从有理函数域显式构造MDS循环码

Shu Liu、Jiang Li 和 Wenqi Huang

arXiv:2611.32165v1 [cs.IT] 24 Nov 2026

摘要

我们提出了一种基于有理函数域构造 $\mathbb{F}_q$ 上最大距离可分（MDS）循环码的统一方法。求值点在一个循环自同构群作用下构成单一轨道，且定义除子在该群作用下保持不变。我们推广了关于码长 n 满足 $n \mid (q-1)$、$n = p$ 或 $n \mid (q+1)$ 的经典存在性结果，其中 $p = \mathrm{char}(\mathbb{F}_q)$。对于 $q+1$ 的奇因子 n，我们利用 $n < q+1$ 的第二个有理点轨道以及针对 $n = q+1$ 的对偶性，构造了每个偶数维数 $2 \le k \le n-1$ 的码。最后，我们利用 $x^n - 1$ 的重根分解，直接证明了这一经典结果：当 $p \mid n$ 且 $n \neq p$ 时，不存在码长为 n 的非平凡 MDS 循环码。

1 引言

最大距离可分（MDS）码是编码理论中的核心主题，因为它们达到了Singleton界，从而为给定的码长和维数提供了可能的最大最小距离。确定MDS码的可能参数并发展显式构造，是编码理论中的重要课题。MDS码最重要的开放问题之一是MDS码的主要猜想，该猜想表述如下：对于每个线性 $[n,k]_q$ MDS码，若定义在 $\mathbb{F}_q$ 上且 $1 < k < q$，则 $n \le q+1$；但当 q 为偶数且 $k = 3$ 或 $k = q-1$ 时除外，在这些情况下 $n \le q+2$。

循环码由于其循环结构以及高效的编码和译码算法，构成了线性码中的一个重要类别。例如，设 α 生成 $\mathbb{F}_q^{\times}$。对于$1 \le k \le q-1$，在有序点1、α、……、α^{q-2} 处对次数小于 k 的多项式求值，可得到一个同时具有循环性和MDS性质的Reed–Solomon（RS）码。我们将具有这两个性质的码称为MDS 循环码。核心问题是确定对于哪些码长 n和维数 k，在 $\mathbb{F}_q$上存在MDS 循环码，以及如何显式构造这类码。

维数为 k 的线性码是 MDS 码，当且仅当生成矩阵的任意 k 列均线性无关。循环码在循环移位一个坐标后保持不变。Cabaña 等人 [1, 第 2] 节利用自同构轨道构造了循环代数几何码。在其循环性判据的基础上，我们针对三种经典长度情形，给出了有理函数域上 MDS 循环码的统一构造。

1.1 已知结果

设 $q = p^s$，其中 p为素数。 $[n, k, d]_q$码是一个 $\mathbb{F}_q$-线性码，其码长为 n、维数为k、最小距离为 d。对于每个 $n \geq 2$，重复码、单奇偶校验码和全空间 $\mathbb{F}_q^n$ 分别是维数为 1、 $n-1$ 和 n 的 MDS 循环码。当 $2 \leq k \leq n-2$ 时，我们称 MDS 循环码为非平凡的。

在码长可被 p整除的情形中，只有 $n = p$ 能够支撑非平凡的MDS循环码 [10,14]。当码长为 p时，对于所有 $1 \leq k \leq p$ [10]都存在MDS 循环码。由于 $p \mid q$，当且仅当 $[q, k]_q$存在一个维数为 $2 \leq k \leq q-2$ 的MDS循环码。Roth和Seroussi [11]证明了每个这样的码都与扩展RS码置换等价。

对于与 p互素的码长，我们考虑两种经典情形。若 $n \mid (q-1)$，则对次数小于 k 的多项式在某个阶为 n 的元素的连续幂处求值，对于每个 $1 \leq k \leq n$ [1, 8]都得到一个循环RS码。若 $n \mid (q+1)$，则在Krishna和Sarwate关于模 $x^n - a$ [5] 的MDS伪循环码的结果中令 $a = 1$，可得如下判据：当且仅当 n和 k中至少有一个为奇数时，存在一个码长为 $[n, k]_q$、维数为 $2 \leq k \leq n-2$ 的MDS循环码。在码长为 $q+1$时，MacWilliams和Sloane [8] 为偶数 q的每个维数构造了码，而Georgiades [2] 排除了奇数 q下的非平凡偶数维数。

表1 总结了关于 $n \geq 4$ 的这些结果。

码长	域大小	已知结果	参考文献
$n \mid (q-1)$	任意 q	始终存在	[8]
$n = q$	$q = p^s$	当且仅当 $q = p$时存在	[11]
$p \mid n, \quad n \neq p$	$q = p^s$	None	[10, 14]
$n = p$	$q = p^s$	所有可容许的 k	[10]
$n \mid (q+1)$	$q = 2^s$	始终存在	[5, 8]
$n \mid (q+1)$	q 为奇数	当且仅当 n或 k 为奇数时存在	[5]

表1：非平凡MDS循环码的已知结果（$2 \leq k \leq n-2$）

表 1 [9], 之外，特定参数下的MDS 循环码也已有研究，近期的构造还包括非RS型码 [6, 13]。我们通过自同构对有理点的作用，重新考察经典的长度情形。

1.2 我们的贡献

定理 3.1 给出了一个统一构造：取 $\mathrm{Aut}(\mathbb{F}_q(x)/\mathbb{F}_q)$ 中一个阶为 $n > 1$ 的循环子群作用下的有理点满轨道。我们按轨道序评估 $\mathcal{L}(A)$，其中 A 是一个支撑与该轨道不相交且满足 $0 \leq \deg(A) < n$ 的不变除子。由此得到的 $[n, \deg(A)+1, n-\deg(A)]_q$ MDS循环码的码长由该轨道决定，而维数由 $\deg(A)$ 决定。

对于 $n \mid (q-1)$ 和 $n = p$的乘法作用与加法作用，二者都固定无穷远处的有理位 P_∞。因此，取 $A = mP_\infty$ 且满足 $0 \leq m < n$，即可得到$[n, m+1, n-m]_q$每个维数下的 MDS 循环码 $1 \leq k \leq n$（推论3.2和3.4）。

对于 $n \mid (q+1)$，该循环子群固定一个次数为二的位点 Q。除子 $A = mQ$ 满足 $0 \le 2m < n$ 时，可得到所有奇数维数下的 $[n, 2m+1, n-2m]_q$MDS循环码（推论 3.6）。当 $n > 1$ 是 $q+1$ 的奇真因子时，另一个有理点轨道与求值轨道不相交。令 D' 为该轨道上各位点之和。不变除子 $D' - mQ$ 的奇数次数为 $n-2m$，并且当 $0 < 2m < n$ 时，可得到偶数维数的 $[n, n-2m+1, 2m]_q$MDS循环码（推论 3.7）。当 $n = q+1$ 为奇数时，求值轨道包含所有有理点。通过取维数为 $n-k$ 的码的对偶码，可得到每个偶数维数 $2 \le k \le n-1$。表 2 总结了 $n > 1$ 可达到的维数，并将其与表 1 中的经典存在性结果联系起来。

码长 n	**维数** k	**与先前结果的关系**
$n \mid (q-1)$	所有 k、 $1 \le k \le n$	[8]
$n = p$	所有 k、 $1 \le k \le p$	[10]
偶数 n、 $n \mid (q+1)$	所有奇数 k、 $1 \le k \le n-1$	[5]
$n \mid (q+1)$ 奇数 $1 < n < q+1$	所有 k、 $1 \le k \le n$	[5]
$n = q+1$，奇数	全部 k（k 偶数，由对偶性）	[5, 8]

表 2：基于轨道的构造

在定理 4.1中，我们利用 $x^n - 1$ 的重根分解，直接证明了这一经典结果：当 n 且 $p \mid n$和 $n \ne p$ [10, 14]时，不存在码长为 n 的非平凡 MDS 循环码。因此，推论 4.2 排除了偶数 $q > 2$时码长为 $q+2$ 的非平凡 MDS 循环码。

不存在定理以及推论 p 中的码长构造 3.4解决了 $p \mid n$的情形。这留下了以下关于与 q 互素的码长的一般存在性问题。

开放问题1.1。 确定对于任意码长 n （与 q 互素，但既不整除 $q-1$，也不整除 $q+1$），非平凡 *MDS* 循环码存在或不存在的条件。

1.3 论文结构

本文其余部分的组织如下。第2 节回顾循环码、代数函数域、代数几何码以及有理函数域的自同构群等背景知识。第3节建立统一轨道构造，并将其应用于三种码长情形 $n \mid (q-1)$、 $n = p$和 $n \mid (q+1)$。第4 节给出码长被特征整除时的不存在性结果，并给出码长为 $q+2$ 且定义在偶特征域上的推论。

2 预备知识

本节将介绍有限域上的MDS码、循环码和全局函数域的背景知识。关于函数域和代数几何码的更详细讨论，请参阅 [12]。

设 $\mathbb{F}_q$ 是一个含有 q 个元素的有限域，其中 q 是素数 p的幂， $\mathbb{F}_q^\times$ 是其乘法群。$[n,k,d]_q$ 上的一个 $\mathcal{C}$ 线性码 $\mathbb{F}_q$ 是 $\mathbb{F}_q^n$ 的一个 k 维线性子空间，其最小汉明距离为 d。

2.1 MDS码

若一个 $[n,k,d]_q$ 线性码 $\mathcal{C}$ 的参数达到 Singleton界 $d \leq n-k+1$，即 $d = n-k+1$，则称其为最大距离可分（MDS）码。MDS码的主要猜想指出：对于每个定义在 $\mathbb{F}_q$ 上的线性 $[n,k]_q$ MDS码，若 $1 < k < q$，则$n \leq q+1$；但当 q 为偶数且 $k = 3$ 或 $k = q-1$ 时， $n \leq q+2$。

2.2 循环码

若 $[n,k]_q$ 线性码 $\mathcal{C}$ 定义在 $\mathbb{F}_q$ 上，且对于码字 $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$，有 $\mathbf{c}' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$，则称该码为循环码，其中 $\mathbf{c}'$ 是 $\mathbf{c}$ 的坐标的循环移位。设 $\mathbb{F}_q[x]$ 为 $\mathbb{F}_q$ 上的多项式环， $\mathbb{F}_q[x]/\langle x^n-1\rangle$ 为将$\mathbb{F}_q[x]$ 模 x^n-1所得的剩余类环。通过将码字 $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ 与 $c(x)$对应起来，可以在 $\mathbb{F}_q[x]/\langle x^n-1\rangle$ 中研究循环码 $\mathcal{C}$ 。根据循环码的定义，循环码 $\mathcal{C}$ 在 $\mathbb{F}_q[x]/\langle x^n-1\rangle$中构成一个理想。注意， $\mathbb{F}_q[x]/\langle x^n-1\rangle$ 中的每个理想都是主理想，因此存在一个首一多项式$g(x) \in \mathbb{F}_q[x]/\langle x^n-1\rangle$ 生成 $\mathcal{C}$，且 $g(x)$是 x^n-1的除子。多项式 $g(x)$称为 $\mathcal{C}$的生成多项式。

2.3 函数域的一般背景

对于素数幂 q，令 $\mathbb{F}_q$ 表示含有 q 个元素的有限域。关于 $\mathbb{F}_q$ 的一元代数函数域是一个域扩张 $F \supseteq \mathbb{F}_q$，其中 F 是 $\mathbb{F}_q(x)$ 的有限代数扩张；这里的 $x \in F$ 是关于 $\mathbb{F}_q$的超越元。如果 $\mathbb{F}_q$ 在 F 中的代数闭包恰好是 $\mathbb{F}_q$，则称 $\mathbb{F}_q$ 为 F 的完全常数域。这样的域称为全局函数域。从此以后，我们用 $F/\mathbb{F}_q$ 表示一个函数域 F，其完全常数域为 $\mathbb{F}_q$。

$F/\mathbb{F}_q$ 上的离散赋值是从 F 到 $\mathbb{Z} \cup \{+\infty\}$ 的映射，并满足某些性质（见 [12, 定义 1.1。9]）。对于 $F/\mathbb{F}_q$上的每个离散赋值 ν，都有一个与之对应的赋值环 $O = \{f \in F : \nu(f) \geq 0\}$，它是一个局部环。$O$ 的极大理想 P定义为 $P = \{f \in F : \nu(f) > 0\}$，称为一个位点。与 P 相关联的赋值 ν 和局部环 O 分别记为 ν_P 和 O_P。剩余类域 O_P/P记为 F_P，是 $\mathbb{F}_q$的有限扩张。扩张次数 $[F_P : \mathbb{F}_q]$ 称为 P的次数，记为 deg(P)。次数为一的位点称为有理位。

令 $\mathbb{P}_F$ 表示 F 的位点集。除子群记为 Div(F)，它是由 $\mathbb{P}_F$ 中所有位点生成的自由阿贝尔群。除子 $G \in \in$Div(F) 是形如 $G = \sum_{P \in \mathbb{P}_F} n_P P$ 的形式和，其中仅有有限多个系数 $n_P \in \mathbb{Z}$ 非零。G 的次数定义为 deg(G) $= \sum_{P \in \mathbb{P}_F} n_P$deg($P$)。$G$ 的支撑记为 supp(G)，定义为 $\{P \in \mathbb{P}_F : n_P \neq 0\}$，它是 $\mathbb{P}_F$ 的有限子集。对于任意非零元素 $f \in F$， f 的零除子定义为 $(f)_0 = \sum_{P \in \mathbb{P}_F,\ \nu_P(f) > 0} \nu_P(f) P$，而极点

f 的除子定义为 $(f)_\infty = \sum_{P\in\mathbb{P}_F,\ \nu_P(f)<0} -\nu_P(f)P$。于是，$f$ 的主除子为 $(f) = (f)_0 - (f)_\infty = \sum_{P\in\mathbb{P}_F} \nu_P(f)P$。

对于任意除子 $G \in \mathrm{Div}(F)$，与 G 关联的黎曼–罗赫空间定义为

$$\mathcal{L}(G) = \{f \in F \setminus \{0\} : (f) \geq -G\} \cup \{0\}.$$

它是一个关于 $\mathbb{F}_q$ 的有限维向量空间，其维数记为 $\ell(G)$。根据黎曼定理 [12, Theorem 1.4.17]，$\ell(G) \geq \deg(G) - g + 1$。此外，若 $\deg(G) < 0$，则 $\ell(G) = 0$；若 $\deg(G) \geq 2g-1$，则 $\ell(G) = \deg(G) - g + 1$。

假设 F'/F 是一个常数域为 $\mathbb{F}_q$ 的有限代数扩张。若位点 $P' \in \mathbb{P}_{F'}$ 位于位点 $P \in \mathbb{P}_F$ 之上，记作 $P' \mid P$，则称 $P' \in \mathbb{P}_{F'}$ 位于 $P \in \mathbb{P}_F$ 之上，当且仅当 $P \subseteq P'$。P' 在 P 之上的分歧指数记为 $e(P' \mid P)$。设 $P_1, \ldots, P_m$ 是位于 P 之上的 F' 的所有位点。若对于某个 $P_i \mid P$，有 $e(P_i \mid P) = [F' : F]$，则 $m = 1$，并称 P 在 F' 中完全分歧。若对于每个 $i = 1, \ldots, m$，都有 $e(P_i \mid P) = 1$，则称 P 在 F' 中非分歧。此外，若 $e(P_i \mid P) = 1$ 且 $m = [F' : F]$，则称 P 在 F' 中完全分裂。

2.4 代数几何码

设 $\mathcal{P} = \{P_1, \ldots, P_n\}$ 是函数域 $F/\mathbb{F}_q$ 中一组 n 个互不相同的有理位点，且该函数域的亏格为 g。设 G 是 F 上次数为 $0 \leq \deg(G) < n$ 的除子，满足 $\mathrm{supp}(G) \cap \mathcal{P} = \emptyset$。定义求值映射如下：

$$\mathrm{ev}_{\mathcal{P}} : \mathcal{L}(G) \to \mathbb{F}_q^n, \quad f \mapsto (f(P_1), \ldots, f(P_n)),$$

由于这些 P_i 不在 G 的支撑上，因此该映射定义良好。注意，$\mathrm{ev}_{\mathcal{P}}$ 是一个 $\mathbb{F}_q$-线性映射，其核为 $\ker(\mathrm{ev}_{\mathcal{P}}) = \mathcal{L}(G - \sum_{i=1}^n P_i)$。由于 $\deg(G) < n$，$\mathrm{ev}_{\mathcal{P}}$ 是单射。于是，与 $\mathcal{P}$ 和 G 关联的代数几何码定义为

$$C_{\mathcal{L}}(\mathcal{P}, G) := \mathrm{ev}_{\mathcal{P}}(\mathcal{L}(G)) = \{(f(P_1), f(P_2), \ldots, f(P_n)) : f \in \mathcal{L}(G)\},$$

这是一个 $[n, k, d]$-线性码，其维数为 $k = \ell(G)$，最小距离为 $d \geq n - \deg(G)$，如 [12, 定理 2.2.2] 所示。

Reed–Solomon码可以在基于有理函数域的代数几何码框架内实现。设 $F = \mathbb{F}_q(x)$ 是一个有理函数域。设 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 是 $\mathbb{F}_q$ 中 n 个互不相同的元素。记 P_i 为 $x - \alpha_i$ 对于 $1 \leq i \leq n$ 的唯一零点，并定义 $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$。设 P_∞ 为 x 的唯一极点，并定义 $G = (k-1)P_\infty$。黎曼–罗赫空间 $\mathcal{L}(G)$ 是由次数小于 k 的多项式构成的 $\mathbb{F}_q$-空间。根据定义，有

$$\begin{aligned} C_{\mathcal{L}}(\mathcal{P}, G) &= \{(f(P_1), f(P_2), \ldots, f(P_n)) : f \in \mathcal{L}(G)\} \\ &= \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) \leq k-1\}. \end{aligned}$$

2.5 有理函数域的自同构

设 $F = \mathbb{F}_q(x)$ 是超越元 $x \in F$ 上的有限域 $\mathbb{F}_q$ 的有理函数域。那么，自同构 $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ 由 $\sigma(x)$ 唯一确定。众所周知，每个自同构 $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ 都可表示为

$$\sigma(x) = \frac{ax + b}{cx + d}, \tag{1}$$

其中 a，b，c，$d \in \mathbb{F}_q$ 以及 $ad-bc \neq 0$ (见 [3])。记 $\mathrm{GL}_2(q)$ 为 2×2 上的可逆矩阵的一般线性群 $\mathbb{F}_q$。因此，每个矩阵

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(q)$$

按照(1)定义，诱导出 F 的一个自同构。$\mathrm{GL}_2(q)$中的两个矩阵诱导出 F 的同一个自同构，当且仅当它们属于 $Z(\mathrm{GL}_2(q))$的同一个陪集，其中$Z(\mathrm{GL}_2(q))$表示$\mathrm{GL}_2(q)$的中心 $\{aI_2 : a \in \mathbb{F}_q^*\}$。这意味着，$\mathrm{Aut}(F/\mathbb{F}_q)$同构于射影线性群$\mathrm{PGL}_2(q) := \mathrm{GL}_2(q)/Z(\mathrm{GL}_2(q))$。因此，我们可以将$\mathrm{Aut}(F/\mathbb{F}_q)$与$\mathrm{PGL}_2(q)$等同起来。

现在，我们考虑$\mathrm{PGL}_2(q)$的以下两个子群:

(1) **仿射线性群** $\mathrm{AGL}_2(q)$:

$$\mathrm{AGL}_2(q) := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}.$$

每个元素

$$A=\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{AGL}_2(q)$$

定义了一个仿射自同构 $\sigma(x) = ax+b$。

(2) **阶为** $q+1$的循环子群：令 $P(x) = x^2+ax+b$为 $\mathbb{F}_q[x]$上的一个本原多项式。考虑元素

$$\sigma=\begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \in \mathrm{PGL}_2(q). \tag{2}$$

σ 的阶为 $q+1$ （见 [4, 引理 5.1]）。因此，$\langle\sigma\rangle$ 诱导出 $\mathrm{Aut}(F/\mathbb{F}_q)$ 的一个 $q+1$阶循环子群。

对于 $\mathrm{Aut}(F/\mathbb{F}_q)$ 的每个元素 $\sigma \in$ ，令 F^σ 表示子群 $\langle\sigma\rangle$的不动域，即 $F^\sigma = \{f \in F: \sigma(f) = f\}$。根据伽罗瓦理论，如果 σ的阶为 s，则 F/F^σ是次数为 s的伽罗瓦扩张，且 $\mathrm{Gal}(F/F^\sigma) = \langle\sigma\rangle$。现在我们介绍扩张 F/F^σ的一些性质，如 [4, 命题 4.2、命题 5.2] 和 [7, 引理 4.2],中所述；这些性质将在下一节中发挥重要作用。这些结果分别对应于三类阶为 $q-1$、 p和 $q+1$的循环子群。

我们首先考虑乘法自同构 $\sigma(x) = \gamma x$。

引理 2.1。设 γ 是 $\mathbb{F}_q^*$ 的本原元，且 $\sigma(x) = \gamma x$。则 $\mathrm{ord}(\sigma) = q-1$，并且有以下性质:

(i) $[F: F^\sigma] = q-1$ 以及 $F^\sigma = \mathbb{F}_q(z)$，其中 $z = x^{q-1}$。

(ii) P_∞ 是 x 的唯一极点，并且在 F/F^σ 中完全分歧。

(iii) Q 是 $z-1$ 在 F^σ 中的唯一零点，并且在 F/F^σ 中完全分裂。此外， F 中位于 Q 之上的有理点为

$$\{P_\gamma, \ldots, P_{\gamma^{q-1}}\},$$

其中， P_{γ^i} 表示当 $i=1$、.....、 $q-1$ 时 $x-\gamma^i$ 的唯一零点。

我们考虑加法自同构 $\sigma(x) = x + 1$，它生成一个阶为 p 的循环子群。与乘法情形一样，该自同构固定极点 P_∞，并具有一个有理点的满轨道，如下述引理所述。

引理 2.2。设 $p = \mathrm{char}(\mathbb{F}_q)$，且 $\sigma(x) = x + 1$。则 σ 的阶为 p，并且满足以下性质：

(i) $[F : F^\sigma] = p$ *and* $F^\sigma = \mathbb{F}_q(z)$ *with* $z = x^p - x$.

(ii) x 的唯一极点 P_∞ 在 F/F^σ中完全分歧。

(iii) F^σ 中 z的唯一零点 Q在 F/F^σ中完全分裂。此外， F 中位于 Q上方的有理点为

$$\{P_0, P_1, \ldots, P_{p-1}\},$$

其中， P_i表示当 $i = 0$时 $x - i$ 的唯一零点，1,. . ., $p - 1$。

接下来讨论一个阶为 $q + 1$ 的循环子群。与前两种情况不同，该子群没有不动有理点，而是不动一个二次点。此外，它在 F 的有理点上具有传递作用。以下引理陈述了这些性质。

引理 2.3。设 $P(x)$ 是 $\mathbb{F}_q[x]$ 中的一个本原二次多项式，且 σ 是一个如方程 (2)所定义的自同构。则 $\mathrm{ord}(\sigma) = q + 1$，并且满足以下性质：

(i) $[F\colon F^\sigma] = q + 1$和 $F^\sigma = \mathbb{F}_q(z)$满足 $z = \frac{u(x)}{x^q - x}$，其中某个次数为$q + 1$的 $u(x) \in \mathbb{F}_q[x]$。(ii) 与不可约多项式 $x^2 P(1/x)$ 对应的二次位点 R 在 $F/F^{\langle\sigma\rangle}$中完全分歧。$(iii)$ z在 F^σ 中的唯一极点 Q_∞在 F/F^σ中完全分裂。此外， F 的所有有理位都位于 F^σ中的 Q_∞ 之上。

3 从有理函数域构造的MDS循环码

本节将建立一个统一的函数域框架，用于构造三族 MDS 循环码。设 $F = \mathbb{F}_q(x)$，使得 $\mathrm{Aut}(F/\mathbb{F}_q) \cong \mathrm{PGL}_2(q)$。在每种构造中，求值点在 $\mathrm{Aut}(F/\mathbb{F}_q)$ 的某个循环子群作用下构成单一轨道，而定义相应黎曼–罗赫空间的除子在该子群作用下保持不变。随后，我们将这一框架应用于 $\mathrm{Aut}(F/\mathbb{F}_q)$ 的三个循环子群，分别对应 $n \mid (q-1)$、 $n = p$ 和 $n \mid (q+1)$ 这几种情形。

3.1 统一轨道构造

定理 3.1。 设 $F = \mathbb{F}_q(x)$，并设 $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ 的阶为 $n > 1$。设 P 是一个有理位，其 $\langle\sigma\rangle$- 轨道长度为 n，并令

$$P_i := \sigma^{-i}(P), \qquad D := \sum_{i=0}^{n-1} P_i.$$

设 A 是满足以下条件的 σ-不变除子

$$\mathrm{supp}(A) \cap \mathrm{supp}(D) = \emptyset, \qquad 0 \le \deg(A) < n.$$

则码

$$C_{\mathcal{L}}(D, A)$$

当其坐标由 P_0、P_1、…、P_{n-1} 编号时，是一个 $[n, \deg(A)+1, n-\deg(A)]_q$ *MDS*循环码。

证明。 由于 F 的亏格为零且 $0 \le \deg(A) < n$，代数几何码的标准参数界给出 $\dim C_{\mathcal{L}}(D, A) = \ell(A) = \deg(A) + 1$，并且

$$d\big(C_{\mathcal{L}}(D, A)\big) \ge n - \deg(A).$$

另一方面，Singleton界给出

$$d\big(C_{\mathcal{L}}(D, A)\big) \le n - (\deg(A) + 1) + 1 = n - \deg(A).$$

因此 $d\big(C_{\mathcal{L}}(D, A)\big) = n - \deg(A)$，所以 $C_{\mathcal{L}}(D, A)$ 是 MDS。

关于循环性，我们使用 Cabaña 等人的自同构判据。 [1, 第 2] 节。由于$\sigma(A) = A$, 黎曼–罗赫空间 $\mathcal{L}(A)$ 是 σ-不变的。此外， $P_i = \sigma(P_{i+1})$，因此 $(\sigma f)(P_i) = f(P_{i+1})$ 对每个 $f \in \mathcal{L}(A)$都成立，其中指标按模 n取值。因此，

$$\big((\sigma f)(P_0), \dots, (\sigma f)(P_{n-1})\big) = \big(f(P_1), \dots, f(P_{n-1}), f(P_0)\big),$$

因此 $C_{\mathcal{L}}(D, A)$ 是循环的。 □

定理 3.1 将 MDS 循环码的构造归结为寻找一个完整的有理轨道以及一个合适的不变除子。现在，我们将这一结果应用于下文讨论的三种长度情形。

3.2 情形 $n \mid (q-1)$

设 $n > 1$ 是 $q-1$的一个除子，并取一个 $\alpha \in \mathbb{F}_q^{\times}$，其乘法阶为 n。那么

$$\sigma(x) = \alpha x$$

定义了一个阶为 n的 F 自同构。零点位 P_0 和极点 P_∞均由 $G := \langle\sigma\rangle$固定。对于任意 $\beta \in \mathbb{F}_q^{\times}$，令 P_β 表示对应于 $x - \beta$零点的有理位。由于 $\sigma^{-i}(P_\beta) = P_{\alpha^i\beta}$， P_β 的 G-轨道为

$$P_\beta, P_{\alpha\beta}, \dots, P_{\alpha^{n-1}\beta}.$$

由于 $\beta \neq 0$ 和 α 的乘法阶为 n，这些位点两两不同。令

$$D := \sum_{i=0}^{n-1} P_{\alpha^i\beta}.$$

推论 3.2。 对于每个整数 $0 \le m < n$，该码

$$C(m) := C_{\mathcal{L}}(D, mP_\infty)$$

是一个 $[n, m+1, n-m]_q$ *MDS*循环码。

证明。 应用定理 3.1 并取 $A = mP_\infty$。 □

注记 3.3。 推论*3.2*中构造的 *MDS* 循环码涵盖了长度为 $n \mid (q-1)$ 的经典 *Reed–Solomon*码 *[8]*。由于 $\mathcal{L}(mP_\infty) = \mathbb{F}_q[x]_{\le m}$，码$C(m)$恰好是通过在乘法陪集 $\beta\langle\alpha\rangle$上对次数不超过 m 的多项式求值而得到的 *Reed–Solomon*码。从函数域视角看，其循环移位由自同构 $x \mapsto \alpha x$诱导。

3.3 n = p 的情形

设 $p =$ 的特征为 $\mathbb{F}_q$，并选取 $b \in \mathbb{F}_q^\times$。则

$$\sigma(x) = x + b$$

定义了一个阶为 p 的 F 自同构。极点 P_∞ 在 σ 作用下保持不变，而每个有限有理点在 $\langle\sigma\rangle$ 作用下都有一个满轨道。对于任意 $\beta \in \mathbb{F}_q$，由于 $\sigma^{-i}(P_\beta) = P_{\beta+ib}$，$P_\beta$ 的轨道为

$$P_\beta, P_{\beta+b}, \ldots, P_{\beta+(p-1)b}.$$

Set

$$D := \sum_{i=0}^{p-1} P_{\beta+ib}.$$

推论 3.4. 对于每个整数 $0 \le m < p$，码

$$C(m) := C_{\mathcal{L}}(D, mP_\infty)$$

是一个 $[p, m+1, p-m]_q$ *MDS*循环码。

证明. 应用定理 3.1 取 $A = mP_\infty$。 □

注记 3.5. 若 $W \subseteq \mathbb{F}_q$ 是一个 r维的 $\mathbb{F}_p$子空间，则

$$G_W := \{x \mapsto x + w : w \in W\}$$

是一个阶为 p^r 的初等阿贝尔群，因此仅当 $r = 1$ 时才是循环群。因此，由这些自同构得到的循环码的码长为 p，而非任意整除 q 的码长。特别地，当 $q = p$ 时，这一构造涵盖了 *Roth* 和 *Seroussi* *[11]* 所确立的码长为 q 的 *MDS* 循环码的存在性。更一般地，对于 $q = p^s$，它给出了 $\mathbb{F}_q$ 上码长为 p 的 *MDS* 循环码，这与关于码长可被特征 *[14]* 整除时的限制相符。

3.4 $n \mid (q+1)$ 的情形

设 $n > 1$ 是 $q+1$ 的一个除子，且 $h(T) = T^2 + aT + b \in \mathbb{F}_q[T]$ 是一个二次本原多项式。特别地，$h(T)$ 不可约，且 $b \neq 0$。射影矩阵

$$A = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$$

在 $\mathrm{PGL}_2(q)$ 中的阶为 $q+1$，并诱导自同构

$$\tau(x) = \frac{1}{-bx - a}$$

F。令

$$\sigma := \tau^{(q+1)/n}, \qquad G := \langle \sigma \rangle.$$

于是 σ 的阶为 n，因此 G 是阶为 n的循环群。

不动点方程 $\tau(x) = x$ 等价于

$$q_Q(x) := x^2 + \frac{a}{b}x + \frac{1}{b} = 0.$$

由于 $q_Q(x)$ 在 $\mathbb{F}_q$上不可约，因此它定义了一个次数为二的位点 Q。此外，Q 被 τ固定，因而也被 $G = \langle \sigma \rangle$固定（参见 [1, 第 4]节）。根据引理 2.3，群 $\langle \tau \rangle$ 在 $q+1$ 的有理点上 F正则作用。因此，每个有理点都有一个长度为 G的 n轨道。取一个有理点 P，并令

$$P_i := \sigma^{-i}(P), \qquad D := \sum_{i=0}^{n-1} P_i.$$

推论 3.6. 对于满足 $2m < n$ 的每个整数 $m \geq 0$，码

$$C(m) := C_{\mathcal{L}}(D, mQ)$$

是一个 $[n, 2m+1, n-2m]_q$*MDS*循环码。

证明。 应用定理 3.1，取 $A = mQ$。 □

推论 3.6 中的单点除子 mQ 次数为偶数，因此只产生奇数维码。然而，当 $n < q+1$ 时，未使用的有理点提供了第二个不变除子，只要 n 为奇数，就能得到偶数维码。事实上，有理点可分解为 $(q+1)/n$ 个互不相交的 G 轨道，每个轨道长度为 n。因此，我们可以选取一个有理位点 $P' \notin \mathrm{supp}(D)$ 并令

$$P'_i := \sigma^{-i}(P'), \qquad D' := \sum_{i=0}^{n-1} P'_i.$$

那么 D' 是 G-不变的，并且 $\mathrm{supp}(D') \cap \mathrm{supp}(D) = \emptyset$。

推论 3.7。 假设 $n < q+1$ 为奇数。对于每个满足条件的整数 m g

$$0 < 2m < n,$$

该码

$$C'(m) := C_{\mathcal{L}}(D, D' - mQ)$$

是一个

$$[n, n-2m+1, 2m]_q$$

*MDS*循环码。特别地，这些码具有从 2 到 $n-1$的所有偶数维数。

证明。 除子 $A = D' - mQ$ 在 σ作用下保持不变，其支撑与 D不相交，并且

$$\deg(A) = n - 2m, \qquad 0 < \deg(A) < n.$$

因此，结论直接由定理3.1推出。由于 n为奇数，维数$n-2m+1$（其中 $1 \le m \le (n-1)/2$）恰为 $n-1$、$n-3$、.....、2。 □

注 3.8。 推论 *3.6* 和 *3.7* 共同实现了奇数 $n < q+1$的所有维数。当 $n = q+1$ 为奇数时，求值轨道包含所有有理点。对于每个满足 $2 \le k \le n-1$的偶数k，推论 *3.6* 给出一个 $[n, n-k, k+1]_q$*MDS*循环码，因为$n-k$ 为奇数。其对偶码也是一个 $[n, k, n-k+1]_q$ *MDS*循环码。因此，奇数 n的所有维数均可实现。对于偶数 n，推论 *3.6* 实现了所有奇数维数，而经典存在性判据排除了非平凡的偶数维数 *[5]*。

表3 总结了每种码长对应的构造方法和可达到的维数。在推论 3.7中， $k = n-1$ 对应单奇偶校验码；因此，非平凡的偶数维数为 $2 \le k \le n-3$。

码长	自同构	不变除子或方法	维数 k
$n \mid (q-1)$	$\sigma(x) = \alpha x$	mP_∞	$1 \le k \le n$
$n = p$	$\sigma(x) = x + b$	mP_∞	$1 \le k \le p$
$n \mid (q+1)$ 奇数 $1 < n < q+1$	$\sigma = \tau^{(q+1)/n}$	mQ, $D' - mQ$	所有 k, $1 \le k \le n$
$n = q+1$，奇数	$\sigma = \tau$	mQ当 k为奇数时 偶数 k 的对偶性	所有 k, $1 \le k \le n$
$n \mid (q+1)$，偶数	$\sigma = \tau^{(q+1)/n}$	mQ	奇数 k, $1 \le k \le n$

表 3：MDS 循环码的基于轨道的族

4 MDS循环码的不存在性结果

现在我们证明，除码长 p 外，能被特征整除的码长不可能支撑非平凡的 MDS循环码。

定理4.1。 令 $q = p^s$，其中 p =char($\mathbb{F}_q$)。若

$$p \mid n \qquad and \qquad n \neq p,$$

那么不存在码长为 n 的非平凡 q 元 *MDS*循环码。

证明。 令 $n = p^a m$，其中 $a \geq 1$ 且 gcd(p, m) $= 1$，并设 C 是一个生成多项式为 $g(x)$ 的非平凡 MDS循环码。于是

$$d(C) = \deg g + 1. \tag{3}$$

首先假设 $m > 1$。由于

$$x^n - 1 = (x^m - 1)^{p^a}, \qquad x^m - 1 = \prod_{i=1}^{r} f_i(x),$$

其中 f_i's 是互不相同的首一不可约多项式，我们可以写成

$$g(x) = \prod_{i=1}^{r} f_i(x)^{e_i}, \qquad 0 \leq e_i \leq p^a.$$

若某个 $e_i = 0$，令 $g_0 = \prod_{e_i>0} f_i$。由于对每个 i 都有 $e_i \leq p^a$，因此我们有

$$g(x) \mid g_0(x)^{p^a}.$$

此外，由于至少有一个指数 e_i 为零，

$$\deg g_0 < m,$$

因此

$$\deg\left(g_0^{p^a}\right) = p^a \deg g_0 < p^a m = n.$$

因此，多项式 $g_0^{p^a}$ 是 C 的一个非零码字。由于 p^a 是特征的幂，Frobenius恒等式给出

$$\mathrm{wt}(g_0^{p^a}) = \mathrm{wt}(g_0) \leq \deg g_0 + 1.$$

如果某个正整数 e_i 至少为二，那么 deg $g \geq \deg g_0 + 1$，这与（3）矛盾。否则$g \mid x^m - 1$。由于 $\deg(x^m - 1) = m < n$，多项式 $x^m - 1$ 表示 C的一个非零码字。此外，由于 $m > 1$,

$$\mathrm{wt}(x^m - 1) = 2.$$

因此， $d(C) \leq 2$。如果 $\deg g \geq 2$，那么（3）给出 $d(C) \geq 3$，产生矛盾。因此，唯一可能的非平凡生成元次数也被排除，只剩下 $\deg g = 1$，它对应于平凡单奇偶校验码。

因此，我们可以假设每个 $e_i > 0$。令 $t = \max_i e_i$。若 $t < p^a$，则 $(x^m - 1)^t$是一个重量至多为 $t + 1$ 的非零码字，并且

$$d(C) \leq t + 1, \qquad \deg g \geq m + t - 1 \geq t + 1,$$

这又导出了矛盾。若 $t = p^a$，则要么 $g = x^n - 1$，要么 MDS循环码 $C^\perp$ 的生成多项式的指数（经过倒数变换后）为 $p^a - e_i$。在后一种情况下，某个指数为零，且所有指数都小于 p^a。因此，将前面的论证应用于$C^\perp$ 会导出矛盾，除非 $C^\perp$ 是单奇偶校验码；在这个例外情形下， C 是重复码，仍属平凡情形。

剩下的情况是 $m = 1$。于是 $n = p^a$，而 $n \neq p$ 推出 $a \geq 2$。因此，$g = (x-1)^e$。除四种平凡情况 $e \in \{0, 1, n-1, n\}$ 外，假设 $2 \leq e \leq n-2$，并令 $B = n/p = p^{a-1}$。若 $e < B$，由于 B 是 p 的幂，根据 Frobenius恒等式可得 $(x-1)^B = x^B - 1$。码字 $x^B - 1$ 的重量为二。若 $B \leq e \leq n - B$，则$c = \lceil e/B \rceil \leq p - 1$，根据 Frobenius恒等式，码字

$$(x-1)^{cB} = (x^B - 1)^c$$

的重量为 $c + 1$，因为 $c < p$，因此其二项式系数模 p 均非零。此外， $c+1 \leq e$。这两个结论都与 $d(C) = e+1$ 矛盾。最后，若 $e > n-B$，则 $C^\perp$的生成多项式在相差一个非零标量的意义下为 $(x-1)^{n-e}$，且 $2 \leq n - e < B$；将第一种子情况应用于 $C^\perp$ ，便得到最终矛盾。

□

下面的推论讨论偶特征域上的特定码长 $q + 2$ 。

推论4.2。 设 $q = 2^s > 2$。则不存在码长为 $q + 2$的非平凡 q元*MDS*循环码。

证明。 由于 $2 \mid (q + 2)$ 以及 $q + 2 \neq 2$，结论直接由定理 4.1得到。 □

注4.3。 对于偶数 $q > 2$，*MDS*猜想允许码长为$q + 2$ 且维数为 3 和 $q - 1$的线性*MDS*码。推论 *4.2* 排除了在 $\mathbb{F}_q$上任何非平凡*MDS*循环码取此码长的可能性。

参考文献

[1] Gustavo Cabaña、María Chara、Ricardo A. Podestá和Ricardo Toledano。论循环代数几何码。有限域及其应用，82:102064，2022年。

[2] J. Georgiades. 奇数阶 q 且维数为偶数 k 的循环（$q + 1$， k）码并非最优。摩德纳大学数学与物理研讨会纪要，30:284–285，1982。

[3] James WilliamPeterHirschfeld、GáborKorchmáros 和 Fernando Torres。有限域上的代数曲线。普林斯顿应用数学丛书。普林斯顿大学出版社，2008。

[4] Lingfei Jin、Liming Ma 和 Chaoping Xing。通过有理函数域的自同构群构造最优局部可修复码。*IEEE* 信息论汇刊，66(1):210–221，2020。

[5] A. Krishna 和 D. V. Sarwate。伪循环最大距离可分码。*IEEE*信息论汇刊，36(4):880–884，1990年7月。

[6] F. Li、Y. Chen、H. Chen 和 Y. Niu。非Reed-Solomon型循环MDS码。*IEEE*信息论汇刊，71(5)：3489–3496，2025年5月。[7] Songsong Li 和 Chaoping Xing。通过有理函数域的自同构群实现快速傅里叶变换。载于 David P. Woodruff 编，*2024*年*ACM-SIAM*离散算法研讨会论文集，*SODA 2024*，美国弗吉尼亚州亚历山大港，*2024*年*1*月7日至*10*日，第3836–3859页。SIAM，2024年。[8] F. J. MacWilliams 和 N. J. A. Sloane。纠错码理论。North-Holland，荷兰阿姆斯特丹，1983年。[9] T. Maruta。关于循环MDS码和伪循环MDS码的存在性。*Eur. J. Com-binatorics*，19(2)：159–174，1998年2月。[10] Jens P. Pedersen 和 Carsten Dahl。伪循环MDS码的分类。*IEEE*信息论汇刊，37(2)：365–370，1991年3月。[11] R. Roth 和 G. Seroussi。关于码长为 q 、定义在GF(q)上的循环MDS码（通信）。*IEEE*信息论汇刊，32(2)：284–285，1986年3月。[12] Henning Stichtenoth。代数函数域与码，数学研究生教材第254卷。Springer，第2版，2009年。[13] C. Xiang 和 C. Tang。通过圆分域约化研究有限域上的非RS型循环MDS码。*arXiv*预印本 *arXiv:2604.06822*，2026年。[14] E. Zehendner。循环MDS码的不存在性定理。摩德纳大学数学与物理研讨会论文集，32：203–205，1983年。