arXiv:2602.20455v1 [cs.IT] 24 Feb 2026

来自 Hermitian 曲线和范数-迹曲线的代数几何码的置换译码

´MONICA LICHTENWALNER、HIRAM H. LOPEZ、GRETCHEN L. MATTHEWS 和 PADMAPANI SENEVIRATNE

Abstract. 置换译码是一种利用线性码的置换自同构群来纠正接收字中错误的过程。给定一个接收词，一组称为 PD 集的自同构会将错误移出信息位，从而确定原始消息。本文研究若干类代数几何码的置换译码。利用底层曲线的自同构来指定码的置换自同构。具体而言，我们描述了用于单点码的置换译码集，可纠正 Hermitian 曲线和范数-迹曲线上的特定突发错误。

1. Introduction

Prange [28] 于 1962 年为循环码引入了置换译码，MacWilliams 随后将这一概念扩展到线性码 1964 [25]。另见其他早期研究 [34, 33]。后续研究着重于寻找支持置换译码的最小码自同构集 [9]，尤其关注 Golay 码 [38]。Chabanne 研究了阿贝尔码的置换译码 1992 [8],，之后又将其应用于群码 [4]。后来，人们引入了部分置换译码 [17, 20]，以实现对所有 r 个错误集合的纠正，其中 $r \leq t$， t 表示该码可纠正错误的数量。置换译码已应用于来自图、有限几何和设计的码 [18, 19], 、一阶和二阶 Reed-Muller 码 [2, 32],，以及 Reed-Solomon 码的一些映像 [23]。

置换译码使用线性码的一组自同构，称为 PD 集 C，将接收字中的错误移出信息位置。

2020年 数学主题分类。 94B05, 11T71, 14G50。关键词和短语。 线性码、置换译码、代数几何码、Hermitian 曲线、范数-迹曲线。Monica Lichtenwalner 的部分工作获得 NSF DMS-2201075 资助。Hiram H. L´opez 的部分工作获得 NSF 资助，项目编号为 DMS-2401558 和 DMS-2502705。Gretchen L. Matthews 的部分工作获得 NSF DMS-2201075、NSF DMS-2502705 以及 Commonwealth Cyber Initiative 资助。

因此，具有较多自同构的码非常适合采用这种译码方法。以往的许多研究都考虑了从定义码的底层结构继承自同构的码。这促使人们研究定义在有限域上的曲线之上的代数几何码。对于有限域 $\mathbb{F}_q$ （含 q 个元素）上的亏格为 $g \geq 2$ 的曲线 $\mathcal{X}$ ，其自同构群 $Aut(\mathcal{X})$ 满足

$$\mid Aut(\mathcal{X}) \mid \leq 16g^4,$$

其可能显著大于 Hurwitz 界

$$\mid Aut(\mathcal{X}') \mid \leq 84(g-1)$$

对于定义在特征0域上的曲线 $\mathcal{X}'$ ；但以下定义的厄米特曲线除外:

$$\mathcal{X}_q : y^q + y = x^{q+1}$$

根据 [35], ，其自同构群更大，为

$$\mid Aut(\mathcal{X}_q) \mid = 16g^4 + 4q^7 - 7q^6 + 5q^5 - q^4 - q^3$$

且亏格为 $g = {}^{q}{}_{(q-1)\ 2}$。

本文研究范数—迹曲线和厄米特曲线上的代数几何码的置换译码，以处理特定的突发错误。我们为这些错误给出了显式的 PD 集。对于正亏格的代数几何码，除了 Joyner 关于超椭圆曲线 [15]上码的置换译码猜想之外，其他进展甚少。Reed-Solomon 码（即射影直线这一亏格为 0 的曲线上的代数几何码）本身是循环码，因此其置换译码可由 MacWilliams 的工作 [25] 以及 Prange 的工作 [28]推出。我们的方法不同于 Ren [29], 的方法，后者旨在降低厄米特码中突发错误的译码复杂度。我们的方法适用于更广泛的码族，并利用码的自同构群，将其直接应用于代数几何码。此外，这些码还能根据最小距离纠正随机错误。相比之下，Ren 对厄米特码表示方式所作的改动虽优化了突发错误纠正能力，却限制了其处理随机错误的能力。我们确定了厄米特曲线和范数—迹曲线上单点码纠正某些突发错误的 PD 集。我们还强调了信息集对于这些码的作用。码自同构本身也具有独立研究价值。如今，它们支持多种应用，包括容错量子计算 [10, 30]；极化编码 [5, 13, 16, 27], ，证明某些码可达到容量 [21, 22]；以及基于码的密码学 [1, 3]。

本文组织结构如下。本节最后概述全文将使用的记号。第2节包含置换译码、代数几何码的必要预备知识，

以及码自同构。第3节重点讨论埃尔米特码的置换译码以及结构化信息集。第4节将置换译码推广到范数迹码，其信息集由任意有理点集给出。本文在第5节以总结与结束语收尾。各节均包含示例以说明所得结果。

记号。对于正整数 n，令 $[n] := \{1, \ldots, n\}$，并用 S_n表示由 n 个符号构成的对称群。对于 $I \subseteq [n]$ 和 $\sigma \in S_n$，我们记$\sigma(I) := \{\sigma(i) : i \in I\}$。以 $\mathbb{F}_q^{m\times n}$表示所有元素属于含有 q 个元素的有限域 $\mathbb{F}_q$ 的 $m \times n$ 矩阵构成的集合。令 $\mathbb{F}_q^n := \mathbb{F}_q^{1\times n}$，并令$e_1$，……，$e_n$表示标准基向量，使得 $e_i := (0, \ldots\ldots, 0, 1, 0, \ldots\ldots, 0)$，其中$i$是其唯一的非零坐标。$n \times n$ 单位矩阵记为$I_n \in \mathbb{F}_q^{n\times n}$。向量 $v \in \mathbb{F}_q^n$的重量为 $wt(v) := |\{i \in [n] : v_i \neq 0\}|$。

$\mathbb{F}_q$ 上的 $[n, k, d]$ 码 C 是 $\mathbb{F}_q^n$的一个 $\mathbb{F}_q$-子空间，维数为 k，最小距离为 d，即 u与 $v \in \mathbb{F}_q^n$之间的汉明距离 $d(u, v) := |\{i \in [n] : u_i \neq v_i\}|$对任意 c、$c' \in C$ 满足 $d(c, c') \geq d$。这样的码 C称为$\underline{t}$-纠错码，其中$t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$。当距离参数 d 在该语境中并不重要时，我们也称 C为 $[n, k]$ 码。C 的生成矩阵是其各行构成 C的一个基的任意矩阵 $G \in \mathbb{F}_q^{k\times n}$。$C$的对偶码是 $\mathbb{F}_q$上由 $C^\perp := \left\{w \in \mathbb{F}_q^n : wc^T = 0 \ \forall c \in C\right\}$给出的 $[n, n-k, d']$ 码。C 的校验矩阵是作为 $C^\perp$的生成矩阵的任意矩阵，等价地，是使得对所有 $c \in C$均有 $Hc^T = 0$ 的任意矩阵 $H \in \mathbb{F}_q^{n-k\times n}$。一组$k$ 个坐标 $I \subseteq [n]$是 C 的信息集，只要 G 中相应的列集合线性无关。给定 $y \in \mathbb{F}_q^n$与 $I := \{i_1, \ldots, i_l\} \subseteq [n]$，令 $y|_I := (y_{i_1}, \ldots, y_{i_l}) \in \mathbb{F}_q^l$。

2. Preliminaries

本节介绍后续各节主要结果所需的背景知识。我们将讨论置换译码，并回顾代数几何码及其置换自同构群。

2.1. 置换译码。

给定一个码 $C \subseteq \mathbb{F}_q^n$ 和 $\sigma \in S_n$，

$$\sigma(c) = \left(c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)}, \ldots, c_{\sigma^{-1}(n)}\right).$$

码 C 的置换自同构群为

$$Aut(C) := \{\sigma \in S_n : \sigma(C) = C\}.$$

本文中，我们用“码自同构”表示码的置换自同构群的一个元素，因为我们不考虑单项式自同构。

设 $[n, k, d]$ 为一个定义在 $\mathbb{F}_q$ 上的 C 码，其生成矩阵为 $G = [I_k \mid A] \in \mathbb{F}_q^{k\times n}$，校验矩阵为 $H = [-A^T \mid I_{n-k}] \in \mathbb{F}_q^{n-k\times n}$。那么 $I = [k]$

表示相应的信息集。置换译码取决于码的表示形式，因此有必要为生成矩阵（及其相应的校验矩阵）固定一种特定的系统形式。为方便起见，我们取上述的 G，使得 $I = [k]$。下述方法也适用于处于标准形式的生成矩阵 G，这意味着 e_1、.....、$e_k \in \mathbb{F}_q^k$ 是其列，但不一定是第 1、.....、k 列，如系统形式中那样。

定义 2.1. 子集 $S \subseteq Aut(C)$ 是 C 的一个 r-PD 集，当且仅当对于每个由 r 个坐标位置组成的集合$\{i_1, \ldots, i_r\} \subseteq [n]$，都存在一个元素 $\sigma \in S$，使得$\sigma(\{i_1, \ldots, i_r\}) \subseteq \{k+1, \ldots, n\}$。如果 $r = t := \left\lfloor \frac{d-1}{2} \right\rfloor$，则称 S为 C的t-PD 集。如果 $r < t$，则称 S 为 C 的部分置换译码集。

引理 2.2. [12, 定理 8。1] 考虑一个定义在 $\mathbb{F}_q$上的 $[n, k, d]$码 C，其信息集为 $I = [k]$，校验矩阵为 $H = [-A^T \mid I_{n-k}] \in \mathbb{F}_q^{n-k \times n}$。对于任意接收词 $y \in \mathbb{F}_q^n$，$y\,|_I$ 正确（也就是说，y的前 k个坐标中没有错误）当且仅当 $wt(Hy^T) \leq t$其中 $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

置换译码过程： 给定一个 PD 集 $S = \{\varphi_1, \ldots, \varphi_s\} \subseteq Aut(C)$ 和一个接收词 $y \in \mathbb{F}_q^n$:

(1) Find $i \in [s]$ such that

$$wt\left(H\varphi_i(y)^T\right) \leq t. \tag{2.1}$$

(2) 将 Decode y 译为

$$\varphi_i^{-1}\left(\varphi_i(y)\,|_I\right) \in C.$$

步骤 (1) 可通过计算所有 $i \in [s]$ 对应的 $wt\left(H\varphi_i(y)^T\right)$，直到找到满足方程 2.1 的 i 来完成。然后，根据引理 2.2，$\varphi_i(y)\,|_I$ 不含错误。因此，如果 S 是一个 r-PD 集，则可使用置换译码过程纠正任意 r 个错误。

对于一个 $[n, k]$ 码，使用 r-PD 集 S 的置换译码算法，其最坏情况下的时间复杂度为 $O(nk|S|)$，因此我们希望 PD 集尽可能小。当然，并非所有码都存在部分 PD 集。事实上，

$$|S| \geq \left\lceil \frac{n}{n-k} \left\lceil \frac{n-1}{n-k-1} \cdots \left\lceil \frac{n-r+1}{n-k-r+1} \right\rceil \cdots \right\rceil \right\rceil;$$

参见 $[9, 12, 31]$。鉴于码 C 甚至可能没有足够的自同构来构成部分 PD 集，因此考虑一些可用于纠正特定错误模式的自同构集合是合理的，具体如以下定义所述。

定义 2.3。子集 $S \subseteq Aut(C)$ 是 $E \subseteq [n]$ 的一个 r-PD 集，如果对于任意由 r 个坐标位置组成的集合 $\{i_1, \ldots, i_r\} \subseteq E$，都存在一个自同构 $\sigma \in S$，使得 $\sigma(\{i_1, \ldots, i_r\}) \subseteq \{k+1, \ldots, n\}$。

显然，对于 $E = [n]$，r-PD 集也是一个 r-PD 集。

2.2. 代数几何码。设 $D = P_1 + \cdots + P_n$ 和 G 是定义在域 $\mathbb{F}_q$ 上的光滑射影曲线 $\mathcal{X}$ 上的除子，且其支集不交，使得 $\deg G < n$ 且对于所有满足 $i \neq j$ 的 $i, j \in [n]$，都有 $P_i \neq P_j$。考虑代数几何码 $C(D,G) := \{ev(f) : f \in \mathcal{L}(G)\}$，其中 $ev(f) := (f(P_1) \ldots, f(P_n))$，且 $\mathcal{L}(A) := \{f \in \mathbb{F}_q(\mathcal{X}) : (f) \geq -A\} \cup \{0\}$ 表示除子 A 的黎曼-罗赫空间。回顾一下，$C(D,G)$ 是一个 $[n, \ell(G) - \ell(G-D) \geq n - \deg G]$ 码，其中 $\ell(G) := \dim_{\mathbb{F}_q} \mathcal{L}(G)$。正亏格曲线上的代数几何码的标准示例包括单点 Hermitian 码和范数-迹码，下面将对它们进行介绍。

厄米特曲线 $\mathcal{X}_q$：$y^q + y = x^{q+1}$ 在 $\mathbb{F}_{q^2}$ 上是极大曲线，亏格为 $g = \frac{q(q-1)}{2}$。$\mathcal{X}_q$ 的仿射 $\mathbb{F}_{q^2}$-有理点集为

$$\mathcal{X}_q(\mathbb{F}_{q^2}) = \bigcup_{a \in \mathbb{F}_{q^2}} \mathcal{P}_a, \quad \text{where} \quad \mathcal{P}_a := \{(a, b+\beta) : \beta \in \ker(Tr)\}$$

对满足 $b^q + b = a^{q+1}$ 和 Tr 的某个 $b \in \mathbb{F}_{q^2}$：$\mathbb{F}_{q^2} \to \mathbb{F}_q$ 表示关于扩张 $\mathbb{F}_{q^2}/\mathbb{F}_q$ 的迹映射。类似地，$\mathcal{X}_q$ 的 $\mathbb{F}_{q^2}$-有理点可划分为

$$\mathcal{X}_q(\mathbb{F}_{q^2}) = \bigcup_{b \in \mathbb{F}_{q^2}} \mathcal{Q}_b, \quad \text{where} \quad \mathcal{Q}_b := \{(\alpha a, b) : \alpha \in \ker(N)\}$$

对满足 $b^q + b = a^{q+1}$ 和 N 的某个 $a \in \mathbb{F}_{q^2}$：$\mathbb{F}_{q^2} \to \mathbb{F}_q$ 表示关于扩张 $\mathbb{F}_{q^2}/\mathbb{F}_q$ 的范数映射。此外，$\mathcal{X}_q$ 有唯一的无穷远点 $P_\infty := (0:1:0)$。

定义在 $\mathbb{F}_{q^s}$ 上的范数-迹曲线由下式定义

$$\mathcal{X}_{q,s} : y^{q^{s-1}} + \cdots + y^q + y = x^{\frac{q^s-1}{q-1}}$$

其中 $s \geq 2$ 表示 $Tr(y) = N(x)$，其中 Tr：$\mathbb{F}_{q^s} \to \mathbb{F}_q$ 是关于扩张 $\mathbb{F}_{q^s}/\mathbb{F}_q$ 的迹映射。$\mathcal{X}_{q,s}$ 的亏格为 $g = \frac{1}{2}\left(\frac{q^s-1}{q-1} - 1\right)(q^{s-1} - 1)$，而 $\mathcal{X}_{q,s}$ 有 $q^{2s-1} + 1$ 个 $\mathbb{F}_{q^s}$ 有理点，其中包括唯一的无穷远点 $P_\infty := (0:1:0)$。当 $s = 2$ 时，范数-迹曲线就是厄米特曲线。

为方便起见，我们将这些曲线上的仿射点写作 $P_{ab} := (a, b)$。此外，我们使用 $\mathcal{I}$ 来表示曲线上与某个码的信息位相关联的点集，并使用 $\mathcal{H}$ 来表示曲线上与某个码的校验位相关联的点集。

2.3. **由曲线自同构导出的码自同构**。设 $\mathcal{X}$ 是亏格为 g 的曲线。我们将看到，码 $C(D,G)$ 继承了曲线 $\mathcal{X}$ 的某些自同构；需要注意的是，该码可能还具有其他自同构，而这些自同构并非源自 $\mathcal{X}$ 的自同构。

$\mathcal{X}$ 的每个固定 D 和 G的自同构，也就是说，属于

$$Aut_{D,G}(\mathcal{X}) = \{\sigma \in Aut(\mathcal{X}) : \sigma(D) = D, \sigma(G) = G\},$$

由此得到码 $C(D,G)$ 的一个置换自同构，具体如下。给定 $\sigma \in Aut_{D,G}(\mathcal{X})$，我们可通过以下方式定义 $\sigma \in S_n$

$$\begin{array}{rccc} \overline{\sigma}: & [n] & \to & [n] \\ & i & \mapsto & j \end{array}$$

当且仅当 $\sigma(P_i) = P_j$。若 $\deg D > 2g-2$，则该映射

$$\begin{array}{rccc} \varphi: & Aut_{D,G}(\mathcal{X}) & \to & Aut\left(C(D,G)\right) \\ & \sigma & \mapsto & \overline{\sigma} \end{array}$$

是单射 [36, 命题 8.2.3], ，且等同关系 $\sigma \leftrightarrow \sigma$ 给出

$$Aut_{D,G}(\mathcal{X}) \leq Aut\left(C(D,G)\right). \tag{2.2}$$

Wesemeyer [37] 给出了保证可容许曲线上的单点码在表达式 (2.2) 中等式成立的条件。回忆： $\mathcal{X}$ 是可容许的，如果$g > 0$，则存在有理函数 $x, y \in \mathbb{F}_q(\mathcal{X})$，其极点除子为 $(x)_\infty = l_1 P_\infty$ 与 $(y)_\infty = l_2 P_\infty$，其中 $l_1, l_2 \in Z^+$，并且 $\mathcal{L}(\gamma P_\infty)$ 具有由$\langle x^i y^j$ 给出的基： $il_1 + jl_2 \leq \gamma\rangle$，对 $\gamma \in \mathbb{Z}^+$ [37, 定义 5.1]。

引理 2.4. [37, 定理 5.12] 设 $\mathcal{X}$ 是定义在 $\mathbb{F}_q$上的一条可容许曲线。假设 $1 \leq l_1 < l_2 \leq \gamma$。若

$$\deg D > \max\left\{2g+2, 2\gamma, l_1\left(l_2 + \frac{l_1-1}{\beta}\right), l_1 l_2\left(1 + \frac{l_1-1}{\gamma - l_1 + 1}\right)\right\}, \tag{2.3}$$

其中 $\beta =$最小值$\{l_1 - 1, r : y^r \in \mathcal{L}(\gamma P_\infty)\}$，则

$$Aut_{D,\gamma P_\infty}(\mathcal{X}) = Aut\left(C(D, \gamma P_\infty)\right).$$

注意到，厄米特曲线以及更一般的范数-迹曲线都是可容许的，因此引理 2.4 适用于与之相关且满足方程 (2.3) 的单点码。厄米特曲线的情形总结如下。

引理 2.5. [37, 定理5.15，推论 5.16] 设 $\mathcal{X}_q$ 是定义在 $\mathbb{F}_{q^2}$上的厄米特曲线，且 $D = \sum_{P \neq P_\infty} P$。假设 $q > 2$。若

$$q+1 \leq \gamma \leq \frac{q^3-1}{2} \quad or \quad \frac{q^3+1}{2} + q^2 - q - 2 \leq \gamma \leq q^3 + q^2 - 2q - 3,$$

then

$$Aut(C(D, \gamma P_\infty)) = Aut_{D,\gamma P_\infty}(\mathcal{X}_q).$$

根据以下结果，对于维数适中的更一般的代数几何码，也有类似的结论。

引理 2.6。 [14, 推论 3] 设 $\mathcal{X}$ 是一条亏格为 $g \geq 2$ 的曲线，其除子 D 和 G 的支集不交。若$\deg\ D \geq (1+g)\deg\ G$ 且$\deg\ G \geq 2g+1$，则

$$Aut_{D,G}(\mathcal{X}) = Aut\left(C(D,G)\right).$$

进行置换译码时，我们不一定需要该码的整个自同构群。在接下来的章节中，我们将看到，表达式 2.2 为我们关注的突发错误集合提供了 r-PD 集。

3. 厄米特码

3.1. 自同构。Stichtenoth 在 1973 [35] 中首次研究了厄米特曲线的自同构。以下便于使用的矩阵表示取自 [26, 引理 2]。

引理 3.1。设 $(a:\ b:\ e)$ 和 $(c:\ d:\ f)$ 是 $\mathcal{X}_q(\mathbb{F}_{q^2})$ 的任意两个不同点，且 ϵ 是 $\mathbb{F}_{q^2}^*$ 的一个元素。那么，存在一个由 $\mathbb{P}^2$ 上的线性映射诱导的 $\mathcal{X}_q$ 自同构，该映射由左乘矩阵定义

$$M = \begin{bmatrix} \epsilon(ed-bf)^q & \epsilon^{q+1}\xi c & a \\ \epsilon(ad-bc)^q & \epsilon^{q+1}\xi d & b \\ \epsilon(ec-af)^q & \epsilon^{q+1}\xi f & e \end{bmatrix},$$

其中 $\xi = -c^q a + d^q e + f^q b$。此外， $Aut(\mathcal{X}_q)$ 的每个元素都可以在适当选取 ϵ 和这两个点后写成这种形式。

因此，

$$Aut\left(\mathcal{X}_q\right) = \left\{\varphi_{a,b,e,c,d,f,\epsilon} : (a:b:e), (c:d:f) \in \mathcal{X}_q(\mathbb{F}_{q^2}), \epsilon \in \mathbb{F}_{q^2}^*\right\}$$

其中

$$\varphi_{a,b,e,c,d,f,\epsilon} : \begin{cases} x \mapsto \epsilon(ed-bf)^q x + \epsilon^{q+1}\xi c y + az \\ y \mapsto \epsilon(ad-bc)^q x + \epsilon^{q+1}\xi d y + bz \\ z \mapsto \epsilon(ec-af)^q x + \epsilon^{q+1}\xi f y + ez. \end{cases}$$

注意到

$$\varphi_{a,b,e,c,d,f,\epsilon}(x:y:z) = M(x:y:z)^T.$$

我们有

$$\varphi_{a,b,1,c,d,1,\epsilon}(P_{00}) = P_{ab} \quad \text{and} \quad \varphi_{a,b,1,c,d,1,\epsilon}(P_\infty) = P_{cd}.$$

也可以验证

$$\varphi_{a,b,e,c,d,f,\epsilon}(P_{00}) = (a:b:e) \quad \text{and} \quad \varphi_{a,b,e,c,d,f,\epsilon}(P_\infty) = (c:d:f).$$

因此，给定 $\mathcal{X}_q$ 上的任意两个点 $(a:\ b:\ e)$ 和 $(c:\ d:\ f)$，存在 q^2-1自同构 $\varphi_{a,b,e,c,d,f,\epsilon}$，使得 $\varphi_{a,b,e,c,d,f,\epsilon}(P_{00}) = (a:\ b:\ e)$，且 $\varphi_{a,b,e,c,d,f,\epsilon}(P_\infty) = (c:\ d:\ f)$。由此可知，$|Aut\left(\mathcal{X}_q\right)| = (q^3+1)q^3(q^2-1)$。

为确定 $\Gamma := \{\sigma \in Aut(\mathcal{X}_q) : \sigma(P_\infty) = P_\infty\}$，考虑满足 $\varphi_{a,b,e,c,d,f,\epsilon}(P_\infty) = P_\infty$ 的那些 $\varphi_{a,b,e,c,d,f,\epsilon}$。回忆一下，$\varphi_{a,b,e,c,d,f,\epsilon}(P_\infty) = (c : d : f)$，因此 $(c : d : f) = (0 : 1 : 0)$，这迫使 $c = f = 0$。唯一这样的映射为

$$\varphi_{a,b,e,0,d,0,\epsilon} : \begin{cases} x \mapsto \epsilon(ed)^q x + az \\ y \mapsto \epsilon(ad)^q x + \epsilon^{q+1}\xi dy + bz \\ z \mapsto ez \end{cases}$$

其中 $\xi = d^q e$. 我们还可以通过注意到可假设 $d = e = 1$，进一步简化这一描述。由此得到

$$\varphi_{a,b,1,0,1,0,\epsilon} : \begin{cases} x \mapsto \epsilon x + az \\ y \mapsto \epsilon a^q x + \epsilon^{q+1} y + bz \\ z \mapsto z, \end{cases} \tag{3.1}$$

或者等价地，由矩阵左乘定义的线性映射

$$M = \begin{bmatrix} \epsilon & 0 & a \\ \epsilon a^q & \epsilon^{q+1} & b \\ 0 & 0 & 1 \end{bmatrix},$$

我们注意到，鉴于每个 P_{ab} 和 $\epsilon \in \mathbb{F}_{q^2}^*$ 都会产生这样一个映射，因此 $|\Gamma| = q^3(q^2 - 1)$。

厄米特码的自同构 $C(D, \gamma P_\infty)$ 最早由 Xing 在 1995 [39]中进行研究。事实上，

$$Aut_{D,G}(\mathcal{X}_q) = \left\{\varphi_{a,b,\epsilon} : P_{ab} \in \mathcal{X}_q(\mathbb{F}_{q^2}), \epsilon \in \mathbb{F}_{q^2}^*\right\}$$

其中 $\varphi_{a,\ b,\ \epsilon} := \varphi_{a,\ b,\ 1,\ 0,\ 1,\ 0,\ \epsilon}$ 如表达式 3.1 中所示，因此

$$\varphi_{a,b,\epsilon} : \begin{array}{ccc} x & \mapsto & \epsilon x + a \\ y & \mapsto & \epsilon a^q x + \epsilon^{q+1} y + b \end{array}$$

对于形如 $\varphi_{a,b,1}$ 的映射，我们通常写作$\varphi_{a,b}$。

3.2. 系统表示。本节将看到，具有较大阶的厄米特码 $C(D, \gamma P_\infty)$ 的自同构会将 $\mathcal{X}_q$ 的仿射点划分为少数几个轨道。这些轨道给出了 $C(D, \gamma P_\infty)$ 的系统形式生成矩阵的描述。

考虑自同构

$$\sigma : \begin{cases} x \mapsto \zeta x \\ y \mapsto \zeta^{q+1} y \end{cases}$$

其中 $\mathbb{F}_{q^2}^* = \langle\zeta\rangle$；也就是说，$\sigma = \varphi_{0,\ 0,\ \zeta}$。于是，$\mathcal{X}_q$上的仿射点有 $q + 2$ 个轨道：

- q orbits of the form $O_i := \left\{P_{\zeta b_1}, P_{\zeta^2 b_2}, P_{\zeta^3 b_3}, \ldots, P_{1,b_{q^2-1}}\right\}$,

- $O_{q+1} := \{P_{0b} : b \neq 0\}$, and
- $O_{q+2} := \{P_{00}\}$.

特别地，若固定 $b \in \mathbb{F}_{q^2}$，使得 $(\zeta^{\ell}, b) \in \mathcal{X}_q(\mathbb{F}_{q^2})$，并将 $\ker(Tr) = \{\beta_1, \ldots, \beta_q\}$ 记作 $\beta_1 = 0$，则对于 $i \in [q]$,

$$O_i = \left\{(\zeta^t, \zeta^{(t-1)q+t}b + \zeta^{(t-1)(q+1)}\beta_i) : t \in [q^2-1]\right\} \tag{3.2}$$

and

$$O_{q+1} = \{(0, \beta_i) : i \in [q]\}.$$

注意，如果 $(\zeta^t, \zeta^{\ell}) \in O_j$，那么

$$\sigma^n(\zeta^t, \zeta^{\ell}) = (\zeta^{t+n}, \zeta^{n(q+1)+\ell}) = (\zeta^{t+n}, \zeta^{\ell}) \in O_j$$

对于所有 $n \in \{k(q-1) : k \in [q+1]\}$。由于 $|\{k(q-1) : k \in [q+1]\}| = q+1 = |\mathcal{Q}_{\zeta^{\ell}}|$，因此，对于某个 $j \in [q]$，有 $\mathcal{Q}_{\zeta^{\ell}} \subseteq O_j$。于是，对于任意 $b \in \mathbb{F}_{q^2}$，$\mathcal{Q}_b$ 中的所有点都属于 σ的同一轨道。

σ 的轨道给出了单点厄米特码 $C(D, \gamma P_\infty)$的系统生成矩阵的描述，如 [24]所示；另见 [11]。

命题3.2。 [24, 定理3.3和3.4] 令 $C(D, \gamma P_\infty)$ 为一个厄米特码，其中 $O_1, \ldots, O_q$ 按表达式 *(3.2)* 指定。如果 $\gamma = (i+1)(q^2-1) - q + j$且 $0 \leq j \leq q-1$，则可以取

(1) 将 $O_1, \ldots, O_i$ 中的所有点以及 O_{i+1} 中最前面的 $q_{(q-1)\,2} \quad +j$ 个点作为信息位；*(2)* 将 $O_{i+2}, \ldots, O_q, O_{q+1}, O_{q+2}$ 中的所有点以及 O_{i+1} 中的 $q^2 - 1 - \left(\binom{q(q-1)}{2} + j\right)$ 个点作为校验位。

若 $\gamma = i(q^2-1) + tq + r$ 满足 $0 \leq r \leq q-1$，则可以取

(1) 将 $O_1, \ldots, O_{i-1}$ 中的所有点、 O_i 中最前面的 $t + \cdots + q - 1 + r - (t+1)$ 个点以及 O_{i+1} 中最前面的 $1 + \cdots + q - t + r$ 个点作为信息位；*(2)* 将 $O_{i+2}, \ldots, O_q, O_{q+1}, O_{q+2}$ 中的所有点、 O_i 中剩余的 $q^2 - 1 - (t + \cdots + q - 1 + r - (t+1))$ 个点以及 O_{i+1} 中剩余的 $q^2 - 1 - (1 + \cdots + q - t + r)$ 个点作为校验位。

由于我们利用了命题3.2所提供的有理点的组织方式，我们纳入以下例子来加以说明。

例3.3. 考虑 $\mathcal{X}_4$： $y^4 + y = x^5$ 在 $\mathbb{F}_{16}$ 上。令 $\mathbb{F}_{16}^* = \langle\zeta\rangle$，其中$\zeta^4 = \zeta + 1$。考虑映射

$$\begin{array}{rccc} \sigma : & x & \mapsto & \zeta x \\ & y & \mapsto & \zeta^5 y. \end{array}$$

Then

$$\begin{aligned} O_1 &= \{(\zeta^t, \zeta^{5t+1}) : t \in [15]\} = \mathcal{Q}_\zeta \cup \mathcal{Q}_{\zeta^6} \cup \mathcal{Q}_{\zeta^{11}} \\ O_2 &= \{(\zeta^t, \zeta^{5t+2}) : t \in [15]\} = \mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^7} \cup \mathcal{Q}_{\zeta^{12}} \\ O_3 &= \{(\zeta^t, \zeta^{5t+8}) : t \in [15]\} = \mathcal{Q}_{\zeta^3} \cup \mathcal{Q}_{\zeta^8} \cup \mathcal{Q}_{\zeta^{13}} \\ O_4 &= \{(\zeta^t, \zeta^{5t+4}) : t \in [15]\} = \mathcal{Q}_{\zeta^4} \cup \mathcal{Q}_{\zeta^9} \cup \mathcal{Q}_{\zeta^{14}} \\ O_5 &= \{(0, \zeta^5), (0, \zeta^{10}), (0, 1)\} = \mathcal{Q}_{\zeta^5} \cup \mathcal{Q}_{\zeta^{10}} \cup \mathcal{Q}_{\zeta^{15}} \\ O_6 &= \{(0, 0)\} = \mathcal{Q}_0. \end{aligned}$$

例 3.4. 考虑 $\mathcal{X}_5$： $y^5+y = x^6$在 $\mathbb{F}_{25}$ 上。令 $\mathbb{F}_{25}^* = \langle\zeta\rangle$，其中 $\zeta^2-\zeta+2 = 0$。那么 $\ker(Tr) = \{0, \zeta^3, \zeta^9, \zeta^{15}, \zeta^{21}\}$ 且 $\ker(N) = \{1, \zeta^4, \zeta^8, \zeta^{12}, \zeta^{16}, \zeta^{20}\}$。考虑映射

$$\begin{aligned} \sigma : \ x &\mapsto \zeta x \\ y &\mapsto \zeta^6 y. \end{aligned}$$

Then

$$\begin{aligned} O_1 &= \{(\zeta^t, \zeta^{6t+1}) : t \in [24]\} = \mathcal{Q}_\zeta \cup \mathcal{Q}_{\zeta^7} \cup \mathcal{Q}_{\zeta^{13}} \cup \mathcal{Q}_{\zeta^{19}} \\ O_2 &= \{(\zeta^t, \zeta^{6t+18}) : t \in [24]\} = \mathcal{Q}_{\zeta^6} \cup \mathcal{Q}_{\zeta^{12}} \cup \mathcal{Q}_{\zeta^{18}} \cup \mathcal{Q}_{\zeta^{24}} \\ O_3 &= \{(\zeta^t, \zeta^{6t+4}) : t \in [24]\} = \mathcal{Q}_{\zeta^4} \cup \mathcal{Q}_{\zeta^{10}} \cup \mathcal{Q}_{\zeta^{16}} \cup \mathcal{Q}_{\zeta^{22}} \\ O_4 &= \{(\zeta^t, \zeta^{6t+5}) : t \in [24]\} = \mathcal{Q}_{\zeta^5} \cup \mathcal{Q}_{\zeta^{11}} \cup \mathcal{Q}_{\zeta^{17}} \cup \mathcal{Q}_{\zeta^{23}} \\ O_5 &= \{(\zeta^t, \zeta^{6t+20}) : t \in [24]\} = \mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^8} \cup \mathcal{Q}_{\zeta^{14}} \cup \mathcal{Q}_{\zeta^{20}} \\ O_6 &= \{(0, \zeta^3), (0, \zeta^9), (0, \zeta^{15}), (0, \zeta^{21})\} = \mathcal{Q}_{\zeta^3} \cup \mathcal{Q}_{\zeta^9} \cup \mathcal{Q}_{\zeta^{15}} \cup \mathcal{Q}_{\zeta^{21}} \\ O_7 &= \{(0, 0)\} = \mathcal{Q}_0. \end{aligned}$$

3.3. **置换译码**。现在我们将说明如何使用置换译码纠正单点厄米特码中的突发错误。首先，我们使用置换译码来纠正与具有相同 x 值的点相关联位置上的突发错误，具体如下述结果所述。

定理 3.5. 设 $C(D, \gamma P_\infty)$ 为一个厄米特码，其 γ 具有命题*3.2*的形式，且满足 $i \le q$。对于每个 $a \in \mathbb{F}_{q^2}$，固定 b_a 使得$(a : b_a) \in \mathcal{P}_a$。那么

$$\left\{\varphi_{-a,(-a)^{q+1}-b_a} : a \in \mathbb{F}_{q^2}\right\}$$

是一个大小为 q^2-1 的部分 q-*PD* 集，可用于纠正影响由 $\mathcal{P}_a$, $a \in \mathbb{F}_{q^2}$ 编号位置的突发错误。

证明。固定 $a \in \mathbb{F}_{q^2}$。我们首先证明 $(-a,(-a)^{q+1}-b_a) \in \mathcal{X}_q(\mathbb{F}_{q^2})$。假设$a = 0$。如果 q 为偶数，则 $(-a,(-a)^{q+1}-b_a) = (a : b_a) \in \mathcal{X}_q(\mathbb{F}_{q^2})$。如果 q 为奇数，则

$$(-b_a)^q + (-b_a) = -b_a^q - b_a = -(b_a^q + b_a) = -(a^{q+1}) = 0.$$

接下来，假设 $a \neq 0$。那么

$$\begin{aligned} \left((-a)^{q+1} - b_a\right)^q + (-a)^{q+1} - b_a &= (-a)^{q^2+q} + (-a)^{q+1} + (-b_a)^q + (-b_a) \\ &= (-a)^{q^2-1}(-a)^{q+1} + (-a)^{q+1} + (-b_a)^q + (-b_a) \\ &= 2(-a)^{q+1} + (-b_a)^q + (-b_a). \end{aligned}$$

如果 q 是偶数，那么

$$2(-a)^{q+1}+(-b_a)^q+(-b_a)=b_a^q+b_a=a^{q+1}=(-a)^{q+1}.$$

若 q 为奇数，则

$$\begin{aligned}2(-a)^{q+1}+(-b_a)^q+(-b_a)&=2a^{q+1}-(b_a^q+b_a)\\&=2a^{q+1}-a^{q+1}\\&=a^{q+1}=(-a)^{q+1}.\end{aligned}$$

因此，$(-a,(-a)^{q+1}-b_a)\in\mathcal{X}_q(\mathbb{F}_{q^2})$，由此可得，对于所有 $a\in\mathbb{F}_q^2$，$\varphi_{-a,(-a)^{q+1}-b_a}\in Aut(C(D,\gamma P_\infty))$。

接下来，注意到

$$\varphi_{-a,(-a)^{q+1}-b_a}((a,b_a))=(0,0)\in O_{q+2}$$

并且对于所有 $\beta\in\ker(Tr)$,

$$\varphi_{-a,(-a)^{q+1}-b_a}((a,b_a+\beta))=(0,\beta)\in O_{q+1}.$$

因此,

$$\varphi_{-a,(-a)^{q+1}-b_a}(\mathcal{P}_a)\subseteq O_{q+1}\cup O_{q+2}\subseteq\mathcal{H}$$

其中，$\mathcal{H}$ 是 $\mathcal{X}_q$ 上与 $C(D,\gamma P_\infty)$的校验位相关联的点集。□

仅使用轨道 O_{q+1} 和 O_{q+2}，我们最多只能纠正大小为 q的错误集，因为 $|O_{q+1}\cup O_{q+2}|=q$。

例3.6。考虑 $\mathcal{X}_4$：如例3.3所示，在 $\mathbb{F}_{16}$ 上定义的 $y^4+y=x^5$。为方便记号起见，将 $\mathcal{X}_4$ 上的64个点标记为 $P_1,\ldots,P_{64}$。假设收到 $y=c+e\in\mathbb{F}_{16}^{64}$，其中 $c=ev(f)\in C(D,\gamma P_\infty)$且 $e=\lambda_1e_1+\lambda_2e_{16}+\lambda_3e_{31}+\lambda_4e_{46}$。那么

$$\begin{aligned}\varphi_{1,1-a,1}(y)=\ &(f(P_{64}),f(P_{2'}),\ldots,f(P_{15'}),f(P_{61}),f(P_{17'}),\ldots,f(P_{30'}),\\&f(P_{62}),f(P_{32'}),\ldots,f(P_{45'}),f(P_{63}),f(P_{47'}),\ldots,f(P_{60'}),\\&f(P_1)+\lambda_1,f(P_{16})+\lambda_2,f(P_{31})+\lambda_3,f(P_{46})+\lambda_4)\end{aligned}$$

其中，对于 $i\in[64]$，$P_{i'}=P_{\varphi_1^{-1},1-a,1(i)}$。我们可以看出，$\varphi_{1,1-a,1}(y)\mid_{[60]}$ 没有错误。因此，$c'\coloneqq\varphi_{1,1-a,1}(y)\mid_I G\in C(D,\gamma P_\infty)$，且$c=\varphi_1^{-1},1-a,1(c')\mid_I G$。

接下来我们将证明，置换译码能够纠正与具有相同 y 值的点所对应位置中的突发错误。

定理3.7。给定一个厄米特码 $C(D,\gamma P_\infty)$，其中 γ 具有命题*3.2*的形式，且满足 $i\le q-2$，则对于影响由 $\mathcal{Q}_b$, $b\in\mathbb{F}_{q^2}$ 索引的位置的突发错误，存在一个大小为 q 的部分(q^2-1)-*PD* 集

$$\{\varphi_{0,\beta}:\beta\in\ker(Tr)\}.$$

此外，这些集合还能纠正由 $\varphi_{0\,\beta}^{-1},(O_q)$ 中的点索引的 q^2-1 个位置上的错误。

证明。若 $b \in \ker(Tr)$，则 $\varphi_{0,0}(\mathcal{Q}_b) = \mathcal{Q}_b = \{(0,b)\} \subseteq O_{q+1} \cup O_{q+2} \subseteq [n]\backslash I$，其中 I 是 $C(D,\gamma P_\infty)$ 的信息集。

若 $b \notin \ker(Tr)$，则取定 $a \in \mathbb{F}_{q^2}^*$，使得 $(a,b) \in \mathcal{X}_q$。存在 $\beta \in \ker(Tr)$，使得 $(a,b+\beta) \in O_q$。于是 $\varphi_{0,\beta}(a,b) = (a,b+\beta) \in O_q$。此外，$\varphi_{0,\beta}(\alpha a,b) = (\alpha a, b+\beta) \in O_q$ 对每个 $\alpha \in \ker(N)$ 成立。因此，

$$\varphi_{0,\beta}(\mathcal{Q}_b) \in O_q \subset \mathcal{H},$$

其中，$\mathcal{H}$ 是 $C(D,\ \gamma P_\infty)$中与校验位相关联的 $\mathcal{X}_q$ 上的点。□

例3.8。考虑如例3.3中的 $\mathbb{F}_{16}$ 上的 $\mathcal{X}_4$：$y^4+y=x^5$。对于$b \in \ker(Tr) = \{0,\zeta^5,\zeta^{10},1\}$，注意到

$$\varphi_{0,0}(\mathcal{Q}_b) = \mathcal{Q}_b = \{(0,b)\} \subseteq O_{q+1} \cup O_{q+2}.$$

因此，在这些位置上的任何错误都会在置换译码过程中得到纠正。

对于其他位置，回想一下 $O_4 = \mathcal{Q}_{\zeta^4} \cup \mathcal{Q}_{\zeta^9} \cup \mathcal{Q}_{\zeta^{14}}$。此外，

$$\begin{array}{rcl}
\varphi_{0,1}^{-1}(O_4) & = & \mathcal{Q}_\zeta \cup \mathcal{Q}_{\zeta^7} \cup \mathcal{Q}_{\zeta^3}, \\
\varphi_{0,\zeta^5}^{-1}(O_4) & = & \mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{13}} \cup \mathcal{Q}_{\zeta^{11}}, \\
\varphi_{0,\zeta^{10}}^{-1}(O_4) & = & \mathcal{Q}_{\zeta^8} \cup \mathcal{Q}_{\zeta^6} \cup \mathcal{Q}_{\zeta^{12}}, \\
\varphi_{0,0}^{-1}(O_4) & = & \mathcal{Q}_{\zeta^4} \cup \mathcal{Q}_{\zeta^9} \cup \mathcal{Q}_{\zeta^{14}}.
\end{array}$$

因此，对于上述 b，$\{\varphi_{0,0},\varphi_{0,\zeta^5},\varphi_{0,\zeta^{10}}\}$ 是一个部分 PD 集，可用于纠正影响由 $\mathcal{Q}_b$ 索引的位置的突发错误。

例3.9。考虑如例 3.4中的 $\mathbb{F}_{25}$ 上的 $\mathcal{X}_5$：$y^5+y=x^6$。对于$b \in \ker(Tr) = \{0,\zeta^3,\zeta^9,\zeta^{10},\zeta^{21}\}$，注意到

$$\varphi_{0,0}(\mathcal{Q}_b) = \mathcal{Q}_b = \{(0,b)\} \subseteq O_{q+1} \cup O_{q+2}.$$

回顾一下，$O_5 = \mathcal{Q}_{\zeta^{20}} \cup \mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^8} \cup \mathcal{Q}_{\zeta^{14}}$。此外，

$$\begin{array}{rcl}
\varphi_{0,\zeta^{21},}^{-1}(O_5) & = & \mathcal{Q}_\zeta \cup \mathcal{Q}_{\zeta^6} \cup \mathcal{Q}_{\zeta^{10}} \cup \mathcal{Q}_{\zeta^{23}}, \\
\varphi_{0,\zeta^3,}^{-1}(O_5) & = & \mathcal{Q}_{\zeta^7} \cup \mathcal{Q}_{\zeta^{12}} \cup \mathcal{Q}_{\zeta^5} \cup \mathcal{Q}_{\zeta^{16}}, \\
\varphi_{0,\zeta^9,}^{-1}(O_5) & = & \mathcal{Q}_{\zeta^{13}} \cup \mathcal{Q}_{\zeta^{18}} \cup \mathcal{Q}_{\zeta^{11}} \cup \mathcal{Q}_{\zeta^{22}}, \\
\varphi_{0,\zeta^{15},}^{-1}(O_5) & = & \mathcal{Q}_{\zeta^{19}} \cup \mathcal{Q}_1 \cup \mathcal{Q}_{\zeta^{17}} \cup \mathcal{Q}_{\zeta^4}, \\
\varphi_{0,0}(O_5) & = & \mathcal{Q}_{\zeta^{20}} \cup \mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^8} \cup \mathcal{Q}_{\zeta^{14}}.
\end{array}$$

因此，$\{\varphi_{0,0},\varphi_{0,\zeta^3},\varphi_{0,\zeta^9},\varphi_{0,\zeta^{15}},\varphi_{0,\zeta^{21}}\}$ 是一个部分置换译码集，可用于纠正影响索引位置为 $\mathcal{Q}_b$ 的突发错误，适用于上述列出的 b。

命题3.10。 设 $C(D,\gamma P_\infty)$ 是埃尔米特单点码，且γ 属于命题*3.2*所列的某种形式，其中 $i \le q-2$。对于每个 $a \in \mathbb{F}_{q^2}^*$，固定 b_a 使得$(a,b_a) \in \mathcal{X}_q$。那么， $C(D,\gamma P_\infty)$ 具有一个2-*PD* 集

$$\left\{\varphi_{-a,(-a)^{q+1}-b_a+\beta} : a \in \mathbb{F}_{q^2}^*, \beta \in \ker(Tr)\right\}$$

大小为 $q(q^2-1)$。

证明。 考虑与任意两个仿射 $\mathbb{F}_{q^2}$-有理点 (a, b) 和 (c, d) 相关联的位置。若 $a=c$，则结论由定理 3.5 得出。若 $b=d$，则结论由定理3.7 得出。

设 $a \neq b$ 且 $c \neq d$。则

$$\begin{aligned}\varphi_{-a,(-a)^{q+1}-b}(a,b) &= (0,0)\\ \varphi_{-a,(-a)^{q+1}-b}(c,d) &= (c-a,(-a)^q c+d+(-a)^{q+1}-b).\end{aligned}$$

由于 $c-a\neq 0$，存在 $\beta\in\ker(Tr)$，使得 $(c-a,\ (-a)^q c+d+(-a)^{q+1}-b+\beta) \in O_q$。因此，

$$\begin{aligned}\varphi_{0,\beta}\circ\varphi_{-a,(-a)^{q+1}-b}(a,b) &= (0,\beta)\in O_{q+1}\\ \varphi_{0,\beta}\circ\varphi_{-a,(-a)^{q+1}-b}(c,d) &= (c-a,(-a)^q c+d+(-a)^{q+1}-b+\beta)\in O_q.\end{aligned}$$

此外，$\varphi_{-a,\ (-a)^{q+1}-b+\beta} = \varphi_{0,\ \beta}\circ\varphi_{-a,\ (-a)^{q+1}-b}$ 且

$$\varphi_{-a,(-a)^{q+1}-b+\beta}\left(\mathcal{P}_a\cup\{(c,d)\}\right)\subseteq Q_q\cup Q_{q+1}\cup Q_{q+2}\subseteq\mathcal{H},$$

其中 $\mathcal{H}$ 是 $\mathcal{X}_q$ 上与 $C(D,\ \gamma P_\infty)$的校验位相关联的点集。□

表3.3列出了当 $i \le q-2$ 时， γ 取命题3.2所列形式之一且 q较小时的取值。定理3.5、3.7和3.10均适用于由表3.3中 γ 的取值定义的厄米特码。对于 $q \ge 7$， γ可能的取值要多得多。

q	可能的 γ 取值集合
3	$\{2,3,5,6,8,9,13,14\}$
4	$(\{3,\ldots,32\}\backslash\{6,10,14,21,25,29\})\ \cup\{41,42,43\}$
5	$(\{4,...,75\}\backslash\{8,13,18,23,32,37,42,47,56,61,66,71\})\ \cup\{91,...,94\}$

TABLE 1. 符合命题3.2中形式的 γ 值，在某些较小的 q值下满足 $i \le q-2$；这意味着定理3.5、3.7和3.10均适用于由这些γ 值定义的单点码。

4. Norm-trace codes

本节讨论单点范数-迹码的置换译码。上一节讨论的单点厄米特码是这一更一般构造的特例。在那里，对求值点进行自然排序，得到的信息集使厄米特码能够实现突发错误纠正。本节则讨论范数-迹码的任意信息集及其对应的置换译码。

4.1. 自同构。 曲线$\mathcal{X}_{q,\ s}$的自同构群由 Bonini、Montanucci 和 Zini 在 2020 [6, 定理 3.1]中计算得到。对于 $s \geq 3$，他们证明

$$Aut\left(\mathcal{X}_{q,s}\right) = \left\{\psi_{\beta,\epsilon} : \epsilon \in \mathbb{F}_{q^s}^*, \beta \in \ker\left(Tr\right)\right\}$$

其中

$$\begin{array}{rccl} \psi_{\beta,\epsilon}: & x & \mapsto & \epsilon x \\ & y & \mapsto & \epsilon^{\frac{q^s-1}{q-1}} y + \beta. \end{array}$$

因此，

$$\mid Aut\left(\mathcal{X}_{q,s}\right) \mid = q^{2s-1} - q^{s-1}.$$

因此，$Aut(\mathcal{X}_{q,\ s})$对于 $s \geq 3$ 不是传递的（与 $s = 2$ 情形不同，在该情形中曲线的自同构群是双传递的）。然而，他们还证明

$$Aut\left(\mathcal{X}_{q,s}\right) = Aut_{D,\gamma P_\infty}\left(\mathcal{X}_{q,s}\right),$$

因此，曲线的每个自同构都是码的自同构（与 $s = 2$ 情形不同）。

注意，$Aut_{D,\ \gamma P_\infty}(\mathcal{X}_{q,\ s})$ 也固定点集 $(0,\ \beta)$，对所有$\beta \in \ker(Tr)$ 都成立，因此这里采用将厄米特码映射到O_{q+1} 的方法并无帮助。

注4.1。 注意，$\psi_{\epsilon,\ \beta} = \varphi_{0,\ \beta,\ \epsilon}$。给定 $\epsilon \in \ker(N)$ 和 $\beta \in \ker(Tr)$,

$$\mid \psi_{\beta,\epsilon} \mid = lcm\left\{\mid \beta \mid, \mid \epsilon \mid\right\}$$

其中，$\mid \beta \mid$ 是 β 的加法阶，$\mid \epsilon \mid$ 是 ϵ的乘法阶。此外，若 q 是素数，则存在一个具有较大阶的码自同构：

$$\mid \psi_{\beta,\epsilon} \mid = \frac{q^{s+1} - q}{q-1}.$$

为说明这一点，我们必须确认存在 $\epsilon \in \ker(N)$，使得 $|\epsilon| = \frac{q^s-1}{q-1}$ and$\beta \in \ker(Tr)$，且 $|\beta| = q$。事实上，$\mid \ker(Tr) \mid = q$，它是素数，因此 $\ker(Tr)$ 的任意非零元素的阶都是 q。令 $\mathbb{F}_{q^s}^* = \langle\zeta\rangle$。我们可以观察到

$\zeta^{q^s-1}=(\zeta^{q-1})^{\frac{q^s-1}{q-1}}=1$ 意味着 $|\zeta^{q-1}|=\frac{q^s-1}{q-1}$，因为 ζ 是$\mathbb{F}_{q^s}^*$的本原元。由此可得 $\psi_{\beta,\epsilon}$ 有 $q-1$ 个轨道

$$O_i:=\cup_{j=0}^{q}\mathcal{P}_{\zeta^{(q-1)j+i}}$$

对于 $i\in[q-1]$ 和

$$O_q:=\mathcal{P}_0.$$

4.2. 系统表示。 根据 [7, 定理 3.2]，，对于一个在 $\mathbb{F}_{q^s}$ 上的单点范数-迹码 $[n,k]$ $C(D,\gamma P_\infty)$，我们可以指定任意一组 k 仿射 $\mathbb{F}_{q^s}$-有理点，使其构成一个信息集。

命题4.2。 考虑维数为 k、定义在 $\mathbb{F}_{q^s}$ 上的单点范数-迹码 $C(D,\gamma P_\infty)$ 。对于 $i\in[k]$，取 $P_i:=(a_i,b_i)\in\mathcal{X}_{q,r}$。则 $\{P_1,\ldots,P_k\}$是 $C(D,\gamma P_\infty)$的信息集。事实上，如果

$$f_i(x,y):=c_i\left(\frac{x^{q^r-1}+1}{x-a_i}\right)\left(\frac{Tr(y)-Tr(b_i)}{y-b_i}\right) \tag{4.1}$$

其中

$$c_i:=\begin{cases}-1 & \text{if } a_i=0\\ \left(-\frac{q^r-1}{q-1}\right)^{-1} & \text{otherwise,}\end{cases}$$

then

$$f_i(P_j)=\begin{cases}1 & \text{if } i=j\\ 0 & \text{otherwise.}\end{cases}$$

并且存在一个 $C(D,\gamma P_\infty)$ 的生成矩阵 G，其形式为

$$\begin{aligned}Row_i(G) &= (f_i(P_1),\ldots,f_i(P_k),f_i(P_{k+1}),\ldots,f_i(P_n))\\ &= (e_i\mid f_i(P_{k+1}),\ldots,f_i(P_n)),\end{aligned}$$

对于 $i\in[k]$。

注意，命题4.2给出了.....的显式表达式

$$G=[I_k\mid A]\in\mathbb{F}_{q^r}^{k\times n}$$

and

$$A=\begin{bmatrix}f_1(P_{k+1}) & \ldots & f_1(P_n)\\ \vdots & & \vdots\\ f_k(P_{k+1}) & \ldots & f_k(P_n)\end{bmatrix}\in\mathbb{F}_{q^r}^{k\times(n-k)}.$$

例4.3. 考虑范数-迹曲线$\mathcal{X}_{3,\ 3}$： $y^9+y^3+y=x^{13}$ 在$\mathbb{F}_{27}$上，且 $\mathbb{F}_{27}^*=\langle\zeta\rangle$，其中 $\zeta^3-\zeta+1=0$。则关于扩张 $\mathbb{F}_{27}/\mathbb{F}_3$ 所取的范数与迹满足

$$N(\zeta^i)=\begin{cases}1 & \text{if } i \text{ is even}\\ 2 & \text{if } i \text{ is odd}\end{cases}$$

and

$$Tr(\beta)=\begin{cases}0 & \text{if } \beta=\zeta,\zeta^3,\zeta^9,\zeta^{13},\zeta^{14},\zeta^{16},\zeta^{22},\zeta^{26},0\\ 1 & \text{if } \beta=\zeta^5,\zeta^8,\zeta^{15},\zeta^{17},\zeta^{19},\zeta^{20},\zeta^{23},\zeta^{24},\zeta^{25}\\ 2 & \text{if } \beta=\zeta^2,\zeta^4,\zeta^6,\zeta^7,\zeta^{10},\zeta^{11},\zeta^{12},a^{18},\zeta^{21}.\end{cases}$$

$\mathbb{F}_{27}$-有理点 $\mathcal{X}_{3,\ 3}$ 为 $(\zeta^i,\ \beta)$，其中

(1) i 为偶数，且 $\beta=\zeta^5,\zeta^8,\zeta^{15},\zeta^{17},\zeta^{19},\zeta^{20},\zeta^{23},\zeta^{24},\zeta^{25}$(2) i 为奇数，且 $\beta=\zeta^2,\zeta^4,\zeta^6,\zeta^7,\zeta^{10},\zeta^{11},\zeta^{12},\zeta^{18},\zeta^{21}$(3) $a=0$ 且 $\beta=\zeta,\zeta^3,\zeta^9,\zeta^{13},\zeta^{14},\zeta^{16},\zeta^{22},\zeta^{26}$, 0。

对于每个 $(\alpha,\ \beta)\in\mathcal{X}_{3,\ 3}(\mathbb{F}_{27})$，示性函数 $f_{\alpha,\ \beta}(x,\ y)$ 满足

$$f_{\alpha,\beta}(c,d)=\begin{cases}1 & \text{if } c=\alpha \text{ and } d=\beta\\ 0 & \text{otherwise}\end{cases}$$

如表达式 (4.1) 所示，其形式为

$$f_{\alpha,\beta}(x,y):=2\left(\frac{x^{27}-x}{x-\alpha}\right)\left(\frac{y^9+y^3+y-Tr(\beta)}{y-\beta}\right).$$

4.3. 置换译码。 令 $\mathbb{F}_{q^s}^*=\langle\zeta\rangle$，并考虑范数-迹曲线$\mathcal{X}_{q,s}$的如下自同构；它在此处将发挥与第 3.2 节中定义的厄米特曲线自同构 σ 类似的作用。

$$\begin{aligned}\psi:=\psi_{0,\zeta}:\quad x &\mapsto \zeta x\\ y &\mapsto \zeta^{\frac{q^s-1}{q-1}}y.\end{aligned}$$

ψ 将 q^{2s-1} 个仿射 $\mathbb{F}_{q^s}$-有理点划分为 $q^{s-1}+\frac{q^{s-1}-1}{q-1}+1$ 个轨道，如下所述。

- q^{s-1} 个轨道，每个轨道包含 q^s-1 个点，形式如下：

$$\bigcup_{j=1}^{q-1}\mathcal{Q}_{\zeta^{\ell+j\frac{q^s-1}{q-1}}}$$

  对每个满足 $(\zeta,\zeta^\ell)\in\mathcal{X}_{q,s}(\mathbb{F}_{q^s})$ 的 ℓ，
- $\frac{q^{s-1}-1}{q-1}$个轨道，每个轨道包含 $q-1$ 个点，形式为

$$\left\{\left(0,\zeta^{i+j\frac{q^s-1}{q-1}}\right):j\in[q-1]\right\}$$

对于每个 i，使得 $\zeta^i \in \ker(Tr)$,

- 1 仅包含点 (0，0) 的轨道。

例4.4。 考虑 $\mathcal{X}_{3,\ 3}$ 在 $\mathbb{F}_{27}$ 上，如例4.3所示。 $\mathbb{F}_{27}$有理点 $\mathcal{X}_{3,\ 3}$ 为 $(\alpha,\ \beta)$，其中

(1) $\alpha = \zeta^i$, where i is even, and $\beta = \zeta^5, \zeta^8, \zeta^{15}, \zeta^{17}, \zeta^{19}, \zeta^{20}, \zeta^{23}, \zeta^{24}, \zeta^{25}$,
(2) $\alpha = \zeta^i$, where i is odd, and $\beta = \zeta^2, \zeta^4, \zeta^6, \zeta^7, \zeta^{10}, \zeta^{11}, \zeta^{12}, \zeta^{18}, \zeta^{21}$,
(3) $\alpha = 0$ and $\beta = \zeta, \zeta^3, \zeta^9, \zeta^{13}, \zeta^{14}, \zeta^{16}, \zeta^{22}, \zeta^{26}, 0$.

ψ 的轨道如下:

(1) 9个轨道，每个轨道含26个点，形式为 $\mathcal{Q}_{\zeta^i} \cup \mathcal{Q}_{\zeta^{i+13}}$，其中 $(\zeta,\ \zeta^i) \in \mathcal{X}_{3,\ 3}$（因此 $i \in \{2, 4, 6, 7, 10, 11, 12, 18, 21\}$）；(2) 4个轨道，每个轨道含2个点，形式为 $\mathcal{Q}_{\zeta^j} \cup \mathcal{Q}_{\zeta^{j+13}} = \{(0,\ \zeta^j),\ (0,\ \zeta^{j+13})\}$，其中 $j \in \{1, 3, 9, 13\}$；(3) 1个轨道仅包含 (0 : 0)。

根据 [7, 定理 3.2], ，我们可以选择任意 k 个点作为范数-迹码的信息集。特别地，对于维数足够小的码，我们可以选择一个信息集 I 使得

$$\bigcup_{j=1}^{q-1} \mathcal{Q}_{\zeta^{\ell+j\frac{q^s-1}{q-1}}} \subseteq [n] \backslash I$$

对于某个固定的 ℓ，使得 $(\zeta :\ \zeta^\ell) \in \mathcal{X}_{q,\ s}(\mathbb{F}_{q^s})$。然后我们得到一个与范数-迹码的定理3.7等价的结果。

命题4.5。 设 $C(D,\ \gamma P_\infty)$ 为一个 $[n, k]$ 单点范数-迹码，其定义在 $\mathbb{F}_{q^s} = \langle\zeta\rangle$ 上，并满足 $k \leq q^{2s-1} - q^s + 1$. 那么， $\{\psi_{\beta,1} :\ \beta \in \ker(Tr)\}$ 是一个针对由 $\mathcal{Q}_b$ 索引的错误的部分 $\frac{q^s-1}{q-1}$ -*PD* 集，其中某个 $b \notin \ker(Tr)$。

证明。 固定 ℓ 使得 $(\zeta,\ \zeta^\ell) \in \mathcal{X}_{q,\ s}(\mathbb{F}_{q^s})$。由于 $k \leq q^{2s-1} - q^s + 1$，存在一组与校验位 $\mathcal{H}$ 相关联的点，使得

$$\bigcup_{j=1}^{q-1} \mathcal{Q}_{\zeta^{\ell+j\frac{q^s-1}{q-1}}} \subseteq \mathcal{H}.$$

固定 $b \in \mathbb{F}_{q^s}$，其中 $b \notin \ker(Tr)$。则存在某个 $\beta \in \ker(Tr)$，使得 $b + \beta = \zeta^{\ell+j\frac{q^s-1}{q-1}}$ 对某个 $j \in [q-1]$成立。由此可得，对所有 $(a, b) \in \mathcal{Q}_b$,

$$\psi_{\beta,1}(a, b) = (a, b + \beta) \in \bigcup_{j=1}^{q-1} \mathcal{Q}_{\zeta^{\ell+j\frac{q^s-1}{q-1}}}.$$

也就是说，$\psi_{\beta,1}(\mathcal{Q}_b) \subseteq \mathcal{H}$。此外，$\psi_{\beta,1}$ 可以纠正任何大小为 $\frac{q^s-1}{q-1}$ 、对应于由以下索引的位置的错误

$$\psi_{\beta,1}^{-1}\left(\bigcup_{j=1}^{q-1}\mathcal{Q}_{\zeta^{\ell+j\frac{q^s-1}{q-1}}}\right).$$

因此，我们得到一个部分 $\frac{q^s-1}{q-1}$ -PD 集。 □

例4.6。 考虑例4.3中的范数-迹曲线 $\mathcal{X}_{3,\ 3}$ ，其中$\mathbb{F}_{27}^* = \langle\zeta\rangle$。回想一下，ker$(Tr)$ $= \{0, \zeta, \zeta^3, \zeta^9, \zeta^{13}, \zeta^{14}, \zeta^{16}, \zeta^{22}, \zeta^{26}\}$。我们将 $\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}$ 指定为仅包含校验数字。注意

$$\begin{aligned}
\psi_{0,1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}},\\
\psi_{\zeta,1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^4} \cup \mathcal{Q}_{\zeta^{23}},\\
\psi_{\zeta^3,1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^{18}} \cup \mathcal{Q}_{\zeta^{24}},\\
\psi_{\zeta^9,1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^7} \cup \mathcal{Q}_{\zeta^{19}},\\
\psi_{\zeta^{13},1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^{21}} \cup \mathcal{Q}_{\zeta^{25}},\\
\psi_{\zeta^{14},1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^{10}} \cup \mathcal{Q}_{\zeta^{17}},\\
\psi_{\zeta^{16},1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^{11}} \cup \mathcal{Q}_{\zeta^5},\\
\psi_{\zeta^{22},1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^6} \cup \mathcal{Q}_{\zeta^{20}},\\
\psi_{\zeta^{26},1}^{-1}(\mathcal{Q}_{\zeta^2} \cup \mathcal{Q}_{\zeta^{15}}) &= \mathcal{Q}_{\zeta^{12}} \cup \mathcal{Q}_{\zeta^8}.
\end{aligned}$$

因此，我们可以纠正与上述列表右侧各集合中的点相关联的任意突发错误。

5. 结论

本文建立了置换译码方法，可纠正单点厄米特码和范数-迹码中的特定错误模式。据我们所知，这是首次展示正亏格曲线上的代数几何码的置换译码。值得研究其他代数几何码族的自同构群，例如由库默尔扩张或 Castle曲线产生的码族，并探索它们在置换译码方面的潜力。

References

[1] Luke Beckwith、Andre Esser、Edoardo Persichetti、Paolo Santini 和 Floyd Zweydinger。《LESS 更进一步：优化基于码等价的数字签名》。密码学 ePrint 档案，论文2025/1424，2025年。[2] José Joaquín Bernal 和 Juan Jacobo Simón。Reed-Muller 一阶码置换译码的新进展。有限域及其应用，88:102182，2023年。

[3] Jean-François Biasse、Giacomo Micheli、Edoardo Persichetti 和 Paolo Santini。《少即是多：无需伴随式的基于码的签名》。载于密码学进展——非洲密码学*2020*：第*12*届非洲密码学国际会议，埃及开罗，*2020*年*7*月*20*日至*22*日，论文集，第45–65页，柏林、海德堡，2020年。施普林格出版社。[4] E. Biglieri。群码的置换译码。载于*1995*年*IEEE*国际信息论研讨会论文集，第306–页，1995年。[5] Valerio Bioglio、Ingmar Land 和 Charles Pillet。用于自同构集成译码的极化码群性质。*IEEE*信息论汇刊，69(6):3731–3747，2023年。[6] Matteo Bonini、Maria Montanucci 和 Giovanni Zini。关于由分离多项式定义的平面曲线及其自同构。几何学进展，20(1):61–70，2020年。[7] Cícero Carvalho、Hiram H. López 和 Gretchen L. Matthews。范数-迹码的缩减。设计、码与密码学，92(5):1143–1161，2023年12月。[8] H. Chabanne。阿贝尔码的置换译码。*IEEE*信息论汇刊，38(6):1826–1829，1992年。[9] D. Gordon。用于译码二元戈莱码的最小置换集。*IEEE*信息论汇刊，28(3):541–543，1982年。[10] Markus Grassl 和 Martin Roetteler。利用量子码的自同构实现容错量子计算。载于*2013*年*IEEE*国际信息论研讨会，第534–538页，2013年。[11] C. Heegard、J. Little 和 K. Saints。利用格罗布纳基对一类代数几何戈帕码进行系统编码。*IEEE*信息论汇刊，41(6):1752–1761，1995年。[12] W. C. Huffman。《编码理论手册》第*2*卷、第*2*部分、第*17*章：码与群，第1345–1440页。爱思唯尔，1998年。[13] Lucas Johannsen、Claus Kestel、Marvin Geiselhart、Timo Vogt、Stephan Ten Brink 和 Norbert Wehn。极化码的连续消除自同构列表译码。载于*2023*年第*12*届编码专题国际研讨会（*ISTC*），第1–5页，2023年。[14] D. Joyner 和 A. Ksir。若干代数几何码的自同构群。*IEEE*信息论汇刊，52(7):3325–3329，2006年。[15] David Joyner。若干代数几何码的猜想性置换译码。*SIGSAM* 公报，39(1):26–32，2005年3月。[16] Mikhail Kamenev、Yulia Kameneva、Oleg Kurmaev 和 Alexey Maevskiy。极化码的置换译码。载于*2019*年第十六届“信息与控制系统冗余问题”国际研讨会（*REDUNDANCY*），第1–6页，2019年。[17] J.D. Key、T.P. McDonough 和 V.C. Mavron。有限平面码的部分置换译码。欧洲组合学杂志，26(5):665–682，2005年。[18] J.D. Key、T.P. McDonough 和 V.C. Mavron。有限几何码的信息集与部分置换译码。有限域及其应用，12(2):232–247，2006年。[19] J.D. Key 和 P. Seneviratne。来自矩形格图的二元码与置换译码。欧洲组合学杂志，28(1):121–126，2007年。[20] Hans-Joachim Kroll 和 Rita Vincenti。与若干经典簇相关的码的置换译码集。《离散数学》，301(1):89–105，2005年。

[21] Shrinivas Kudekar、Santhosh Kumar、Marco Mondelli、Henry D. Pfister、Eren S¸as¸so˘glu与R¨udiger Urbanke。Reed-Muller 码在擦除信道上达到容量。载于第四十八届 ACM 计算理论年会论文集，STOC ’16，第658–669页，纽约，NY，美国，2016年。计算机协会。[22] Shrinivas Kudekar、Santhosh Kumar、Marco Mondelli、Henry D. Pfister、Eren S¸as¸so˘glu与R¨udiger L. Urbanke。Reed–Muller码在擦除信道上达到容量。IEEE信息论汇刊，63(7):4298–4316，2017年。[23] Fabian Lim、Marc Fossorier与Aleksandar Kav˘ci´c。某些Reed–Solomon码的二进制映像的码自同构与置换译码。IEEE信息论汇刊，56(10):5253–5273，2010年。[24] John Little、Keith Saints与Chris Heegard。论厄米特码的结构。《纯粹与应用代数杂志》，121(3):293–314，1997年。[25] Jessie Macwilliams。系统码的置换译码。《贝尔系统技术杂志》，43(1):485–505，1964年。[26] Gretchen L. Matthews、Dane Skabelund与Michael Wills。厄米特曲线上有理点的三元组及其Weierstrass半群。《纯粹与应用代数杂志》，225(8):106623，2021年。[27] Charles Pillet、Valerio Bioglio与Ingmar Land。用于自同构集成译码的极化码。载于2021年IEEE信息论研讨会（ITW），第1–6页。IEEE出版社，2021年。[28] E. Prange。信息集在循环码译码中的应用。IRE信息论汇刊，8(5):5–9，1962年。[29] J. Ren。论厄米特码的结构及突发错误译码。载于GLOBECOM ’03。IEEE全球电信会议（IEEE目录号03CH37489），第3卷，第1613–1617页，第3卷，2003年。[30] Hasan Sayginel、Stergios Koutsioumpas、Mark Webster、Abhishek Rajput与Dan E. Browne。由码自同构得到的容错逻辑Clifford门。PRX Quantum，6:030343，2025年9月。[31] J. Sch¨onheim。论覆盖。《太平洋数学杂志》，14(4):1405 – 1411，1964年。[32] P. Seneviratne。一阶Reed–Muller码的部分置换译码。《离散数学》，309(8):1967–1970，2009年。[33] S. Shiva与K. Fung。某些三重纠错二进制码的置换译码（通信）。IEEE信息论汇刊，18(3):444–446，1972年。[34] S. Shiva、K. Fung与H. Tan。论某些长度的二元循环双纠错码的置换译码（通信）。IEEE信息论汇刊，16(5):641–643，1970年。.[35]Henning Stichtenoth。论素数特征代数函数域的自同构群。《数学档案》，24:527–544，1973 年。[36] Henning Stichtenoth。《代数函数域与码》。Springer Publishing Company, Incorporated，第2版，2008年。[37] S. Wesemeyer。论各类Goppa码的自同构群。IEEE信息论汇刊，44(2):630–643，1998年。[38] J. Wolfmann。(24, 12, 8) Golay 码的一种置换译码（通信）。IEEE信息论汇刊，29(5):748–750，1983年。[39] Chaoping Xing。论厄米特码的自同构群。IEEE信息论汇刊，41(6):1629–1635，1995年。

(Monica Lichtenwalner) Department of Mathematics, Virginia Tech, Blacks-burg, VA, USA电子邮件地址：mlichtenwalner@vt.edu (Hiram H. L´opez) Department of Mathematics, Virginia Tech, Blacksburg,VA, USA电子邮件地址：hhlopez@vt.edu (Gretchen L. Matthews) Department of Mathematics, Virginia Tech, Blacks-burg, VA, USA电子邮件地址：gmatthews@vt.edu (Padmapani Seneviratne) Department of Mathematics, Texas A&M University-Commerce, Commerce, TX, USA电子邮件地址：padmapani.seneviratne@tamuc.edu