arXiv:2304.00398v1 [cs.IT] 1 Apr 2023

线性代数视角下的单项式码

El Mahdi Mouloua、Mustapha Najmeddine、Maria Isabel Garcia-Planas 和 Hassan Ouazzou

摘要。 本文研究伽罗瓦域 $\mathbb{F}_q$ 上的单项式码，它们可以被视为不变子空间。具体而言，我们探讨单项式码与特征子空间之间的联系，以及单项式码分解为极小不变子空间的问题。此外，我们研究单项式码的一些性质，并通过提出广义单项式码的概念对其加以推广。

关键词： 线性代数、单项式码、超不变子空间、特征子空间。

1 引言

设 $\mathbb{F}_q$ 为含有 q 个元素的有限域，其中 q 为素数幂；设 n 为正整数，满足 $\gcd(q,n) = 1$。长度为 n、维数为k 的码 C称为线性码，如果 C 是 $\mathbb{F}_q^n$的线性子空间。若其最小汉明距离为 d，则称码 C 为$[n,k,d]$ 线性码。

若某个 $[n,k]$ 线性码 C中的向量 $c=(c_0, c_1, \ldots\ldots, c_{n-1})$ 属于 C，则当 $c=(c_0, c_1, \ldots\ldots, c_{n-1})$ 满足相应条件时，向量 $:sc=(c_{n-1}, c_0, \ldots\ldots, c_{n-2})$ 也属于 C，这样的线性码称为循环码。长度为 n 的循环码 C可以看作环 $\frac{\mathbb{F}_q[x]}{<x^n-1>}$的一个理想。循环码易于实现，并且具有丰富的代数结构。更多详情请参阅 [6, 第 4 章和 5]。

E.R Berlekamp 在 [3] 中首次对这一概念进行了推广，定义了常循环码。[4] 的工作则将单项式码引入为循环码和常循环码的推广。

域 $\mathbb{F}_q$ 上长度为 n 的码 C，若相对于向量 $a:=(a_0, \ldots\ldots, a_{n-1}) \in \mathbb{F}_q^n$，满足以下性质，则称为单项式码：只要 $c=(c_0, c_1, \ldots\ldots, c_{n-1})$ 属于 C，那么 $(a_{n-1}c_{n-1}, a_0c_0, \ldots\ldots, a_{n-2}c_{n-2})$ 也属于 C。

循环码是由向量 $a=(1,\ldots,1)$ 诱导的单项式码。如果$a=(1,\ldots,1,\lambda)$，我们称之为 λ-常循环码。

如 [4]，中所述，单项式码被广泛使用，因为可以用移位寄存器对其进行编码。

本文其余部分安排如下：第 2 节简要概述单项式码。我们将单项式码定义为极小不变子空间的直和，并推导出单项式码的一些性质。第 3 节旨在确定超不变子空间与

特定情形下特征子空间之间的关系，并描述单项式码与特征子空间之间的关系。第 4 节介绍单项式码的一种推广及其若干性质。最后，第 5 节总结全文。

2 从不变子空间的角度看单项式码

设 $\mathbb{F}_q$ 为含有 q 个元素的有限域，其中 q 是素数幂；设 $\mathbb{F}_q^n$ 为 n 元组构成的向量子空间，假设 $\gcd(q,\ n) = 1$，因为 $x^n - 1$ 在 $\mathbb{F}_q$ 上没有重复的不可约因子。

我们先回顾单项式矩阵的定义及其一些性质。

定义 1（[5]）。

1. 若 $n \times n$ 矩阵 $A = (a_{ij})_{1\le i,\ j\le n}$ 是一个单项式矩阵，当且仅当它是非奇异矩阵，并且每一行和每一列中恰好有一个非零分量。*2.* 若 $n\times n$ 矩阵 $P = (P_{ij})_{1\le i,\ j\le n}$ 被称为置换矩阵，如果存在一个置换 $\sigma \in S_n$，使得 P 可由对单位矩阵 I_n 的列进行置换得到（即），对于每个 $P_{ij} = \begin{cases} 1 \\ 0 \end{cases}$，如果 $i = \sigma(j)$，则 $i \neq \sigma(j)$，记作 $P = P_\sigma$。

注 *1*。每个置换矩阵 P_σ 都是一个单项式矩阵，其所有非零分量均等于 1。

根据 [5] 我们有以下引理：

引理 1（[5], **引理 2**）。如果 A 是一个阶数为 n 的单项式矩阵，其非零分量 a_0、a_1、……、a_{n-1} 是 $\mathbb{F}_q$的元素，那么存在一个置换 $\sigma \in S_n$，使得 $A =$对角（a_0、a_1、……、a_{n-1}）P_σ

考虑到单项式矩阵的集合具有乘法群结构。

我们关注以下形式的单项式矩阵：

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & a_{n-1} \\ a_0 & 0 & \dots & 0 & 0 \\ 0 & a_1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & a_{n-2} & 0 \end{pmatrix} \tag{1}$$

我们将其称为简单单项式矩阵。下面总结这类矩阵的一些重要性质。

命题 1（[4] 性质）。设 A 是一个简单单项式矩阵，其非零分量为 a_0、a_1、.....、$a_{n-1} \in \mathbb{F}_q$。那么，

- $A^n = a_0 ... a_{n-1} I_n$- $A^{-1} = \frac{1}{\prod_{i=0}^{n-1} a_i} A^{n-1}$.（$\prod_{i=0}^{n-1} a_i \neq 0$因为 A是非奇异的）- 假设 $a = \prod_{i=0}^{n-1} a_i$。那么 A与 A_a相似，其中：

$$A_a = \begin{pmatrix} 0 & 0 & \cdots & 0 & a \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

and

$$S = \begin{pmatrix} 0 & 0 & \cdots & 0 & \prod_{i=0}^{n-1} a_i \\ a_1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 a_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots \prod_{i=0}^{n-2} a_i & & 0 \end{pmatrix}$$

在 [4], 中，作者定义了单项式码的结构：

定义 2 ([4], 定义 3.1, 第 1103 页)。线性码 $C \subseteq {F_q}^n$ 称为带有关联向量 $a = (a_0, a_1, \ldots, a_{n-1}) \in {F_q^*}^n$ 的单项式码，若对于每个码字 $c = (c_0, c_1, \ldots, c_{n-1}) \in C$， $c' = (a_{n-1}c_{n-1}, a_0 c_0, \ldots, a_{n-2}c_{n-2})$也是一个码字。

移位（映射 $c \longrightarrow sc$) 可以表示为矩阵形式：

$$Ac^t = (a_{n-1}c_{n-1}, a_0 c_0, \ldots, a_{n-2}c_{n-2}).$$

A如下所示：

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_{n-1} \\ a_0 & 0 & \ldots & 0 & 0 \\ 0 & a_1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & a_{n-2} & 0 \end{pmatrix} \tag{2}$$

Let:

$$\begin{array}{ccccc} \Phi_a : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & x = (x_0, x_2, \ldots, x_{n-1}) & \longmapsto & (a_{n-1}x_{n-1}, a_1 x_1, .., a_{n-2}x_{n-2}) \end{array} \tag{3}$$

其在 $\mathbb{F}_q^n$ 的标准基下的关联矩阵，恰好就是上面的矩阵 A。

显然， Φ_a 是 $\mathbb{F}_q^n$ 的一个同态。

因此，我们直接得到以下命题：

命题 2. 长度为 n、定义在域 $\mathbb{F}_q$ 上的线性码 C 是单项式的，当且仅当 C 是 $\mathbb{F}_q^n$ 的一个 A-不变子空间。

设 $f_A(x)$ 是矩阵 A 的特征多项式，则有：

$$f_A(x) = \begin{vmatrix} -x & 0 & \dots & 0 & a_{n-1} \\ a_0 & -x & \dots & 0 & 0 \\ 0 & a_1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & -x & \vdots \\ 0 & \dots & 0 & a_{n-2} & -x \end{vmatrix} = (-1)^n \left(x^n - \prod_{i=0}^{n-1} a_i \right)$$

下文中，$f(x)$ 表示 $f_A(x)$。

矩阵 A 的特征值所对应的特征向量使我们能够描述不变子空间。下面给出一个描述这些特征值结构的命题：

命题 3。 对于每个特征值 λ（若存在），向量

$$v(\lambda) = (\lambda^{n-1}, a_0\lambda^{n-2}, a_0a_1\lambda^{n-3}, \dots, a_0a_1 \dots a_{n-2})$$

是一个相应特征向量。

证明。 鉴于矩阵 A是非奇异矩阵，$a_0 \cdot a_1 \cdot \ldots \cdot a_{n-1} \cdot \lambda \neq 0$，因此 $v(\lambda) \neq 0$。

$$\begin{pmatrix} 0 & 0 & \dots & 0 & a_{n-1} \\ a_0 & 0 & \dots & 0 & 0 \\ 0 & a_1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & a_{n-2} & 0 \end{pmatrix} \begin{pmatrix} \lambda^{n-1} \\ a_0\lambda^{n-2} \\ a_0a_1\lambda^{n-3} \\ \vdots \\ a_0 \dots a_{n-2} \end{pmatrix} = \begin{pmatrix} a_{n-1}a_0 \dots a_{n-2} \\ a_0\lambda^{n-1} \\ a_0a_1\lambda^{n-2} \\ a_0a_1a_2\lambda^{n-3} \\ \vdots \\ a_0 \dots a_{n-2}\lambda \end{pmatrix} = \lambda \begin{pmatrix} \lambda^{n-1} \\ a_0\lambda^{n-2} \\ a_0a_1\lambda^{n-3} \\ \vdots \\ a_0 \dots a_{n-2} \end{pmatrix}$$

（注意 $\prod_{i=0}^{n-1} a_i = \lambda^n$）

设 $f(x) = (-1)^n f_1(x) \dots f_r(x)$ 是 f 在 $\mathbb{F}_q$ 上的不可约因子因式分解。根据凯莱-哈密顿定理，我们有 $f(A) = 0$。假设 $(n, q) = 1$，于是 $f(x)$ 有互不相同的因子 $f_i(x)$、$i = 1, \dots, r$，并考虑以下齐次方程组：

$$f_i(A)x = 0, \quad x \in \mathbb{F}_q^n \tag{4}$$

对于 $i = 1, \dots, r$。如果 W_i 表示方程 (4) 的解空间，那么我们可以写作$W_i = \mathrm{Ker}\, f_i(\Phi_a)$。为了研究单项式码分解为极小不变子空间的情形，我们需要以下命题（参见 [2]）。

命题4。设 Φ 是 V 的一个同态，且 U 是 V 的一个 Φ-不变子空间，并且维数$_F V = n$。那么 $f_{\Phi|U}(x)$ 整除 $f_{\Phi(x)}$。特别地，若$V = U \bigoplus W$且 W是 $\mathbb{F}_{11}{}^n$ 的一个 Φ-不变子空间，则 $f_{\Phi(x)} = f_{\Phi|U} f_{\Phi|W}$。并且 $Z = Z_1 \bigoplus \ldots \bigoplus Z_r$。

下面总结极小不变子空间的一般性质；对于定理1的证明，我们采用 [1] 中提出的相同方法:

定理1。 *1.* 对于每个 $i = 1, \ldots, r$， W_i是 $\mathbb{F}_q^n$的 Φ_a-不变子空间。*2.* 如果 Z 是 $\mathbb{F}_q^n$的 Φ_a-不变子空间，且 $Z_i = Z \cap W_i$，对于 $i = 1 \ldots r$，那么，Z_i是 $\mathbb{F}_q^n$的 Φ_a-不变子空间，并且 $Z = Z_1 \bigoplus \ldots \bigoplus Z_r$。*3.* $\mathbb{F}_q^n = W_1 \bigoplus \ldots \bigoplus W_t$。*4.* 维数 $_{\mathbb{F}_q} W_i =$ 次数 $f_i(x) = k_i$。*5.* $f_{\Phi_a|W_i}(x) = (-1)^{k_i} f_i(x)$。*6.* W_i 是 $\mathbb{F}_q^n$的一个极小 Φ_a-不变子空间。

证明。 1. 假设 $w \in W_i$ then $f_i(A)w = 0$，因此 $f_i(A)\Phi_a(w) = f_i(A)Aw = Af_i(A)w = 0$。于是 $\Phi_a(w) \in W_i$，因此 W_i 是一个 Φ_a-不变子空间。

2. 令 $\tilde{f}_i(x) = {}^{f}(\frac{x}{f_i\ x}(\ )$，其中 i= 1, . . . , r，由于 $(\tilde{f}_1(x) \ldots, \tilde{f}_r(x)) = 1$，我们可以找到˜一些多项式 $\tilde{}$ $a_1\ x\ \ldots\ a_r\ x \in \mathbb{F}_q[x]$ $a_1\ x\ \tilde{f}_1\ x + \ldots + (\ ), (\ )$. 使得: $(\ )(\ )\ a_r(x) f_r(\tilde{}\ x = 1$ $\tilde{}\ z \in Z$ $z = a_1\ A\ f_1\ A\ z + \ldots +)$，因此对每个 都有: $(\ )(\ ) a_r(A) f_r(A) z$，令 $\tilde{}\ z_i = a_i(A) f_i(A) z \in Z$。则 $f_i(A) z = a_i(A) f(A) z = 0$，因此 $z_i \in W_i \cap Z$，由此我们确认 $Z = Z_1 + \ldots + Z_r$.。假设 $z \in Z_i \cap \sum_{j \neq i} Z_j$，则 $f_i(A)z = 0$ 且 $f_i(A)z = 0$，由于˜gcd $(f_i(x)\ f_i(x)) = 1$，我们有多项式 $a(x)$ 和 $b(x)$，$\in \mathbb{F}_q[x]$，使得 ˜ ˜$a(x) f_i(x) + b(x) f_i(x) = 1$，因此 $z = a(A) f_i(A) z + b(A) f_i(A) z = 0$。最后$Z_i \cap \sum_{j \neq i} Z_j = 0$，因此 $Z = Z_1 \bigoplus \ldots \bigoplus Z_r$。

3. 我们只需将断言2应用于 $Z = \mathbb{F}_q^n$。

4. 设 $m \geqslant 0$ 为最小的正整数，使得对于所有 $c \in W_i$， c， $\Phi_a(c)$ $\Phi_a^2(c) \ldots, \Phi_a^m(c)$ 线性相关，那么存在元素 $c_0, \ldots, c_{m-1} \in \mathbb{F}_q$，使得:

$$\Phi_a^m(c) = c_{k-1}\Phi_a^{m-1}(c) + \ldots + c_2\Phi_a^2(c) + c_1\Phi_a(c) + c_0 c. \tag{5}$$

设 $t(x) = x^m - c_{m-1}x^{m-1} - .... - c_0$ 是 $\mathbb{F}_q$的一个多项式元素。由于$(t(\Phi_a))(c) = 0$ 且$(f_i(\Phi_a))(c) = 0$，因此 $[(t(x)\ f_i(x))(\Phi_a)](c)$ = 0，或者$(t(x)\ f_i(x))$等于1或 $f_i(x)$。因此$(t(x)\ f_i(x)) = f_i(x)$，所以 $f_i(x)$整除 $t(x)$。由此 $k_i \leqslant \deg t(x) = k$，因此向量c、$\Phi_a(c) \ldots, \Phi_a^{k_i}(c)$线性相关，因为 $c \in W_i$那么$(f_i(\Phi_a))(c) = 0$，根据 k 的最小性可得 $k = k_i$。我们知道dim $W_i \geqslant k_i$,$n = \dim_{\mathbb{F}_q} \mathbb{F}_q^n = \sum_{i=1}^r \dim_{\mathbb{F}_q} W_i \geqslant \sum_{i=1}^r k_i = \deg f = n$。于是dim$_{\mathbb{F}} W_i = k_i$。

5. 假设 $g^{(i)} = (g_1^{(i)}, \ldots\ldots, g_{k_i}^{(i)})$ 是 W_i 在 $\mathbb{F}_q$上的一个基， $i = 1, \ldots\ldots, r$并令 A_i 为相对于该基的 $\Phi_a|W_i$ 的矩阵。令 $f_i = f_{\Phi_a|W_i}$。假设 $(f_i,\ f_i) = 1$。因此，存在多项式 $u(x)\ v(x) \in \mathbb{F}_q[x]$，使得 $u(x) f_i + v(x) f_i(x) = 1$。于是 $u(A_i) f_i(A_i) + v(A_i) f_i(A_i) = I_n$。根据

凯莱-哈密顿定理 $f_i(A_i) = 0$，因此 $b(A_i)f_i(A_i) = E$。让我们验证 $f_i(A_i) = 0$，由此得到矛盾。
根据断言 3，我们得到 $g = (g_1^{(1)}, \ldots\ldots, g^{(1)\ (k_i)} \cdots, g_1^{(r)}, \ldots\ldots, g_{k_r}^{(r)})$ 是 $\mathbb{F}_q^n$ 的一个基，并且我们可以用下面的矩阵表示 Φ_a 关于基 g 的表示：

$$A' = \begin{pmatrix} A_1 & & & & \\ & A_2 & & & \\ & & \ddots & & \\ & & & A_{r-1} & \\ & & & & A_r \end{pmatrix} \tag{6}$$

又因为 $A' = P^{-1}AP$，其中 P 是从 $\mathbb{F}_q^n$ 的标准基到基 g的变换矩阵，因此：

$$f_i(A') = \begin{pmatrix} f_i(A_1) & & & & \\ & f_i(A_2) & & & \\ & & \ddots & & \\ & & & f_i(A_{r-1}) & \\ & & & & f_i(A_r) \end{pmatrix} = f_i(P^{-1}AP) = P^{-1}f_i(A)P$$

设 $g_j^{(i)} = \lambda_{j_1}^{(i)}e_1 + \ldots + \lambda_{j_n}^{(i)}e_n$，$j = 1, \ldots\ldots, k_i$。由于 $g_j \in W_i$，因此：

$$f_i(A') \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = P^{-1}f_i(A)P \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = P^{-1}f_i(A) \begin{pmatrix} \lambda_{j_1}^{(i)} \\ \\ \vdots \\ \\ \lambda_{j_n}^{(i)} \end{pmatrix} = 0$$

其中 1 位于第（$k_1 + \ldots + k_{i-1} + j$）个位置。根据最后一个等式 $f_i(A_i) = 0$，且（f_i，f_i）$\neq 1$。由于 f_i 和 f_i 是次数相同的多项式 k_i，且 f_i 是首一不可约的，因此我们得到 $f_{\Phi_a|W_i} = (-1)^{k_i}f_i$。

6. 设 W 是 $\mathbb{F}_q^n$ 的 Φ_a-不变子空间，并设 $0 \neq W \subseteq W_i$。由命题4可得，$f_{\Phi_a|W}$ 整除 f_i。由于多项式 f_i 不可约，$\dim_{\mathbb{F}_q} W = \dim_{\mathbb{F}_q} W_i$ 且 $W = W_i$。

命题5. 设 U 是 $\mathbb{F}_q^n$ 的一个 Φ-不变子空间。那么，U 是 $\mathbb{F}_q^n$ 的 Φ-不变子空间 W_i 的直和。

证明. 这一结果可由定理1的断言2直接得出。

现在，我们研究将单项式码分解为极小不变子空间；对于定理 2 的证明，我们采用了 [2] 中提出的相同方法。

定理 2。 设 C 是长度为 n、定义在 $\mathbb{F}_q$ 上的线性单项式码。则我们有以下事实：

1. $C = W_{i_1} \bigoplus \ldots \bigoplus W_{i_s}$ 和 维数$_{\mathbb{F}_q} C = k_{i_1} + \ldots + k_{i_s}$. 其中 k_{i_r} 是 W_{i_r}的维数。*2.* $f_{\Phi_a|C} = (-1)^k f_{i_1} \ldots f_{i_s} = g(x)$*3.* $c \in C$ 当且仅当 $g(A)c = 0$*4.* $f_{\Phi_a|C}$ 关于性质 *(3)* 的次数最小。*5.* 秩$(g(A)) = n - k$

证明。 1. 定理 1 的直接应用。

2. 设 $(g_1^{(i_r)}, \ldots, g^{(i_r)k_{i_r}})$ 是 W_{i_r} 在 $\mathbb{F}_q$ 上的一个基， $r = 1, \ldots, s$ 并设 A_{i_r} 为 $\Phi_a|W_{i_r}$ 相对于该基的矩阵，记为 $f_{i_r} = f_{\Phi_a|W_{i_r}}$。 那么，$(g_1^{(i_1)}, \ldots, g^{(i_1)k_{i_1}}, \ldots, g_1^{(i_s)}, \ldots, g^{(i_s)k_{i_s}})$ 是 C 在 $\mathbb{F}_q$ 上的一个基，而 $\Phi_a|C$ 在该基下可由以下矩阵表示：

$$A' = \begin{pmatrix} A_{i_1} & & & & \\ & A_{i_2} & & & \\ & & \ddots & & \\ & & & A_{i_{s-1}} & \\ & & & & A_{i_s} \end{pmatrix} \tag{7}$$

$f_{\Phi_a|C}(x) = f_{i_1}(x) \ldots f_{i_s}(x) = (-1)^{k_{i_1}+\ldots+k_{i_1}} f_{i_1} \ldots f_{i_s}$.

3. 设 $a \in C$那么 $a = w_{i_1} + \ldots + w_{i_s}$对于其中 $w_{i_r} \in W_{i_r}$且 $r = 1, \ldots s$， 以及$g(A)a = (-1)^k[(f_{i_1} \ldots f_{i_s})(A)w_{i_1} + \ldots + (f_{i_1} \ldots f_{i_s})(A)w_{i_s}] = 0$。反过来，假设 $g(A)a = 0$ 对所有 $a \in C$ 都成立，其中某个 $a \in \mathbb{F}_{||}{}^n$ ，并令验证$a \in C$。由定理1的性质3可得 $a = w_{i_1} + \ldots + w_{i_t}$， 其中 $w_{i_r} \in W_{i_r}$ $g(A)a = (-1)^k[(f_{i_1} \ldots f_{i_s})(A)w_1 + \ldots + (f_{i_1} \ldots f_{i_s})(A)w_t]$。因此 $g(A)(w_{j_1} + \ldots + w_{j_l})$， 其中 $\{j_1, \ldots, j_l\} \in \{1, \ldots, t\} \backslash \{i_1, ..., i_s\}$。令 $b = w_{j_1} + \ldots + w_{j_l}$ 且 $h(x) = (-1)^n(x^n - \prod_{i=0}^{n-1} a_i)$ $g(x)$。由于 $(h(x)$ $g(x)) = 1$， 存在多项式 $E(x)$ $F(x) \in \mathbb{F}_q[x]$， 使得 $E(x)h(x)+F(x)g(x) = 1$。因此， $v = E(A)h(A)v + F(A)g(A)v = 0$ ，所以 $a \in C$。

4. 假设 $e(x) \in \mathbb{F}_q[x]$ 是满足对所有 $a \in C$ 都有 $e(A)a = 0$ 的最低次数非零多项式。根据 $\mathbb{F}_q[x]$ 中的带余除法，存在多项式 $q(x)$ $r(x)$，使得 $g(x) = e(x)q(x) + r(x)$，其中 $deg(r(x)) < deg(e(x))$。那么，对每个向量 $a \in C$，都有 $g(A)a = q(A)e(A)a + r(A)a$ ，因此 $r(A)a = 0$。然而，除非 $r(x) = 0$，否则这与 $e(x)$ 的选择矛盾。因此 $e(x)$ 整除 $g(x)$。于是， $e(x)$ 是 $g(x)$ 的若干不可约因子的乘积；不失一般性，可假设 $e(x) = (-1)^{(k_{i_1}+k_{i_2}+\ldots+k_{i_m})} f_{i_1} f_{i_2} \ldots f_{i_m}$ 并且 $m < s$。令 $\widehat{C} = W_{i_1} \bigoplus \ldots \bigoplus W_{i_m}$，$\widehat{}$， 显然 $C \subseteq C$ ，于是 $e(x) = f_{\Phi_a|\widehat{C}}$。又由于对所有 $a \in C$ 都有 $g(A)a = 0$ ，我们得到 $C \subseteq C$。这个矛盾证明了该结论。

5. 根据性质 (3)， C 是齐次方程组$g(A)a = 0$的解空间。因此：$\dim_{\mathbb{F}_q} C = k = n -$ rank$(g(A))$，这就证明了该结论。

例 *1.* 考虑以下特殊情形： $n=4$、 $q=5$ 和 $a=(a_1=1,\ a_2=1,\ a_3=1,\ a_4=3)$。那么：

$$A=\begin{pmatrix}0&0&0&1\\3&0&0&0\\0&4&0&0\\0&0&3&0\end{pmatrix} \tag{8}$$

在 $F_5[t]$, $P_A(t)=(t^4+4)=(t+1)(t+2)(t+3)(t+4)$ 设 C 为定义在 $\mathbb{F}_5$ 上的单项式码，定义如下： $C=\ker(A+I)\bigoplus\ker(A+2I)=<1,\ 2,\ 2,\ 4>\bigoplus<1,\ 1,\ 3,\ 3>=\ker(A^2+3A+2I)=\ker\begin{pmatrix}2&0&3&3\\4&2&0&3\\2&2&2&0\\0&2&4&2\end{pmatrix}=<(1,\ 3,\ 2,\ 1),\ (0,\ 4,\ 1,\ 1)$

$>$因此 $\dim^{\mathbb{F}_q^n}(C)=2$。

3 特征子空间与单项式码

设 A 是域 $\mathbb{F}_q$ 上有限维向量空间 $\mathbb{F}_q^n$ 的一个线性映射。一个 A-不变子空间若在所有与 A 可交换的自同构下都保持不变，则称为特征子空间。若该不变子空间在所有与 A 可交换的 $\mathbb{F}_q^n$ 的线性映射下都保持不变，则称该子空间是 A 的超不变子空间。

注 *2.* - 设 F 是一个 A-不变子空间，则 XF 对所有 $X\in C(A)$ 都是 A-不变的。- F 是一个 A 不变子空间，当且仅当 $\bar{F}=S^{-1}F$ 是关于 $A=SJS^{-1}$ 的 J-不变子空间。然后，我们可以考虑矩阵 A_a。

为了构造特征子空间，描述矩阵 A 的中心化子很有帮助。

请记住， A 的中心化子 $C(A)$ 是与 A 可交换的矩阵 X 的集合。

命题 6. *a)* $C(A_a)$ 的中心化子 A_a 是由满足以下条件的矩阵 X 组成的集合：

$$X=\begin{pmatrix}x_{n-1}&ax_0&ax_1&ax_2&\cdots&ax_{n-3}&ax_{n-2}\\x_{n-2}&x_{n-1}&ax_0&ax_1&\cdots&ax_{n-4}&ax_{n-3}\\\vdots&&\ddots&\ddots&&&\\\vdots&&&\ddots&\ddots&&\\x_2&x_3&x_4&x_5&\cdots&ax_0&ax_1\\x_1&x_2&x_3&x_4&\cdots&x_{n-1}&ax_0\\x_0&x_1&x_2&x_3&\cdots&x_{n-2}&x_{n-1}\end{pmatrix}=x_{n-1}I+x_{n-2}A_a+\ldots+x_0A_a^{n-1}$$

b) 设 $\bar{A}=TA_aT^{-1}$ 是与 A_a 等价的矩阵。那么 $C(\bar{A})=\{Y\mid Y=TXT^{-1}\}$。

证明。 a) 只需解方程组 $XA_a = A_aX$。b)
$XA_a = XT^{-1}AT = T^{-1}ATX, TXT^{-1}ATT^{-1} = TT^{-1}ATXT^{-1}$。

设 $x = (x_1, \ldots\ldots, x_n)$ 是 $\mathbb{F}_q^n$中的一个向量，并考虑由 x生成的 $\mathbb{F}_q^n$的子空间 $C_{A_0}(x)$： $C_{A_0}(x) = \{x, A_0x, \ldots\ldots, A_0^rx, \ldots\ldots\}$
凯莱-哈密顿定理保证存在一个 $r \leq n-1$，使得$C_{A_0}(x) = [x, A_0x, \ldots, A_0^rx]$，并令 r为具有此性质的最小数。

推论1. 子空间 $C_{A_0}(x)$ 是特征子空间。（事实上，它是超不变子空间。）

证明。

$$(x_{n-1}I + x_{n-2}A_a + \ldots + x_0A_a^{n-1})(\alpha_0x + \alpha_1A_0x + \ldots + \alpha_rA^rx) =$$
$$x_{n-1}\alpha_0x + (x_{n-1}\alpha_1 + x_{n-2}\alpha_0)\ldots + x_0\alpha_rA_0^{n+r-1}x =$$
$$\sum_{i=0}^{r}\beta_iA^ix \in C_{A_0}(x).$$

推论2. 设 A 是一个简单单项式矩阵。那么，子空间 $C_A(x)$ 是特征子空间。

证明。 只需考虑 $A = TA_0T^{-1}$，并针对这种情况重复之前的计算。

命题7。 令 $F = \mathrm{Ker}(A - \lambda I)$ 为 A上特征值为 λ 的 A 的特征向量子空间。那么， F 是 A的特征子空间。

一般而言，令 $G = \mathrm{Ker}(p(A))$ 为 A中的某个多项式对应的子空间。那么G 是一个特征子空间。

证明。 $\forall v \in F$，并且对于所有 $X \in C(A)$、 $AXv = XAv = X(\lambda v) = \lambda Xv$，则$Xv \in F$。

$$\forall v \in G, \text{ and for all } X \in C(A),\ p(A)Xv = Xp(A)v = X0 = 0, \text{ then } Xv \in G.$$

定理3。 长度为 n 、定义在域 $\mathbb{F}_q$ 上的线性码 C 是单项式码，当且仅当 C 是 $\mathbb{F}_q^n$ 的 A- 特征子空间。

4 广义单项式码

定义 3。当且仅当线性码 C （长度为 n，定义在域 $\mathbb{F}_q$ 上）对任意单项式矩阵都满足 C 是 $\mathbb{F}_q^n$ 的不变子空间时，称其为广义单项式码。

为了求出任意单项式矩阵的不变子空间，我们分析该矩阵的特征多项式。

已知，$\{1, \ldots, n\}$ 上的任意置换 σ 都可以写成若干个不相交循环的乘积，因此我们有

命题 8. 任何单项式矩阵都可以写成若干互不相交的简单单项式矩阵的乘积（如 (1) 所示）。

命题 9. 单项式矩阵的特征多项式等于其简单单项式因子的特征多项式之积。

特征多项式分解为不可约因子，不仅取决于简单单项式因子，还取决于有限域。设 $\sigma = \sigma_1\sigma_2\ldots\sigma_r$，为 r 个 n_i–循环的乘积，且设$\sigma_i = (i_1, \ldots, i_{n_i})$ 是 σ 分解为 $r-$ 个不相交循环时的一个长度为 n_i 的循环；令 a_{i_1}，a_{i_2}，...，$a_{i_{n_i}}$ 为单项式矩阵在第 i_1，...，i_{n_i} 列中的系数。为了找出单项式矩阵下新的不变子空间，我们给出置换的最小多项式的定义，

定义 4（σ 的最小多项式）。给定置换 σ 的最小多项式 $m_\sigma(x)$ 定义为其关联矩阵 P_σ. 的最小多项式

命题 10。设 σ 是一个长度为 n 的置换，其最小多项式为$m_\sigma(x)$。

1. $m_\sigma(x) = x^n - 1$ 如果 σ 是一个 n–循环。 *2.* $m_\sigma(x) = x^{\mathrm{lcm}(n_1,n_2,\ldots,n_r)} - 1$, 如果 $\sigma = \sigma_1\sigma_2\ldots\sigma_r$ 是 n_i–循环的乘积 σ_i.

证明。 1. 假设 σ 具有平凡形式（即）：$\sigma(1, 2, \ldots, n) = (n, 1, \ldots, n-1)$，那么 P_σ 是 $x^n - 1$ 的伴随矩阵，因此 $m_\sigma = x^n - 1$。另一方面，如果 σ 不具有平凡形式，那么存在置换 σ'， ρ，使得 $\sigma = \sigma'^{-1} \circ \rho \circ \sigma$，其中 ρ是平凡的n–循环。因此 $P_\sigma = P_{\sigma'^{-1}}P_\rho P_{\sigma'} = P_{\sigma'}^{-1}P_\rho P_{\sigma'}$， 所以 $m_\sigma(x) = m_\rho(x) = x^n - 1$。 2. 我们可以将 $x^{n_i} - 1$ 写成循环的乘积。于是 $m_\sigma(x) = \mathrm{lcm}_{1\le i\le r}\{x^{n_i} - 1\} = x^{\mathrm{lcm}(n_1,n_2,\ldots,n_r)} - 1$。

下面给出当 σ r 个互不相交的 n_i-循环的乘积为 σ_i 时单项式码的分解：

定理 4. 设 $C \subseteq \mathbb{F}_q^n$ 为单项式码， $\sigma = \sigma_1\sigma_2\ldots\sigma_r$为 r 个互不相交的 n_i-循环的乘积，则 C 可分解为

$$C = C_1 \oplus C_2 \oplus \ldots \oplus C_r$$

其中每个 C_i 都是单项式。

证明。 对每个 $i = 1, \ldots, r$，设其最小多项式为 σ_i.。因此，由于 σ_i，$1 \le i \le r$ 互不相交，可以将其分解写为 $\mathbb{F}_q^n$

$$\mathbb{F}_q^n = \ker(m_1(\sigma)) \oplus \ker(m_2(\sigma)) \oplus \ldots \oplus \ker(m_r(\sigma)).$$

由此可得

$$C = C \cap \mathbb{F}_q^n = C \cap \ker(m_1(\sigma)) \oplus C \cap \ker(m_2(\sigma)) \oplus \ldots \oplus C \cap \ker(m_r(\sigma)).$$

显然， $C_i = C \cap \ker(m_r(\sigma))$ 在 $\sigma/_{\ker(m_i(\sigma))}$ 下是不变的，因此它在 σ_i，下也是不变的，所以 C_i 在 σ_i 下是不变的。

单项式矩阵下不变子空间具有特征的（事实上是超不变的子空间）这一性质，无法推广到广义单项式

Example 2. $\mathbb{F}[5]$, $n=6$, $\gcd(5,6)=1$

$$A=\begin{pmatrix}0&0&1&0&0&0\\2&0&0&0&0&0\\0&3&0&0&0&0\\0&0&0&0&0&1\\0&0&0&2&0&0\\0&0&0&0&3&0\end{pmatrix}$$

$V=[(1,2,1,0,0,0)]$ is an A-invariant subspace

Let

$$C=\begin{pmatrix}0&0&0&1&3&1\\0&0&0&2&1&2\\0&0&0&1&3&1\\1&3&1&0&0&0\\2&1&2&0&0&0\\1&3&1&0&0&0\end{pmatrix}\in C(A)$$

$$\begin{pmatrix}0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\end{pmatrix}\begin{pmatrix}1\\2\\1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\\2\\1\end{pmatrix}\notin V.$$

Since, the sub空间 is no characteristic

更一般地，计算广义单项式码的中心化子

de:

$$\begin{pmatrix}A_1&&\\&\ddots&\\&&A_r\end{pmatrix}$$

with simple 单项式矩阵

$$\begin{pmatrix}A_1&&\\&\ddots&\\&&A_r\end{pmatrix}\begin{pmatrix}X_{11}&\dots&X_{1r}\\\vdots&&\vdots\\X_{r1}&\dots&X_{rr}\end{pmatrix}-\begin{pmatrix}X_{11}&\dots&X_{1r}\\\vdots&&\vdots\\X_{r1}&\dots&X_{rr}\end{pmatrix}\begin{pmatrix}A_1&&\\&\ddots&\\&&A_r\end{pmatrix}=0.$$

等价地，

$$A_iX_{ii}-X_{ii}A_i=0, i=1,\dots,r$$
$$A_iX_{ij}-X_{ij}A_j=0, i,j=1,\dots,r, i\neq j$$

$A_iX_{ii}-X_{ii}A_i$ 对应于简单单项式矩阵的中心化子。现在假设 $A_1,\dots,A_r\in M_n(\mathbb{F})$，并且 $gcd(f_{A_i}(x)\ f_{A_j}(x)=1$ 对所有 $i,j=1,\dots,r, i\neq j$

命题 11. 在这些条件下，方程 $A_iX_{ij} - X_{ij}A_j = 0, i, j = 1, \ldots, r, i \neq j$ 有唯一解 $X_{ij} = 0$

证明。 $f_{A_i}(x) = x^n - \alpha_i$ 其中 $\alpha_i \neq \alpha_j$ 对所有 $i \neq j$ 均成立。
由 $A_iX = XA_j$ 左乘 A_i：$A_i^2X = A_iXA_j$ 将 A_iX 替换为 XA_j，
得到 $A_i^2X = XA_j^2$。重复此过程，得到

$$A_i^nX = XA_j^n$$

凯莱-哈密顿定理保证了 $A_i^n = \alpha_iI$ 和 $A_j^n = \alpha_jI$
于是，$\alpha_iIX = X\alpha_jI$ 但等价地：$(\alpha_i - \alpha_j)X = 0$ $(\alpha_i - \alpha_j) \neq 0$，所以 $X = 0$

5 结论

本文介绍了单项式码这一类码，并得出了一些关于这类码的新结果。本文讨论了特征子空间的概念，并将其与单项式码联系起来；单项式码被视为特殊同态下的不变子空间。最后，本文提出了广义单项式码这一新概念，并介绍了它的一些新性质。

参考文献

1. D. Radkova、A. Bojilov、A.J. Van Zanten，《循环码与拟扭曲码：一种代数方法》，报告 MICC 07-08，马斯特里赫特大学，2007 年。2. D. Radkova、A.J. Van Zanten，《常循环码作为不变子空间》，《线性代数及其应用》，430（2009），855-864。3. E.R. Berlekamp，《代数编码理论》，McGraw-Hill，纽约，1968 年。4. M. I. García-Planas、M. D. Magret、L. E. Um，《作为不变子空间的单项式码》，《开放数学》，（2017）。5. M.I. Garcia-Planas、M. D. Magret，《单项式矩阵的特征值与特征向量》，载于：《微分方程与应用大会/应用数学大会》，《第二十四届微分方程与应用大会/第十四届应用数学大会论文集》。加的斯：加的斯大学，2015 年，第 963-966 页。6. W.C. Huffuman、V. Pless，《纠错码基础》，剑桥大学出版社（2003 年）。