arXiv:2602.01383v1 [cs.IT] 1 Feb 2026

由带自同构和导子的斜多项式构造MDS矩阵

Atif AhmadKhan[1], *, Shakir Ali[1], Elif Segah Oztas[2], Abhishek Kesarwani[3]1阿里格尔穆斯林大学理学院数学系，阿里格尔 202002，印度
atifkhanalig1997@gmail.com，shakir.ali.mm@amu.ac.in2卡拉曼奥卢·穆罕默德贝大学数学系，土耳其
elifsegahoztas@gmail.com3 印度信息技术学院瓦多达拉分校数学与计算系，第乌国际校区，达曼和第乌 362520，印度 abhishek kesarwani@iiitvadodara.ac.in

-

摘要

最大距离可分（MDS）矩阵凭借其最优扩散性质，在编码理论和对称密钥密码学中发挥着核心作用。本文利用斜多项式环 $\mathbb{F}_q[X;\ \theta,\ \delta]$构造MDS矩阵，其中 θ是自同构， δ是θ上的 $\mathbb{F}_q$导子。我们引入 δ_θ-循环矩阵的概念，并研究其结构性质。我们推导出了这些矩阵为对合的并满足MDS性质的充要条件。所得 δ_θ-循环矩阵可视为在不存在 θ导子时所得经典构造的推广。本文的主要贡献之一是构造准递归MDS矩阵。在斜多项式环 $\mathbb{F}_q[X;\ \theta]$的框架下，我们构造了与友矩阵相关的准递归MDS矩阵。结果表明，这些矩阵是对合的，相较于文献中先前报道的准对合构造有了显著改进。文中还给出了若干说明性结果和示例。

关键词：MDS矩阵，导子，拟递归矩阵，对合的矩阵*2020*年数学主题分类：
94A60, 15A99, 11T06, 16S36

1 引言

加密系统设计中的混淆和扩散概念最早由 Shannon 在其开创性论文《保密系统的通信理论》 [37]中提出。混淆层旨在模糊密钥与密文之间的关系，而扩散层则旨在隐藏明文与密文之间的关系。在迭代分组密码中交替使用混淆层和扩散层，可确保明文和密钥的每一位都会以复杂且非线性的方式影响密文的每一位。因此，扩散层的设计会直接影响密码学基元的安全性和效率

*通讯作者

。特别是，正如 [17] 所强调的，扩散层在抵御差分密码分析和线性密码分析方面发挥着至关重要的作用。在衡量扩散能力的定量指标中，分支数 [17] 是评估扩散强度的基本参数。通过多重置换 [36, 38] 或使用最大距离可分（MDS）矩阵 [17]，可以实现最优扩散。

由于具有良好的代数结构和有利的实现特性，循环和递归MDS矩阵及其各种推广形式，构成了密码学中研究最广泛的MDS矩阵族之一。这类矩阵已应用于重要的密码设计中，包括 AES [17]和 SHARK [33], 等分组密码，以及 PHOTON [22]等轻量级哈希函数。这些构造的一项关键优势是，可以用多项式环 $\mathbb{F}_q[X]$及其商结构对它们进行简洁的代数描述。关于更多背景和进展，请参阅 [19, 14, 15]及其中的参考文献。文献中已提出多个结构化的MDS矩阵族，旨在实现强扩散的同时保持高效的实现。其中，循环和递归MDS矩阵尤其受到关注。

由于结构简单且易于在扩散层中高效实现，循环 MDS 矩阵得到了广泛研究；例如，参见 [1, 3, 4, 14, 20]。在这一方向上，Gupta 等人 [20]证明了不存在阶为偶数且同时具有最大距离可分和对合性质的循环矩阵。随后，Cauchois等人 [14] 基于斜多项式环所导出的多项式表示，为循环 MDS 矩阵建立了一个代数框架。通过利用自同构 θ推广经典循环矩阵，他们定义了 θ-循环矩阵，并证明这种推广结构允许存在阶为偶数的对合MDS矩阵。

另一项重要的研究方向关注递归 MDS 矩阵，这类矩阵对资源受限实现尤其有吸引力。此类矩阵已应用于密码学基元，包括 PHOTON 哈希函数族 [22] 和 LED 分组密码 [23]。递归 MDS 矩阵是指可表示为与多项式 $g(X) \in \mathbb{F}_q[X]$相关的伴随矩阵的幂的矩阵，从而能够利用线性反馈移位寄存器实现高效构造，并在软件中将内存需求降至最低 [22, 23, 21]。继 Guo 等人的工作之后，研究人员利用专用搜索技术和编码理论方法提出了众多构造方案 [8, 9, 10, 21, 34, 35, 26]。值得注意的是，Berger [11] 从 Gabidulin码导出了递归 MDS 矩阵的无穷族，这些矩阵同时满足最大秩距离性质；随后，Augot 和 Finiasz [9] 提出了一种基于缩短BCH码的直接构造方法。2016年，Cauchois等人 [15] 在斜多项式框架下研究了递归和准递归 MDS 矩阵，并在一类受限的有限域上获得了准对合 MDS 矩阵。

我们的构造是在斜多项式环的框架下进行的；由于底层系数环上存在一个自同构和一个 θ-导子，斜多项式环自然地出现了。这类非交换多项式环最早由 Ore [30] 引入。因此，在进一步讨论之前，我们先简要回顾导子的概念。Jacobson 在其经典著作《环的结构》 [24],中引入了（θ, γ）-导子的概念。具体而言，映射 $\delta\colon \mathfrak{R} \to \mathfrak{R}$ 若满足 $\delta(ab) = \theta(a)\delta(b) + \delta(a)\gamma(b)$，对所有 a, $b \in \mathfrak{R}$均成立，则称其为 $\mathfrak{R}$ 上的（θ, γ）-导子，其中 θ 和 γ 是 $\mathfrak{R}$的自同态。若取 γ 为 $\mathfrak{R}$上的恒等映射，则 δ 称为 θ-导子。自同构与导子理论在纯数学与应用数学中都发挥着至关重要的作用（参见； [6], [7], 和 [29]）。第二作者与其他合作者通过导子研究了环与代数的结构（更多详情见 [2], [5] ）。近年来，若干数学家已将导子理论应用于编码理论和密码学（例如； [12], [13], 和 [31]）。具体而言，Boucher 和 Ulmer [12]率先使用导子理论。他们提出了一种斜多项式的新型求值方式，构造出新类的求值码。此外，他们推广了适用于秩度量的 Gabidulin 解码算法，并构造了满足最大距离可分和最大秩距离（MRD）性质的码族。

受上述关于循环矩阵和递归最大距离可分矩阵的研究启发，我们使用斜多项式环来开展构造。通过这种方式，斜多项式环提供了一个统一的代数框架，可在其中研究这两类矩阵。具体而言，我们研究非交换环$\mathbb{F}_q[X;\theta,\ \delta]$，其中 θ是有限域 $\mathbb{F}_q$的一个自同构，而 δ是一个 θ-导子。乘法由规则 $Xa = \theta(a)X + \delta(a)$确定。当限制在有限域上时，每个 θ-导子都具有如下形式的简单刻画： $\delta(a) = \beta(\theta(a)-a)$，其中 $\beta \in \mathbb{F}_q$ [16, 第8章，定理3。1]，，这使得我们能够对所得构造进行显式控制。受早期关于（$\theta,\ \delta$）-码和（$\theta,\ \delta$）-循环矩阵的研究启发 [13, 31]，我们通过引入一个 θ-导子推广了现有的 θ-循环矩阵构造。这一扩展产生了一类新的结构化矩阵，称为 δ_θ-循环矩阵。我们通过其关联的、具有如下形式的斜多项式来分析这些矩阵

$$h\langle X\rangle = X^m - 1 + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X;\theta,\delta],$$

在条件 $m = 2^t$ 对某个 $t \in \mathbb{N}$成立时。我们推导出生成多项式的明确判据，以确保所得矩阵是对合的。尽管此前已在斜多项式框架下发现对合MDS矩阵。特别是，Cauchois等人 [14] 研究了θ-循环矩阵，并展示了一个阶为 4、同时满足对合性和最大距离可分性的例子。在经典循环矩阵情形下不存在这样的例子。受此启发，我们将 θ-导子引入构造，以扩大 θ-循环矩阵的类别。

本文的一项核心成果是分析了由斜多项式框架导出的准递归MDS矩阵。与以往仅限于特定有限域类别、且只能构造出偶数阶准对合MDS矩阵的方法 [15, 定理 2], 不同，我们的方法适用于更广泛的域。我们证明，对于适当选择的自同构 θ，所得准递归构造能够产生偶数阶对合MDS矩阵。这显著加强了现有成果，因为对合MDS矩阵具有较低的实现成本，因此在密码学应用中备受青睐。

最后，除了这些主要构造外，我们还通过适当的代数变换，从已有矩阵导出其他最大距离可分矩阵，进一步展示了所提出框架的灵活性。特别是，我们使用 Hadamard积作为生成新最大距离可分矩阵的有效工具。

本文结构如下：第2节概述 θ-导子、斜多项式环和最大距离可分矩阵。第3节重点介绍 δ_θ-循环最大距离可分矩阵的构造与分析，包括其对合性质。本节最后提出一个开放问题，涉及对此类 δ_θ-循环最大距离可分矩阵的完整刻画。在第4节中，我们推导出相关结果，表明每个准递归最大距离可分矩阵都能导出更多准递归最大距离可分矩阵。第5节探讨了利用伴随矩阵构造准递归最大距离可分矩阵的方法。此外，我们还给出了一些最大距离可分矩阵的例子，以说明其性质和构造方法。

2 记号与预备知识

本节将介绍一些基本定义和结果，这些内容将用于推导后续结果。现在，我们从有限域上的 θ-导子的定义开始。设 $\mathbb{F}_q$ 是一个有限域， θ 是 $\mathbb{F}_q$的一个自同构。 θ-导子是一个映射 $\delta\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$，满足对任意 $a, b \in \mathbb{F}_q$,

$$\delta(a+b) = \delta(a) + \delta(b)$$

and

$$\delta(ab) \quad = \quad \delta(a)b + \theta(a)\delta(b).$$

本文中始终使用以下记号:

$n,\ m,\ l,\ k,\ d,\ t$	正整数。
$\mathbb{F}_q$	含有 q 个元素的特征为 2 的有限域，其中 q 是 2 的幂。
$\mathbb{F}_q^n$	$\mathbb{F}_q$ 上维数为 n 的线性空间。
$M(m,\ \mathbb{F}_q)$	域 $\mathbb{F}_q$上所有 m 阶方阵的集合。
$GL(m,\ \mathbb{F}_q)$	由所有可逆矩阵组成的一般线性群 $m\times m$ 在 $\mathbb{F}$ 上$_q$.
$P(m,\ \mathbb{F}_2)$	所有在 $\mathbb{F}_2$ 上的 m 阶置换矩阵的集合。
$\mathbb{F}_q[X;\ \theta,\ \delta]$	斜多项式环，其中 $\theta:\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个自同构且 $\delta:\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个 θ-导子。
$Q\langle X\rangle$	一个关于 $\mathbb{F}_q$的斜多项式。

例1. 设 α 是有限域 $\mathbb{F}_2$上多项式 $1+X+X^4$ 的一个根。那么， $\mathbb{F}_{2^4}=\mathbb{F}_2(\alpha)$ 是一个阶为16的有限域。考虑映射 $\theta,\delta:\ \mathbb{F}_{2^4}\to\mathbb{F}_{2^4}$，定义如下:

$$\theta(a)=a^2 \quad and \quad \delta(a)=a^2-a.$$

那么， δ 是 $\mathbb{F}_{2^4}$上的一个 θ-导子。

下面的事实说明，自同构 θ 与其关联的 θ-导子 δ 一般不交换。

事实1. 设 $\delta:\mathbb{F}_q\longrightarrow\mathbb{F}_q$ 是一个 θ-导子。接下来，设 $\theta:\ \mathbb{F}_q\longrightarrow\mathbb{F}_q$ 是一个非恒等自同构，满足对所有 $a\in\mathbb{F}_q$，若 $\theta(\beta)\neq\beta$，则有 $\delta(a)=\beta(\theta(a)-a)$。那么，存在一个元素 $r\in\mathbb{F}_q$，使得

$$(\delta\circ\theta)(r)\neq(\theta\circ\delta)(r).$$

例2. 设 α 是多项式 $1+X+X^4$ 在 $\mathbb{F}_2$上的一个根。那么， $\mathbb{F}_{2^4}=\mathbb{F}_2(\alpha)$ 是一个阶为16的有限域。考虑映射 θ, $\delta:\ \mathbb{F}_{2^4}\to\mathbb{F}_{2^4}$，定义为

$$\theta(a)=a^2 \quad and \quad \delta(a)=\alpha(a^2-a).$$

那么， δ 是 $\mathbb{F}_{2^4}$上的一个 θ-导子。

定义1. 设 $\theta:\mathbb{F}_q\to\mathbb{F}_q$ 为域自同构。 $\mathbb{F}_q$ 在 θ 下的不变域定义为

$$(\mathbb{F}_q)^\theta=\{\,a\in\mathbb{F}_q:\theta(a)=a\,\}.$$

定义2. 设 $\theta:\ \mathbb{F}_q\longrightarrow\mathbb{F}_q$ 为自同构，且 $\delta:\ \mathbb{F}_q\longrightarrow\mathbb{F}_q$ 为导子。域 $\mathbb{F}_q$ 上带有自同构 θ 与 θ-导子 δ 的斜多项式环，记作 $\mathbb{F}_q[X;\theta,\delta]$，定义为集合

$$\mathbb{F}_q[X;\theta,\delta]:=\left\{a_0+a_1X+\cdots+a_{n-1}X^{n-1}:a_i\in\mathbb{F}_q,\,n\in\mathbb{N}\right\},$$

配备通常的多项式加法，以及按如下法则进行的乘法

$$\begin{aligned} X*a &= \theta(a)X+\delta(a) \quad for\ all\ a\in\mathbb{F}_q,\\ a*X &= aX \quad for\ all\ a\in\mathbb{F}_q. \end{aligned}$$

在相关 关于文献中一些著名的多项式环，我们作如下备注 s.

备注 1. 请注意，斜多项式环 $\mathbb{F}_q[X;\theta,\delta]$ （参见 *[27]*）的结构取决于自同构 θ 和 θ-导子 δ的性质。

1. 若 δ 是零导子，即对于所有 $a \in \mathbb{F}_q$， $\delta(a) = 0$，则该环简化为 $\mathbb{F}_q[X;\theta]$，称为扭曲多项式环。*2.* 若 θ 是恒等自同构，即对于所有 $a \in \mathbb{F}_q$， $\theta(a) = a$，则环 $\mathbb{F}_q[X;\delta]$ 称为微分多项式环。*3.* 若 θ 是恒等自同构且 δ 是零导子，则该结构退化为普通多项式环 $\mathbb{F}_q[X]$。

斜多项式环的行为与普通多项式环大不相同，但仍保留了具有带余除法这一重要性质。在下面的命题中，我们汇总斜多项式环带余除法的性质。

命题1。 *[27,* 命题 *2]* $\mathbb{F}_q[X;\theta,\delta]$ 是右欧几里得整环。

根据命题1，对于任意多项式 $f\langle X\rangle, g\langle X\rangle \in \mathbb{F}_q[X;\ \theta,\delta]$，若满足 $g\langle X\rangle \neq 0$，则存在唯一的多项式 $q\langle X\rangle$（商）和 $r\langle X\rangle$（余式），属于 $\mathbb{F}_q[X;\theta,\delta]$，使得

$$f\langle X\rangle \quad = \quad q\langle X\rangle * g\langle X\rangle + r\langle X\rangle, \tag{1}$$

其中 $r\langle X\rangle = 0$ 或 $\deg(r\langle X\rangle) < \deg(g\langle X\rangle)$。若 $r\langle X\rangle = 0$， 则 $f\langle X\rangle = q\langle X\rangle * g\langle X\rangle = 0$ 模 $*g$.

有限域上的线性码是一类纠错码，其中每个码字都是有限域 $\mathbb{F}_q$上的向量空间中的一个向量。线性码 C 定义为 $\mathbb{F}_q^n$的一个子空间。该码通常记作 $[n,m,d]_q$，其中 n是 C的长度， m是 C的维数，而 d是 C中不同码字之间的最小汉明距离。当 $d = n - m + 1$时，该码称为最大距离可分码，其生成矩阵的冗余部分构成一个MDS矩阵。接下来，我们先给出以下定义和引理，它们在后续讨论中起着关键作用。

定义 3。 *[19,* 生成矩阵为 $G = [M|I]$ 的 *4]*码 $[n,m,d]_q$，其中 M 是一个 $m \times (n-m)$ 矩阵，当且仅当 M 的每个方子矩阵都是非奇异的，才是最大距离可分的。若相应的码 C 是最大距离可分码，则称 M 为最大距离可分矩阵。

引理 1。 *[28,* 推论 *3*，第 *319]* 页。设 $M \in M(m,\mathbb{F}_q)$。那么，矩阵 M 是最大距离可分矩阵，当且仅当 $G = [M|I]$ 的任意 m 列在 $\mathbb{F}_q$ 上线性无关。此外， M 是最大距离可分矩阵，当且仅当 $\bar{G} = \begin{bmatrix} I \\ M \end{bmatrix}$ 的任意 m 行在 $\mathbb{F}_q$ 上线性无关。

引理 2。设 C 是有限域 $\mathbb{F}_q$ 上的一个最大距离可分码 $[2m,m,d]$。那么， C 中任意非零码字的最小汉明重量满足:

$$wt(C) \geq m + 1.$$

从密码学的角度来看，我们需要一个矩阵的逆矩阵；因此，我们将注意力限制在方阵上。特别地，我们专注于为某个正整数 m 构造 $[n = 2m,\ m,\ d = m+1]_q$ 码。由这些码，我们可以推导出在 $\mathbb{F}_q$ 上的大小为 $m \times m$ 的MDS矩阵。

定义 4。 若方阵 A 的阶为 m，且 A 的每个方子矩阵都是非奇异的，则称其为 *MDS*。

定义 5. 设 r 为正整数。若矩阵M^r 为*MDS*矩阵，则称矩阵 M 为递归最大距离可分矩阵或 *r-MDS*矩阵。若 M 为 *r-MDS*，则称 M 生成一个*MDS*矩阵。

3 δ_θ-循环 MDS 矩阵

本节沿用Cauchois等人 [14] 针对循环矩阵与θ-循环矩阵所建立的代数框架。我们将他们的工作推广到斜多项式环$\mathbb{F}_q[X;\theta,\delta]$这一更一般的情形。我们首先引入 δ_θ-循环矩阵的定义。

定义 6. 设 $\theta:\mathbb{F}_q\longrightarrow\mathbb{F}_q$ 为一个自同构，且 $\delta:\mathbb{F}_q\longrightarrow\mathbb{F}_q$ 为一个 θ-导子。一个矩阵

$$A=\begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m-1}\\ a_{1,0} & a_{1,1} & \cdots & a_{1,m-1}\\ \vdots & \vdots & \ddots & \vdots\\ a_{j,0} & a_{j,1} & \cdots & a_{j,m-1}\\ a_{j+1,0} & a_{j+1,1} & \cdots & a_{j+1,m-1}\\ \vdots & \vdots & \ddots & \vdots\\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,m-1}\end{bmatrix}_{m\times m},$$

称为 δ_θ-循环矩阵，如果 A 的第$(j+1)^{th}$ 行可以写成

$$(\delta(a_{j,0})+\theta(a_{j,m-1}),\delta(a_{j,1})+\theta(a_{j,0}),\ldots,\delta(a_{j,m-1})+\theta(a_{j,m-2})),$$

对 $1\le j\le m-1$。我们将该 δ_θ-循环矩阵记为 δ_θ-*circ*$(a_{0,0},a_{0,1},\ldots,a_{0,m-1})$。

该 δ_θ-循环矩阵可以用更显式的形式表示，以便更好地理解其结构。为此，我们固定记号 $x_1=\theta$、$x_2=\delta$ 以及 $a_{0,t}=h_t$ （对 $0\le t\le m-1.$）。设 $\eta_{s_{x_1}}$ 与 $\eta_{s_{x_2}}$ 分别表示 x_1 与 x_2 在表达式 $x_{i_1}x_{i_2}\cdots x_{i_s}$ 中出现的次数。采用这些记号，定义 6 中的矩阵取如下形式

$$\delta_\theta\text{-circ}(h_0,h_1,\ldots,h_{m-1})=(a_{st})=\left(\sum_{l=0}^{s}\sum_{\substack{\eta_{s_{x_1}}=l,\\ \eta_{s_{x_2}}=s-l}} x_{i_1}x_{i_2}\ldots x_{i_s}(\sigma^l(h_t))\right),$$

其中 $0\le s,\ t\le m-1$、$\{i_1,i_2,\ldots,i_s\}=\{1,2\}$ 和 $\sigma=\begin{bmatrix} h_0 & h_{m-1} & h_{m-2} & \ldots & h_1\\ h_{m-1} & h_{m-2} & h_{m-3} & \ldots & h_0\end{bmatrix}$ 是符号 $\{h_0,h_1,\ldots,h_{m-1}\}$. 上的一个置换

现在考虑如下 δ_θ-循环 MDS矩阵：

例 3. 设 $\mathbb{F}_{2^4}=\mathbb{F}_2(\alpha)$，其中 $\alpha^4+\alpha+1=0$。令 $\theta:\mathbb{F}_{2^4}\longrightarrow\mathbb{F}_{2^4}$ 为由 $\theta(a)=a^4$ 定义的自同构，并令 θ-导子 $\delta:\mathbb{F}_{2^4}\longrightarrow\mathbb{F}_{2^4}$ 由 $\delta(a)=\alpha(\theta(a)-a)$ 给出。对于 $a_{0,0}=1$、$a_{0,1}=\alpha^3$、$a_{0,2}=\alpha$ 和 $a_{0,3}=\alpha^2+\alpha+1$, δ_θ-循环矩阵为

$$B=\begin{bmatrix} 1 & \alpha^3 & \alpha & \alpha^2+\alpha+1\\ \alpha^2+\alpha+1 & \alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 & \alpha+1\\ \alpha & \alpha^3+1 & \alpha^2 & \alpha^3+1\\ \alpha^3+\alpha^2 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2 & \alpha^3+\alpha+1\end{bmatrix}_{4\times4}.$$

此外，矩阵 B 是最大距离可分的。

注 2. 对自同构 θ 和导子 δ施加特定条件后，我们可以立即得到以下观察结果：

1. 如果在定义 *6* 中令 $\delta = 0$，那么我们就得到一个 θ-循环矩阵

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m-1} \\ \theta(a_{0,m-1}) & \theta(a_{0,0}) & \cdots & \theta(a_{0,m-2}) \\ \vdots & \vdots & \ddots & \vdots \\ \theta(a_{0,1}) & \theta(a_{0,2}) & \cdots & \theta(a_{0,0}) \end{bmatrix}_{m\times m}.$$

2. 如果在定义 *6* 中令 $\delta = 0$ 和 $\theta = I|_{\mathbb{F}_q}$，则可得到循环矩阵

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m-1} \\ a_{0,m-1} & a_{0,0} & \cdots & a_{0,m-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,1} & a_{0,2} & \cdots & a_{0,0} \end{bmatrix}_{m\times m}.$$

在本节中，我们固定一些记号。设 $\theta:\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个阶为 m 的自同构，即对于所有 $a \in \mathbb{F}_q$，$\theta^m(a) = a$，并且设 $\delta:\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是满足 $\delta\circ\theta = \theta\circ\delta$. 的 θ-导子。对于 $X^m - 1 \in \mathbb{F}_q[X;\ \theta, \delta]$，若 $m = 2^t$，则 $J = (X^m - 1)$ 表示由 $X^m - 1$ 生成的双边理想。现在，利用理想 J 定义如下商环:

$$\frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)} = \left\{ b_0 + b_1X + \cdots + b_{m-1}X^{m-1} + (X^m-1);\ b_i \in \mathbb{F}_q,\ 0 \le i \le m-1 \right\}.$$

下面的定理建立了多项式 $h\langle X\rangle = (X^m-1)+\sum_{i=0}^{m-1} h_iX^i \in \mathbb{F}_q[X;\ \theta,\ \delta]$ 与 δ_θ-circ(h_0, h_1, .., h_{m-1}) 矩阵之间的关系。

定理 1. 设 $\theta:\mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个自同构，且 $\delta:\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个 θ-导子。接下来，设 $h\langle X\rangle = (X^m-1) + \sum_{i=0}^{m-1} h_iX^i \in \mathbb{F}_q[X;\theta,\delta]$ 是一个次数为 m 的首一多项式。那么，与线性变换对应的矩阵

$$\begin{aligned} \psi: \frac{\mathbb{F}_q[X;\theta;\delta]}{(X^m-1)} &\longrightarrow \frac{\mathbb{F}_q[X;\theta;\delta]}{(X^m-1)} \\ \psi\Big(Q\langle X\rangle\Big) &:= Q\langle X\rangle * h\langle X\rangle, \end{aligned}$$

相对于基 $\{1, X, X^2, \ldots, X^{m-1}\}$ 的形式为

$$A = (a_{su}) = \left(\sum_{i=0}^{s} \binom{s}{i} \theta^i \circ \delta^{s-i}(\sigma^i(h_u)) \right),$$

其中 $0 \le s$、$u \le m-1$ 和 $\sigma = \begin{bmatrix} h_0 & h_{m-1} & h_{m-2} & \ldots & h_1 \\ h_{m-1} & h_{m-2} & h_{m-3} & \ldots & h_0 \end{bmatrix}$ 是集合 $\{h_0, h_1, \ldots, h_{m-1}\}$. 上的一个置换

证明. 已知 $\theta:\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个自同构，且 $\delta:\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个 θ-导子。接下来，设 $h\langle X\rangle = (X^m-1) + \sum_{i=0}^{m-1} h_iX^i \in \mathbb{F}_q[X;\theta,\delta]$ 是一个次数为 m 的首一多项式。为证明 A 是与线性变换对应的矩阵

$$\psi: \frac{\mathbb{F}_q[X;\theta;\delta]}{(X^m-1)} \longrightarrow \frac{\mathbb{F}_q[X;\theta;\delta]}{(X^m-1)}$$

由.....定义

$$\psi\Big(Q\langle X\rangle\Big) = Q\langle X\rangle * h\langle X\rangle,$$

相对于基 $\{1, X, X^2, \ldots, X^{m-1}\}$，只需证明

$$X^k * h\langle X\rangle = \sum_{j=0}^{m-1}\left(\sum_{i=0}^{k}\theta^i \circ \delta^{k-i}(\sigma^i(h_j))\right)X^j \tag{2}$$

对所有 $k \in \{1, 2, \ldots, m-1\}$。我们通过对 k 使用数学归纳法来证明该结果。对于 $k = 1$，我们有

$$\begin{aligned} X * h\langle X\rangle &= X * (h_0 + h_1X + \cdots + h_{m-1}X^{m-1}) \\ &= (\theta(h_0)X + \delta(h_0)) + (\theta(h_1)X^2 + \delta(h_1)X) + \cdots + (\theta(h_{m-1})X^m + \delta(h_{m-1})X^{m-1}) \\ &= (\delta(h_0) + \theta(h_{m-1})) + (\delta(h_1) + \theta(h_0))X + \cdots + (\delta(h_{m-1}) + \theta(h_{m-2}))X^{m-1} \\ &= \sum_{j=0}^{m-1}\left(\sum_{i=0}^{1}\theta^i \circ \delta^{1-i}(\sigma^i(h_j))\right)X^j, \end{aligned} \tag{3}$$

当取 $k = 1$ 时，这与 (2) 相同。我们假设该结果对 $1 < k < m-1$ 成立。现在证明该结果对 $k+1$ 成立。

$$\begin{aligned} X^{k+1} * h\langle X\rangle &= X * (X^k * h\langle X\rangle) \\ &= X * \left(\sum_{j=0}^{m-1}\left(\sum_{i=0}^{k}\theta^i \circ \delta^{k-i}(\sigma^i(h_j))\right)X^j\right) \\ &= \sum_{j=0}^{m-1}\theta\left(\sum_{i=0}^{k}\theta^i \circ \delta^{k-i}(\sigma^i(h_j))\right)X^{j+1} + \sum_{j=0}^{m}\delta\left(\sum_{i=0}^{k}\theta^i \circ \delta^{k-i}(\sigma^i(h_j))\right)X^j \\ &= \sum_{j=0}^{m-1}\left(\sum_{i=0}^{k+1}\theta^i \circ \delta^{k+1-i}(\sigma^i(h_j))\right)X^j, \end{aligned}$$

其中 σ 是集合 $\{h_0,\ h_1, \ldots, h_{m-1}\}$ 上的一个置换，其定义为

$$\sigma = \begin{bmatrix} h_0 & h_{m-1} & h_{m-2} & \ldots & h_1 \\ h_{m-1} & h_{m-2} & h_{m-3} & \ldots & h_0 \end{bmatrix}.$$

至此证明完毕。 □

推论 1. 设 $C_{h,\theta,\delta}$ 与 $C_{p,\theta,\delta}$ 分别是与多项式 $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_iX^i$、$p\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} p_iX^i \in \mathbb{F}_q[X; \theta, \delta]$相关联的 δ_θ-循环矩阵。则 $C_{h,\theta,\delta} \cdot C_{g,\theta,\delta}$也是 δ_θ-循环矩阵。

若在定理 1 中取 $\delta = 0$，则可得到如下推论：

推论 2. *[14, 命题 2]* 设 $\theta\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 为一个自同构。接下来，设 $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_iX^i \in \mathbb{F}_q[X; \theta]$ 为一个次数为 m 的首一多项式。那么，与线性变换相关联的矩阵

$$\begin{aligned} \psi : \frac{\mathbb{F}_q[X;\theta]}{(X^m-1)} &\longrightarrow \frac{\mathbb{F}_q[X;\theta]}{(X^m-1)} \\ \psi\Big(Q\langle X\rangle\Big) &:= Q\langle X\rangle * h\langle X\rangle, \end{aligned}$$

相对于基 $\{1, X, X^2, \ldots, X^{m-1}\}$ 的形式为

$$A = (a_{su}) = \Big(\theta^s(\sigma^s(h_u))\Big),$$

其中 $0 \le s$、 $u \le m-1$ 和 $\sigma = \begin{bmatrix} h_0 & h_{m-1} & h_{m-2} & \dots & h_1 \\ h_{m-1} & h_{m-2} & h_{m-3} & \dots & h_0 \end{bmatrix}$ 是集合 $\{h_0, h_1, \dots, h_{m-1}\}$. 上的一个置换

若在定理 1 中令 $\delta = 0$ 和 θ 为恒等映射，则可得到以下推论 :

推论 3. *[14,* 命题 *1]* 设 $\theta : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 为一个自同构。接下来，令 $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$ 为一个次数为 m的首一多项式。那么，与线性变换相关联的矩阵

$$\begin{aligned} \psi : \frac{\mathbb{F}_q[X]}{(X^m-1)} &\longrightarrow \frac{\mathbb{F}_q[X]}{(X^m-1)} \\ \psi\Big(Q\langle X\rangle\Big) &:= Q\langle X\rangle * h\langle X\rangle, \end{aligned}$$

关于基 $\{1, X, X^2, \dots, X^{m-1}\}$ 的形式为

$$A = (a_{su}) = (\sigma^s(h_u)),$$

其中 $0 \le s$、 $u \le m-1$和 $\sigma = \begin{bmatrix} h_0 & h_{m-1} & h_{m-2} & \dots & h_1 \\ h_{m-1} & h_{m-2} & h_{m-3} & \dots & h_0 \end{bmatrix}$ 是集合 $\{h_0, h_1, \dots, h_{m-1}\}$.上的一个置换

定义 7. *[28,* 定义 *6。3]*对于有限域上的给定多项式 $f\langle X\rangle = a_0 + a_1 X + \cdots + a_n X^n$ *te* 域 $\mathbb{F}_q$, $f\langle X\rangle$ 的权定义为

$$wt(f\langle X\rangle) = |\{i \mid a_i \neq 0,\ 0 \le i \le n\}|.$$

基于定理 1 中构造的 δ_θ-循环矩阵，我们能够给出该矩阵为最大距离可分矩阵的代数充要条件。

定理 2。 设 $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X;\ \theta, \delta]$。那么，当且仅当对于所有 $Q_1\langle X\rangle \in \mathbb{F}_q[X; \theta, \delta]$, 都有， δ_θ-*circ*$(h_0, h_1, \dots, h_{m-1})$ 是最大距离可分矩阵。

$$wt(Q_1\langle X\rangle) + wt(Q_1\langle X\rangle h\langle X\rangle \mod (X^m - 1)) \ge m + 1.$$

证明。 $A = \delta_\theta$-循环矩阵$(h_0,\ h_1,\ \dots,\ h_{m-1})$是最大距离可分的。

$$\begin{aligned} &\Leftrightarrow \quad (I_m|A) \text{ is the generator matrix of MDS code} \\ &\Leftrightarrow \quad \text{for all } (q_0, q_1, \dots, q_{m-1}) \in \mathbb{F}_q^m,\ wt((q_0, q_1, \dots, q_{m-1}) \cdot (I_m|A)) \ge m+1 \\ &\Leftrightarrow \quad wt(q_0, q_1, \dots, q_{m-1}) + wt((q_0, q_1, \dots, q_{m-1}) \cdot A) \ge m+1. \end{aligned}$$

若考虑 $Q_1\langle X\rangle = \sum_{i=0}^{m-1} q_i X^i$, 则

$$wt(q_0, q_1, \dots, q_{m-1}) = wt(Q_1).$$

根据 定理 1，我们知道 A 对应于在 $\mathbb{F}_q[X;\theta,\ \delta]\ (X^m-1)$中右乘 $h\langle X\rangle$ 。因此，w——— e 有:

$$wt((q_0, q_1, \dots, q_{m-1}) \cdot A) = wt(Q_1\langle X\rangle h\langle X\rangle \mod (X^m - 1)),$$

这就证明了该定理。 □

注 3. 由定理 *1* 可知，所得的 δ_θ-循环 *MDS* 矩阵的阶为 $m = 2^t$ ，其中 t 是某个正整数。注意，奇数阶的 δ_θ-循环 *MDS* 矩阵确实存在；然而，它们不一定是由定理 *1* 中描述的线性变换得到的。

下面的例子说明了上述注记:

例4. 设 $\mathbb{F}_{q^n}$ *(*$n > 2$*)* 为一个有限域，映射 θ、δ： $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ 分别定义为 $\theta(a) = a^2$ 和$\delta(a) = \beta(\theta(a) - a)$，其中 $\beta \in \mathbb{F}_q$。那么， δ_θ-循环矩阵 A 定义为

$$\begin{aligned} A &= \delta_\theta\text{-circ}(\alpha, 1, 1) \\ &= \begin{bmatrix} \alpha & 1 & 1 \\ \delta(\alpha)+\theta(1) & \delta(1)+\theta(\alpha) & \delta(1)+\theta(1) \\ \delta^2(\alpha)+\theta^2(1) & \delta^2(1)+\theta^2(\alpha) & \delta^2(1)+\theta^2(1) \end{bmatrix}_{3\times 3}, \end{aligned}$$

其中 α 是$\mathbb{F}_{2^n}$的生成多项式的一个根。容易验证，对于 $n > 4$， A 是一个*MDS*矩阵。

下面的定理给出了多项式所满足的条件，在这些条件下， δ_θ-循环矩阵是对合的:

定理3. 设 $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X;\theta、\ \delta]$ 和 $g\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} g_i X^i \in \mathbb{F}_q[X;\theta、\ \delta]$ 为次数为 m的首一多项式。设$C_{h,\theta,\delta}$和$C_{g,\theta,\delta}$ 分别为与多项式 h 和 g相关联的 δ_θ-循环矩阵。则，

$$C_{g,\theta,\delta} \cdot C_{h,\theta,\delta} = I_m \quad \textit{if and only if} \quad 1 \equiv g\langle X\rangle * h\langle X\rangle \mod {}_*(X^m - 1).$$

证明。设

$$\phi_h, \phi_g : \frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)} \longrightarrow \frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)},$$

为这些映射。对于 $U\langle X\rangle \in \frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)}$，我们有

$$\phi_h(U\langle X\rangle) = U\langle X\rangle * h\langle X\rangle \quad \text{and} \quad \phi_g(U\langle X\rangle) = U\langle X\rangle * g\langle X\rangle.$$

根据定理 1，我们有与映射 ϕ_h 和 ϕ_g 分别相关的矩阵 $C_{h,\ \theta,\ \delta}$ 和$C_{g,\ \theta,\ \delta}$。为了说明映射 ϕ_h 和 ϕ_g 之间的关系，我们首先考虑复合映射

$$\phi_h \circ \phi_g : \frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)} \longrightarrow \frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)},$$

定义为

$$\phi_h \circ \phi_g(U\langle X\rangle) \longrightarrow U\langle X\rangle * g\langle X\rangle * h\langle X\rangle.$$

现在，假设 $g\langle X\rangle * h\langle X\rangle = 1 \mod {}_*(X^m - 1)$。那么，对于任意多项式 $P\langle X\rangle \in \frac{\mathbb{F}_q[X;\ \theta,\ \delta]}{(X^m-1)}$，我们有

$$\begin{aligned} \phi_h \circ \phi_g(P\langle X\rangle) &= \phi_h(P\langle X\rangle * g\langle X\rangle) \\ &= P\langle X\rangle * g\langle X\rangle * h\langle X\rangle \mod {}_*(X^m - 1) \\ &= P\langle X\rangle \mod {}_*(X^m - 1). \end{aligned}$$

接下来，我们计算基集 $B = \{1,\ X,\ X^2, \ldots,\ X^{m-1}\}$ 在复合映射$\phi_h \circ \phi_g$下的像

$$\begin{aligned} \phi_h \circ \phi_g(1) &= 1 \mod {}_*(X^m - 1), \\ \phi_h \circ \phi_g(X) &= X \mod {}_*(X^m - 1), \\ &\vdots \end{aligned}$$

$$\phi_h \circ \phi_g(X^{m-1}) = X^{m-1} \mod *(X^m - 1).$$

这就证明了 $[\phi_h \circ \phi_g]_B = I_m$，或者等价地，

$$C_{g,\theta,\delta} \cdot C_{h,\theta,\delta} = I_m.$$

反过来，假设 $C_{g,\theta,\delta} \cdot C_{h,\theta,\delta} = I_m$。根据 [18, Page 67], ，我们有

$$C_{g,\theta,\delta} \cdot C_{h,\theta,\delta} = [\phi_h \circ \phi_g]_B = I_m.$$

这意味着，对于所有 $i = 0, 1, \ldots, m-1$, $\phi_h \circ \phi_g(X^i) = X^i$。因此，我们得出

$$\phi_h \circ \phi_g = I|_{\frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)}}, \text{ where } I|_{\frac{\mathbb{F}_q[X;\theta,\delta]}{(X^m-1)}} \text{ is an identity map.}$$

对于任意多项式 $P\langle X\rangle \in {}^{\mathbb{F}_q[X;\theta,\delta]}/_{(X^m-1)}$，我们有

$$\phi_h \circ \phi_g(P\langle X\rangle) = P\langle X\rangle * g\langle X\rangle * h\langle X\rangle \mod (X^m - 1) = P\langle X\rangle \mod *(X^m - 1).$$

这表明 $g\langle X\rangle * h\langle X\rangle = 1$ 模 $*(X^m - 1)$。 □

我们以简要总结研究结果并提出一个开放问题来结束本节。众所周知，每个 θ-导子 on $\mathbb{F}_q$ 均可表示为 $\delta(a) = \beta\big(\theta(a) - a\big)$，对所有 $a \in \mathbb{F}_q$，其中某个 $\beta \in \mathbb{F}_q$。本节研究了 δ_θ-循环矩阵满足MDS性质的条件。在 $\beta \in (\mathbb{F}_q)^\theta$的情形下，我们得到了部分刻画。更具体地说，在这一假设下，定理 1 给出了与相应线性变换相关联的 δ_θ-循环矩阵的显式形式，即

$$\begin{bmatrix} h_0 & h_1 & \cdots & h_{m-1} \\ \sum_{i=0}^{1} \binom{1}{i} \delta^{1-i}\theta^i\big(\sigma^i(h_0)\big) & \sum_{i=0}^{1} \binom{1}{i} \delta^{1-i}\theta^i\big(\sigma^i(h_1)\big) & \cdots & \sum_{i=0}^{1} \binom{1}{i} \delta^{1-i}\theta^i\big(\sigma^i(h_{m-1})\big) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{m-1} \binom{m-1}{i} \delta^{m-1-i}\theta^i\big(\sigma^i(h_0)\big) & \sum_{i=0}^{m-1} \binom{m-1}{i} \delta^{m-1-i}\theta^i\big(\sigma^i(h_1)\big) & \cdots & \sum_{i=0}^{m-1} \binom{m-1}{i} \delta^{m-1-i}\theta^i\big(\sigma^i(h_{m-1})\big) \end{bmatrix}_{m\times m}.$$

此外，在定理 2 中，我们推导出了这类矩阵具有 MDS性质的必要条件。然而，当 $\beta \notin (\mathbb{F}_q)^\theta$ 时，上述形式的 δ_θ-循环矩阵不再适用，而关于 MDS δ_θ-循环矩阵的完整刻画仍然未知。这引出了以下开放问题：

开放问题 1。设 $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X;\ \theta, \delta]$。那么，当且仅当对所有 $Q_1\langle X\rangle \in \mathbb{F}_q[X;\ \theta, \delta]$，都有，$\delta_\theta$-*circ*$(h_0, h_1, \ldots, h_{m-1})$是 *MDS*。

$$wt(Q_1\langle X\rangle) + wt(Q_1\langle X\rangle h\langle X\rangle \mod (X^m - 1)) \geq m + 1.$$

4 准递归 MDS 矩阵的分类与等价性

本节将介绍关于递归MDS矩阵的相似性与等价性的一些基本结果。为建立这些结果，我们先固定若干贯穿本节使用的概念。设 $\theta\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个自同构，且 $\delta\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 是一个 θ-导子，使得 $\delta \circ \theta = \theta \circ \delta$。

现在，我们从以下定义开始本节：

定义 8. $M(m, \mathbb{F}_q)$ 中的两个矩阵 M和 M'称为对角相似，如果存在一个对角矩阵 $D \in GL(m, \mathbb{F}_q)$ 使得 $M' = D^{-1}MD$。

定义 9. $M(m,\mathbb{F}_q)$ 中的两个矩阵 M和 M'称为置换相似，如果存在置换矩阵 $P \in P(m,\mathbb{F}_2)$ 使得 $M' = PMP^{-1}$。

为了定义准递归MDS矩阵，我们先引入一些记号。对于元素 $a \in \mathbb{F}_q$，我们使用记号

$$a^{\langle i \rangle} = \sum_{k=0}^{i} \binom{i}{k} \delta^{i-k} \theta^k(a). \tag{4}$$

我们引入记号 $a^{\langle i \rangle}$，它在我们的分析中起着关键作用。对于任意两个正整数s，t使得 $1 \le s$，$t \le m$，令 $A = (a_{s,\ t})$ 为一个阶为 m 的矩阵。我们将矩阵 $A^{\langle i \rangle}$ 定义为

$$A^{\langle i \rangle} \quad = \quad \left(a_{s,t}^{\langle i \rangle}\right). \tag{5}$$

若取 $\delta = 0$，则由 (4) 和 (5) 可得

$$a^{[i]} \quad = \quad \theta^i(a), \quad A^{[i]} = (\theta^i(a_{s,t})). \tag{6}$$

(5) 和 (6) 中定义的矩阵幂 $A^{\langle i \rangle}$ 不同于通过经典矩阵乘积得到的通常幂 A^i 。

动机 受递归 MDS 矩阵（r-MDS矩阵）定义的启发，我们引入该定义 of 拟递 归MDS矩阵（拟 r-MDS矩阵），涉及 θ-导子。

定义 10. 设 r 为正整数。若矩阵 $M^{\langle r-1 \rangle} \cdot M^{\langle r-2 \rangle} \cdots M^{\langle 1 \rangle} \cdot M$是最大距离可分的，则称矩阵 M 为拟递归最大距离可分或拟 r-最大距离可分。若 M是拟 r-最大距离可分的，则称 M生成一个*MDS*矩阵。此外，若 M 是伴随矩阵，则称 M 为拟 r-最大距离可分伴随矩阵。

现在，在给出本节的主要结果之前，我们先介绍若干辅助结果。

命题 2. 设 $A = (a_{s,t})$ 与 $B = (b_{s,t})$ 为有限域 $\mathbb{F}_q$上的两个 m 阶矩阵。则

$$(A^{\langle i \rangle})^{\langle j \rangle} = A^{\langle i+j \rangle}.$$

证明. 设 $A = (a_{s,t})$ 与 $B = (b_{s,t})$ 为 $\mathbb{F}_q$ 上的两个 m 阶矩阵。我们需要证明 $(A^{\langle i \rangle})^{\langle j \rangle} = A^{\langle i+j \rangle}$. 为此，只需证明对 $a \in \mathbb{F}_q$，有 $(a^{\langle i \rangle})^{\langle j \rangle} = a^{\langle i+j \rangle}$. 现在，我们计算

$$a^{\langle i+j \rangle} \quad = \quad \sum_{k=0}^{i+j} \binom{i+j}{k} \delta^{i+j-k} \theta^k(a), \tag{7}$$

$$a^{\langle i \rangle} \quad = \quad \sum_{k=0}^{i} \binom{i}{k} \delta^{i-k} \theta^k(a). \tag{8}$$

现在，对于任意正整数 j，我们计算

$$\begin{aligned} (a^{\langle i \rangle})^{\langle j \rangle} &= \sum_{k=0}^{j} \binom{j}{k} \delta^k \theta^{j-k} \left(\sum_{k'=0}^{i} \binom{i}{k'} \delta^{i-k'} \theta^{k'}(a) \right) \\ &= \sum_{k=0}^{i+j} \left(\sum_{l+t=k} \binom{j}{l} \binom{i}{t} \right) \delta^k \theta^{i+j-k}(a). \end{aligned} \tag{9}$$

由于,

$$\sum_{l+t=k}\binom{j}{l}\binom{i}{t}=\binom{i+j}{k}, \tag{10}$$

因此，由（7）、（9）和（10），我们有 $(a^{\langle i\rangle})^{\langle j\rangle}=a^{\langle i+j\rangle}$. 这意味着 $(A^{\langle i\rangle})^{\langle j\rangle}=A^{\langle i+j\rangle}$. □

例5。设 $\mathbb{F}_{2^4}=\mathbb{F}_2(\alpha)$，其中 $\alpha^4+\alpha+1=0$。令 θ： $\mathbb{F}_{2^4}\longrightarrow\mathbb{F}_{2^4}$ 为由 $\theta(a)=a^4$ 定义的自同构，并令 θ-导子 δ： $\mathbb{F}_{2^4}\longrightarrow\mathbb{F}_{2^4}$ 由 $\delta(a)=(\alpha^2+\alpha)(\theta(a)-a)$给出。令$A=\begin{bmatrix}1&0\\ \alpha&\alpha\end{bmatrix}_{2\times2}$ 以及 $B=\begin{bmatrix}0&1\\ \alpha&\alpha\end{bmatrix}_{2\times2}$。在这种情况下，我们得到 $(AB)^{\langle1\rangle}\neq A^{\langle1\rangle}B^{\langle1\rangle}$.

例5表明，式(5)中定义的乘积不一定满足矩阵乘法的分配律。也就是说,

$$(AB)^{\langle i\rangle}\neq A^{\langle i\rangle}B^{\langle i\rangle}.$$

命题3。设 $a\in(\mathbb{F}_q)^{\theta}$。则,

$$\delta^k(ab)=a\delta^k(b)\text{ for all }b\in\mathbb{F}_q.$$

证明。该证明可利用数学归纳法原理建立。 □

命题 4。设 $a\in(\mathbb{F}_q)^{\theta}$ 以及 $b\in\mathbb{F}_q$. 则,

$$(ab)^{\langle i\rangle}=ab^{\langle i\rangle}.$$

证明。给定 $a\in(\mathbb{F}_q)^{\theta}$ 和 $b\in\mathbb{F}_q$. 则，我们计算

$$\begin{aligned}(ab)^{\langle i\rangle}&=\sum_{k=0}^{i}\binom{i}{k}\delta^{i-k}\theta^k(ab)\\ &=\sum_{k=0}^{i}\delta^{i-k}(a\theta^k(b))\\ &=a\sum_{k=0}^{i}\delta^{i-k}\theta^k(b)\\ &=ab^{\langle i\rangle}.\end{aligned}$$

□

命题5。设 $A\in M$（m、$\mathbb{F}_q$），且 D 是域 $(\mathbb{F}_q)^{\theta}$. 上任意一个 m 阶的对角矩阵。则,

(i) $(DA)^{\langle t\rangle}=D^{\langle t\rangle}A^{\langle t\rangle}$
(ii) $(AD)^{\langle t\rangle}=A^{\langle t\rangle}D^{\langle t\rangle}$.

证明。*(i)* 令 $A\in M(m,\ \mathbb{F}_q)$ 和 $D\in M(m,\ (\mathbb{F}_q)^{\theta})$ 满足

$$A=\begin{bmatrix}a_{0,0}&a_{0,1}&\cdots&a_{0,m-1}\\ a_{1,0}&a_{1,1}&\cdots&a_{1,m-1}\\ \vdots&\vdots&\ddots&\vdots\\ a_{m-1,0}&a_{m-1,1}&\cdots&a_{m-1,m-1}\end{bmatrix}_{m\times m}\text{ and }D=\begin{bmatrix}d_0&0&\cdots&0\\ 0&d_1&\cdots&0\\ \vdots&\vdots&\ddots&\vdots\\ 0&0&\cdots&d_{m-1}\end{bmatrix}_{m\times m}.$$

现在，我们计算

$$DA = \begin{bmatrix} d_0a_{0,0} & d_0a_{0,1} & \dots & d_0a_{0,m-1} \\ d_1a_{1,0} & d_1a_{1,1} & \dots & d_1a_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ d_{m-1}a_{m-1,0} & d_{m-1}a_{m-1,1} & \dots & d_{m-1}a_{m-1,m-1} \end{bmatrix}_{m\times m}$$

$$(DA)^{\langle t\rangle} = ((d_ia_{ij})^{\langle t\rangle}).$$

根据命题 4，我们得到

$$\begin{aligned} (DA)^{\langle t\rangle} &= ((d_ia_{ij})^{\langle t\rangle}) \\ &= (d_i^{\langle t\rangle}a_{ij}^{\langle t\rangle}) \\ &= (d_ia_{ij}^{\langle t\rangle}) \\ &= D^{\langle t\rangle}A^{\langle t\rangle}. \end{aligned}$$

由此可知

$$(DA)^{\langle t\rangle} = D^{\langle t\rangle}A^{\langle t\rangle}.$$

(*ii*) 类似地，我们可以证明 $(AD)^{\langle t\rangle} = A^{\langle t\rangle}D^{\langle t\rangle}$。 □

推论 4. 设 $M_1 \in M(m,\mathbb{F}_q)$ 与对角矩阵 $D_1, D_2 \in M(m,(\mathbb{F}_q)^\theta)$。则，

$$(D_1M_1D_2)^{\langle t\rangle} = D_1^{\langle t\rangle}M_1^{\langle t\rangle}D_2^{\langle t\rangle}.$$

类似地，我们可以证明如下命题：

命题 6. 设 $A \in M(m,\mathbb{F}_q)$ 与 $P,\ P_1,\ P_2 \in P(m,\mathbb{F}_2)$。则，

(i) $(PA)^{\langle t\rangle} = P^{\langle t\rangle}A^{\langle t\rangle}$

(ii) $(AP)^{\langle t\rangle} = A^{\langle t\rangle}P^{\langle t\rangle}$

(iii) $(P_1AP_2)^{\langle t\rangle} = P_1^{\langle t\rangle}A^{\langle t\rangle}P_2^{\langle t\rangle}$.

根据命题5和6，我们有以下结果：

定理 4. 设 $\theta\colon \mathbb{F}_q \to \mathbb{F}_q$ 是一个自同构， $\delta\colon \mathbb{F}_q \to \mathbb{F}_q$ 是一个导子，且 $\delta\circ\theta = \theta\circ\delta$.

(i) 假设两个矩阵 $M_1, M_2 \in M(m,\mathbb{F}_q)$ 对角相似，使得

$$M_2 = DM_1D^{-1},\quad D \in GL(m,(\mathbb{F}_q)^\theta).$$

那么， M_1 是准 r-最大距离可分当且仅当 M_2 是准 r-最大距离可分。

(ii) 假设两个矩阵 $M_1, M_2 \in M(m,\mathbb{F}_q)$ 置换相似，使得

$$M_2 = PM_1P^{-1},\ P \in P(m,\mathbb{F}_2)$$

那么， M_1 是准 r-最大距离可分当且仅当 M_2 是准 r-最大距离可分。

证明。 (i) 我们有 $M_1, M_2 \in M(m, \mathbb{F}_q)$对角相似，使得

$$M_2 = DM_1D^{-1}.$$

设 M_1 是准 r-最大距离可分矩阵。这意味着存在正整数 r ，使得$M_1^{\langle r-1\rangle} \cdot M_1^{\langle r-2\rangle} \cdots M_1^{\langle 1\rangle} \cdot M_1$是准 r-最大距离可分矩阵。现在我们计算

$$M_2^{\langle r-1\rangle} \cdot M_2^{\langle r-2\rangle} \cdots M_2^{\langle 1\rangle} \cdot M_2 \quad = \quad (DM_1D^{-1})^{\langle r-1\rangle}(DM_1D^{-1})^{\langle r-2\rangle} \cdots (DM_2D^{-1}). \tag{11}$$

由于 $D \in GL(m, (\mathbb{F}_q)^\theta)$，因此由命题5和（11）可得

$$M_2^{\langle r-1\rangle} \cdot M_2^{\langle r-2\rangle} \cdots M_2^{\langle 1\rangle} \cdot M_2 \quad = \quad DM_1^{\langle r-1\rangle} \cdot M_1^{\langle r-2\rangle} \cdots M_1^{\langle 1\rangle} \cdot M_1D^{-1}.$$

这表明 M_2 是准 r-最大距离可分矩阵。

(ii) 利用命题 6，可以通过与证明部分(i)时所用的类似论证，轻松证明这一结果。

□

5 多项式给出的准递归MDS矩阵的刻画

上一节中，我们介绍了准 r-最大距离可分矩阵的概念，并强调了它们在构造最大距离可分矩阵中的作用。本节将重点分析和构造这类矩阵，具体而言，它们源自与 $\mathbb{F}_q[X;\theta]$ 中的首一斜多项式相关联的友矩阵。遵循 Cauchois等人 [15], 的框架，我们回顾一下，准递归MDS矩阵可分解为以下形式

$$M \ = \ C_g^{[r-1]}\, C_g^{[r-2]} \cdots C_g^{[1]}\, C_g,$$

其中 $g(X) \in \mathbb{F}_q[X;\theta]$ 是次数为 m 的首一多项式，且 $r \geq m$。在这种情况下，我们称 $g(X)$ 生成一个准递归MDS矩阵。

Cauchois等人 [15] 构造了满足拟对合恒等式 $M \cdot M^{[m]} = I_m$ 的结构。相比之下，我们的方法生成的准递归MDS矩阵是对合的。为此，给定任意一个阶为 m 的方阵 $A = (a_{s,\ t})$，并取式 (5) 中的 $\delta = 0$ ，我们采用以下记号

$$A^{[i]} = (a_{s,t}^{[i]}), \qquad 1 \leq s, t \leq m. \tag{12}$$

现在我们回顾有限域上的 θ-循环码的概念，它在我们的研究中起着核心作用。若线性码 $C \subseteq \mathbb{F}_q^n$ 在 θ-移位下封闭，则称其为 θ-循环码（或斜循环码），即

$$(c_0, c_1, \ldots, c_{n-1}) \in C \implies (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

当 $|\theta| \mid n$ 时，多项式 $X^n - 1$ 属于斜多项式环 $\mathbb{F}_q[X$ 的中心； $\theta]$，因此 $\langle X^n - 1\rangle$ 成为一个双边理想。这使我们可以考虑商环

$$\frac{\mathbb{F}_q[X;\theta]}{\langle X^n - 1\rangle} = \left\{ a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + \langle X^n - 1\rangle \ ;\ a_i \in \mathbb{F}_q \right\}.$$

全文中，我们假设 $|\theta|$ 整除 n。根据上述讨论，一个 θ-循环码有如下两种等价描述：

(i) 它是 $\mathbb{F}_q^n$ 的一个 $\mathbb{F}_q$-子模，满足

$$C := \left\{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n;\ (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C\right\};$$

(ii) 它是商环 $\frac{\mathbb{F}_q[X;\theta]}{\langle X^n-1\rangle}$ 中的一个左理想，即，

$$C := {}^*\langle g(X)\rangle = \left\{ a(X)g(X) \mid a(X) \in \frac{\mathbb{F}_q[X;\theta]}{\langle X^n-1\rangle} \right\}.$$

为此，设 $g(X) = g_0 + g_1X + \cdots + g_{m-1}X^{m-1} + X^m \in \mathbb{F}_q[X;\theta]$ 是 $X^n - 1$ 的右因子，并设 C 为主 θ-循环码，即 $C = {}^*\langle g(X)\rangle$. C 的生成矩阵为

$$G = \begin{bmatrix} g(X) \\ X * g(X) \\ \vdots \\ X^{n-m-1} * g(X) \end{bmatrix}_{n-m\times n}. \tag{13}$$

将该生成矩阵写成系统形式，可得

$$\begin{bmatrix} -X^m \bmod {}_*g & 1 & 0 & \cdots & 0 \\ -X^{m+1} \bmod {}_*g & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -X^{m-1} \bmod {}_*g & 0 & 0 & \cdots & 1 \end{bmatrix}_{n-m\times n}. \tag{14}$$

特别地，若取 $n = 2m$，则 (14) 化简为

$$\begin{bmatrix} -X^m \bmod {}_*g & 1 & 0 & \cdots & 0 \\ -X^{m+1} \bmod {}_*g & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -X^{2m-1} \bmod {}_*g & 0 & 0 & \cdots & 1 \end{bmatrix}_{m\times 2m} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} & 1 & 0 & \ldots & 0 \\ 0 & g_0^{[1]} & g_1^{[1]} & \ldots & g_{m-2}^{[1]} & g_{m-1}^{[1]} & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & & & \\ 0 & 0 & 0 & \ldots & g_0^{[m-1]} & g_1^{[m-1]} & \ldots & g_{m-1}^{[m-1]} & 1 \end{bmatrix}_{m\times 2m}.$$

现在，分离出冗余部分，可得矩阵

$$N_g = \begin{bmatrix} X^m \bmod {}_*g(x) \\ X^{m+1} \bmod {}_*g(x) \\ \vdots \\ X^{2m-1} \bmod {}_*g(x) \end{bmatrix}_{m\times m}. \tag{15}$$

为了分析 N_g，引入与多项式 $g(X$ 相关的伴随矩阵很方便).

定义11。令 $g(X) = g_0 + g_1X + g_2X^2 + \cdots + g_{m-1}X^{m-1} + X^m \in \mathbb{F}_q[X;\ \theta]$ 是有限域 $\mathbb{F}_q$ 上次数为 m 的首一多项式。$g(X)$的伴随矩阵记作 C_g，定义如下:

$$C_g = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -g_0 & -g_1 & -g_2 & \cdots & -g_{m-1} \end{bmatrix}_{m\times m}.$$

对于每个整数 $i \geq 0$，我们用 $C_g^{[i]}$表示将 θ^i 应用于 C_g 的每个元素后得到的矩阵。具体而言，

$$C_g^{[i]} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\theta^i(g_0) & -\theta^i(g_1) & -\theta^i(g_2) & \cdots & -\theta^i(g_{m-1}) \end{bmatrix}_{m\times m}.$$

$$(C_{g^{[i]}})^{-1} = \begin{bmatrix} \frac{\theta^i(g_1)}{\theta^i(g_0)} & \frac{\theta^i(g_2)}{\theta^i(g_0)} & \cdots & \frac{\theta^i(g_{m-1})}{\theta^i(g_0)} & \frac{1}{\theta^i(g_0)} \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}_{m\times m}. \tag{16}$$

注意t 帽，若 A 是一个阶为 k的方阵，即 $A = (a_{ij})$，其中 $a_{ij} \in \mathbb{F}_q$ 对于 $1 \leq i,\ j \leq m$，则n $A^{[t]} = (\theta^t(a_{ij}))$，其中某个 $t \in \mathbb{N} \cup \{0\}$。

2016年，Cauchois等人 [15], 证明了如下适用于形如 (12) 的矩阵的一些乘法规则：

命题 7。 *[15,* 命题 *1]* 设 $A = (a_{s,t})$ 和 $B = (b_{s,t})$ 是有限域 $\mathbb{F}_q$ 上的两个阶为 m 的矩阵。则有

(i) $(A^{[i]})^{[j]} = A^{[i+j]}$.

(ii) $(AB)^{[i]} = A^{[i]}B^{[i]}$.

沿用 Cauchois等人 [15, 定理 2], 的方法，下面的引理将 (15) 中的冗余矩阵 N_g 表示为伴随矩阵的一系列连续 θ-扭转的结构化乘积。现在我们可以确立本节的一项主要结果，即通过准递归方法构造对合最大距离可分矩阵。

定理 5. 设 $g\langle X\rangle = g_0 + g_1X + \cdots + g_{m-1}X^{m-1} + X^m \in \mathbb{F}_{q^{2m}}[X;\theta]$ 是次数为 m的多项式，且自同构 $\theta:\ \mathbb{F}_{q^{2m}} \longrightarrow \mathbb{F}_{q^{2m}}$定义为 $\theta(a) = a^{q^2}$. 则 N_g 满足准递归性质，即

$$N_g = C_g^{[m-1]} \cdot C_g^{[m-2]} \cdots C_g^{[1]} \cdot C_g.$$

此外，若 g 是 *MDS* 码的生成多项式，则 N_g 是最大距离可分的，并满足对合性质，即 $N_g^2 = I_m$.

证明. 我们用归纳法证明，对所有整数 $i \geq 1$，下列性质 P_i 成立：

$$P_i \quad : \quad \begin{bmatrix} X^i & \mod {}_*g \\ X^{i+1} & \mod {}_*g \\ & \vdots \\ X^{i+m-1} & \mod {}_*g \end{bmatrix}_{m\times m} = C_g^{[i-1]} \cdot C_g^{[i-2]} \cdots C_g^{[1]} \cdot C_g. \tag{17}$$

对于 $i = 0$

$$P_0 \quad : \quad \begin{bmatrix} X^0 & \mod {}_*g \\ X^1 & \mod {}_*g \\ & \vdots \\ X^{m-1} & \mod {}_*g \end{bmatrix}_{m\times m} = C_g. \tag{18}$$

Thu当 $i=0$ 时，s (17) 成立。假设我们的假设对于 $1,2,\ldots,\ i-1$ 成立。那么，我们有

$$\begin{bmatrix} X^i & \mod {}_*g \\ X^{i+1} & \mod {}_*g \\ & \vdots \\ X^{i+m-1} & \mod {}_*g \end{bmatrix}_{m\times m} = C_g^{[i-1]} \cdot C_g^{[i-2]} \cdots C_g^{[1]} \cdot C_g.$$

现在，我们针对 i 证明 (17)。为此，我们计算

$$\begin{aligned} & C_g^{[i]} C_g^{[i-1]} \cdot C_g^{[i-2]} \cdots C_g^{[1]} \cdot C_g \\ = & \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \theta^i(g_0) & \theta^i(g_1) & \theta^i(g_2) & \cdots & \theta^i(g_{m-1}) \end{bmatrix}_{m\times m} \cdot \begin{bmatrix} X^i & \mod {}_*g \\ X^{i+1} & \mod {}_*g \\ & \vdots \\ X^{i+m-1} & \mod {}_*g \end{bmatrix}_{m\times m} \\ = & \begin{bmatrix} & X^{i+1} & \mod {}_*g \\ & X^{i+2} & \mod {}_*g \\ & & \vdots \\ \theta^i(g_0)X^i + \cdots + \theta^i(g_{m-1})X^{i+m-1} & & \mod {}_*g \end{bmatrix}_{m\times m} \\ = & \begin{bmatrix} & X^{i+1} & \mod {}_*g \\ & X^{i+2} & \mod {}_*g \\ & & \vdots \\ \left(\sum_{j=0}^{m-1} \theta^i(g_j) X^{j+i}\right) & & \mod {}_*g \end{bmatrix}_{m\times m} . \end{aligned} \tag{19}$$

由于,

$$X^i * g_t \quad = \quad \theta^i(g_t) X^i.$$

因此，我们有

$$\begin{aligned} X^i & *(g_0 + g_1 X + g_2 X^2 + \cdots + g_{m-1} X^{m-1}) \\ = & \ \theta^i(g_0) X^i + \theta^i(g_1) X^{i+1} + \cdots + \theta^i(g_{m-1}) X^{i+m-1} \\ = & \sum_{j=0}^{m-1} \theta^i(g_j) X^{i+j}. \end{aligned} \tag{20}$$

由 (19) 中矩阵的最后一行以及 (20)，我们得到

$$\left(\sum_{j=0}^{m-1} \theta^i(g_j) X^{j+i}\right) \quad \mod {}_*g \quad = \quad X^{i+m} \quad \mod {}_*g. \tag{21}$$

鉴于（19）中的（21），我们得出

$$C_g^{[i]} \cdot C_g^{[i-1]} \cdot C_g^{[i-2]} \cdots C_g^{[1]} \cdot C_g = \begin{bmatrix} X^{i+1} & \mod {}_*g \\ X^{i+2} & \mod {}_*g \\ & \vdots \\ X^{i+m} & \mod {}_*g \end{bmatrix}_{m\times m} . \tag{22}$$

因此，对于所有整数 $i \geq 0.$， P_i 均成立。如果我们在（22）中取 $i = 2m-1$，则得到

$$C_g^{[2m-1]} \cdots C_g = \begin{bmatrix} X^{2m} & \mod {}_*g \\ X^{2m+1} & \mod {}_*g \\ & \vdots \\ X^{3m-1} & \mod {}_*g \end{bmatrix}_{m\times m}.$$

由于 $\theta^m = I|_{\mathbb{F}_{q^{2m}}}$，因此可得 $C_g^{[m]} = C_g$。考虑到命题 7，我们计算得

$$\begin{aligned} C_g^{[2m-1]} \cdots C_g &= C_g^{[2m-1]} \cdots C_g^{[m]} C_g^{[m]} C_g^{[m-1]} \cdots C_g \\ &= (C_g^{[m-1]} \cdots C_g)(C_g^{[m-1]} \cdots C_g) \\ &= N_g \cdot N_g. \end{aligned} \tag{23}$$

由 (15) 和 (23)，可得

$$N_g^2 = \begin{bmatrix} X^{2m} & \mod {}_*g \\ X^{2m+1} & \mod {}_*g \\ & \vdots \\ X^{3m-1} & \mod {}_*g \end{bmatrix}_{m\times m}.$$

由于 $X^{2m} = 1$ 在 $\underline{\mathbb{F}_{q^{2m}}[X;\ \theta]}_{(X^{2m}-1)}$ 中，方程 (23) 得出

$$N_g^2 = \begin{bmatrix} X^0 & \mod {}_*g \\ X^1 & \mod {}_*g \\ & \vdots \\ X^{m-1} & \mod {}_*g \end{bmatrix}_{m\times m}.$$

这意味着 $N_g^2 = I_m.$。由于 N_g 生成一个最大距离可分码，并且是最大距离可分码系统形式的冗余部分。因此， N_g 是一个MDS矩阵。 □

例 6. 设 $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$，其中 $\alpha^4 + \alpha + 1 = 0$，并设 θ： $\mathbb{F}_{2^4} \longrightarrow \mathbb{F}_{2^4}$ 是由$\theta(a) = a^4$定义的映射。根据 ***(1)***，我们将多项式分解为

$$X^4 + 1 = (X^2+1) * (X^2+1) = (X^2 + \alpha X + \alpha^3 + \alpha) * (X^2 + \alpha X + \alpha^3 + \alpha^2).$$

取 $g(X) = X^2 + \alpha X + \alpha^3 + \alpha^2$。那么，

$$N_g = C_g^{[1]} \cdot C_g = \begin{bmatrix} 0 & 1 \\ \alpha^3+\alpha & \alpha^3+\alpha \end{bmatrix}_{2\times 2} \cdot \begin{bmatrix} 0 & 1 \\ \alpha^3+\alpha^2 & \alpha \end{bmatrix}_{2\times 2} = \begin{bmatrix} \alpha^3+\alpha^2 & \alpha \\ 1+\alpha+\alpha^2 & \alpha^3+\alpha^2 \end{bmatrix}_{2\times 2}.$$

该矩阵是一个对合 *MDS* 矩阵。

Gupta 等人 [19, 定理 1] 给出了判断多项式是否生成递归 MDS 矩阵的关键准则。我们将这一刻画推广到准递归MDS矩阵，从而拓展了递归 MDS 框架，并为扩散矩阵构造提供了新的见解。

定理 6. 设 $g\langle X\rangle \in \mathbb{F}_{q^{2m}}[X,\theta]$ 是次数为 m 的首一多项式，其中 $g(0) \neq 0$ $ord(g) = n \geq 2$ 且 θ： $\mathbb{F}_{q^{2m}} \to \mathbb{F}_{q^{2m}}$，定义为 $\theta(a) = a^q$。设 $E = \{0, 1, \ldots, m-1, t, t+1, \ldots, t+m-1\}$ 为某个

整数 $t, m \le t \le n-m.$。那么，矩阵 $M = C_g^{[t-1]} C_g^{[t-2]} \cdots C^{[1]} C_g$ 是最大距离可分的，当且仅当任意非零右倍式 $f\langle X\rangle$（其中 $g\langle X\rangle$）的权具有如下形式

$$f\langle X\rangle = \sum_{e\in E} f_e X^e \in \mathbb{F}_{q^{2m}}[X,\theta]$$

大于 m。

证明。根据（17），我们有

$$N_g = C_g^{[t-1]} \cdot C_g^{[t-2]} \cdots C^{[1]} \cdot C_g = \begin{bmatrix} X^t & \bmod {}_*g \\ X^{t+1} & \bmod {}_*g \\ & \vdots \\ X^{t+m-1} & \bmod {}_*g \end{bmatrix}_{m\times m}.$$

T　　¯矩阵 N_g 是最大距离可分的，当且仅当矩阵 G的任意 m 行都线性无关，其中　　e

$$\bar{G} = \left[\frac{I}{N_g}\right] = \begin{bmatrix} 1 \\ X \\ X^2 \\ \cdots \\ X^{m-1} \\ X^t \quad \bmod {}_*g \\ X^{t+1} \quad \bmod {}_*g \\ \cdots \\ X^{t+m-1} \quad \bmod {}_*g \end{bmatrix}_{2m\times m}.$$

现在很容易看出，后一个条件等价于任意非零倍数 $\ge m$的权。因此，定理得证。

□

定义 12。 设 $\mathbb{F}_q$ 是一个有限域，$g\langle X\rangle = g_0 + g_1X + \cdots + g_{m-1}X^{m-1} + X^m$ 是 $\mathbb{F}_{2^{2m}}$上的一个次数为 m 的多项式。$g\langle X\rangle$ 的倒数多项式记为 $g_*\langle X\rangle$，定义如下：

$$g_*\langle X\rangle = X^m + \frac{\theta^m(g_1)}{\theta^m(g_0)}X^{m-1} + \frac{\theta^m(g_2)}{\theta^m(g_0)}X^{m-2} + \cdots + \frac{\theta^m(g_{m-1})}{\theta^m(g_0)}X + \frac{1}{\theta^m(g_0)}.$$

由于很容易观察到

$$C_{g_*} = P(C_g^{-1})^{[m]}P, \quad \text{where} \quad P = \mathrm{circ}(0,0,\ldots,1),$$

因此，我们可以通过考察 $g\langle X\rangle$ 的倒数多项式来推导出该结果。

定理 7. 设 $g\langle X\rangle \in \mathbb{F}_{q^{2m}}[x,\theta]$ 是一个次数为 m 且满足 $g(0) \neq 0$ 的首一多项式，并设 $\mathrm{ord}(g) = n \ge 2$。考虑由 $\theta(a) = a^q$ 定义的映射 $\theta: \mathbb{F}_{q^{2m}} \to \mathbb{F}_{q^{2m}}$。如果 $g\langle X\rangle$ 能递归地生成对合*MDS*矩阵，那么其倒数多项式 $g_*\langle X\rangle$ 也能递归地生成对合*MDS*矩阵。

证明. 该证明得到定理 4 中所给证据的支持。 □

为了更好地理解新的最大距离可分矩阵与现有结构之间的关系，我们首先介绍 Hadamard积。这一运算将在证明由已有矩阵导出的新最大距离可分矩阵相关结果时发挥关键作用。

定义 ion 13. *[32,* 定义*1.3]* 设 $P\langle X\rangle$ 和 $Q\langle X\rangle$ 是 $\mathbb{F}_q[X;\ \ \theta]$ 中的两个多项式，使得

$$P\langle X\rangle = \sum_{i=0}^{m} a_i X^i,$$

and

$$Q\langle X\rangle = \sum_{i=0}^{n} b_i X^i.$$

那么， $P\langle X\rangle$ 与 $Q\langle X\rangle$ 的*Hadamard*积 $h\langle X\rangle$ 为

$$h\langle X\rangle = P\langle X\rangle \diamond Q\langle X\rangle,$$

其中， $\diamond$ 表 示*Hadamard*积，多项式 $h\langle X\rangle$ 由其系数定义如下 *ws:*

$$h\langle X\rangle = \sum_{i=0}^{\min(m,n)} c_i X^i,$$

其中

$$c_i = a_i b_i \ for\ i = 0, 1, \ldots, \min(m, n).$$

$P\langle X\rangle$ 的*Hadamard* s次幂记为 $P\langle X\rangle^{\diamond s}$，定义为

$$P\langle X\rangle^{\diamond s} = \sum_{i=0}^{m} (a_i)^s X^i.$$

定理 8. 设 $g\langle X\rangle$ 是 $\mathbb{F}_{q^{2m}}[X,\theta]$ 上次数为 m 的多项式，并假设 $g\langle X\rangle$ 给出一个准递归 *MDS* 矩阵。则($g\langle X\rangle)^{\diamond 2^t}$ 也给出一个准递归 *MDS* 矩阵，其中 $2^t \leq q^{2m} - 1$.

证明. 设 $g\langle X\rangle = g_0 + g_1 X + \cdots + g_{m-1} X^{m-1} + X^m \in \mathbb{F}_{q^{2m}}[X,\theta]$ 给出准递归 MDS 矩阵。则这意味着

$$N_g \ = \ C_g^{[m-1]} \cdot C_g^{[m-2]} \cdots C_g^{[1]} \cdot C_g, \tag{24}$$

是一个MDS矩阵。对 $g\langle X\rangle$ 取关于 $2^t \leq q^{2m} - 1$的Hadamard积，

$$h\langle X\rangle = (g\langle X\rangle)^{\diamond 2^t} = g_0^{2^t} + g_1^{2^t} X + g_2^{2^t} X^2 + \cdots + g_{m-1}^{2^t} X^{m-1} + X^m.$$

假设

$$\begin{aligned} N_g \ &= \ C_g^{[m-1]} \cdot C_g^{[m-2]} \cdots C_g^{[1]} \cdot C_g \\ &= \ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}_{m \times m}. \end{aligned}$$

设由多项式 $h\langle X\rangle$ 定义的拟递归矩阵为

$$
\begin{aligned}
N_h &= C_h^{[m-1]} \cdot C_h^{[m-2]} \cdots C_h^{[1]} \cdot C_h \\
&= \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \theta^{m-1}(g_0^{2^t}) & \theta^{m-1}(g_1^{2^t}) & \cdots & \theta^{m-1}(g_{m-1}^{2^t}) \end{bmatrix}_{m\times m} \cdot \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \theta^{m-2}(g_0^{2^t}) & \theta^{m-2}(g_1^{2^t}) & \cdots & \theta^{m-2}(g_{m-1}^{2^t}) \end{bmatrix}_{m\times m} \\
&\quad \cdots \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \ddots & 1 \\ \theta(g_0^{2^t}) & \theta(g_1^{2^t}) & \cdots & \theta(g_{m-1}^{2^t}) \end{bmatrix}_{m\times m} \cdot \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \ddots & 1 \\ g_0^{2^t} & g_1^{2^t} & \cdots & g_{m-1}^{2^t} \end{bmatrix}_{m\times m} .
\end{aligned}
$$

取 N_h 的任意一个 s 阶子矩阵，例如 N_{h_s}

$$
N_{h_s} = \begin{bmatrix} a'_{i_1 j_1} & a'_{i_1 j_2} & \cdots & a'_{i_1 j_s} \\ a'_{i_2 j_1} & a'_{i_2 j_2} & \cdots & a'_{i_2 j_s} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{i_s j_1} & a'_{i_s j_2} & \cdots & a'_{i_s j_s} \end{bmatrix}_{m\times m} .
$$

矩阵 N_{h_s} 对应于 N_g 的某个 s 阶子矩阵，例如 N_{g_s}，使得

$$
\det(N_{h_s}) = (\det(N_{g_s}))^{2^t}.
$$

由于 N_g 是最大距离可分矩阵，上述关系意味着 $\det(N_{h_s}) \neq 0$. 因此， N_h 是最大距离可分矩阵。 □

若在定理 8 中取 $\theta = I|_{\mathbb{F}_{2^{2m}}}$，则可得到以下推论:

推论5。 设 $g\langle X\rangle$ 是 $\mathbb{F}_{q^m}[X]$ 上的多项式，并假设 $g\langle X\rangle$ 给出一个递归最大距离可分矩阵 $i.e.,\ C_g^m$ 是最大距离可分矩阵。那么，$(g\langle X\rangle)^{\diamond 2^t}$ 给出一个适用于 $2^t \leq q^m - 1$. 的准递归最大距离可分矩阵

Hadamard积使我们能够在保持最大距离可分性质的同时，构造许多不同的准递归最大距离可分矩阵。这使得我们在选择具有理想结构且可在 $\mathbb{F}_q$ 上高效实现的扩散矩阵时拥有更大的灵活性。为说明这一思路，我们给出以下示例，展示如何通过 Hadamard积获得新的准递归最大距离可分矩阵。

例7。 考虑有限域 $\mathbb{F}_{2^8} = {}^{\mathbb{F}_2[X]}/_{(\mu(X))}$，其中 $\mu\langle X\rangle = X^8+X^4+X^3+X^2+1$是 $\mathbb{F}_2$上的一个本原多项式。接下来，令 $\alpha \in \mathbb{F}_{2^8}$ 为 $\mu(X)$的一个根，即 $\mathbb{F}_{2^8}$的一个本原元。设多项式 $g(X)$ $= X^4+\alpha^{76}X^3+\alpha^{251}X^2+\alpha^{81}X+\alpha^{10}$. 那么，根据 *[19, 例 2]*， $C_g = Companion(\alpha^{10}, \alpha^{81}, \alpha^{251}, \alpha^{76})$ 和C_g^4 是一个*MDS*矩阵。利用推论*5*，我们借助乘积找到了*7*个多项式

Hadamard $g(X)$，由此得到7个新的递归*MDS*矩阵。这七个多项式为 :

$$\begin{aligned}
g_1(X) = g(X)^{\diamond 2^1} &= X^4 + \alpha^{152}X^3 + \alpha^{247}X^2 + \alpha^{162}X + \alpha^{20},\\
g_2(X) = g(X)^{\diamond 2^2} &= X^4 + \alpha^{49}X^3 + \alpha^{239}X^2 + \alpha^{69}X + \alpha^{40},\\
g_3(X) = g(X)^{\diamond 2^3} &= x^4 + \alpha^{98}X^3 + \alpha^{223}X^2 + \alpha^{138}X + \alpha^{80},\\
g_4(X) = g(X)^{\diamond 2^4} &= X^4 + \alpha^{196}X^3 + \alpha^{191}X^2 + \alpha^{138}X + \alpha^{160},\\
g_5(X) = g(X)^{\diamond 2^5} &= X^4 + \alpha^{137}X^3 + \alpha^{127}X^2 + \alpha^{21}X + \alpha^{65},\\
g_6(X) = g(X)^{\diamond 2^6} &= X^4 + \alpha^{19}X^3 + \alpha^{254}X^2 + \alpha^{42}X + \alpha^{130},\\
g_7(X) = g(X)^{\diamond 2^7} &= X^4 + \alpha^{38}X^3 + \alpha^{253}X^2 + \alpha^{84}X + \alpha^{5},
\end{aligned}$$

与上述多项式相关联的递归*MDS*矩阵如下:

$$C_{g_1} = \begin{bmatrix} \alpha^{20} & \alpha^{162} & \alpha^{247} & \alpha^{152} \\ \alpha^{172} & \alpha^{126} & \alpha^{129} & \alpha^{75} \\ \alpha^{95} & \alpha^{79} & \alpha^{149} & \alpha^{13} \\ \alpha^{33} & \alpha^{8} & \alpha^{108} & \alpha^{39} \end{bmatrix}_{4\times 4}, \quad C_{g_2} = \begin{bmatrix} \alpha^{40} & \alpha^{69} & \alpha^{239} & \alpha^{49} \\ \alpha^{89} & \alpha^{252} & \alpha^{3} & \alpha^{150} \\ \alpha^{190} & \alpha^{158} & \alpha^{43} & \alpha^{26} \\ \alpha^{66} & \alpha^{16} & \alpha^{216} & \alpha^{78} \end{bmatrix}_{4\times 4},$$

$$C_{g_3} = \begin{bmatrix} \alpha^{80} & \alpha^{138} & \alpha^{223} & \alpha^{98} \\ \alpha^{178} & \alpha^{249} & \alpha^{6} & \alpha^{45} \\ \alpha^{125} & \alpha^{61} & \alpha^{86} & \alpha^{52} \\ \alpha^{32} & \alpha^{32} & \alpha^{177} & \alpha^{156} \end{bmatrix}_{4\times 4}, \quad C_{g_4} = \begin{bmatrix} \alpha^{160} & \alpha^{21} & \alpha^{191} & \alpha^{196} \\ \alpha^{101} & \alpha^{243} & \alpha^{12} & \alpha^{90} \\ \alpha^{250} & \alpha^{79} & \alpha^{149} & \alpha^{13} \\ \alpha^{33} & \alpha^{8} & \alpha^{108} & \alpha^{39} \end{bmatrix}_{4\times 4},$$

$$C_{g_5} = \begin{bmatrix} \alpha^{65} & \alpha^{42} & \alpha^{127} & \alpha^{137} \\ \alpha^{202} & \alpha^{231} & \alpha^{24} & \alpha^{180} \\ \alpha^{245} & \alpha^{244} & \alpha^{89} & \alpha^{208} \\ \alpha^{18} & \alpha^{128} & \alpha^{198} & \alpha^{114} \end{bmatrix}_{4\times 4}, \quad C_{g_6} = \begin{bmatrix} \alpha^{130} & \alpha^{84} & \alpha^{254} & \alpha^{19} \\ \alpha^{149} & \alpha^{207} & \alpha^{48} & \alpha^{105} \\ \alpha^{235} & \alpha^{233} & \alpha^{178} & \alpha^{161} \\ \alpha^{36} & \alpha^{1} & \alpha^{141} & \alpha^{228} \end{bmatrix}_{4\times 4}$$

$$C_{g_7} = \begin{bmatrix} \alpha^{5} & \alpha^{168} & \alpha^{253} & \alpha^{38} \\ \alpha^{43} & \alpha^{159} & \alpha^{96} & \alpha^{210} \\ \alpha^{215} & \alpha^{211} & \alpha^{101} & \alpha^{67} \\ \alpha^{72} & \alpha^{2} & \alpha^{27} & \alpha^{201} \end{bmatrix}_{4\times 4}.$$

6 结论与未来工作

借助斜多项式环，研究了 δ_θ-循环 MDS 矩阵和准递归MDS矩阵的构造，并给出了一些此类构造的示例。请注意，若取 $\delta = 0$和$\theta = I_{\mathbb{F}_q}$，则所得矩阵分别涵盖了 [14] 和 [15], 中的矩阵。针对对合MDS矩阵的一项重要要求，我们在定理 5 中得到了对合的准递归MDS矩阵。

尽管准递归MDS矩阵早已为人熟知，但我们对自同构参数的选择产生了一个对合 MDS 矩阵，从而能够高效地计算其逆矩阵。这促使我们进一步研究结构化MDS矩阵；尤其是，利用θ-导子构造准递归MDS矩阵仍是一个开放问题。我们还将MDS δ_θ-循环矩阵的完整刻画留作开放问题（见开放问题 1）。此外，研究δ_θ-循环矩阵是否具有正交性质也值得探索。未来的工作还可以探讨这些构造能否扩展，以生成半对合或半正交MDS矩阵。

7 声明

经费
本研究未获得来自公共部门、商业部门或非营利部门的任何专项经费。

数据可用性声明
由于本研究未生成或分析任何数据集，因此本文不适用数据共享。

利益冲突
作者声明不存在利益冲突。

参考文献

[1] Adhiguna, I.，Arifin, I. S. N.，Yuliawan, F.，Muchtadi-Alamsyah, I.：关于正交循环MDS矩阵，《国际数学与计算机科学杂志》，**17**(4)(2022)，1619-1637。[2] Ali, S.，Ashraf, M.，De Filippis, V.，Oukhtite, L.，Rehman, N. U. (2025)。环与代数中的微分恒等式及其应用。CRC出版社。[3] Ali, S.，Khan, A. A.，Singh, B.：关于有限交换环上的循环对合正交MDS矩阵。《应用代数、工程、通信与计算》，**36**(2024)，1151-1165。[4] Ali, S.，Alali, A. S.，Khan, A. A.，Wijayanti, I. E.，Wong, K. B.：有限交换环上的异或计数与分块循环MDS矩阵。《*AIMS*数学》，**9**(11)(2024)，30529-30547。[5] Ali, S.，Rafiquee, N. N.，Varshney, V.：环中的某些类型的导子：综述，《印度尼西亚数学学会杂志》，**30**(2)(2024)。[6] Argac, N.；Kaya, A.；Kisir, A.：(σ，τ)-导子在素环中的研究，《冈山大学数学杂志》，**29**(1987)，173-177。[7] Ashraf, M.，Ali, S.，Haetinger, C.：关于环中的导子及其应用。《阿里格尔数学通报》，**25**(2)(2006)，79-107。[8] Augot, D.，Finiasz, M.：为分组密码和哈希函数穷举搜索小维数递归MDS扩散层，载于：*2013*年*IEEE*国际信息论研讨会论文集，1551-1555，2013。[9] Augot, D.，Finiasz, M.：使用缩短BCH码直接构造递归MDS扩散层，载于：*FSE 2014*，《计算机科学讲义》，**8540**(2015)，3-17。施普林格，海德堡。[10]Berger, T.P.：从Gabidulin码构造递归MDS扩散层：载于：*IN- DOCRYPT 2013*，《计算机科学讲义》**8250**，274-285，施普林格。[11] Berger, T. P.，Ourivski, A.：从Gabidulin码构造新的MDS码，载于*ACCT 2009*论文集，克拉内沃，保加利亚，第40–47页，2004。[12] Boucher, D.，Ulmer, F.：使用带自同构和导子的斜多项式的线性码。《*Des. Codes Cryptogr.*》，**70**(2014)，405-431。

[13] Boulagouaz, M.，Leroy, A.：(σ-δ)-码，《Adv. Math. Commun.》，7(4)(2013)。[14]Cauchois, V.，Loidreau, P.：关于循环对合MDS矩阵，《Des. Codes Cryptogr.》，87(2)(2019)，249-260。[15] Cauchois, V.，Loidreau, P.，Merkiche, N.：从2-循环码直接构造准对合递归型MDS矩阵，《IACR 对称密码学汇刊》，2016年。[16] Cohn, P. M.：自由环及其关系，Academia Press，伦敦，1971。[17] Daemen J.，Rijmen V.：Rijndael的设计：AES——高级加密标准。载于：《信息安全与密码学》，施普林格，纽约，2002。[18] Friedberg, S. H.，Insel, A. J.，Spence, L. E.：线性代数，培生新版国际版。培生高等教育，2013。[19] Gupta, K. C.，Pandey, S. K.，Venkateswarlu, A.：迈向递归MDS扩散层的一般构造，《Des. Codes Cryptogr.》，82(2017)，179-195。[20] Gupta, K. C.，Ray, I. G.：基于循环矩阵和类循环矩阵、面向轻量级应用的密码学上重要的MDS矩阵，《Cryptogr. Commun.》，7(2)(2015)，257-287。[21] Gupta, K. C.，Ray, I. G.：利用伴随矩阵构造面向轻量级密码学的MDS矩阵，载于CD-ARES 研讨会 2013，《计算机科学讲义》，第8128卷，第29–43页，施普林格，纽约，2013。[22] Guo, J.，Peyrin, T.，Poschmann A.：PHOTON 系列轻量级哈希函数。载于：CRYPTO 2011。《计算机科学讲义》，6841，222-239。施普林格，海德堡，2011。[23] Guo, J.，Peyrin, T.，Poschmann A.，Robshaw M. J. B.：LED 分组密码。载于：CHES 2011，《计算机科学讲义》6917，326-341。施普林格，海德堡，2011。[24] Jacobson, N.：环的结构，美国数学学会，37(1956)。[25] Hou, X. D.：有限域讲义，美国数学学会，190(2018)[26] Kesarwani, A.，Pandey, S.，Sarkar, S.，Venkateswarlu, A.：有限交换环上的递归MDS矩阵，《离散应用数学》，304(2021)，384-396。[27] Liu, S.，Manganiello, F.，Kschischang, F. R.：K¨otter在斜多项式环中的插值，《Des. Codes Cryptogr.》，72(2014)，593-608。[28] MacWilliams, F. J.，Sloane, N. J. A.：纠错码理论，北荷兰出版社，阿姆斯特丹（1977）。[29] Nowicki, A.：积分导子，《代数杂志》，110(1)(1987)，262-276。[30] Ore, O.：非交换多项式理论，《数学年刊》，第2辑，34(3)(1933)，480-508。[31] Ou-azzou, H.，Najmeddine, M.，Aydin, N.，Mouloua, E. M.：关于(M, σ,δ)-斜码的代数结构。《代数杂志》，637(2024)，156-192。[32] Render, H.，Sauer, A.：带Hadamard乘法的全纯函数代数。UD，数学系，1995。[33] Rijmen, V.，Daemen, J.，Preneel, B.，Bosselaers, A.，Win, E.D.：密码SHARK。载于：快速软件加密国际研讨会，FSE-1996，《计算机科学讲义》1039，99-112。施普林格。

[34] Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P.：用于分组密码和哈希函数的递归扩散层，载于*FSE 2012*，《计算机科学讲义》第 7549 卷，第 385–401 页，施普林格，纽约，2012 年。[35] Wu, S., Wang, M., Wu, W.：用于（轻量级）分组密码和哈希函数的递归扩散层。载于：*SAC 2013*，《计算机科学讲义》，**7707**，355-371，施普林格，海德堡，2013 年。[36] Schnorr, C. P., Vaudenay, S.：基于多重置换的哈希网络的黑盒密码分析。载于：*EUROCRYPT 1994*，《计算机科学讲义》，**950**，47-57。施普林格，纽约。[37] Shannon, C. E.：保密系统的通信理论，《贝尔系统技术期刊》，**28**(1949)，656-715。[38] Vaudenay, S.：论多重置换的必要性：MD4 和 SAFER 的密码分析，载于：快速软件加密 *1994*，《计算机科学讲义》，**1008**，286-297。施普林格，纽约，1995 年。