MDS codes are given by Carlet et al. in 2018. Recently, several display constructions of LCD MDS codes are given by scholars via the generalized Reed-Solomon codes, the algebraic geometry codes, the constacyclic codes and so on. In this paper, we will introduce the main methods, results and recent progress of constructing LCD MDS codes.

Keywords linear complementary dual code, MDS code, Reed-Solomon code

MSC(2020) 81P45, 11B75, 11T71

doi: 10.1360/SSM-2020-0351