分类号：O157.2　　单位代码：10335
密　级：　　学　　号：11635025

浙江大学

# 博士学位论文

中文论文题目：有限典型群及其子群结构在有限几何和编码理论中的应用

英文论文题目：**Finite classical groups and their applications in finite geometries and coding theory**

申请人姓名：陶然
指导教师：冯涛
专业名称：应用数学
研究方向：组合数学
所在学院：数学科学学院

论文提交日期：二〇二一年四月

# 有限典型群及其子群结构在有限几何和编码理论中的应用


**论文作者签名：**_____

**指导教师签名：**_____

论文评阅人 1：_____
评阅人 2：_____
评阅人 3：_____
评阅人 4：_____
评阅人 5：_____

答辩委员会主席：王军　教授　上海师范大学
委员 1：王军　教授　上海师范大学
委员 2：李吉有　教授　上海交通大学
委员 3：李松　教授　浙江大学
委员 4：蔺宏伟　教授　浙江大学
委员 5：谈之奕　教授　浙江大学

答辩日期：二〇二一年五月

# Finite classical groups and their applications in finite geometries and coding theory


**Author's signature:** _____

**Supervisor's signature:** _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committe Chairperson:

Prof. Jun Wang  Shanghai Normal University

Examining Committe Members:

Prof. Jun Wang  Shanghai Normal University

Prof. Jiyou Li  Shanghai Jiao Tong University

Prof. Song Li  Zhejiang University

Prof. Hongwei Lin  Zhejiang University

Prof. Zhiyi Tan  Zhejiang University

Date of oral defence: May, 2021

# 浙江大学研究生学位论文独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得浙江大学 或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：　　签字日期：　　年　　月　　日

# 学位论文版权使用授权书

本学位论文作者完全了解浙江大学 有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交本论文的复印件和磁盘，允许论文被查阅和借阅。本人授权浙江大学 可以将学位论文的全部或部分内容编入有关数据库进行检索和传播，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：　　导师签名：

签字日期：　　年　　月　　日　　签字日期：　　年　　月　　日

# 致　谢

首先我要衷心地感谢我最敬爱的导师冯涛老师. 从二年级开始, 冯老师带我进入有限几何的领域, 他经常在讨论班上为我讲解一些论文中的证明, 他的言传身教让我受用终生. 感谢冯老师为我们提供了许多与同领域的专家学者们交流讨论的机会, 使我得以开拓学术视野. 在五年的博士生涯中, 冯老师在科研和生活中给予我非常多的指导与帮助. 在此, 我想向冯老师再次表达我诚挚的感谢.

我还要感谢这五年在学习和生活中给予过我帮助和鼓励的所有老师们. 感谢南方科技大学的向青教授和首都师范大学的葛根年教授. 他们在访问浙大期间作了精彩的学术报告, 让我得以拓宽研究视野, 感受代数组合的魅力, 体验科研的乐趣.

感谢我的各位同门：胡思煌师兄、李抒行师兄、张一炜师兄、张韬师兄、上官冲师兄、汪馨师兄、Jerod Michel、丁报昆师兄、马景学师兄、钱昺辰师兄、戚立波师兄、李伟聪师兄、何智文、王野、奚元霄、徐子翔、韩雪姣、周靖坤、兰昭君、陈婷婷、孙秀芳、陆建兵、狄文帝、林培贤等. 在五年的时光里, 感谢他们对我的照顾和陪伴, 我们留下了很多美好的回忆. 感谢李伟聪师兄为我解答了很多关于有限几何和典型群方面的问题. 感谢胡思煌师兄、张一炜师兄和张韬师兄对我的帮助与指导.

感谢我亲爱的朋友们：曹媛媛、韩冰洁、纪阳、张海燕、林怡雯、景博、冉清华、蒋晓颖、孔祥雪等人. 感谢她们在我攻读博士学位期间倾听我诉说烦恼与焦虑, 给予我宽慰和鼓励, 与我交流对未来的选择, 陪我探讨人生.

感谢王永帅同学七年来的理解、支持与陪伴! 感谢我挚爱的父母, 他们的默默鼓励与支持, 激励着我不畏困难, 勇往直前. 谨此祝他们开心, 健康, 幸福!

感谢所有帮助过我的人.

由于作者水平有限, 加之时间和篇幅所限, 文中难免有谬误和不详之处, 敬请各位专家学者不吝批评指正!

# 摘　要

本学位论文主要探究有限典型群及其子群结构在有限几何和编码理论中的应用. 本文展示了, 运用有限典型群及其子群结构可以得到有限经典极空间中特定的几何结构 $m$-ovoids 和 $i$-tight sets, 二者统称为 intriguing sets. 特定的有限极空间的某种类型的 intriguing sets 会对应得到偏差集. 而参数满足一定条件的偏差集可以用来构造极小线性码. 特别地, 某些二次曲面本身也构成偏差集, 可产生极小线性码. 从而, 作为这些二次曲面自同构群的典型群自然也是相应的极小线性码的一个自同构群. 由此可见, 探究典型群的子群结构及相应的几何构型之间的联系, 是非常有意义的, 而且具有一定的实际应用价值. 本文综合运用有限域, 群论, 特征和等代数工具, 给出了几类二次曲面中 $m$-ovoids 的无穷类, 并给出了运用偏差集构造极小线性码的方法. 下面进行详细介绍.

在第 1 章中, 我们简要介绍本文的研究背景和主要贡献。

在第 2 章中, 我们简要介绍了有限经典极空间的概念, 简述了有限经典极空间的 intriguing sets, 特别是 $m$-ovoids 的定义以及它们与强正则图, 偏差集之间的联系. 我们也给出了有限典型群的概念和性质的一些介绍和说明.

在第 3 章中, 我们运用典型群及其子群结构给出了几类二次曲面中 $m$-ovoids 的无穷类的构造. 具体包括当 $q \equiv 1(\mathrm{mod}\ 4)$ 且 $q > 5$ 的情形, 我们取结构为 $C_{\frac{q^2-1}{2}} \rtimes C_2$ 的自同构群构造了 $Q(4,q)$ 中 $\frac{q-1}{2}$-ovoids 的无穷类; 当 $q \equiv 2(\mathrm{mod}\ 3)$ 的情形, 证明了 $Q^+(7,q)$ 中有以 $\mathrm{PGU}_3(q)$ 作为自同构群的 $(q^2+q)$-ovoid 和 $q^3$-ovoid; 当 $q = 3^{2k+1}$ 且 $k \geq 1$ 时, 证明了 $Q(6,q)$ 中有以 ${}^2G_2(q)$ 作为自同构群的 $q^2$-ovoid 和 $q$-ovoid.

在第 4 章中, 我们提供了一种由偏差集构造极小线性码的思路和方法. 通过我们的方法可以得出许多该类码的构造, 其中包括一些以典型群作为自同构群的极小线性码, 这种码的自同构群阶数往往较大, 从而使得它可以有快速的译码算法.

最后, 我们简要地介绍了作者攻读博士学位期间的其他工作. 此外, 也介绍了本文工作相关的一些展望和进一步可行的问题.

**关键词:** 有限经典极空间; 有限典型群; $m$-ovoids; 强正则图; 偏差集; 极小线性码

# Abstract

In this thesis, we mainly explore the applications of finite classical groups and their subgroups on finite geometry and coding theory. By finite classical groups and their subgroups, we can construct specific geometric structures in finite polar space, namely, $m$-ovoids and $i$-tight sets. They are collectively referred to as intriguing sets. A certain type of intriguing set in a specific finite polar space will correspond to a partial difference set. The partial difference sets whose parameters satisfy certain conditions can be used to construct minimal linear codes. In particular, some quadrics are partial difference sets, which can produce minimal linear codes. Therefore, the finite classical groups as automorphism groups of these quadrics naturally form the automorphism groups of the corresponding minimal linear codes. It can be seen that exploring the relationships between subgroups of classical groups and the corresponding geometric configuration is meaningful and has certain practical applications. In this thesis, we comprehensively use the algebraic tools including finite fields, group theory and character sums to give $m$-ovoids of several quadrics. We also provide a method of using partial difference sets to construct minimal linear codes. The following is a detailed introduction.

In Chapter 1, we briefly introduce the research background and the main contributions of this thesis.

In Chapter 2, we briefly introduce the concept of finite classical polar spaces, intriguing sets especially $m$-ovoids of finite classical polar spaces, and the relationships between them and strongly regular graphs, partial difference sets. Finally, we give some definitions and properties of finite classical groups.

In Chapter 3, we use the finite classical groups and their subgroups to give the constructions of $m$-ovoids in several quadrics. In specific, when $q \equiv 1 (\mathrm{mod}\ 4)$ and $q > 5$, we choose an automorphism group with the structure $C_{\frac{q^2-1}{2}} \rtimes C_2$ to construct an infinite family of $\frac{q-1}{2}$-ovoids of $Q(4, q)$; when $q \equiv 2 (\mathrm{mod}\ 3)$, we show that $Q^+(7, q)$ has a $(q^2 + q)$-ovoid and $q^3$-ovoid with $\mathrm{PGU}_3(q)$ as an automorphism group; when $q = 3^{2k+1}$ and $k \geq 1$, we show that $Q(6, q)$ has a $q^2$-ovoid and $q$-ovoid with ${}^2G_2(q)$ as an automorphism group.

In Chapter 4, we provide a method for constructing minimal linear codes from partial

difference sets. Many minimal linear codes can be obtained from our method. Some of them admit an automorphism group as a finite classical group, and such a group often has large order, which potentially makes them admit a fast decoding algorithm.

Finally, we briefly introduce other problems considered in my PhD learning phase. In addition, we also introduce some prospects and further feasible issues related to the work of this thesis.

**Keywords:** Finite classical polar spaces; Finite classical groups; $m$-ovoids; Strongly regular graphs; Partial difference sets; Minimal linear codes

# 图 目 录

# 表 目 录

# 目　次

# 1 绪论

有限几何是仅有有限个点的几何结构. 很多有限几何结构是可以通过线性代数的方法来进行构造. 任何维数大于等于 3 的有限射影空间都同构于有限域上的射影空间. 因此绝大多数的有限几何结构都可以放在有限域上的向量空间中, 从代数的角度进行分析和考虑. 而对有限域上向量空间的研究离不开空间上的矩阵群, 特别是一般线性群的讨论. 可以说, 有趣的几何构型是源于有趣的群在空间上的作用, 例如, 有限经典极空间的自同构群分别是几类特殊的典型群. 所以很多有限几何结构的研究依赖于有限典型群及其子群结构的分析. 探索典型群的子群结构及相应的几何构型之间的联系, 这个工作是非常有意义而且十分有趣的. 此外, 有限几何是组合数学中的有趣分支, 它与许多研究领域都有着密切的联系, 如图论、结合方案、编码理论、密码学等. 本学位论文的主要工作包括通过典型群及其子群构造了有限经典极空间中的一类有趣的几何构型: $m$-ovoids. 我们也展示了很多几何构型可以用来构造出具有良好性质的线性码. 本文所用到的主要代数工具包括有限域、群论、特征和等.

我们的主要工作之一是利用典型群及其子群结构对几类二次曲面中的 $m$-ovoids 做了一些构造性的工作. 一些特定的有限极空间的 $m$-ovoids 可以用来构造强正则图和射影二重码, 详情请参阅文献[6,17]. 下面将具体介绍一下这方面研究课题的背景意义, 并对这些工作进行概括.

一个阶为 $(s,t)$ 的广义四边形是一个点线关联结构满足如下性质: 任意两个点与至多一条线关联; 每个点与 $t+1$ 条线关联; 每条线与 $s+1$ 个点关联; 且对于任意一个点 $P$ 和一条不与 $P$ 关联的线 $\ell$, 存在 $\ell$ 上的唯一点与 $P$ 共线. 阶为 $(s,t)$ 的广义四边形的点线对偶是一个阶为 $(t,s)$ 的广义四边形. 在 $s=t$ 的情况下, 我们称该广义四边形的阶为 $s$. 在研究中, 我们只关心厚的 (thick) 广义四边形, 即阶 $(s,t)$ 满足 $s$ 和 $t$ 均大于 1 的广义四边形. 我们称由秩为 2 的有限经典极空间构成的点线关联结构为经典的广义四边形. 若要了解更多关于广义四边的相关理论, 请读者参考著作[67].

关于广义四边形的部分, 我们主要讨论经典广义四边形 $Q(4,q)$ 中的 $m$-ovoids. 广义四边形 $Q(4,q)$ 中的点和线分别是包含在射影空间 $\mathrm{PG}(4,q)$ 上抛物线二次曲面中的完全奇异点和完全奇异线. 一个 $Q(4,q)$ 的 ovoid 是 $Q(4,q)$ 中的点集, 使得该点集与每条完全奇异线恰好相交于一点. $Q(4,q)$ 的 ovoid 是一类非常重要的有限几何结构. 例如, 其点线对偶会产生广义四边形 $W(3,q)$ 中的 spreads, 进一步通过 Bruck-Bose/André 构造可以得到阶为 $q^2$ 的平移平面 (translation planes). 目前已知的 $Q(4,q)$ 中的 ovoid 的构造非常少, 文献[68] 对已有的构造进行了总结. 关于 $m$-ovoid 的概

念, 最早是由 Thas[75] 所提出, 可将其视为对 ovoid 概念的推广. 现在, $m$-ovoids 作为 intriguing sets 的一种特殊情况为人们所熟知. 广义四边形的 intriguing sets 是由 Bamberg 等人在文献[7] 中引入的, 然后在[6] 中将 intriguing sets 的概念推广到了有限经典极空间. 简言之, $Q(4,q)$ 的 $m$-ovoid 是 $Q(4,q)$ 的点集满足: 该点集与每条完全奇异线相交于 $m$ 个点.

我们现在对 $Q(4,q)$ 中满足 $m>1$ 的 $m$-ovoids 的已知构造进行总结. 对于 $q$ 是偶数的情形, 广义四边形 $W(3,q)$ 与 $Q(4,q)$ 同构. Cossidente 等人在文献[23] 中证明了对于所有整数 $m$ 使得 $1\leq m\leq q$, $W(3,q)$ 都具有 $m$-ovoids. 因此, 当 $q$ 是偶数时, 对于所有整数 $m$ 使得 $1\leq m\leq q$, 广义四边形 $Q(4,q)$ 也具有 $m$-ovoids. 一般地, 如果 $q$ 是偶数, $\mathcal{O}$ 是 $W(3,q)$ 的一个 ovoid, 则存在 $W(3,q)\setminus\mathcal{O}$ 的 $q/2$ 个不可约 2-ovoids 的划分, 详见文献[25]. 对于 $q$ 是奇数的情形, Cossidente 和 Penttila 在文献[27] 中对所有奇素数幂 $q$ 构造了 $H(3,q^2)$ 的 hemisystem, 随后很多学者在 $H(3,q^2)$ 中得到了更多 hemisystem 的构造, 参见文献[5,8,24,47]. 通过对偶性, 可以得到 $Q^-(5,q)$ 中的 $\frac{q+1}{2}$-ovoid, 其与非切超平面 (non-tangent hyperplane) 的交会产生 $Q(4,q)$ 中的 $\frac{q+1}{2}$-ovoid. 对于 $q\equiv 3(\mathrm{mod}\ 4)$ 的情形, 在文献[35] 中, 作者们构造了 $Q(4,q)$ 中第一个 $\frac{q-1}{2}$-ovoids 的无穷类. 该结果推广了文献[7] 中列出的一些零星示例. 表 1.1即来自[7], 其中列出了 $q$ 较小时, $Q(4,q)$ 中一些已知的 $m$-ovoids.

表 1.1　$q$ 较小时, $Q(4,q)$ 的 $m$-ovoids

| $q$ | 已知的参数 $m$ | 未知的参数 $m$ |
|---|---|---|
| 3 | 1,2,3 | - |
| 5 | 1,2,3,4,5 | - |
| 7 | 1,3,4,5,7 | 2,6 |
| 9 | 1,3,4,5,6,7,9 | 2,8 |
| 11 | 1,5,6,7,11 | 2,3,4,8,9,10 |

在文献[35] 的结尾处, 作者们评论说:“把文献[7] 例 5 中 $q=5$ 或 9 的例子推广成 $Q(4,q)$ 中 $\frac{q-1}{2}$-ovoids 的无穷类将会是很有趣的. 但在这些例子中, 我们没有找到它们自同构群的一种统一形式.” 在本文第 3.1节, 我们对于 $q\equiv 1(\mathrm{mod}\ 4)$ 并且 $q>5$ 的情形构造了 $Q(4,q)$ 中 $\frac{q-1}{2}$-ovoids 的无穷类. 再结合文献[7] 和[35] 的结论可以知道, 对于每个奇素数幂 $q$, $Q(4,q)$ 中都存在 $\frac{q-1}{2}$-ovoids. 该结果对于广义四边形 $Q(4,q)$ 中的 $m$-ovoids 的分类工作有着重要的意义. 这部分的工作发表在期刊《Finite Fields and Their Applications》.

著名的数学家 Kantor 在 1982 年利用典型群 $\mathrm{PGU}_3(q)$, $q\equiv 2(\mathrm{mod}\ 3)$, 构造了双曲二次曲面 $Q^+(7,q)$ 中的一类 ovoid, 这类 ovoid 被称为 unitary ovoid 或 Kantor ovoid, 详见文献[43]. 事实上, 该构造也可以得到 $Q^+(7,q)$ 中的 $m$-ovoids. 但因为 $m$-ovoids

的概念是 Thas 在 1989 年提出, 而后在 2007 年左右被 Bamberg 等人进行了系统的研究, 所以大家并没有对 Kantor 的构造从 $m$-ovoids 的角度去进行研究. 我们在第 3.2节用特征和等代数方法计算并证明了, 在 $q \equiv 2(\text{mod } 3)$ 的情形, 除 Kantor ovoid 外, $Q^+(7,q)$ 中还有自同构群为 $\text{PGU}_3(q)$ 的 $(q^2+q)$-ovoid 和 $q^3$-ovoid.

Ree 在 1960 年引入了类型为 ${}^2G_2(3^{2k+1})$ 的 Ree 群[69], 他证明了当 $k \geq 1$ 时它们都是单群. Wilson 在文献[77] 中给出了该类型的 Ree 群的简化结构, 具体也可参考著作[76]. Tits 用 ${}^2G_2(3^{2k+1})$ 类型的 Ree 群作为自同构群构造了抛物二次曲面 $Q(6,3^{2k+1})$ 中的 ovoid, 它被命名为 Ree-Tits ovoid. 同样地, 由于 $m$-ovoids 的概念出现较晚, 大家也没有考虑 $Q(6,3^{2k+1})$ 中自同构群为 ${}^2G_2(3^{2k+1})$ 的 $m$-ovoids. 我们在第 3.3节用代数方法计算并证明了除 Ree-Tits ovoid 外, $Q(6,3^{2k+1})$ 中还有自同构群为 ${}^2G_2(3^{2k+1})$ 的 $3^{2(2k+1)}$-ovoid 和 $3^{2k+1}$-ovoid.

特定的有限极空间中的 $m$-ovoids 与强正则图, 偏差集, 二重量码等组合编码对象都有着密切的联系. 我们会在第 2 章详细介绍. 事实上, 有限几何中有很多有趣的的构型, 利用它们可以在编码和密码等领域构造出很多具有优良性质的线性码和密码函数. 由典型群和有限几何相辅相成的关系可以看出, 典型群在编码密码等领域也有着重要的应用. 本论文的另一个主要工作是利用偏差集构造一些极小线性码, 用我们的构造方法可以得到很多极小线性码, 它们以阶数较大的典型群作为自同构群, 从而使得这种码可以有快速的译码算法. 下面将具体介绍一下这方面研究的背景意义, 并对这些工作进行概括.

令 $\mathcal{C}$ 是一个 $[n,k,d]$ 线性码, 对于码字 $u, v \in \mathcal{C}$, 如果 $\{1 \leq i \leq n : u_i \neq 0\} \subseteq \{1 \leq i \leq n : v_i \neq 0\}$, 则我们称 $v$ 覆盖 (covers) $u$. 如果线性码 $\mathcal{C}$ 的一个非零码字 $c$ 只覆盖它的倍数, 不再覆盖其它的码字, 则称码字 $c$ 为极小的; 如果线性码 $\mathcal{C}$ 中的每个非零码字均为极小的, 则称码 $\mathcal{C}$ 为极小线性码. 作为一种特殊类型的线性码, 极小线性码在秘密共享方案[18,54,55,80] 和安全双方计算[22] 等领域都有着广泛的应用. Ashikhmin 和 Barg[2] 给出了有限域 $\mathbb{F}_q$ 上的线性码 $\mathcal{C}$ 是极小的一个简单的判据: 如果码 $\mathcal{C}$ 的最小重量和最大重量之比大于 $\frac{q-1}{q}$, 则码 $\mathcal{C}$ 是极小的. 该判别方法被称为 AB 条件. 该条件对于判别极小线性码而言是充分而非必要条件. 迄今为止, 已经有许多不满足 AB 条件的极小线性码被构造出来. 我们在下面的表 1.2中总结了一些已知的极小线性码. 当这些极小线性码的参数满足某些条件时, 它们不满足 AB 条件. 有关这些极小线性码的更多构造和信息, 请参阅文献[9,12,30,42,56,72,78,79,81].

在这些工作中, Bonini 和 Borello[12] 利用切块集构造了极小线性码, 该方法是非常有效的. 我们在第 4章中通过 $\mathbb{F}_q^*$-不变的偏差集, 给出了 $\mathbb{F}_q$ 上极小线性码的构造, 并计算了该类码的重量分布. 我们的构造提供了很多不满足 AB 条件的极小线性码.

表 1.2　一些已知的极小线性码

| $[n, k]$ | 极小距离 $d$ | 重量个数 | 条件 | 方法 | 文献 |
|---|---|---|---|---|---|
| $[3^m-1, m+1]$ | $\sum_{j=1}^{k} 2^j \binom{m}{j}$ | $\leq m+2$ | $m \geq 5,\ 2 \leq k \leq \lfloor (m-1)/2 \rfloor$ | Boolean 函数 | [42] |
| $[2^m-1, m+1]$ | $\min(s(2^t-1),\ 2^{m-1}-s)$ | 3 或 4 | $m \geq 6$ 偶数, $t=m/2$<br>$s \notin \{1, 2^t, 2^t+1\}$ | Boolean 函数 | [30] |
| | $2^{m-1}-2^{m-s-1}(s-1)$ | $s+3$($s$ 奇数)<br>$s+2$($s$ 偶数) | $m \geq 7$ 奇数, $s=(m+1)/2$ | | |
| | $\sum_{j=1}^{k} \binom{m}{j}$ | $\leq m+2$ | $m \geq 7,\ 2 \leq k \leq \lfloor (m-3)/2 \rfloor$ | | |
| $[p^m-1, m]$ | $(p-1)^2 p^{m-2}$ | 3 | $m>2$ | $p$-元函数 | [78] |
| $[p^m-1, m-1]$ | | 2 | | | |
| $[p^m-1, m]$ | $p^{m-1}(p-2)$ | | | | |
| $[p^m-1, m+1]$ | - | 3 或 4 | $m=2t, t \geq 2$ | partial spreads | |
| $[p^m-1, m+1]$ | $p^{m-s-1}(p-1)(s(p-1)+1)$ | $\leq s+4$ | $(p-1)(p^{s-2}-s)>1$ | Maiorana-McFarland 函数 | [79] |
| | $a(p^{m-s}-p^{m-s-1})(p^k-1)$ | 6 | $k \geq 2, (k,p) \neq (2,2)$,<br>$s=2k, 2 \leq a \leq (p-1)p^{k-2}$ | | |
| $[p^m-1, m+1]$ | - | 4 或 5 | 定理 3.8 | 对应子空间的特征函数 | [56] |
| | | 6 或 7 | 定理 3.12 | | |
| $[q^m-1, m+1]$ | - | - | - | 切块集 | [9], [12] |

此外, 我们也得到了不是由切块集产生的极小线性码的例子. 在 4.3.3小节中, 我们展示了偏差集的每个自同构会诱导对应码的自同构. 特别地, 在很多情况下, 我们获得了具有较大自同构群的极小线性码, 这使得我们的极小线性码可以具有快速的译码算法. 这部分的工作已被期刊《IEEE Transactions on Information Theory》录用.

# 2 有限极空间中的几何结构和有限典型群

## 2.1 有限经典极空间

在本节中我们主要介绍一些关于有限经典极空间的概念, 关于这部分知识的比较好的代数角度的讲解请参考 Simeon Ball 的著作[4]. 令 $\mathbb{F}_q$ 为一个有 $q$ 个元素的有限域, $V = V(n, q)$ 为 $\mathbb{F}_q$ 上的 $n$ 维向量空间. 一个 $V$ 上的 $\sigma$-半双线性型 ($\sigma$-sesquilinear form) 是一个映射

$$\mathbf{b} : V \times V \mapsto \mathbb{F}_q,$$

使得

$$\mathbf{b}(\mathbf{u} + \mathbf{w}, \mathbf{v}) = \mathbf{b}(\mathbf{u}, \mathbf{v}) + \mathbf{b}(\mathbf{w}, \mathbf{v}),$$

$$\mathbf{b}(\mathbf{u}, \mathbf{w} + \mathbf{v}) = \mathbf{b}(\mathbf{u}, \mathbf{w}) + \mathbf{b}(\mathbf{u}, \mathbf{v}),$$

$$\mathbf{b}(\lambda\mathbf{u}, \mu\mathbf{v}) = \lambda\mu^{\sigma}\mathbf{b}(\mathbf{u}, \mathbf{v}),$$

对任意的 $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in V$, $\lambda$, $\mu \in \mathbb{F}_q$ 都成立, 这里 $\sigma$ 是 $\mathbb{F}_q$ 的一个自同构. 如果 $\sigma = \mathrm{id}$, 则称 $\mathbf{b}$ 是双线性的, 这里 id 表示 $\mathbb{F}_q$ 的恒等自同构. 为了简单起见, 接下来我们将直接用 $v$ 代替 $\mathbf{v}$ 表示 $V$ 中的向量.

如果存在 $w \neq 0$ 使得 $\mathbf{b}(u, w) = 0$, 或 $\mathbf{b}(w, u) = 0$ 对所有的 $u \in V$ 都成立, 则称 $\mathbf{b}$ 是退化的 (degenerate); 否则, 称 $\mathbf{b}$ 是非退化的 (non-degenerate). 一个 $\sigma$-半线性型 $\mathbf{b}$ 如果满足由 $\mathbf{b}(u, v) = 0$ 可得到 $\mathbf{b}(v, u) = 0$ 对任意的 $u$, $v \in V$ 都成立, 则称 $\mathbf{b}$ 为自反的 (reflexive). 一般情况下, 我们研究的都是自反的非退化的 $\sigma$-半双线性型. 关于这样的 $\sigma$-半双线性型, Birkhoff 和 Von Neumann 已对其进行了分类, 在有限域情形下的证明, 请参考文献[4] 中的定理 3.6.

**定理 2.1**: 令 $\mathbf{b}$ 是一个 $V$ 上的非退化, 自反的 $\sigma$-半双线性型. 在相差一个倍数 (scalor) 的情况下, $\mathbf{b}$ 一定是下列情况的一种:

1. $\mathbf{b}$ 是交错型 (alternating form), 即, 对于所有 $u \in V$, 有 $\mathbf{b}(u, u) = 0$ 成立.
2. $\mathbf{b}$ 是对称型 (symmetric form), 即, 对于所有 $u$, $v \in V$, 有 $\mathbf{b}(u, v) = \mathbf{b}(v, u)$ 成立.
3. $\mathbf{b}$ 是厄尔米特型 (Hermitian form), 即, 对于所有 $u$, $v \in V$, 有 $\mathbf{b}(u, v) = \mathbf{b}(v, u)^{\sigma}$ 成立, 这里 $\sigma^2 = \mathrm{id}$, 且 $\sigma \neq \mathrm{id}$, 其中 id 是 $\mathbb{F}_q$ 的恒等自同构.

注意到该引理的第 3 条意味着对于 $w \in V$, 我们有 $\mathbf{b}(w, w) \in \mathbb{F}_{\sqrt{q}}$.

一个 $V$ 上的二次型 (quadratic form) 是一个函数 $Q : V \to \mathbb{F}_q$ 满足以下性质:

1. $Q(av) = a^2Q(v)$ 对于所有的 $a \in \mathbb{F}_q$ 和 $v \in V$ 成立;

2. $\mathbf{b}(u, v) = Q(u + v) - Q(u) - Q(v)$ 是一个双线性型.

我们称这里的 **b** 为 $Q$ 的极型 (polar form). 注意到这里的 **b** 是对称的. 如果存在一个非 0 向量 $u \in V$ 使得 $Q(u) = 0$ 且 $\mathbf{b}(u, v) = 0$ 对所有的 $v \in V$ 成立, 则称二次型 $Q$ 是退化的; 否则, 称 $Q$ 是非退化的. 更多有关二次型的描述, 请参阅文献[4] 的 3.6 节. 下面的定理给出了非退化的二次型 $Q$ 的分类情况, 可参考文献[4] 的定理 3.28 或 Moorhouse 的讲义 Incidence Geometry 中的定理 24.1.

**定理 2.2**：令 $V$ 是 $\mathbb{F}_q$ 上的 $n$ 维向量空间, 令 $Q$ 是 $V$ 上的一个非退化的二次型. 则有 $n = 2r, 2r + 1$ 或 $2r + 2$, 且通过对坐标进行适当的线性变换, $Q$ 的形式分别为

$$Q(u) = u_1u_2 + u_3u_4 + \ldots + u_{2r-1}u_{2r}, \tag{2.1}$$

$$Q(u) = u_1u_2 + u_3u_4 + \ldots + u_{2r-1}u_{2r} + \lambda u_{2r+1}^2, \tag{2.2}$$

其中当 $q$ 是偶数时, $\lambda = 1$; 当 $q$ 是奇数时, $\lambda = 1$ 或 $\delta$, 这里 $\delta$ 为 $\mathbb{F}_q$ 中的一个给定的非平方元,

$$Q(u) = u_1u_2 + u_3u_4 + \ldots + u_{2r-1}u_{2r} + u_{2r+1}^2 + a_1u_{2r+1}u_{2r+2} + a_2u_{2r+2}^2, \tag{2.3}$$

其中二次多项式 $X^2 + a_1X + a_2 \in \mathbb{F}_q[X]$ 是 $\mathbb{F}_q$ 上的不可约多项式.

在上面定理中, 如果 $n = 2r$, 则我们称等式(2.1)定义的 $Q$ 是双曲的; 如果 $n = 2r + 1$, 则我们称等式(2.2)定义的 $Q$ 是抛物的; 如果 $n = 2r + 2$, 则我们称等式(2.3)$Q$ 是椭圆的.

令 **b** 是一个 $\sigma$-半双线性型或一个二次型的极型. 对于任意的 $V$ 的子空间 $U$, 我们可以定义 $U$ 相对于 **b** 的正交空间为

$$U^{\perp} = \{v \in V | \mathbf{b}(u, v) = 0, \forall\, u \in U\}.$$

从几何上来讲, 空间 $U^{\perp}$ 表示了与 $U$ 中每个点都共线的点的集合.

采用上述符号, 仍令 $V = V(n, q)$ 是有限域 $\mathbb{F}_q$ 上的一个 $n$ 维向量空间. 令 **b** 是一个 $\sigma$-半双线性型. 如果一个向量 $u \in V$ 满足 $\mathbf{b}(u, u) = 0$, 则称 $u$ 是迷向的 (isotropic). 一个 $V$ 的子空间 $U$ 如果满足对任意的 $u, v \in U$ 都有 $\mathbf{b}(u, v) = 0$ 成立, 则称 $U$ 是完全迷向的 (totally isotropic). 令 $Q$ 是 $V$ 上的一个非退化的二次型. 如果一个向量 $u \in V$ 满足 $Q(u) = 0$, 则称 $u$ 是奇异的 (singular). 一个 $V$ 的子空间 $U$ 如果满足对任意的 $u \in U$ 都有 $Q(u) = 0$ 成立, 则称 $U$ 是完全奇异的 (totally singular). 令 $\kappa$ 表示

$V$ 上的一个非退化的自反的 $\sigma$-半双线性型 (或二次型), 在 $V$ 上对应于 $\kappa$ 的极空间是这样的几何结构, 它的点, 线, 面, ..., 分别由 $V$ 的完全迷向 (或完全奇异) 1 维, 2 维, 3 维, ...子空间构成. 我们称极空间中的维数最大的完全迷向 (或完全奇异) 子空间为该极空间的生成子 (generators). 由 Witt's 引理 ([46], 命题 2.1.6), 一个极空间的所有生成子的向量维数是相等的, 我们称该维数为这个极空间的秩. 在有限极空间中有许多有着几何意义的有趣结构, 其中 ovoid 就是一个典型的例子. 一个有限极空间 $\mathcal{P}$ 的 ovoid 是 $\mathcal{P}$ 中的一个点集满足它和 $\mathcal{P}$ 中的每个生成子恰好交于一个点. 秩为 $r$ 的有限极空间的每个 ovoid 的点的个数是相同的, 参考文献[74], 我们称这个个数为 ovoid 数 (ovoid number), 记为 $\Theta_r$. 由文献[4] 的定理 4.3 可知, 对于 $r \geq 2$, 在同构意义下 $\mathbb{F}_q$ 上共有 6 种极空间, 如表 2.1所示. 其中秩为 $r$ 的有限极空间 $\mathcal{P}$ 中的点个数为 $\Theta_r \frac{q^r-1}{q-1}$, 这里 $\Theta_r$ 为 $\mathcal{P}$ 的 ovoid 数, $\frac{q^r-1}{q-1}$ 表示 $\mathcal{P}$ 的每个生成子的点的个数. 具体的计算过程请参阅文献[4] 的定理 4.11.

表 2.1　有限经典极空间

| $\kappa$ | $n$ | $q=p^f$ | 极空间 $\mathcal{P}$ | 秩 $r$ | $\Theta_r$ | $\lvert\mathcal{P}\rvert$ |
|---|---|---|---|---|---|---|
| 交错型 | 偶数 | - | $W(n-1,q)$ | $n/2$ | $q^{n/2}+1$ | $\frac{q^n-1}{q-1}$ |
| 双曲二次型 | 偶数 | - | $Q^+(n-1,q)$ | $n/2$ | $q^{n/2-1}+1$ | $(q^{n/2-1}+1)\frac{q^{n/2}-1}{q-1}$ |
| 椭圆二次型 | 偶数 | - | $Q^-(n-1,q)$ | $n/2-1$ | $q^{n/2}+1$ | $(q^{n/2}+1)\frac{q^{n/2-1}-1}{q-1}$ |
| 抛物二次型 | 奇数 | - | $Q(n-1,q)$ | $(n-1)/2$ | $q^{(n-1)/2}+1$ | $\frac{q^{n-1}-1}{q-1}$ |
| 厄尔米特型 | 奇数 | $f$ 偶数 | $H(n-1,q)$ | $(n-1)/2$ | $q^{n/2}+1$ | $(q^{n/2}+1)\frac{q^{(n-1)/2}-1}{q-1}$ |
| | 偶数 | $f$ 偶数 | $H(n-1,q)$ | $n/2$ | $q^{(n-1)/2}+1$ | $(q^{(n-1)/2}+1)\frac{q^{n/2}-1}{q-1}$ |

## 2.2 Intriguing sets, 强正则图和偏差集

在上一节中我们介绍了有限极空间中的 ovoid 的概念, 后来 Thas 在文献[75] 中对这个概念进行了推广. 一个有限极空间 $\mathcal{P}$ 的 $m$-ovoid 是 $\mathcal{P}$ 中的一个点集满足它和 $\mathcal{P}$ 中的每个生成子恰好交于 $m$ 个点. 秩为 2 的有限极空间中紧点集 (tight set) 的概念最初是由 Payne 在文献[66] 中引入的, 后来被 Drudge 在博士论文[31] 中推广到了拥有更高秩的有限极空间中. 如果 $\mathcal{T}$ 是秩为 $r$ ($r \geq 2$) 的有限经典极空间 $\mathcal{P}$ 中的一个点集, 则 $\mathcal{T}$ 中与一个给定点共线的点的个数的平均数的上界是 $i\frac{q^{r-1}-1}{q-1}+q^{r-1}-1$, 这里 $i$ 是由 $\mathcal{T}$ 的大小所决定的. 如果达到该上界, 则我们称 $\mathcal{T}$ 是 $\mathcal{P}$ 的一个 $i$-tight set, 可参阅文献[31] 的定理 8.1. 本文的主要研究内容是秩大于等于 2 的有限极空间中的 $m$-ovoid, 故这里着重介绍一下关于 $m$-ovoid 的一些性质, 对于 $i$-tight set 也有下列类似的性质, 详见文献[6] 的第 2 和第 3 小节. 仍假设 $\mathcal{P}$ 为秩 $r, r \geq 2$ 的有限极空间, 令 $\mathcal{A}$ 和 $\mathcal{B}$ 分别为 $\mathcal{P}$ 的 $n_1$-ovoid 和 $n_2$-ovoid. 如果 $\mathcal{A} \subseteq \mathcal{B}$, 则 $\mathcal{B} \setminus \mathcal{A}$ 是 $\mathcal{P}$ 的 $(n_2-n_1)$-ovoid. 如果 $\mathcal{A}$ 和 $\mathcal{B}$ 不交, 则 $\mathcal{A} \cup \mathcal{B}$ 是 $\mathcal{P}$ 的 $(n_1+n_2)$-ovoid. 特别地, $\mathcal{P}$ 的所有点构成的集合是一

个 $\mathcal{P}$ 的 $\frac{q^r-1}{q-1}$-ovoid, 因此 $\mathcal{P}$ 的任一 $m$-ovoid 的补是 $\mathcal{P}$ 的 $\left(\frac{q^r-1}{q-1}-m\right)$-ovoid.

有限极空间 $\mathcal{P}$ 的一个点集 $\mathcal{I}$ 如果满足

$$|P^\perp \cap \mathcal{I}| = \begin{cases} h_1, & \text{if } P \in \mathcal{I}, \\ h_2, & \text{if } P \in \mathcal{P} \setminus \mathcal{I} \end{cases}$$

对于常数 $h_1$ 和 $h_2$ 成立, 则称点集 $\mathcal{I}$ 为 $\mathcal{P}$ 的一个 intriguing set, 称 $h_1$ 和 $h_2$ 为 $\mathcal{I}$ 的相交数. 由文献[6] 的引理 1 可知, 秩为 $r$ 的有限极空间 $\mathcal{P}$ 的 $i$-tight set 是 $\mathcal{P}$ 中相交数分别为 $h_1 = i\frac{q^{r-1}-1}{q-1} + q^{r-1}$, $h_2 = i\frac{q^{r-1}-1}{q-1}$ 的 intriguing set; 极空间 $\mathcal{P}$ 的 $m$-ovoid 是 $\mathcal{P}$ 中相交数分别为 $h_1 = m\Theta_{r-1} - \Theta_{r-1} + 1$, $h_2 = m\Theta_{r-1}$ 的 intriguing set. 这里, 对于每种类型的有限极空间 $\mathcal{P}$, $\Theta_r$ 的大小由表 2.1所给出. 反之, Bamberg 等人从代数图论的角度证明了, 有限极空间 $\mathcal{P}$ 中的一个真子集 $\mathcal{I}$ 如果是 intriguing set, 那么它是 $\mathcal{P}$ 中的 $i$-tight set 或 $m$-ovoid, 参见文献[6] 的定理 6. 从定义和该定理的证明过程我们可以看出, intriguing sets 与强正则图之间有着密切的联系, 在下面我们将介绍一下二者之间的联系.

强正则图 $(v, k, \lambda, \mu)$ 是一个无向的单图 $\Gamma_0$, 既不是完全图也不是无边图, 使得下列性质成立:

(i) 该图是阶为 $v$ 的 $k$-正则图.

(ii) 任意两个相邻的点有 $\lambda$ 个公共邻点.

(iii) 任意两个不相邻的点有 $\mu$ 个公共邻点.

如果图 $\Gamma_0$ 的一个特征值的特征向量垂直于全一向量 (all-one vector), 则称该特征值为限制 (restricted) 特征值, 参考文献[14]. 以下结果是为大家所熟知的.

**引理 2.3**: ([40], 10.2 节) 令 $\Gamma_0$ 是强正则图 $(v, k, \lambda, \mu)$, 它的限制特征值为 $\theta_1$ 和 $\theta_2$, 这里 $\theta_1 > 0 > \theta_2$. 则

$$\theta_1 = \frac{(\lambda-\mu) + \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}}{2},$$
$$\theta_2 = \frac{(\lambda-\mu) - \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}}{2}$$

它们的重数分别为

$$m_1 = \frac{1}{2}\left((v-1) - \frac{2k + (v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2 + 4(k-\mu)}}\right),$$
$$m_2 = \frac{1}{2}\left((v-1) + \frac{2k + (v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2 + 4(k-\mu)}}\right).$$

令 $G$ 是一个 $v$ 阶的 (加法) 交换群, $D$ 为 $G$ 的子集使得 $0 \notin D$ 并且 $-D = D$, 这里 $-D = \{-d : d \in D\}$. 凯莱图 (Cayley graph) $\Gamma_0 = \mathrm{Cay}(G, D)$ 是一个图, 它的顶点集是 $G$ 的所有元素, 对于任意 $x, y \in G$, $x$ 与 $y$ 相邻当且仅当 $x - y \in D$, 这里 $D$ 称作该凯莱图的连通集. 如果凯莱图 $\mathrm{Cay}(G, D)$ 是一个强正则图 $(v, k, \lambda, \mu)$, 则连通集 $D$ 也被称为参数为 $(v, k, \lambda, \mu)$ 的偏差集 (partial difference set). 对于凯莱图 $\Gamma_0 = \mathrm{Cay}(G, D)$ 使得 $G$ 是交换群, 则 $\{\phi(D) := \sum_{d\in D} \phi(d), \phi \in \widehat{G}\}$ 构成了凯莱图 $\Gamma_0$ 的所有特征值, 这里 $\widehat{G}$ 是 $G$ 的特征群. 对于参数为 $(v, k, \lambda, \mu)$ 的偏差集 $D$ 而言, 我们有 $k = \phi_0(D) = |D|$, 这里 $\phi_0$ 表示 $G$ 的平凡特征. 更多关于偏差集的知识和研究背景, 请参考综述文献[53].

强正则图 $(v, k, \lambda, \mu)$ 若存在正整数 $u$, $s$ 使得

$$(v, k, \lambda, \mu) = (u^2, s(u - \epsilon), \epsilon u + s^2 - 3\epsilon s, s^2 - \epsilon s),$$

则当 $\epsilon = 1$ 时, 称之为拉丁方型 (Latin square type); 当 $\epsilon = -1$ 时, 称之负拉丁方型 (negative Latin square type). 如果强正则凯莱图 $\mathrm{Cay}(G, D)$ 是拉丁方型或负拉丁方型, 则相应地称偏差集 $D$ 拉丁方型或负拉丁方型.

秩大于等于 2 的有限极空间的 intriguing sets 与强正则凯莱图之间有着密切的联系, 具体体现在下面两个定理中, 可参考[6] 的定理 11 和定理 12, 或文献[63] 的定理 4.20 和定理 4.22.

**定理 2.4**: 令 $\mathcal{P}$ 为 $H(2r, q^2)$, $Q^-(2r-1, q)$ 或 $W(2r-1, q)$ 中的某个有限极空间, 这里 $r \geq 2$. 令 $\mathcal{M}$ 是 $\mathcal{P}$ 的一个 $m$-ovoid, 可生成对应的射影空间. 令 $D = \{xy : y \in \mathbb{F}_q^*, \langle x\rangle \in \mathcal{M}\}$, 设 $V$ 是 $\mathcal{P}$ 的基础向量空间. 则图 $\mathrm{Cay}(V, D)$ 是一个参数为 $(u^2, s(u+1), -u+s^2+3s, s^2+s)$ 的负拉丁方型强正则图, 这里当 $\mathcal{P} = H(2r, q^2)$, $Q^-(2r-1, q)$ 或 $W(2r-1, q)$ 时, 分别有 $(u, s) = (q^{2r+1}, m(q^2-1))$, $(q^r, m(q-1))$ 或 $(q^r, m(q-1))$.

对于 $r \geq 2$, 有限极空间 $H(2r, q^2)$, $Q^-(2r-1, q)$ 或 $W(2r-1, q)$ 中的 $m$-ovoids 的构造性的工作请参阅文献[5–7,23,25,36] 等.

**定理 2.5**: 令 $\mathcal{P}$ 为 $H(2r-1, q^2)$, $Q^+(2r-1, q)$ 或 $W(2r-1, q)$ 中的某个有限极空间, 这里 $r \geq 2$. 令 $\mathcal{T}$ 是 $\mathcal{P}$ 的一个 $i$-tight set, 可生成对应的射影空间. 令 $D = \{xy : y \in \mathbb{F}_q^*, \langle x\rangle \in \mathcal{T}\}$, 设 $V$ 是 $\mathcal{P}$ 的基础向量空间. 则图 $\mathrm{Cay}(V, D)$ 是一个参数为 $(u^2, s(u-1), u+s^2-3s, s^2-s)$ 的拉丁方型强正则图, 这里当 $\mathcal{P} = H(2r-1, q^2)$, $Q^+(2r-1, q)$ 或 $W(2r-1, q)$ 时, 分别有 $(u, s) = (q^{2r}, i)$, $(q^r, i)$ 或 $(q^r, i)$.

对于 $r \geq 2$, 有限极空间 $H(2r-1, q^2)$, $Q^+(2r-1, q)$ 或 $W(2r-1, q)$ 中的 $i$-tight sets

的构造性的工作请参阅文献[6,7,23,25,32,33,60,61] 等.

由此可见, 利用 intriguing sets 可以得到拉丁方型或负拉丁方型的强正则图, 关于这两类图, 最典型的的构造之一是利用分圆的方法.

在文献[15] 中, 作者们利用分圆给出了偏差集的构造, 我们现给出该构造的描述. 设 $p$ 是一个素数并且 $q = p^e$. 令 $m$ 是一个正整数使得 2 整除 $em$ 且 $\gamma$ 是有限域 $\mathbb{F}_{q^m}$ 中一个固定的本原元. 对于 $q^m - 1$ 的一个真因子 $N$, 我们定义 $\mathbb{F}_{q^m}$ 的 $N$ 次分圆类 (cyclotomic classes) 如下:

$$C_i = \{\gamma^{jN+i} : 0 \le j \le \frac{q^m-1}{N} - 1\},$$

这里 $0 \le i \le N-1$. 集合 $C_0$ 构成 $\mathbb{F}_{q^m}^*$ 的指数为 $N$ 的子群, 并且对于 $0 \le i \le N-1$ 我们有 $C_i = \gamma^i C_0$.

**引理 2.6：**[15] 采用上述符号, 令 $N$ 是 $q^m - 1$ 的一个真因子满足 $N \neq 1$ 且 $p^{\ell_1} \equiv -1 (\text{mod } N)$ 对于某个正整数 $\ell_1$ 成立, 并取 $\ell_1$ 为最小值, 记 $em = 2\ell_1 t$. 取一个大小为 $u$ 的真子集 $J \subset \mathbb{Z}_N$. 如果 $q$ 是奇数, 我们进一步假设 $N | \frac{q^m-1}{2}$ 且 $J + \frac{q^m-1}{2} \equiv J (\text{mod } N)$. 设

$$D = D_J = \bigcup_{j \in J} C_j.$$

则图 $\text{Cay}(\mathbb{F}_{q^m}, D)$ 是一个强正则图, 它的特征值为

$$k = |D| = \frac{q^m-1}{N} u, \text{ 重数为 } 1;$$

$$\theta_1 = \frac{u}{N}(-1 + (-1)^t \sqrt{q^m}), \text{ 重数为} q^m - 1 - k;$$

$$\theta_2 = \theta_1 + (-1)^{t+1} \sqrt{q^m}, \text{ 重数为} k.$$

具体而言, 令 $\zeta_p$ 表示 $p$ 次本元单位根. 对于 $x \in \mathbb{F}_{q^m}$, 定义 $\Psi(x) = \zeta_p^{\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_p}(x)}$ 和 $\Psi(D) = \sum_{x \in D} \Psi(x)$. 对于 $i = 0, 1, \ldots, N-1$, 我们有

$$\Psi(\gamma^i D) = \begin{cases} \theta_2, & \text{如果 } \varepsilon^t = 1, i \in -J (\text{mod } N) \text{ 或} \\ & \varepsilon^t = -1, i \in -J + N/2 (\text{mod } N), \\ \theta_1, & \text{否则,} \end{cases}$$

这里 $\varepsilon = \begin{cases} -1, & \text{如果} N \text{是偶数且} \frac{p^{\ell_1}+1}{N} \text{是奇数,} \\ 1, & \text{否则.} \end{cases}$

如果 $t$ 是奇数, 则 $\text{Cay}(\mathbb{F}_{q^m}, D)$ 是拉丁方型; 如果 $t$ 是偶数, 则 $\text{Cay}(\mathbb{F}_{q^m}, D)$ 是负拉丁方型.

设 $S$ 是 $\mathbb{F}_{q^m}^*$ 的一个子集, 如果对任意的 $s \in S, \lambda \in \mathbb{F}_q^*$, 都有 $\lambda s \in S$, 则我们称 $S$ 是 $\mathbb{F}_q^*$-不变的. 因为 $\mathbb{F}_q^*$ 是 $\mathbb{F}_{q^m}^*$ 的由所有非零 $\frac{q^m-1}{q-1}$ 次幂构成的子群, 则显然有下面的引理.

**引理 2.7**: 采用上述符号, 令 $D = D_J = \bigcup_{j\in J} C_j$ 如引理 2.6中所定义. 则 $D$ 是 $\mathbb{F}_q^*$-不变的当且仅当集合 $J$ 在映射 $\rho : j \to j + \frac{q^m-1}{q-1} (\mathrm{mod}\ N)$ 下是不变的.

我们将在第 4 章利用上述强正则凯莱图给出一些极小线性码的构造.

## 2.3 有限典型群

令 $p$ 为一个素数, $q = p^f$ 为一个素数幂, 令 $V$ 表示有限域 $\mathbb{F}_q$ 上的 $n$ 维向量空间. 我们定义半线性群 $\Gamma\mathrm{L}_n(q)$ 是由 $V$ 上的全体可逆半线性变换所构成的群. 一般线性群 (general linear group) $\mathrm{GL}_n(q)$ 是由 $V$ 上的全体可逆线性变换构成的群, 由线性代数的知识可知, 这些可逆线性变换可以看作 $\mathbb{F}_q$ 上全体 $n \times n$ 的可逆矩阵. 特殊线性群 (special linear group) $\mathrm{SL}_n(q)$ 是由 $\mathrm{GL}_n(q)$ 中所有行列式为 1 的矩阵构成. 在不引起混淆的情况下, 我们将 $\Gamma\mathrm{L}_n(q)$, $\mathrm{GL}_n(q)$ 和 $\mathrm{SL}_n(q)$ 分别简记为 $\Gamma\mathrm{L}(V)$, $\mathrm{GL}(V)$ 和 $\mathrm{SL}(V)$.

现将向量空间 $V$ 赋予一个型 $\kappa$, 其中 $\kappa$ 或者恒等于 0, 或者为一个非退化的 $\sigma$-半双线性型, 或者为一个非退化的二次型. 根据本章第 1 小节的论述可知, 有下表中的情形. 表中第三行 $\varepsilon = +, -, \circ$ 分别对应于 $\kappa$ 定义双曲, 椭圆和抛物的二次型.

表 2.2 向量空间 $V$ 上的 form

| | |
|---|---|
| **L** | $\kappa$ 恒为 0 |
| **S** | $\kappa$ 为非退化的交错型 |
| $\mathbf{O}^\varepsilon$ | $\kappa$ 为非退化的二次型 |
| **U** | $\kappa$ 为非退化的厄尔米特型 |

我们采用与文献[46] 相同的符号来给出典型群的定义. 如果 $\kappa$ 是一个 $\sigma$-半双线性型, 我们定义 $\kappa$-半相似群 ($\kappa$-semisimilarity group) 如下:

$$\Gamma(V,\kappa) = \{g \in \Gamma\mathrm{L}(V) : \kappa(xg, yg) = \tau(g)\kappa(x,y)^{\sigma(g)},\ \forall\, x, y \in V\}, \tag{2.4}$$

这里 $\sigma(g) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, 为 $\mathbb{F}_q$ 的 Frobenius 自同构, $\tau(g) \in \mathbb{F}_q^*$.

如果 $\kappa$ 是一个二次型, 我们定义 $\kappa$-半相似群 ($\kappa$-semisimilarity group) 如下:

$$\Gamma(V,\kappa) = \{g \in \Gamma\mathrm{L}(V) : \kappa(xg) = \tau(g)\kappa(x)^{\sigma(g)},\ \forall\, x \in V\}, \tag{2.5}$$

这里 $\sigma(g) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, 为 $\mathbb{F}_q$ 的 Frobenius 自同构, $\tau(g) \in \mathbb{F}_q^*$.

显然, 如果 $\kappa$ 恒为 0, 则 $\Gamma(V,\kappa) = \Gamma\mathrm{L}(V)$.

在 $\Gamma(V,\kappa)$ 的定义的基础上, 我们定义相似群 (similarity grouup) $\Delta(V,\kappa)$ 为 $\sigma$ 在 $\Gamma(V,\kappa)$ 中的核 (kernel), 以二次型为例, 即

$$\Delta(V,\kappa)=\{g\in \mathrm{GL}(V):\ \kappa(xg)=\tau(g)\kappa(x),\ \forall\ x\in V\}.$$

定义等距群 (isometry group) $I(V,\kappa)$ 为 $\tau$ 在 $\Delta(V,\kappa)$ 中的核 (kernel), 以二次型为例, 即

$$I(V,\kappa)=\{g\in \mathrm{GL}(V):\ \kappa(xg)=\kappa(x),\ \forall\ x\in V\}.$$

且定义 $S(V,\kappa)$ 为 $I(V,\kappa)$ 中行列式为 1 的元素构成的子群. 以二次型为例, 即

$$S(V,\kappa)=\{g\in \mathrm{SL}(V):\ \kappa(xg)=\kappa(x),\ \forall\ x\in V\}.$$

在 **L**, **S**, **U** 的情形下, 我们将 $\Omega(V,\kappa)$ 定义为 $S(V,\kappa)$; 在 **O** 的情形, 我们定义 $\Omega(V,\kappa)$ 为 $S(V,\kappa)$ 的指数为 2 的子群. 更多关于群 $\Omega(V,\kappa)$ 的讨论, 请参考文献[46] 的 2.5 节. 我们进一步定义群 $\mathrm{A}\Gamma(V,\kappa)$, 在 **L** 且 $n\geq 3$ 的情形, 群 $S(V,\kappa)=\mathrm{SL}_n(q)$ 有一个逆转置 (inverse-transpose) 自同构 $\iota$, 参考文献[46] 的 2.2 节, 在该种情形下, 我们定义 $\mathrm{A}\Gamma(V,\kappa)=\Gamma(V,\kappa)\langle\iota\rangle$; 在其他情形, 定义 $\mathrm{A}\Gamma(V,\kappa)=\Gamma(V,\kappa)$. 因此, 我们便得到了一个群的链:

$$\Omega(V,\kappa)\leq S(V,\kappa)\leq I(V,\kappa)\leq\Delta(V,\kappa)\leq\Gamma(V,\kappa)\leq\mathrm{A}\Gamma(V,\kappa).$$

令 $Z$ 是由全体数量阵 $\lambda I_n$ 构成的群, 这里 $\lambda\in\mathbb{F}_q^*$, $I_n$ 是 $n$ 阶单位阵. 商群 $\mathrm{GL}_n(q)/Z$ 被称为射影一般线性群 (projective general linear group), 表示为 $\mathrm{PGL}_n(q)$. 如果 $X$ 是 $\mathrm{GL}(V)$ 的子群, 则我们记 PX 为 $X$ 所对应的射影群 $X/(X\cap Z)$. 例如, 射影特殊线性群 (projective special linear group) $\mathrm{PSL}_n(q)=\mathrm{SL}_n(q)/(\mathrm{SL}_n(q)\cap Z)$, 它通常情况下是单群, 且在射影空间 $\mathrm{PG}(n-1,q)$ 上有一个自然的作用. 与 $P$ 这个符号一起, 符号 $-$ 也用来表示模掉数量阵后的既约群. 因此 $\overline{\mathrm{GL}(V)}=\mathrm{PGL}(V)$, 如果 $g\in\mathrm{GL}(V)$, 则 $\overline{g}$ 表示 $g$ 在 $\mathrm{PGL}(V)$ 中的像.

在以上概念的基础上, 如果群 $G$ 在 **L**, **S**, **O**, **U** 四种情形之一满足

$$\Omega(V,\kappa)\leq G\leq\mathrm{A}\Gamma(V,\kappa)\ \text{或}\overline{\Omega(V,\kappa)}\leq G\leq\overline{\mathrm{A}\Gamma(V,\kappa)},$$

则称群 $G$ 是一个 (有限) 典型群. 读者可参考文献[46] 的 2.1 节进行更深入的阅读. 通过向量空间, 矩阵和型对典型群的研究可以参考 Dickson 的著名著作[29]. 有关典型群的更多几何描述，请参阅 Taylor 的著作[73] 和 Grove 的著作[41]. 限于文章篇幅, 我们这里不作过多的解释说明. 下面仅对典型群的阶作如下介绍, 表 2.3和表 2.4分别摘自文献[46] 的表 2.1.C 和 2.1.D.

表 2.3　有限典型群的阶

| 情形 | $\lvert I\rvert$ | $\lvert S:\Omega\rvert$ | $\lvert I:S\rvert$ | $\lvert\Delta:I\rvert$ | $\lvert\Gamma:\Delta\rvert$ | $\lvert A\Gamma:\Gamma\rvert$ |
|---|---|---|---|---|---|---|
| **L** | $q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)$ | 1 | $q-1$ | 1 | $f$ | $2^*$ |
| **U** | $q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-(-1)^i)$ | 1 | $q+1$ | $q-1$ | $2f$ | 1 |
| **S** | $q^{n^2/4}\prod_{i=1}^{n/2}(q^{2i}-1)$ | 1 | 1 | $q-1$ | $f$ | 1 |
| $\mathbf{O}^\circ$ | $2q^{(n-1)^2/4}\prod_{i=1}^{(n-1)/2}(q^{2i}-1)$ | $2^{**}$ | 2 | $\frac{1}{2}(q-1)$ | $f$ | 1 |
| $\mathbf{O}^\pm$ | $2q^{n(n-2)/4}(q^{n/2}\mp 1)\prod_{i=1}^{n/2-1}(q^{2i}-1)$ | 2 | $(2,q-1)$ | $q-1$ | $f$ | 1 |

表 2.4　射影典型群的阶之间的关系

| 情形 | $\lvert I\cap Z\rvert$ | $\lvert\overline{S}:\overline{\Omega}\rvert$ | $\lvert\overline{I}:\overline{S}\rvert$ | $\lvert\overline{\Delta}:\overline{I}\rvert$ | $\lvert\overline{\Gamma}:\overline{\Delta}\rvert$ | $\lvert\overline{A\Gamma}:\overline{\Gamma}\rvert$ |
|---|---|---|---|---|---|---|
| **L** | $q-1$ | 1 | $(q-1,n)$ | 1 | $f$ | $2^*$ |
| **U** | $q+1$ | 1 | $(q+1,n)$ | 1 | $2f$ | 1 |
| **S** | $(2,q-1)$ | 1 | 1 | $(2,q-1)$ | $f$ | 1 |
| $\mathbf{O}^\circ$ | $2^{**}$ | 2 | 1 | 1 | $f$ | 1 |
| $\mathbf{O}^\pm$ | $(2,q-1)$ | $a_\pm^{***}$ | $(2,q-1)$ | $(2,q-1)$ | $f$ | 1 |

**注 2.8**：我们现在对表 2.3和表 2.4作如下注释

(i) 两个表中 $(a,b)$ 表示整数 $a$ 和 $b$ 的最大公因子;

(ii) 对于 **U** 的情形, 因为要求有限域 $\mathbb{F}_q$ 中的 $q$ 是一个平方数, 所以在该情形下 $V$ 表示 $\mathbb{F}_{q^2}$ 上的 $n$ 维向量空间. 表中所表示的群的阶也是对应该空间下的厄尔米特型得到的;

(iii) 对于 $^*$, 当 $n=2$ 时, 我们有 $A\Gamma(V,\kappa)=\Gamma(V,\kappa)$, 因此这时表 2.3中 $2^*$ 应被 1 代替;

(iv) 对于 $^{**}$, 当 $n=1$ 时, 我们有 $S(V,\kappa)=\Omega(V,\kappa)$, 这时表 2.3和表 2.4中 $2^{**}$ 应被 1 代替;

(v) 对于 $^{***}$, 这里 $a_\pm\in\{1,2\}$, $a_+a_-=2^{(2,q)}$, 当 $q$ 是奇数时, $a_+=2$ 当且仅当 $\frac{1}{4}n(q-1)$ 是偶数.

由于本文主要的研究对象是针对 $\kappa$ 是非退化的二次型的情形, 所以我们单独针对表 2.3和表 2.4中 $\mathbf{O}^\varepsilon$, $\varepsilon=+,-,\circ$ 的情形作出下列说明.

**注 2.9**：我们令 $V=V(n,q)$, 令 $\kappa=Q$ 是 $V$ 上的一个非退化的二次型. 我们一般将 $\Gamma(V,Q)$ 记为 $\Gamma O_n^\varepsilon(q)$ 或 $\Gamma O^\varepsilon(n,q)$, 这里 $\varepsilon=+,-,\circ$. 当 $\varepsilon=\pm$ 时, 则 $n$ 必定为偶数. 由表 2.3可知,

$$|I(V,\kappa)|=2q^{n(n-2)/4}(q^{n/2}\mp 1)\prod_{i=1}^{n/2-1}(q^{2i}-1),$$

$$|\Delta(V,\kappa):I(V,\kappa)|=q-1,$$

$$|\Gamma(V,\kappa):\Delta(V,\kappa)|=f.$$

则我们计算 $\Gamma\mathrm{O}_n^{\pm}(q)$ 的阶分别为

$$|\Gamma\mathrm{O}_n^{\pm}(q)|=2q^{n(n-2)/4}(q^{n/2}\mp 1)\prod_{i=1}^{n/2-1}(q^{2i}-1)(q-1)f.$$

**注 2.10**：在第 2 章我们将会提到的群 PGO 是指射影相似群 $\overline{\Delta(V,Q)}$.

**注 2.11**：在第 3.2 节我们将提到的群 $\mathrm{GU}_3(q)$ 是指群 $I(V,\kappa)$, 这里的空间 $V=\mathbb{F}_{q^2}^4$, $\kappa$ 为 $V$ 上的厄尔米特型.

# 3 几类二次曲面上的 $m$-ovoids

本章的内容主要是通过典型群及其子群结构给出几类二次曲面上的 $m$-ovoids 的构造.

## 3.1 $Q(4,q)$ 中的 $\frac{q-1}{2}$-ovoids

在本节中, 我们主要讨论经典广义四边形 $Q(4,q)$ 中的 $m$-ovoids. 在第 2 章, 我们介绍了有限经典极空间, 我们称由秩为 2 的有限经典极空间的点线得到关联结构为经典的广义四边形. 广义四边形 $Q(4,q)$ 中的点和线分别是包含在 PG$(4,q)$ 上抛物二次曲面中的完全奇异点和完全奇异线. 一个 $Q(4,q)$ 的 $m$-ovoid 是 $Q(4,q)$ 的点集满足: 该点集与每条完全奇异线相交于 $m$ 个点. 关于 $Q(4,q)$ 中 $m$-ovoids 的背景知识, 请参考绪论中的介绍. 在本节, 我们对于 $q \equiv 1(\text{mod } 4)$ 并且 $q > 5$ 的情形构造了 $Q(4,q)$ 中 $\frac{q-1}{2}$-ovoids 的无穷类. 这里构造和证明技巧与文献[35] 中的较为相似. 主要困难是要从典型群 PGO$(5,q)$ 的丰富子群结构中选择合适的自同构群来进行构造.

### 3.1.1 $Q(4,q)$ 的模型

令 $q \equiv 1(\text{mod } 4)$ 是一个素数幂, 且令 $V = \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_{q^2} \times \mathbb{F}_q$. 我们可以将 $V$ 看作 $\mathbb{F}_q$ 上的一个 5 维向量空间, 将其元素形式记为 $(x,y,\alpha,z)$, 其中 $x,y,z \in \mathbb{F}_q$ 且 $\alpha \in \mathbb{F}_{q^2}$. 我们定义向量空间 $V$ 上的二次型 $Q$ 如下

$$Q((x,y,\alpha,z)) = xy + \alpha^{q+1} + z^2.$$

则二次型 $Q$ 对应的双线性型 $B$ 为

$$B((x,y,\alpha,z),(x',y',\alpha',z')) = xy' + x'y + \alpha\alpha'^q + \alpha^q\alpha' + 2zz'.$$

很容易验证上述定义的二次型 $Q$ 是非退化的并且对应的二次曲面是抛物二次曲面 $Q(4,q)$. 因此, 我们可以将 $Q(4,q)$ 的点集定义为

$$Q(4,q) = \{\langle(x,y,\alpha,z)\rangle | 0 \neq (x,y,\alpha,z) \in V,\ Q((x,y,\alpha,z)) = 0\}.$$

为简单起见, 在本节的剩余部分, 我们将使用 $(x,y,\alpha,z)$ 代替 $\langle(x,y,\alpha,z)\rangle$ 来表示 PG$(4,q)$ 的射影点.

我们之所以选择此模型, 是因为在该模型下可以使我们选定的自同构群 $G$ 有一个很好的表示形式.

令 $\mathbb{F}_q^*$ 是有限域 $\mathbb{F}_q$ 的乘法群. 对于每个 $\lambda \in \mathbb{F}_q^*$ 和 $\mu \in \mathbb{F}_{q^2}^*$ 使得 $\mu^{\frac{q+1}{2}} = 1$, 我们定义

$$T_{\lambda,\mu} : (x,y,\alpha,z) \mapsto (x\lambda, y\lambda^{-1}, \alpha\lambda^{\frac{q-1}{2}}\mu, z),$$

这是 $Q(4,q)$ 上的一个等距变换, 即等距群 $I(V,Q)$ 中的元素. 令 $H$ 是由这样的 $T_{\lambda,\mu}$ 生成的群, 即,

$$H = \langle T_{\lambda,\mu} : \lambda \in \mathbb{F}_q^*, \mu \in \mathbb{F}_{q^2}^*, \mu^{\frac{q+1}{2}} = 1 \rangle.$$

**引理 3.1：** *以上定义的群 $H$ 是 PGO$(5,q)$ 的一个阶为 $\frac{q^2-1}{2}$ 的循环子群.*

证明. 显然群 $H$ 是两个循环子群 $\langle T_{\lambda,1} : \lambda \in \mathbb{F}_q^* \rangle$ 和 $\langle T_{1,\mu} : \mu \in \mathbb{F}_{q^2}^*, \mu^{\frac{q+1}{2}} = 1 \rangle$ 的直积; 这两个循环子群的阶分别为 $q-1$ 和 $\frac{q+1}{2}$. 对于 $q \equiv 1 (\text{mod } 4)$ 情形, 我们有 gcd$(q-1, \frac{q+1}{2}) = 1$, 从而结论得证. □

进一步地, 我们定义 PGO$(5,q)$ 中的一个二阶元 (involution) $\tau$ 如下:

$$\tau : (x, y, \alpha, z) \mapsto (y, x, \alpha^q, z),$$

它也是 $Q(4,q)$ 上的一个等距变换. 设 $G := \langle H, \tau \rangle$, 其同构于 $C_{\frac{q^2-1}{2}} \rtimes C_2$, 其中 $C_k$ 表示一个 $k$ 阶循环群. 该群 $G$ 即为我们要构造的 $Q(4,q)$ 中 $\frac{q-1}{2}$-ovoids 的一个自同构群.

### 3.1.2 $G$-轨道的结构

我们现在对上述群 $G$ 在 $Q(4,q)$ 上的轨道结构进行描述. 对于一个点 $P \in$ PG$(4,q)$, 令 $O(P)$ 表示包含点 $P$ 的 $G$-轨道.

令 $\gamma$ 为一个给定的 $\mathbb{F}_{q^2}$ 中的元素使得 $\gamma^{q+1} = -1$, 令 $\square_q$ (对应. $\square_{q^2}$) 和 $\blacksquare_q$ (对应. $\blacksquare_{q^2}$) 分别表示 $\mathbb{F}_q$ (对应. $\mathbb{F}_{q^2}$) 中的非零平方元和非平方元的集合. 除以下 3 种情形外, 所有 $G$-轨道的长度为 $\frac{q^2-1}{2}$ 或 $q^2-1$.

1. 唯一一个长度为 2 的轨道 $O(1,0,0,0) = \{(1,0,0,0), (0,1,0,0)\}$;
2. 唯一一个长度为 $q-1$ 的轨道 $O(1,-1,0,1) = C \setminus O(1,0,0,0)$, 其中 $C = \{\langle (x,y,0,z) \rangle | 0 \neq (x,y,0,z) \in V, xy + z^2 = 0\}$ 是一个锥面 (conic), 如图 3.1所示;
3. 唯一一个长度为 $q+1$ 的轨道 $O(0,0,\gamma,1)$.

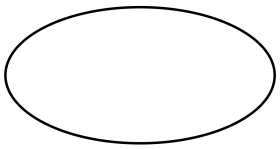

图 3.1 锥面: $xy + z^2 = 0$

我们称长度为 $\frac{q^2-1}{2}$ 的轨道为短轨道, 长度为 $q^2-1$ 的轨道为长轨道.

**引理 3.2：** 令 $x,y\in\mathbb{F}_q^*$, $\alpha\in\mathbb{F}_{q^2}^*$, 且 $(x,y,\alpha,1)\in Q(4,q)$. 则 $G$-轨道 $O(x,y,\alpha,1)$ 是一个短轨道当且仅当 $xy(1+xy)\in\square_q$, 或等价为 $\alpha^{q+1}(1+\alpha^{q+1})\in\square_q$.

证明. 由于 $G$ 的阶为 $q^2-1$, 则 $O(x,y,\alpha,1)$ 是一条短轨道当且仅当点 $(x,y,\alpha,1)$ 在 $G$ 中的稳定子群的阶为 2. 若 $T_{\lambda,\mu}$ 固定点 $(x,y,\alpha,1)$, 那么存在元素 $c\in\mathbb{F}_q^*$ 使得

$$(x\lambda,y\lambda^{-1},\alpha\lambda^{\frac{q-1}{2}}\mu,1)=c(x,y,\alpha,1).$$

从而有 $c=1=\lambda=\lambda^{-1}=\lambda^{\frac{q-1}{2}}\mu$, 可得 $\lambda=\mu=1$. 若 $T_{\lambda,\mu}\cdot\tau$ 固定点 $(x,y,\alpha,1)$, 那么便存在元素 $c'\in\mathbb{F}_q^*$ 使得

$$(y\lambda,x\lambda^{-1},\alpha^q\lambda^{\frac{q-1}{2}}\mu,1)=c'(x,y,\alpha,1).$$

我们有 $c'=1$, $\lambda=xy^{-1}$, $\mu=(yx^{-1})^{\frac{q-1}{2}}\alpha^{1-q}$, 这表明 $\lambda,\mu$ 的值均由 $x,y,\alpha$ 所唯一确定. 要使得 $T_{\lambda,\mu}\cdot\tau$ 属于群 $G$, 需要 $\mu^{\frac{q+1}{2}}=1$, 即, $(yx^{-1})^{\frac{q-1}{2}}\alpha^{\frac{1-q^2}{2}}=1$, 等价于 $xy\alpha^{q+1}$ 是 $\mathbb{F}_q^*$ 的非零平方元. 由于 $xy+\alpha^{q+1}+1=0$ 且在 $q\equiv1(\mathrm{mod}\,4)$ 情形下我们有 $-1\in\square_q$, 从而结论成立. □

令 $\omega$ 为 $\mathbb{F}_{q^2}$ 的一个固定的本原元, 仍令 $\gamma$ 为 $\mathbb{F}_{q^2}$ 的一个固定的元素使得 $\gamma^{q+1}=-1$. 根据引理 3.2, 我们现在准备在接下来给出长短轨道的具体描述. 对于 $S,S'\in\{\square_q,\blacksquare_q\}$, 关于 $S\cap(S'-1)$ 的大小的计算, 请参阅注 3.6. 这里 $S'-1=\{x-1|\,x\in S'\}$.

共有 $q-1$ 个长度为 $\frac{q^2-1}{2}$ 的短轨道, 具体形式如下:

1. 可以看出不存在 $G$ 中的元素将点 $(1,-\omega^{2(q+1)},\omega^2,0)$ 映到点 $(1,-\omega^{q+1},\omega,0)$, 从而点集 $\{(x,y,\alpha,0)\in Q(4,q)|\,\alpha\neq0\}$ 被分成两个轨道, 分别为

   $$O(1,-\omega^{2(q+1)},\omega^2,0)\text{ 和 }O(1,-\omega^{q+1},\omega,0).$$

   与引理 3.2的证明类似, 容易得到 $O(1,-\omega^{2(q+1)},\omega^2,0)$ 和 $O(1,-\omega^{q+1},\omega,0)$ 在 $G$ 中的稳定子群分别是 $\langle T_{-\omega^{-2(q+1)},\omega^{-2(q-1)}}\cdot\tau\rangle$ 和 $\langle T_{-\omega^{-(q+1)},-\omega^{-(q-1)}}\cdot\tau\rangle$. 由于 $T_{-\omega^{-2(q+1)},\omega^{-2(q-1)}}\cdot\tau$ 和 $T_{-\omega^{-(q+1)},-\omega^{-(q-1)}}\cdot\tau$ 都是 $G$ 中的二阶元, 所以这两个轨道长度均为 $\frac{q^2-1}{2}$;

2. 可以看出不存在 $G$ 中的元素将点 $(1,y,\alpha,1)$ 映到点 $(1,y,\alpha\omega^{q-1},1)$, 从而对于每个 $y\in\square_q\cap(\square_q-1)$, 都有两个轨道 $O(1,y,\alpha,1)$ 和 $O(1,y,\alpha\omega^{q-1},1)$ 使得 $y+\alpha^{q+1}+1=0$. 共计有 $2\cdot|\square_q\cap(\square_q-1)|=\frac{q-5}{2}$ 个这样的长为 $\frac{q^2-1}{2}$ 的轨道;

3. 可以看出不存在 $G$ 中的元素将点 $(1,y,\alpha,1)$ 映到点 $(1,y,\alpha^q,1)$, 从而对于每个 $y \in \blacksquare_q \cap (\blacksquare_q - 1)$, 都有两个轨道 $O(1,y,\alpha,1)$ 和 $O(1,y,\alpha^q,1)$ 使得 $y+\alpha^{q+1}+1 = 0$. 共计有 $2 \cdot |\blacksquare_q \cap (\blacksquare_q - 1)| = \frac{q-1}{2}$ 个这样的长为 $\frac{q^2-1}{2}$ 的轨道.

共有 $\frac{q+3}{2}$ 个长度为 $q^2-1$ 的长轨道, 具体形式如下:

1. 由于不存在 $G$ 中的元素将点 $(1,0,\gamma,1)$ 映到点 $(1,0,\gamma\omega^{q-1},1)$, 所以共有 2 个长为 $q^2-1$ 的第二个坐标为 0 的轨道, 分别为 $O(1,0,\gamma,1)$ 和 $O(1,0,\gamma\omega^{q-1},1)$;

2. 对于每个 $y \in \square_q \cap (\blacksquare_q - 1)$, 恰有一个轨道 $O(1,y,\alpha,1)$ 使得 $y+\alpha^{q+1}+1=0$. 共计有 $|\square_q \cap (\blacksquare_q - 1)| = \frac{q-1}{4}$ 个这样的长为 $q^2-1$ 的轨道;

3. 对于每个 $y \in \blacksquare_q \cap (\square_q - 1)$, 恰有一个轨道 $O(1,y,\alpha,1)$ 使得 $y+\alpha^{q+1}+1=0$. 共计有 $|\blacksquare_q \cap (\square_q - 1)| = \frac{q-1}{4}$ 个这样的长为 $q^2-1$ 的轨道.

特别地, 有 7 个代表元坐标包含 0 的轨道, 它们分别是:

$$O(1,0,0,0),\ O(1,-1,0,1),\ O(0,0,\omega^{\frac{q-1}{2}},1),\ O(1,-\omega^{2(q+1)},\omega^2,0),$$

$$O(1,-\omega^{q+1},\omega,0),\ O(1,0,\omega^{\frac{q-1}{2}},1) \text{ 和 } O(1,0,\omega^{\frac{3(q-1)}{2}},1).$$

**注 3.3**：现在我们对群 $G$ 的作用进行更几何的描述. 设 $C_1 = \{\langle(0,0,\alpha,z)\rangle | 0 \neq (0,0,\alpha,z) \in V,\ \alpha^{q+1}+z^2=0\}$, 则 $C_1$ 是 $Q(4,q)$ 的一个锥面. 此外, $C_1^{\perp}$ 是一条 $C_1$ 的外线, 这条线经过轨道 $O(1,0,0,0)$ 中的 $(0,1,0,0)$ 和 $(1,0,0,0)$ 两个点. 群 $G$ 是 $C_1$ 和 $C$ 的稳定子群.

### 3.1.3 $Q(4,q)$ 中 $\frac{q-1}{2}$-ovoids 的构造

现在我们准备描述 $Q(4,q)$ 中 $\frac{q-1}{2}$-ovoids 的构造. 令 $q>5$ 是奇素数幂满足 $q \equiv 1 (\text{mod } 4)$, 令 $\omega$ 是 $\mathbb{F}_{q^2}^*$ 的本原元. 固定 $\mathbb{F}_q^*$ 中的一对元素 $(a,b)$ 使得

$$1+a^2=b^2. \tag{3.1}$$

我们现定义

$$\begin{aligned}\mathcal{M} = \ & O(1,-1,0,1) \cup O(1,-\omega^{2(q+1)},\omega^2,0) \cup \\ & O(1,0,\omega^{\frac{q-1}{2}},1) \cup \mathcal{T} \cup O(1,-b^2,a,1),\end{aligned} \tag{3.2}$$

这里

$$\mathcal{T} = \{(x,y,\alpha,1) \in Q(4,q) \mid 1+b^{-2}xy \in \square_q,\ xy\alpha \neq 0\}. \tag{3.3}$$

**引理 3.4**：上述集合 $\mathcal{T}$ 是一个 $G$-不变集, 它有 $\frac{(q^2-1)(q-5)}{2}$ 个点.

证明. 集合 $\mathcal{T}$ 的 $G$-不变性很容易进行直接验证. 接下来只需要计算集合 $\mathcal{T}$ 的大小. 我们有

$$\begin{aligned}|\mathcal{T}| &= (q-1)|\{z\in\mathbb{F}_q^*,\, \alpha\in\mathbb{F}_{q^2}^*|\, z+1+\alpha^{q+1}=0,\, 1+b^{-2}z\in\square_q\}|\\ &= (q^2-1)|\{z\in\mathbb{F}_q|\, 1+b^{-2}z\in\square_q,\, z\neq 0,-1\}|\\ &= (q^2-1)(|\{z\in\mathbb{F}_q|\, 1+b^{-2}z\in\square_q\}|-2)\\ &= (q^2-1)\left(\frac{q-1}{2}-2\right)=\frac{(q^2-1)(q-5)}{2}.\end{aligned}$$

这里, 我们在第三个等式中利用了 $1-b^{-2}=a^2b^{-2}$ 是一个平方元的条件, 在第四个等式中利用了集合 $b^2(\square_q-1)=\{b^2(x-1):\, x\in\square_q\}$ 的大小为 $\frac{q-1}{2}$ 事实. 证毕. □

由引理 3.4, 我们有

$$|\mathcal{M}|=(q-1)+2(q^2-1)+\frac{(q^2-1)(q-5)}{2}=\frac{q-1}{2}(q^2+1),$$

这恰好是 $Q(4,q)$ 中一个 $\frac{q-1}{2}$-ovoid 的大小. 令 $\eta$ 是 $\mathbb{F}_q$ 的二次（乘法）特征, 即,

$$\eta(x)=\begin{cases}1, & \text{如果 } x\in\square_q,\\ -1, & \text{如果 } x\in\blacksquare_q,\\ 0, & \text{如果 } x=0.\end{cases}\tag{3.4}$$

进一步地, 我们定义 Kronecker delta 函数 $[[\mathcal{X}]]$ 如下

$$[[\mathcal{X}]]=\begin{cases}1, & \text{若性质 } \mathcal{X} \text{ 成立},\\ 0, & \text{否则}.\end{cases}\tag{3.5}$$

**引理 3.5 (Lidl 和 Niederreiter[51], 定理 5.48)：** 令 $g(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$, 这里 $q$ 为奇数且 $a_2\neq 0$. 设 $d=a_1^2-4a_0a_2$, 令 $\eta$ 表示 $\mathbb{F}_q$ 的二次特征. 则有

$$\sum_{c\in\mathbb{F}_q}\eta(g(c))=\begin{cases}-\eta(a_2), & \text{如果 } d\neq 0,\\ (q-1)\eta(a_2), & \text{如果 } d=0.\end{cases}$$

**注 3.6：** 考虑该引理的特殊情形, 令 $g(x)=x(x+1)$, 即 $a_1=a_2=1, a_0=0$. 我们有 $d=a_1^2-4a_0a_2=1$, 因此 $\sum_{c\in\mathbb{F}_q}\eta(g(c))=-1$. 令 $n_1, n_2, n_3, n_4$ 分别表示使得 $(\eta(x),\eta(x+1))=(1,1),(1,-1),(-1,1),(-1,-1)$ 的 $x$ 的个数. 则有

$$\begin{aligned}n_1+n_2&=\frac{q-1}{2}-1,\ n_3+n_4=\frac{q-1}{2},\\ n_1+n_3&=\frac{q-1}{2}-1,\ n_2+n_4=\frac{q-1}{2}.\end{aligned}$$

由 $\sum_{c\in\mathbb{F}_q}\eta(g(c))=-1$ 可得 $n_1-n_2-n_3+n_4=-1$. 从以上等式中我们解得

$$n_1=\frac{q-5}{4},\ n_2=\frac{q-1}{4},\ n_3=\frac{q-1}{4},\ n_4=\frac{q-1}{4}.$$

特别地, 由定义可知, $n_1$ 是集合 $\square_q\cap(\square_q-1)$ 的大小, $n_2$ 是集合 $\square_q\cap(\blacksquare_q-1)$ 的大小, $n_3$ 是集合 $\blacksquare_q\cap(\square_q-1)$ 的大小, 且 $n_4$ 是集合 $\blacksquare_q\cap(\blacksquare_q-1)$ 的大小.

**定理 3.7**：对于 $q\equiv 1(\mathrm{mod}\ 4)$ 且 $q>5$, 由等式 (3.2)定义的点集 $\mathcal{M}$ 是 $Q(4,q)$ 的一个 $\frac{q-1}{2}$-ovoid.

证明. 我们采用与文献[35] 相同的证明技巧, 即, 往证 $Q(4,q)$ 的每条线交 $\mathcal{M}$ 于 $\frac{q-1}{2}$ 个点. 显然, $Q(4,q)$ 的每条线与超平面 $\{(x,y,\alpha,z)\in V|\ y=0\}$ 至少交于一个点. $Q(4,q)$ 中存在四个 $G$-轨道拥有第二个坐标为 0 的代表元, 分别是

$$O(1,0,0,0),\ O(0,0,\omega^{\frac{q-1}{2}},1),\ O(1,0,\omega^{\frac{q-1}{2}},1)\text{ 和 }O(1,0,\omega^{\frac{3(q-1)}{2}},1).$$

由于 $\mathcal{M}$ 是 $G$-不变的, 所以我们只需要考虑经过点

$$(1,0,0,0),\ (0,0,\omega^{\frac{q-1}{2}},1),\ (1,0,\omega^{\frac{q-1}{2}},1)\text{ 或 }(1,0,\omega^{\frac{3(q-1)}{2}},1)$$

的线即可. 由 $q>5$ 的假设条件和引理 3.4可知, 集合 $\mathcal{T}$ 是非空的. 我们分为以下 4 种情况进行讨论.

情况 **1.** $Q(4,q)$ 的线 $\ell$ 经过点 $P=(1,0,0,0)$.

线 $\ell$ 恰好交超平面 $\{(x,y,\alpha,z)\in V:\ x=0\}$ 于点 $Q$, 因为点 $Q$ 与 $P$ 垂直, 则 $Q=(0,y_1,\alpha_1,z_1)$. 由于 $B(P,Q)=0$, 再结合 $B$ 和 $Q(4,q)$ 的定义, 我们有 $y_1=0$ 且 $\alpha_1^{q+1}+z_1^2=0$, $z_1\neq 0$. 我们可以设 $z_1=1$. 因此, 我们有 $\ell=\langle P,Q\rangle$, 其中 $Q=(0,0,\alpha_1,1)$, $\alpha_1\in\mathbb{F}_{q^2}^*$ 使得 $\alpha_1^{q+1}+1=0$. 线 $\ell$ 可以表示为 $\ell=\{(t,0,\alpha_1,1)|t\in\mathbb{F}_q\}\cup\{(1,0,0,0)\}$. 可以看出 $P=(1,0,0,0)\notin\mathcal{M}$. 对任意的 $(x,y,\alpha,z)\in O(1,-1,0,1)$, $O(1,-\omega^{2(q+1)},\omega^2,0)$, $\mathcal{T}$ 或 $O(1,-b^2,a,1)$, 我们有 $y\neq 0$, 故其不可能落在线 $\ell$ 上. 因此, $|\ell\cap\mathcal{M}|=|\ell\cap O(1,0,\omega^{\frac{q-1}{2}},1)|$. 我们往证该大小为 $\frac{q-1}{2}$.

轨道 $O(1,0,\omega^{\frac{q-1}{2}},1)$ 是一个长度为 $q^2-1$ 的长轨道. 它是集合

$$U_1=\{(\lambda,0,\lambda^{\frac{q-1}{2}}\mu\omega^{\frac{q-1}{2}},1)|\lambda\in\mathbb{F}_q^*,\mu\in\mathbb{F}_{q^2}^*,\mu^{\frac{q+1}{2}}=1\},\tag{3.6}$$

和

$$U_2=\{(0,\lambda,-\lambda^{\frac{q-1}{2}}\mu^{-1}\omega^{-\frac{q-1}{2}},1)|\lambda\in\mathbb{F}_q^*,\mu\in\mathbb{F}_{q^2}^*,\mu^{\frac{q+1}{2}}=1\}\tag{3.7}$$

的并集. 通过检验第二个坐标可以看出 $U_2\cap\ell=\emptyset$. 假设 $\ell$ 上的点 $(t,0,\alpha_1,1)$, 这里 $t\in\mathbb{F}_q$, 落在 $U_1$ 中, 那么存在 $\lambda\in\mathbb{F}_q^*$, $\mu\in\mathbb{F}_{q^2}^*$ 满足 $\mu^{\frac{q+1}{2}}=1$ 使得

$$(t,0,\alpha_1,1)=c(\lambda,0,\lambda^{\frac{q-1}{2}}\mu\omega^{\frac{q-1}{2}},1)$$

对某个 $c \in \mathbb{F}_q^*$ 成立. 由最后一个坐标可知 $c = 1$, 进一步地, 由第一个坐标可知 $\lambda = t$, 这意味着 $t \neq 0$. 通过比较第三个坐标, 我们有

$$\mu = \alpha_1 t^{-\frac{q-1}{2}} \omega^{-\frac{q-1}{2}}$$

且

$$\mu^{\frac{q+1}{2}} = \alpha_1^{\frac{q+1}{2}} t^{-\frac{q-1}{2}} \omega^{-\frac{q^2-1}{4}} = 1.$$

因此,

$$\begin{aligned} |\ell \cap U_1| &= \#\{t \in \mathbb{F}_q^* | \, t^{\frac{q-1}{2}} = \alpha_1^{\frac{q+1}{2}} \omega^{-\frac{q^2-1}{4}}\} \\ &= \frac{q-1}{2}. \end{aligned}$$

最后一个等式成立是由 $\alpha_1^{q+1} + 1 = 0$ 可得

$$\left(\alpha_1^{\frac{q+1}{2}} \omega^{-\frac{q^2-1}{4}}\right)^2 = (\alpha_1^{q+1})(\omega^{-\frac{q^2-1}{2}}) = 1,$$

从而 $\alpha_1^{\frac{q+1}{2}} \omega^{-\frac{q^2-1}{4}} \in \{1, -1\}$.

情况 **2.** $Q(4,q)$ 的线 $\ell$ 经过点 $P = (0,0,\omega^{\frac{q-1}{2}},1)$.

线 $\ell$ 恰好交超平面 $\{(x,y,\alpha,z) \in V | \, z = 0\}$ 于一点 $Q = (x_1, y_1, \alpha_1, 0)$, 这里 $x_1 y_1 + \alpha_1^{q+1} = 0$. 如果 $\alpha_1 = 0$, 则有 $x_1 y_1 = 0$. 这意味着 $Q = (1,0,0,0)$ 或 $(0,1,0,0)$. 这两个点落在相同的 $G$-轨道中, 则我们可归结到情形 1. 现假设 $\alpha_1 \neq 0$. 由 $P \perp Q$, 我们有 $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha_1 \omega^{\frac{q^2-q}{2}}) = 0$, 即 $\alpha_1 = \omega^{-1} a_1$ 对于某个 $a_1 \in \mathbb{F}_q^*$. 这里 $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ 表示 $\mathbb{F}_{q^2}$ 到 $\mathbb{F}_q$ 的迹函数. 因为 $x_1 y_1 \neq 0$, 所以我们可以假设点 $Q$ 为 $(1, y_1, \alpha_1, 0)$ 满足 $y_1 + \alpha_1^{q+1} = 0$. 则该线

$$\ell = \{(1, y_1, \alpha_1 + t\omega^{\frac{q-1}{2}}, t) | t \in \mathbb{F}_q\} \cup \{(0,0,\omega^{\frac{q-1}{2}},1)\}.$$

点 $P = (0,0,\omega^{\frac{q-1}{2}},1) \notin \mathcal{M}$ 且 $\alpha_1 = \omega^{-1} a_1$ 是 $\mathbb{F}_{q^2}^*$ 的一个非平方元. 下面我们计算 $\ell$ 与 $\mathcal{M}$ 的每个部分相交的点的个数.

情况 **2.1.** $|\ell \cap O(1,-1,0,1)| = 0$.

假设线 $\ell$ 上的点 $(1, y_1, \alpha_1 + t\omega^{\frac{q-1}{2}}, t)$ 落在 $O(1,-1,0,1)$ 中, 这里 $t \in \mathbb{F}_q$. 则这样的点的第三个坐标必定为 0, 即, $\alpha_1 + t\omega^{\frac{q-1}{2}} = 0$. 我们已经证明了 $\alpha_1$ 是 $\mathbb{F}_{q^2}^*$ 的非平方元. 另一方面, 由于 $q \equiv 1 (\mathrm{mod}\ 4)$, 则 $-\omega^{\frac{q-1}{2}} t$ 为 0 或 $\mathbb{F}_{q^2}^*$ 的平方元. 该矛盾使得结论 $|\ell \cap O(1,-1,0,1)| = 0$ 成立.

情况 **2.2.** $|\ell \cap O(1, -\omega^{2(q+1)}, \omega^2, 0)| = 0$.

线 $\ell$ 与 $O(1, -\omega^{2(q+1)}, \omega^2, 0)$ 相交的每个点最后一个坐标为 **0**, 线 $\ell$ 中具有此性质的唯一点是 $Q$. 但点 $Q$ 不落在轨道

$$O(1, -\omega^{2(q+1)}, \omega^2, 0) = \{(\lambda, -\omega^{2(q+1)}\lambda^{-1}, \omega^2\lambda^{\frac{q-1}{2}}\mu, 0) | \lambda \in \mathbb{F}_q^*, \mu \in \mathbb{F}_{q^2}^*, \mu^{\frac{q+1}{2}} = 1\}$$

中. 否则, 便存在 $\lambda \in \mathbb{F}_q^*$ 使得 $y_1 = -\omega^{2(q+1)}\lambda^{-2}$, 通过比较点 $Q = (1, y_1, \alpha_1, 0)$ 和 $(1, -\omega^{2(q+1)}\lambda^{-2}, \omega^2\lambda^{\frac{q-3}{2}}\mu, 0)$ 的第二个坐标会得到一个矛盾, 因为 $y_1 = -\alpha_1^{q+1}$ 是 $\mathbb{F}_q$ 的一个非平方元.

情况 **2.3.** $|\ell \cap O(1, 0, \omega^{\frac{q-1}{2}}, 1)| = 0$.

线 $\ell$ 与 $O(1, 0, \omega^{\frac{q-1}{2}}, 1)$ 相交的每个点第二个坐标为 **0**, 由于 $y_1 \neq 0$, 则 $\ell$ 中具有此性质的唯一点是 $P$. 然而, $O(0, 0, \omega^{\frac{q-1}{2}}, 1)$ 和 $O(1, 0, \omega^{\frac{q-1}{2}}, 1)$ 是不同的 $G$-轨道, 因此 $P = (0, 0, \omega^{\frac{q-1}{2}}, 1) \notin O(1, 0, \omega^{\frac{q-1}{2}}, 1)$.

情况 **2.4.** $|\ell \cap \mathcal{T}| = \frac{q-1}{2}$.

假设 $\ell$ 上的点 $(1, y_1, \alpha_1 + t\omega^{\frac{q-1}{2}}, t)$ 落在 $\mathcal{T}$ 中, 这里 $t \in \mathbb{F}_q$, 则存在 $(x, y, \alpha, 1) \in \mathcal{T}$ 使得

$$(1, y_1, \alpha_1 + t\omega^{\frac{q-1}{2}}, t) = c(x, y, \alpha, 1)$$

对于某个 $c \in \mathbb{F}_q^*$ 成立. 由最后一个坐标可知 $c = t$. 特别地, $t \neq 0$. 通过比较其他坐标, 我们有

$$1 = tx,\ y_1 = ty,\ \alpha_1 + t\omega^{\frac{q-1}{2}} = t\alpha.$$

从而 $x = t^{-1}$, $y = t^{-1}y_1$ 并且 $\alpha = t^{-1}\alpha_1 + \omega^{\frac{q-1}{2}}$. 由等式(3.3)中 $\mathcal{T}$ 的定义可得

$$|\ell \cap \mathcal{T}| = \#\{t \in \mathbb{F}_q^* | 1 + (tb)^{-2}y_1 \in \square_q\}.$$

如上所述, $y_1$ 是 $\mathbb{F}_q^*$ 的一个非平方元. 因此

$$\begin{aligned} |\ell \cap \mathcal{T}| &= 2 \cdot |b^{-2}y_1\square_q \cap (\square_q - 1)| \\ &= 2 \cdot |\blacksquare_q \cap (\square_q - 1)| = \frac{q-1}{2}. \end{aligned}$$

情况 **2.5.** $|\ell \cap O(1, -b^2, a, 1)| = 0$.

轨道 $O(1, -b^2, a, 1)$ 是一个短轨道, 其形式如下:

$$O(1, -b^2, a, 1) = \{(\lambda, -b^2\lambda^{-1}, a\lambda^{\frac{q-1}{2}}\mu, 1) : \lambda \in \mathbb{F}_q^*, \mu \in \mathbb{F}_{q^2}^*, \mu^{\frac{q+1}{2}} = 1\}. \quad (3.8)$$

假设 $\ell$ 中的点 $(1, y_1, \alpha_1 + t\omega^{\frac{q-1}{2}}, t)$ 落在 $O(1, -b^2, a, 1)$ 中, 这里 $t \in \mathbb{F}_q$. 通过比较坐标, 我们有 $y_1 = -t^2b^2$, 这与 $y_1$ 是 $\mathbb{F}_q$ 的一个非平方元的事实矛盾.

总之, 我们有 $|\ell \cap \mathcal{M}| = \frac{q-1}{2}$. 从而完成了情况 2 的证明.

情况 **3.** $Q(4,q)$ 的线 $\ell$ 经过点 $P = (1, 0, \omega^{\frac{q-1}{2}}, 1)$.

与情况 2 类似, 我们只需要考虑这样一种情况: 线 $\ell$ 经过点 $Q$ 使得

$$Q = (1, -\alpha_1^{q+1}, \alpha_1, 0)$$

对于某个 $\alpha_1 \in \mathbb{F}_{q^2}^*$ 成立. 由 $P \perp Q$, 我们推得 $-\alpha_1^{q+1} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha_1 \omega^{\frac{q^2-q}{2}}) = 0$. 设

$$y_1 = -\alpha_1^{q+1}, \quad \beta = \alpha_1 \omega^{-\frac{q-1}{2}}.$$

则有

$$\beta^{q+1} = (\alpha_1 \omega^{-\frac{q-1}{2}})^{q+1} = -\alpha_1^{q+1} = y_1, \tag{3.9}$$

并且

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) = -\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha_1 \omega^{\frac{q^2-q}{2}}) = -\alpha_1^{q+1} = y_1. \tag{3.10}$$

特别地, 对于这里的 $\beta \in \mathbb{F}_{q^2}^*$, 我们有 $\beta^{q+1} = \beta + \beta^q$, 等价于

$$\beta^q = \beta^{q-1} + 1 \tag{3.11}$$

且

$$\beta - 1 = \beta^{-(q-1)}. \tag{3.12}$$

我们往证 $\beta \in \mathbb{F}_q$ 当且仅当 $\beta = 2$: 如果 $\beta \in \mathbb{F}_q$, 则由等式(3.11)得 $\beta = \beta^q = \beta^{q-1} + 1 = 2$; 反之是显然的. 情况 $\beta = 2$ 和 $\beta \neq 2$ 的证明基本相同, 而前者更容易, 因此我们仅在下面证明 $\beta \neq 2$ 的情形. 在该情形中, 由等式(3.9)和(3.10)可知 $\beta$ 在 $\mathbb{F}_q$ 上的极小多项式是 $X^2 - y_1 X + y_1$; 由于 $\beta \notin \mathbb{F}_q$, 则判别式 $d' = y_1(y_1 - 4)$ 是 $\mathbb{F}_q$ 的非平方元.

现在, 我们可以计算 $\ell$ 与 $\mathcal{M}$ 的每个部分的交集大小. 我们有

$$\ell = \{(t+1, y_1, (\beta + t)\omega^{\frac{q-1}{2}}, t) | t \in \mathbb{F}_q\} \cup \{(1, 0, \omega^{\frac{q-1}{2}}, 1)\}$$

使得 $y_1 \neq 4$ (即, $\beta \neq 2$) 并且 $\beta = \alpha_1 \omega^{-\frac{q-1}{2}}$. 在该情况下, $P = (1, 0, \omega^{\frac{q-1}{2}}, 1) \in O(1, 0, \omega^{\frac{q-1}{2}}, 1) \subset \mathcal{M}$.

情况 **3.1.** $|\ell \cap O(1, -1, 0, 1)| = 0$.

假设 $\ell$ 上的点 $(t+1, y_1, (\beta + t)\omega^{\frac{q-1}{2}}, t)$ 落在 $O(1, -1, 0, 1)$ 中, 这里 $t \in \mathbb{F}_q$. 通过比较第三个坐标则有 $\beta = -t \in \mathbb{F}_q$, 即, $y_1 = 4$. 与假设矛盾.

情况 **3.2.** $|\ell \cap O(1,-\omega^{2(q+1)},\omega^2,0)| = [[y_1 \in \square_q]]$.

假设 $\ell$ 上的点 $(t+1, y_1, (\beta+t)\omega^{\frac{q-1}{2}}, t)$ 落在 $G$-轨道 $O(1,-\omega^{2(q+1)},\omega^2,0)$ 中, 这里 $t \in \mathbb{F}_q$. 则该点的最后一个坐标必定为 **0**, 因此 $t = 0$. 通过比较其他坐标可得, 条件

$$(1, y_1, \beta\omega^{\frac{q-1}{2}}, 0) \in \ell \cap O(1,-\omega^{2(q+1)},\omega^2,0)$$

成立当且仅当 $y_1$ 是 $\mathbb{F}_q$ 的非零平方元. 由等式(3.5)中 Kronecker delta 函数的定义可得 $|\ell \cap O(1,-\omega^{2(q+1)},\omega^2,0)| = [[y_1 \in \square_q]]$.

情况 **3.3.** $|\ell \cap O(1,0,\omega^{\frac{q-1}{2}},1)| = 1$.

一方面, $P$ 是 $\ell$ 与 $O(1,0,\omega^{\frac{q-1}{2}},1)$ 的一个交点. 另一方面, 假设存在 $\ell$ 的一个点 $(t+1, y_1, (\beta+t)\omega^{\frac{q-1}{2}}, t)$ 满足 $y_1 \neq 0$ 落在 $O(1,0,\omega^{\frac{q-1}{2}},1)$ 中, 由 $y_1 \neq 0$, 以及等式(3.6)和(3.7)可知, 该点必定在 $U_2$ 中. 因此, 我们有 $t = -1$. 则存在 $\lambda \in \mathbb{F}_q^*$, $\mu \in \mathbb{F}_{q^2}^*$ 满足 $\mu^{\frac{q+1}{2}} = 1$ 使得

$$(0, y_1, (\beta-1)\omega^{\frac{q-1}{2}}, -1) = c(0, \lambda, -\lambda^{\frac{q-1}{2}}\mu^{-1}\omega^{-\frac{q-1}{2}}, 1)$$

对某个 $c \in \mathbb{F}_q^*$ 成立. 从而 $c = -1, \lambda = -y_1$,

$$\mu = \lambda^{\frac{q-1}{2}}(\beta-1)^{-1}\omega^{-(q-1)},$$

并且

$$\mu^{\frac{q+1}{2}} = -\lambda^{\frac{q-1}{2}}(\beta-1)^{-\frac{q+1}{2}} = 1.$$

则我们有

$$y_1^{\frac{q-1}{2}} = (-\lambda)^{\frac{q-1}{2}} = -(\beta-1)^{\frac{q+1}{2}} = -(\beta^q-1)^{\frac{q^2+q}{2}}. \tag{3.13}$$

根据等式(3.11)和(3.13), 我们推得 $y_1^{\frac{q-1}{2}} = -\beta^{\frac{q^2-1}{2}}$. 另一方面, 由等式 (3.9)我们有 $y_1 = \beta^{q+1}$, 从而 $y_1^{\frac{q-1}{2}} = \beta^{\frac{q^2-1}{2}}$. 矛盾.

情况 **3.4.** $|\ell \cap \mathcal{T}| = \frac{q-3}{2} - \frac{1}{2}(\eta(y_1(4b^2-y_1))+1) - [[y_1 \in \square_q]]$.

假设 $\ell$ 上的点 $(t+1, y_1, (\beta+t)\omega^{\frac{q-1}{2}}, t)$ 落在 $\mathcal{T}$ 中, 这里 $t \in \mathbb{F}_q$. 则存在 $(x, y, \alpha, 1) \in \mathcal{T}$ 使得

$$(t+1, y_1, (\beta+t)\omega^{\frac{q-1}{2}}, t) = c(x, y, \alpha, 1)$$

对于某个 $c \in \mathbb{F}_q^*$ 成立. 由最后一个坐标可得 $c = t$. 特别地, 由 $t+1 = tx, tx \neq 0$ 以及 $t = c$ 可知 $t \neq 0$ 并且 $t \neq -1$. 再通过比较其他坐标, 我们有

$$t+1 = tx,\ y_1 = ty,\ (\beta+t)\omega^{\frac{q-1}{2}} = t\alpha.$$

从而 $x=1+t^{-1}, y=t^{-1}y_1$ 并且 $\alpha=t^{-1}(\beta+t)\omega^{\frac{q-1}{2}}$. 因此,

$$\begin{aligned}|\ell\cap\mathcal{T}| &= \#\{t\in\mathbb{F}_q|\, 1+b^{-2}(1+t^{-1})t^{-1}y_1\in\square_q,\, t\neq 0,-1\}\\ &= \#\{t\in\mathbb{F}_q|\, b^2t^2+y_1t+y_1\in\square_q,\, t\neq 0,-1\}.\end{aligned}$$

设 $g(X)=b^2X^2+y_1X+y_1$. 我们有 $g(0)=y_1$ 且 $g(-1)=b^2\in\square_q$. 令 $\eta$ 是等式(3.4)所给出的二次特征. $g(X)$ 的判别式非 0, 即, $y_1^2-4b^2y_1\neq 0$. 否则, 我们有 $y_1=4b^2$ 且 $d'=y_1(y_1-4)=4b^2(4(b^2-1))=16b^2a^2\in\square_q$, 矛盾. 因此我们可根据判别式 $y_1^2-4b^2y_1$ 是非零平方元或非平方元来判定 $g(X)=0$ 在 $\mathbb{F}_q$ 中有两个解或 0 个解. 换言之, $g(X)=0$ 在 $\mathbb{F}_q$ 中的解得个数等于 $\eta(y_1(4b^2-y_1))+1$. 从而我们有

$$\begin{aligned}|\ell\cap\mathcal{T}| &= \frac{1}{2}\sum_{t\in\mathbb{F}_q, b^2t^2+y_1t+y_1\neq 0}\big(\eta(b^2t^2+y_1t+y_1)+1\big)-[[y_1\in\square_q]]-1\\ &= \frac{1}{2}\sum_{t\in\mathbb{F}_q}\big(\eta(b^2t^2+y_1t+y_1)+1\big)-\frac{1}{2}|\{t\in\mathbb{F}_q|\, b^2t^2+y_1t+y_1=0\}|\\ &\quad -[[y_1\in\square_q]]-1\\ &= \frac{q-2}{2}+\frac{1}{2}\sum_{t\in\mathbb{F}_q}\eta(b^2t^2+y_1t+y_1)-\frac{1}{2}|\{t\in\mathbb{F}_q|\, b^2t^2+y_1t+y_1=0\}|\\ &\quad -[[y_1\in\square_q]]\\ &= \frac{q-2}{2}+\frac{1}{2}(-\eta(b^2))-\frac{1}{2}|\{t\in\mathbb{F}_q|\, b^2t^2+y_1t+y_1=0\}|-[[y_1\in\square_q]]\\ &= \frac{q-3}{2}-\frac{1}{2}\big(\eta(y_1(4b^2-y_1))+1\big)-[[y_1\in\square_q]].\end{aligned}$$

由 $y_1^2-4b^2y_1\neq 0$ 和引理 3.5可得上式中第四个等式成立.

情况 **3.5.** $|\ell\cap O(1,-b^2,a,1)|=\frac{1}{2}\left(\eta(y_1(4b^2-y_1))+1\right)$.

回忆一下 $y_1\neq 4b^2$. 在 $\eta(y_1(4b^2-y_1))=-1$, 即, $y_1(4b^2-y_1)\in\blacksquare_q$ 的情形下, 我们往证 $|\ell\cap O(1,-b^2,a,1)|=0$. 回忆一下 $O(1,-b^2,a,1)$ 中的元素已在等式(3.8)中列出. 假设 $\ell$ 上的点 $(t+1,y_1,(\beta+t)\omega^{\frac{q-1}{2}},t)$ 落在 $O(1,-b^2,a,1)$ 中, 则存在 $\lambda\in\mathbb{F}_q^*, \mu\in\mathbb{F}_{q^2}^*$ 满足 $\mu^{\frac{q+1}{2}}=1$ 使得

$$(t+1,y_1,(\beta+t)\omega^{\frac{q-1}{2}},t)=c(\lambda,-b^2\lambda^{-1},a\lambda^{\frac{q-1}{2}}\mu,1)$$

对某个 $c\in\mathbb{F}_q^*$ 成立. 通过比较坐标, 我们有

$$c=t,\ t+1=c\lambda,\ y_1=-cb^2\lambda^{-1},\ (\beta+t)\omega^{\frac{q-1}{2}}=ca\lambda^{\frac{q-1}{2}}\mu.$$

特别地, 由于 $c \neq 0$ 且 $\lambda \neq 0$, 我们有 $t \neq 0, -1$. 从而 $\lambda = 1 + t^{-1}$. 将该式代入上面第三个等式中可得

$$y_1\lambda + cb^2 = y_1(1 + t^{-1}) + tb^2 = 0,$$

即,

$$b^2t^2 + y_1t + y_1 = 0.$$

这意味着 $b^2X^2 + y_1X + y_1 = 0$ 在 $\mathbb{F}_q$ 中有一个解. 然而, 由假设条件知 $b^2X^2 + y_1X + y_1 = 0$ 的判别式 $-y_1(4b^2 - y_1) \in \blacksquare_q$, 故其在 $\mathbb{F}_q$ 上无解, 矛盾.

接下来, 我们考虑 $\eta(y_1(4b^2-y_1)) = 1$, 即, $y_1(4b^2-y_1) \in \square_q$ 的情形. 在该情形下, 我们往证 $|\ell \cap O(1, -b^2, a, 1)| = 1$. 假设 $\ell$ 上的点 $(t + 1, y_1, (\beta + t)\omega^{\frac{q-1}{2}}, t)$ 落在 $O(1, -b^2, a, 1)$ 中. 用上述同样的推导方法, 我们有 $t \neq 0, -1$ 并且存在 $\lambda \in \mathbb{F}_q^*$, $\mu \in \mathbb{F}_{q^2}^*$ 满足 $\mu^{\frac{q+1}{2}} = 1$ 使得

$$\lambda = t^{-1} + 1,\ b^2t^2 + y_1t + y_1 = 0,$$

并且

$$\mu = (\beta + t)\omega^{\frac{q-1}{2}}(at(t^{-1} + 1)^{\frac{q-1}{2}})^{-1}.$$

在这种情形下, $b^2X^2 + y_1X + y_1 = 0$ 在 $\mathbb{F}_q$ 中有 $t_1, t_2$ 两个不同的解, 它们满足

$$\begin{cases} t_1 + t_2 = -y_1b^{-2}, \\ t_1t_2 = y_1b^{-2}. \end{cases} \tag{3.14}$$

我们根据等式(3.14)推得

$$t_1^{-1} + t_2^{-1} = \frac{t_1 + t_2}{t_1t_2} = -1$$

且

$$(t_1^{-1} + 1)(t_2^{-1} + 1) = (t_1t_2)^{-1} + (t_1^{-1} + t_2^{-1}) + 1 = b^2y_1^{-1}. \tag{3.15}$$

令 $\lambda_i$, $\mu_i$ 是 $t = t_i$, $i = 1, 2$ 时 $\lambda$ 和 $\mu$ 所对应的取值. 我们现在证明恰好有一个 $\mu_i$ 满足 $\mu_i^{\frac{q+1}{2}} = 1$, 这样一来则结论成立. 我们计算

$$\begin{aligned} \mu_i^{q+1} &= \omega^{\frac{q^2-1}{2}}(\beta^q + t_i)(\beta + t_i)(a^2t_i^2)^{-1}(t_i^{-1} + 1)^{-(q-1)} \\ &= -(\beta^{q+1} + (\beta^q + \beta)t_i + t_i^2)(a^2t_i^2)^{-1} \\ &= -(y_1 + t_iy_1 + t_i^2)(a^2t_i^2)^{-1} \\ &= -(-(b^2 - 1)t_i^2)(a^2t_i^2)^{-1} = 1. \end{aligned}$$

对于 $i=1,2$ 成立. 这里我们利用了等式(3.1), (3.9),(3.10)以及 $a,\ t_i\in\mathbb{F}_q$, $b^2t_i^2+y_1t_i+y_1=0$ 对于 $i=1,2$ 成立的事实. 因此, 我们有 $\mu_i^{\frac{q+1}{2}}\in\{1,-1\}$ 对于 $i\in\{1,2\}$ 成立.

我们接下来计算

$$\begin{aligned}
\mu_1^{\frac{q+1}{2}}\mu_2^{\frac{q+1}{2}} &= \left(\frac{(\beta+t_1)\omega^{\frac{q-1}{2}}}{at_1(t_1^{-1}+1)^{\frac{q-1}{2}}}\cdot\frac{(\beta+t_2)\omega^{\frac{q-1}{2}}}{at_2(t_2^{-1}+1)^{\frac{q-1}{2}}}\right)^{\frac{q+1}{2}}\\
&= \omega^{\frac{q^2-1}{2}}((t_1^{-1}+1)(t_2^{-1}+1))^{-\frac{q-1}{2}}\left(\frac{\beta^2+(t_1+t_2)\beta+t_1t_2}{a^2t_1t_2}\right)^{\frac{q+1}{2}}\\
&= -y_1^{\frac{q-1}{2}}\left[(\beta^2-y_1b^{-2}(\beta-1))\left(a^2y_1b^{-2}\right)^{-1}\right]^{\frac{q+1}{2}}\\
&= -y_1^{\frac{q-1}{2}}\left[(\beta^2-y_1b^{-2}\beta^{-(q-1)})(a^2y_1b^{-2})^{-1}\right]^{\frac{q+1}{2}}\\
&= -y_1^{\frac{q-1}{2}}\left((b^2-1)\beta^2(a^2y_1)^{-1}\right)^{\frac{q+1}{2}}\\
&= -y_1^{\frac{q-1}{2}}\cdot y_1\cdot y_1^{-\frac{q+1}{2}}=-1.
\end{aligned}$$

在这里我们利用了等式(3.1), (3.9), (3.12), (3.14)和(3.15).

因此, 对于 $i\in\{1,2\}$, 恰好只有一个 $\mu_i$ 使得 $\mu_i^{\frac{q+1}{2}}=1$.

总之, 我们推得 $|\ell\cap\mathcal{M}|=\frac{q-1}{2}$, 从而完成了情况 3 的证明.

情况 **4.** $Q(4,q)$ 的线 $\ell$ 经过点 $P=(1,0,\omega^{\frac{3(q-1)}{2}},1)$.

我们只需要考虑 $\ell$ 经过一个点 $Q$, 这里 $Q=(1,-\alpha_1^{q+1},\alpha_1,0)$ 对某个 $\alpha_1\in\mathbb{F}_{q^2}^*$ 成立的情形即可. 由 $P\perp Q$, 我们有 $-\alpha_1^{q+1}+\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha_1\omega^{\frac{3(q^2-q)}{2}})=0$. 在这种情况下, 我们令

$$y_1=-\alpha_1^{q+1},\quad \beta=\alpha_1\omega^{-\frac{3(q-1)}{2}}.$$

与等式(3.9)和(3.10)的情形类似, 我们也可推得

$$\beta^{q+1}=y_1,\quad y_1=\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta).$$

特别地, 对于这里的 $\beta\in\mathbb{F}_{q^2}^*$, 我们同样有 $\beta^{q+1}=\beta+\beta^q$, (即, $\beta^q=\beta^{q-1}+1$) 并且 $\beta-1=\beta^{-(q-1)}$ 也成立. 因此, 与情况 3 类似, 我们同样可证得 $\beta\in\mathbb{F}_q$ 当且仅当 $\beta=2$, 并定义

$$\ell=\{(t+1,y_1,(\beta+t)\omega^{\frac{3(q-1)}{2}},t)|t\in\mathbb{F}_q\}\cup\{(1,0,\omega^{\frac{3(q-1)}{2}},1)\}$$

满足 $y_1\neq 4$ (即, $\beta\neq 2$) 和 $\beta=\alpha_1\omega^{-\frac{3(q-1)}{2}}$.

与情况 3 主要的不同点在于在这种情况下, $P=(1,0,\omega^{\frac{3(q-1)}{2}},1)\notin\mathcal{M}$. 然而, 可直接验证 $\ell\cap O(1,0,\omega^{\frac{q-1}{2}},1)=(0,y_1,(\beta-1)\omega^{\frac{3(q-1)}{2}},-1)$, 大小为 1. 通过与情况 3 相同的推导方式, 我们可以得到

$$|\ell\cap O(1,-1,0,1)|=0,$$

$$|\ell\cap O(1,-\omega^{2(q+1)},\omega^2,0)|=[[y_1\in\square_q]],$$

$$|\ell\cap\mathcal{T}|=\frac{q-3}{2}-\frac{1}{2}(\eta(y_1(4b^2-y_1))+1)-[[y_1\in\square_q]],$$

以及

$$|\ell\cap O(1,-b^2,a,1)|=\frac{1}{2}\left(\eta(y_1(4b^2-y_1))+1\right).$$

从而有 $|\ell\cap\mathcal{M}|=\frac{q-1}{2}$. 计算过程与情况 3 几乎相同, 于是我们省略这些细节.

综上所述, 每条 $Q(4,q)$ 的线交点集 $\mathcal{M}$ 于 $\frac{q-1}{2}$ 个点. 因此, $\mathcal{M}$ 是 $Q(4,q)$ 的一个 $\frac{q-1}{2}$-ovoid. 证毕. □

**注 3.8：** 这里 $q>5$ 的条件是必须的. 首先, 在 $\mathbb{F}_5$ 中不存在元素 $a,b$ 使得 $1+a^2=b^2$ 成立, 因此不能定义 $O(1,-b^2,a,1)$ 和 $\mathcal{T}$. 其次, 我们通过计算机验证集合 $O(1,-1,0,1)\cup O(1,-\omega^{2(q+1)},\omega^2,0)\cup O(1,0,\omega^{\frac{q-1}{2}},1)$ 不能构成 $Q(4,5)$ 的一个 $G$-不变的 2-ovoid.

**注 3.9：** 我们定义 $Q(4,q)$ 上的一个二阶等距变换如下:

$$\sigma:(x,y,\alpha,z)\to(y,x,\alpha,z).$$

直接验证可知 $\sigma$ 固定我们的 $\frac{q-1}{2}$-ovoid $\mathcal{M}$, 并且 $\langle\sigma\rangle$ 正规化 $G$. 对于 $q=9,13,17$, 我们通过 Magma[13] 验证了群 $\langle G,\sigma\rangle$, 同构于 $C_{\frac{q^2-1}{2}}\rtimes(C_2\times C_2)$, 是 $\mathcal{M}$ 在 $\mathrm{PGO}(5,q)$ 中的全稳定子群.

## 3.2 $Q^+(7,q)$ 中自同构群为 $\mathbf{PGU}_3(q)$ 的 $m$-ovoids

在本小节, 我们给出 $Q^+(7,q)$ 中自同构群为 $\mathrm{PGU}_3(q)$ 的 $m$-ovoids, 该构造是基于文献[43] 的第 4 节 Kantor 给出的 $Q^+(7,q)$ 中的 unitary ovoid 的构造得到的. 具体而言, 令 $q$ 是一个素数 $p$ 的幂使得 $q\equiv 2(\mathrm{mod}\,3)$ 且 $q>2$. 对于 $\alpha\in\mathbb{F}_{q^2}$, 设 $\overline{\alpha}=\alpha^q$, $\mathrm{Tr}(\alpha)=\alpha+\overline{\alpha}$ 和 $\mathrm{Norm}(\alpha)=\alpha\overline{\alpha}$. 有限域 $\mathbb{F}_q$ 上的 8 维向量空间 $V$ 可由下列矩阵形式构成:

$$M=\begin{pmatrix}\alpha&\beta&c\\ \gamma&a&\overline{\beta}\\ b&\overline{\gamma}&\overline{\alpha}\end{pmatrix},\tag{3.16}$$

这里 $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}, a, b, c \in \mathbb{F}_q$ 且 $a + \mathrm{Tr}(\alpha) = 0$. 定义 $V$ 上的一个二次型

$$Q(M) = \alpha^2 + \alpha\overline{\alpha} + \overline{\alpha}^2 + \mathrm{Tr}(\beta\gamma) + bc \tag{3.17}$$

其对应的双线性型为

$$B(M, N) = Q(M + N) - Q(M) - Q(N) = \mathrm{tr}(MN), \tag{3.18}$$

这里 $\mathrm{tr}(MN)$ 表示矩阵 $MN$ 的迹. 相应的二次曲面的点集为

$$\mathcal{Q} = \{\langle M\rangle_{\mathbb{F}_q} : M \in V, Q(M) = 0\},$$

这里 $\langle M\rangle_{\mathbb{F}_q}$ 表示 $V$ 中元素 $M$ 的 $\mathbb{F}_q$ 射影点. 简单起见, 在本节中我们将 $\langle M\rangle_{\mathbb{F}_q}$ 简记为 $\langle M\rangle$. 设 $J = \mathrm{antidiag}(1, 1, 1)$, 这里 antidiag 表示反对角矩阵. 令

$$G_0 = \{A : A \in \mathrm{GL}_3(q^2) | J^{-1}AJ = (\overline{A}^T)^{-1}\},$$

这里 $\overline{A}^T$ 表示矩阵 $A$ 的共轭转置. 我们有 $G_0 \cong \mathrm{GU}_3(q)$, 群 $G_0$ 通过共轭作用来作用在空间 $V$ 上, 这样可以诱导群 $\mathrm{PGU}_3(q)$ 在 $V$ 所对应的射影空间上的一个作用. 此外, 由文献[43] 的第 4 节可知, 群 $G_0$ 保持等式(3.17)定义的二次型 $Q$ 不变.

令 $\omega \in \mathbb{F}_{q^2}$ 使得 $\omega^3 = 1$ 且 $\omega \neq 1$. 由于 $q \equiv 2(\mathrm{mod}\ 3)$ 且 $q > 2$, 则

$$\omega^q + \omega + 1 = \omega^2 + \omega + 1 = 0.$$

取三个 $\mathcal{Q}$ 中的点:

$$X_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, X_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \text{ 和 } X_3 = \begin{pmatrix} \omega & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \overline{\omega} \end{pmatrix}.$$

由文献[43] 中第 4 节的论断可知, 对于 $q \equiv 2(\mathrm{mod}\ 3)$ 且 $q > 2$ 的情形, 群 $G_0$ 在 $\mathcal{Q}$ 上恰有 3 个轨道, 其中轨道代表元分别为 $\langle X_1\rangle, \langle X_2\rangle$ 和 $\langle X_3\rangle$. 事实上, 对于 $i = 1, 2, 3$, 轨道 $O_i = O(\langle X_i\rangle)$ 恰好是由 $\mathcal{Q}$ 中秩为 $i$ 的矩阵构成. 其中轨道 $O_1$ 即为 $Q^+(7, q)$ 的 unitary ovoid, 也称为 Kantor ovoid. 在当时, Kantor 只对 unitary ovoid (即, 轨道 $O_1$) 进行了研究, 在本小节我们将用综合运用特征和等代数方法对剩余两个轨道 $O_2$ 和 $O_3$ 进行研究. 我们证明了, $O_2$ 和 $O_3$ 分别为 $Q^+(7, q)$ 的一个 $(q^2 + q)$-ovoid 和 $q^3$-ovoid.

**定理 3.10：** 采用上述符号, 我们有 $|O_2| = (q^2 + q)(q^3 + 1)$ 且 $|O_3| = q^3(q^3 + 1)$, 这里 $|O_2|$ 和 $|O_3|$ 分别表示轨道 $O_2$ 和 $O_3$ 的长度.

证明. 令

$$M = \begin{pmatrix} \alpha & \beta & c \\ \gamma & a & \overline{\beta} \\ b & \overline{\gamma} & \overline{\alpha} \end{pmatrix}$$

由等式(3.16)所定义. 如果 $\langle M\rangle$ 属于 $O_2$, 由于 $O_2$ 恰好是 $\mathcal{Q}$ 中秩为 2 的所有矩阵, 那么 $M$ 在以下三种情况之一中. 对于 $j=1,2,3$, 令 $N_j$ 表示属于情况 $j$ 的 $O_2$ 中的点 $\langle M\rangle$ 的个数.

情况 **1.** 矩阵 $M$ 的其中一行是 $(0,0,0)$, 剩余两行线性无关.

在该种情况下, 我们有第二行 $(\gamma,a,\overline{\beta})\neq(0,0,0)$. 否则, 由 $M$ 的定义可知 $\overline{\alpha}=-\alpha$, 再由 $Q(M)=0$ 经过直接计算可得

$$\alpha^2+bc=0.$$

从而 $M$ 的第一行与第三行线性相关, 即 $\langle M\rangle\in O_1$, 这与 $\langle M\rangle\in O_2$ 矛盾. 因此, 我们有或者 $M=\begin{pmatrix}0&0&0\\ \gamma&0&0\\ b&\overline{\gamma}&0\end{pmatrix}$ 使得 $\gamma\in\mathbb{F}_{q^2}^*$, $b\in\mathbb{F}_q$; 或者 $M=\begin{pmatrix}0&\beta&c\\ 0&0&\overline{\beta}\\ 0&0&0\end{pmatrix}$ 使得 $\beta\in\mathbb{F}_{q^2}^*$, $c\in\mathbb{F}_q$. 由于 $O_2$ 中的点均为射影点, 再结合 $N_1$ 的定义, 我们有

$$\begin{aligned}N_1&=2\frac{1}{q-1}(q^2-1)q\\ &=2q(q+1).\end{aligned}\tag{3.19}$$

情况 **2.** 矩阵 $M$ 中没有行 $(0,0,0)$ 但 $M$ 中存在两行线性相关.

在该种情况下, 假设存在 $\lambda\in\mathbb{F}_{q^2}^*$ 使得

$$(\alpha,\beta,c)=\lambda(\gamma,a,\overline{\beta}),$$

则

$$\alpha=\lambda\gamma,\ a=-(\lambda\gamma+\overline{\lambda\gamma}),$$

$$\beta=-\lambda(\lambda\gamma+\overline{\lambda\gamma}),\ c=-\lambda^{q+1}(\lambda\gamma+\overline{\lambda\gamma}).$$

由 $Q(M)=0$ 可以得到

$$-b(\lambda\gamma+\overline{\lambda\gamma})=\gamma^{q+1},$$

再由 $\overline{\alpha}a=\overline{\beta}\overline{\gamma}$ 可知, $M$ 的第二行和第三行线性相关, 则 $M\in O_1$, 与 $\langle M\rangle\in O_2$ 矛盾. 因此, $M$ 的第一行和第二行线性无关. 用同样的方法可以得出 $M$ 的第二行和第三行线性无关. 则唯一可能的情况只有 $(\alpha,\beta,c)=\lambda(b,\overline{\gamma},\overline{\alpha})$ 对于某个 $\lambda\in\mathbb{F}_{q^2}^*$ 成立. 则我们有

$$M=\begin{pmatrix}\lambda b&\lambda\overline{\gamma}&\lambda^{q+1}b\\ \gamma&-(\lambda+\overline{\lambda})b&\overline{\lambda}\gamma\\ b&\overline{\gamma}&\overline{\lambda}b\end{pmatrix},\tag{3.20}$$

其中 $b, \gamma, \lambda$ 要满足

$$-\gamma^{q+1} \neq b^2(\lambda + \overline{\lambda}). \tag{3.21}$$

从而

$$Q(M) = (\lambda + \overline{\lambda})^2 b^2 + (\lambda + \overline{\lambda})\gamma^{q+1} = 0. \tag{3.22}$$

结合等式(3.21)和等式(3.22)可知, 在该种情形下, $\langle M \rangle \in O_2$ 当且仅当 $M$ 如等式(3.20)所示, 其中 $\lambda + \overline{\lambda} = 0$ 且 $\lambda, \gamma \in \mathbb{F}_{q^2}^*$. 由 $N_2$ 的定义, 我们有

$$\begin{aligned} N_2 &= \frac{1}{q-1}\#\{(\lambda, \gamma, b) : \lambda, \gamma \in \mathbb{F}_{q^2}^*, b \in \mathbb{F}_q | \lambda + \overline{\lambda} = 0\} \\ &= \frac{1}{q-1}(q-1)q(q^2-1) = q(q^2-1). \end{aligned} \tag{3.23}$$

情况 **3.** 矩阵 $M$ 的任意两行线性无关, 且其中一行是另外两行的线性组合.

在该种情况下, 则存在 $\lambda_1, \lambda_2 \in \mathbb{F}_{q^2}^*$ 使得

$$(\alpha, \beta, c) = \lambda_1(\gamma, a, \overline{\beta}) + \lambda_2(b, \overline{\gamma}, \overline{\alpha}),$$

其中 $(\gamma, a, \overline{\beta})$ 和 $(b, \overline{\gamma}, \overline{\alpha})$ 线性无关. 此时有

$$\alpha = \lambda_1\gamma + \lambda_2 b,\ a = -(\alpha + \overline{\alpha}),$$

$$\beta = \lambda_1 a + \lambda_2\overline{\gamma}.$$

从而有

$$\overline{\alpha}\gamma = \overline{\lambda_1}\gamma^{q+1} + \overline{\lambda_2}b\gamma,$$

且

$$\overline{\beta}b = \overline{\lambda_1}ab + \overline{\lambda_2}b\gamma.$$

因此, $(\gamma, a, \overline{\beta})$ 和 $(b, \overline{\gamma}, \overline{\alpha})$ 线性无关等价于 $\gamma^{q+1} \neq ab$, 这里 $a = -(\lambda_1\gamma + \overline{\lambda_1\gamma} + \lambda_2 b + \overline{\lambda_2}b)$.

经计算可得

$$Q(M) = (\lambda_1^{q+1} - (\lambda_2 + \overline{\lambda_2}))(ab - \gamma^{q+1}) = 0.$$

从而, 矩阵 $\langle M \rangle \in O_2$ 等价于 $\lambda_2 + \overline{\lambda_2} = \lambda_1^{q+1}$ 且 $\gamma^{q+1} \neq ab$, 这里 $a = -(\lambda_1\gamma + \overline{\lambda_1\gamma} + \lambda_1^{q+1}b)$.

由 $N_3$ 的定义, 我们有

$$\begin{aligned} N_3 &= \frac{1}{q-1}\#\{(\lambda_1,\lambda_2,\gamma,b)\colon \lambda_1,\lambda_2\in\mathbb{F}_{q^2}^*,\gamma\in\mathbb{F}_{q^2},\, b\in\mathbb{F}_q| \\ &\qquad \lambda_2+\overline{\lambda_2}=\lambda_1^{q+1},\, b(\lambda_1\gamma+\overline{\lambda_1\gamma}+\lambda_1^{q+1}b)+\gamma^{q+1}\neq 0\} \\ &= \frac{q}{q-1}\#\{(\lambda_1,\gamma,b)\colon \lambda_1\in\mathbb{F}_{q^2}^*,\gamma\in\mathbb{F}_{q^2},\, b\in\mathbb{F}_q|b(\lambda_1\gamma+\overline{\lambda_1\gamma}+\lambda_1^{q+1}b)+\gamma^{q+1}\neq 0\} \\ &= \frac{q(q^2-1)\cdot q^3}{q-1}-\frac{q}{q-1}K, \end{aligned} \tag{3.24}$$

这里 $K=\#\{(\lambda_1,\gamma,b)\colon \lambda_1\in\mathbb{F}_{q^2}^*,\gamma\in\mathbb{F}_{q^2},\, b\in\mathbb{F}_q|b(\lambda_1\gamma+\overline{\lambda_1\gamma}+\lambda_1^{q+1}b)+\gamma^{q+1}=0\}$.

接下来, 我们将会使用特征和计算 $K$. 由于这里要求 $q\equiv 2(\mathrm{mod}\,3)$, 则我们分为特征 $p$ 为奇数和偶数两种情况进行计算.

情况 **3.1.** 特征 $p$ 是奇数. 我们在 $\mathbb{F}_{q^2}$ 中取 $\mathbb{F}_q$ 上的一组基 $1,\delta$ 使得 $\delta^q+\delta=0$, 这里 $\delta\in\mathbb{F}_{q^2}^*$; 我们令 $\lambda_1=x_1+x_2\delta$ 和 $\gamma=r_1+r_2\delta$. 显然 $\delta^2$ 是 $\mathbb{F}_q$ 的一个非平方元. 我们有

$$K=\#\{(x_1,x_2,r_1,r_2,b)\in\mathbb{F}_q^5\colon \{x_1,\,x_2\}\neq\{0\},\, F(x_1,x_2,r_1,r_2,b)=0\},$$

这里

$$F(x_1,x_2,r_1,r_2,b)=(x_1^2-x_2^2\delta^2)b^2+(2x_1r_1+2\delta^2x_2r_2)b+(r_1^2-r_2^2\delta^2). \tag{3.25}$$

这里我们再细分为以下两种情况来计算 $K$ 的值.

情况 **3.1.1.** $x_2=0$; 这时, 令

$$K_1=\#\{(x_1,r_1,r_2,b)\in\mathbb{F}_q^4\colon x_1\neq 0, r_1^2+2bx_1r_1+b^2x_1^2-r_2^2\delta^2=0\}.$$

仍令 $\psi$ 是 $\mathbb{F}_q$ 的标准加法特征. 则我们有

$$\begin{aligned} K_1 &= \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{x_1\in\mathbb{F}_q^*}\sum_{r_1,r_2,b\in\mathbb{F}_q}\psi(\lambda(r_1^2+2bx_1r_1+b^2x_1^2-r_2^2\delta^2)) \\ &= \frac{(q-1)q^3}{q}+\frac{1}{q}\sum_{\lambda,\,x_1\in\mathbb{F}_q^*}\sum_{b\in\mathbb{F}_q}\psi(\lambda b^2x_1^2)\sum_{r_2\in\mathbb{F}_q}\psi(-\lambda\delta^2r_2^2)\sum_{r_1\in\mathbb{F}_q}\psi(\lambda r_1^2+2\lambda bx_1r_1) \end{aligned}$$

由文献[51] 的定理 5.33 可得,

$$\sum_{r_1\in\mathbb{F}_q}\psi(\lambda r_1^2+2\lambda bx_1r_1)=\psi(-\lambda x_1^2b^2)G(\eta,\psi)\eta(\lambda), \tag{3.26}$$

这里 $\eta$ 表示 $\mathbb{F}_q$ 的二次乘法特征; $G(\eta,\psi)$ 是 $\mathbb{F}_q$ 上的 Gauss 和, 可参考[51] 的第 5 章. 同样地, 再次利用文献[51] 的定理 5.33, 我们有

$$\sum_{r_2\in\mathbb{F}_q}\psi(-\lambda\delta^2r_2^2)=G(\eta,\psi)\eta(-\lambda\delta^2).$$

由于 $\overline{\eta}=\eta$ 且 $G(\eta,\psi)G(\overline{\eta},\psi)=\eta(-1)q$, 则有

$$G(\eta,\psi)^2=\eta(-1)q.$$

由于 $\delta^2$ 是 $\mathbb{F}_q$ 中的非平方元, 则有 $\eta(\delta^2)=-1$. 因此, 我们有

$$\begin{aligned}K_1&=q^2(q-1)+\frac{1}{q}\sum_{\lambda,\,x_1\in\mathbb{F}_q^*}\sum_{b\in\mathbb{F}_q}\psi(\lambda b^2x_1^2)G(\eta,\psi)^2\eta(-\lambda^2\delta^2)\psi(-\lambda b^2x_1^2)\\&=q^2(q-1)+(q-1)^2\eta(\delta^2)\sum_{b\in\mathbb{F}_q}\psi(0)\\&=q(q-1).\end{aligned}\tag{3.27}$$

情况 **3.1.2.** $x_2\neq 0$; 这时, 令

$$K_2=\#\{(x_1,x_2,r_1,r_2,b)\in\mathbb{F}_q^5:\,x_2\neq 0,\,F(x_1,x_2,r_1,r_2,b)=0\},$$

这里 $F(x_1,x_2,r_1,r_2,b)$ 由等式(3.25)给出. 通过指数和计算, 我们有

$$\begin{aligned}K_2&=\frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{x_2\in\mathbb{F}_q^*}\sum_{x_1,r_1,r_2,b\in\mathbb{F}_q}\psi\left(\lambda F(x_1,x_2,r_1,r_2,b)\right)\\&=\frac{(q-1)q^4}{q}+\frac{1}{q}\sum_{\lambda,\,x_2\in\mathbb{F}_q^*}\sum_{x_1,\,b\in\mathbb{F}_q}\psi(\lambda(x_1^2-\delta^2x_2^2)b^2)Z(x_1,x_2,b),\end{aligned}$$

这里

$$Z(x_1,x_2,b)=\sum_{r_1\in\mathbb{F}_q}\psi(\lambda r_1^2+2\lambda x_1br_1)\sum_{r_2\in\mathbb{F}_q}\psi(\lambda(-\delta^2r_2^2+2\delta^2x_2br_2)).$$

同上, 我们有

$$\sum_{r_2\in\mathbb{F}_q}\psi(\lambda(-\delta^2r_2^2+2\delta^2x_2br_2))=\psi(\lambda\delta^2x_2^2b^2)G(\eta,\psi)\eta(-\lambda\delta^2),$$

再结合等式(3.26), 我们得到

$$\begin{aligned}K_2&=q^3(q-1)+\frac{1}{q}\sum_{\lambda,x_2\in\mathbb{F}_q^*}\sum_{x_1\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_q}\psi(0)G(\eta,\psi)^2\eta(-\delta^2)\\&=q^3(q-1)-q^2(q-1)^2\\&=q^2(q-1).\end{aligned}\tag{3.28}$$

由等式(3.27)和(3.28)可知, 在特征为奇数的情形下,

$$K=K_1+K_2=q^3-q.\tag{3.29}$$

情况 **3.2.** 特征 $p$ 是偶数. 在该种情况下, 我们在 $\mathbb{F}_{q^2}$ 中取 $\mathbb{F}_q$ 上的一组基 $1, \delta$ 使得 $\delta^q + \delta = 1$; 我们令 $\lambda_1 = x_1 + x_2\delta$ 和 $\gamma = r_1 + r_2\delta$. 我们有

$$K = \#\{(x_1, x_2, r_1, r_2, b) \in \mathbb{F}_q^5 : \{x_1, x_2\} \neq \{0\}, F(x_1, x_2, r_1, r_2, b) = 0\},$$

这里

$$\begin{aligned} F(x_1, x_2, r_1, r_2, b) = \ & (x_1^2 + x_1x_2 + x_2^2\delta^{q+1})b^2 + (x_1r_2 + x_2r_1 + x_2r_2)b + \\ & (r_1^2 + r_1r_2 + r_2^2\delta^{q+1}). \end{aligned} \tag{3.30}$$

这里我们再细分为以下两种情况来计算 $K$ 的值.

情况 **3.2.1.** $x_2 = 0$; 这时, 令

$$K_1 = \#\{(x_1, r_1, r_2, b) \in \mathbb{F}_q^4 : x_1 \neq 0, x_1^2b^2 + bx_1r_2 + r_1^2 + r_1r_2 + r_2^2\delta^{q+1} = 0\},$$

同样地, 令 $\psi$ 是 $\mathbb{F}_q$ 的标准加法特征. 则我们有

$$\begin{aligned} K_1 &= \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{x_1\in\mathbb{F}_q^*}\sum_{r_1,r_2,b\in\mathbb{F}_q}\psi(\lambda(x_1^2b^2 + bx_1r_2 + r_1^2 + r_1r_2 + r_2^2\delta^{q+1})) \\ &= \frac{(q-1)q^3}{q} + \frac{1}{q}\sum_{\lambda,\, x_1\in\mathbb{F}_q^*}\sum_{r_1,\, r_2\in\mathbb{F}_q}\psi\left(\lambda(r_1^2 + r_1r_2 + r_2^2\delta^{q+1})\right)\sum_{b\in\mathbb{F}_q}\psi\left(\lambda(b^2x_1^2 + bx_1r_2)\right) \\ &= q^2(q-1) + \sum_{\lambda,\, x_1\in\mathbb{F}_q^*}\sum_{r_1,\, r_2\in\mathbb{F}_q}\psi\left(\lambda(r_1^2 + r_1r_2 + r_2^2\delta^{q+1})\right)[[r_2 = \sqrt{\lambda}^{-1}]] \end{aligned}$$

由于 $\psi(\delta^{q+1}) = \psi(\delta^2 + \delta) = -1$, 则有

$$\begin{aligned} K_1 &= q^2(q-1) + \sum_{\lambda,\, x_1\in\mathbb{F}_q^*}\sum_{r_1\in\mathbb{F}_q}\psi\left(\lambda r_1^2\right)\psi\left(\sqrt{\lambda}r_1\right)\psi(\delta^{q+1}) \\ &= q^2(q-1) - q(q-1)^2 \\ &= q(q-1) \end{aligned} \tag{3.31}$$

情况 **3.2.2.** $x_2 \neq 0$; 这时, 令

$$K_2 = \#\{(x_1, x_2, r_1, r_2, b) \in \mathbb{F}_q^5 : x_2 \neq 0, F(x_1, x_2, r_1, r_2, b) = 0\},$$

这里 $F(x_1, x_2, r_1, r_2, b)$ 由等式(3.30)给出. 通过指数和计算, 我们有

$$\begin{aligned} K_2 &= \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{x_2\in\mathbb{F}_q^*}\sum_{x_1,r_1,r_2,b\in\mathbb{F}_q}\psi\left(\lambda F(x_1, x_2, r_1, r_2, b)\right) \\ &= \frac{(q-1)q^4}{q} + \frac{1}{q}\sum_{\lambda,\, x_2\in\mathbb{F}_q^*}\sum_{x_1,\, b\in\mathbb{F}_q}\psi\left(\lambda(x_1^2 + x_1x_2 + \delta^{q+1}x_2^2)b^2\right)Z(x_1, x_2, b), \end{aligned}$$

这里

$$Z(x_1,x_2,b)=\sum_{r_2\in\mathbb{F}_q}\psi\left(\lambda(\delta^{q+1}r_2^2+b(x_1+x_2)r_2)\right)\sum_{r_1\in\mathbb{F}_q}\psi\left(\lambda r_1^2+\lambda(r_2+x_2b)r_1\right).$$

我们有

$$\sum_{r_1\in\mathbb{F}_q}\psi\left(\lambda r_1^2+\lambda(r_2+x_2b)r_1\right)=q[[r_2=\sqrt{\lambda}^{-1}+x_2b]].$$

代入上式, 我们得到

$$\begin{aligned}K_2&=q^3(q-1)+\sum_{\lambda,x_2\in\mathbb{F}_q^*}\sum_{x_1,\,b\in\mathbb{F}_q}\psi(0)\psi(\delta^{q+1})\\&=q^3(q-1)-q^2(q-1)^2\\&=q^2(q-1)\end{aligned}\tag{3.32}$$

由等式(3.31)和等式 (3.32)可知, 在特征为偶数的情形, 我们有同样有

$$K=K_1+K_2=q^3-q.\tag{3.33}$$

综合特征为奇数和偶数的情形, 再由等式(3.24)可得

$$\begin{aligned}N_3&=q^4(q+1)-\frac{q}{q-1}K\\&=q^5+q^4-q^3-q^2.\end{aligned}\tag{3.34}$$

综上, 由等式(3.19), (3.23)和(3.34), 我们算得轨道 $O_2$ 的长度为

$$|O_2|=N_1+N_2+N_3=(q^2+q)(q^3+1).$$

已知轨道 $|O_1|$ 作为 $Q^+(7,q)$ 的 ovoid, 其长度为 $q^3+1$. 由表 2.1可知, 双曲二次曲面 $Q^+(7,q)$ 的点的个数为 $(q^3+q^2+q+1)(q^3+1)$. 从而

$$\begin{aligned}|O_3|&=(q^3+q^2+q+1)(q^3+1)-|O_1|-|O_2|\\&=q^3(q^3+1).\end{aligned}$$

证毕. □

**定理** 3.11：采用上述符号, 我们有轨道 $O_2$ 是 $Q^+(7,q)$ 的一个 $(q^2+q)$-ovoid; 轨道 $O_3$ 是 $Q^+(7,q)$ 的一个 $q^3$-ovoid.

证明. 由等式(3.18)中 $Q^+(7,q)$ 的双线性型 $B$ 的定义, 我们可以看出

$$X_2^{\perp}\cap O_2=\left\{\langle M\rangle\in O_2:\,M=\begin{pmatrix}\alpha&\beta&c\\\gamma&a&\overline{\beta}\\b&-\gamma&\overline{\alpha}\end{pmatrix}\right\}.\tag{3.35}$$

假设 $M=\begin{pmatrix}\alpha & \beta & c\\ \gamma & a & \overline{\beta}\\ b & -\gamma & \overline{\alpha}\end{pmatrix}$ 使得 $\langle M\rangle\in X_2^{\perp}\cap O_2$, 由定理 3.10的证明可以得到, $M$ 必定属于下列三种情况之一. 对于 $j=1,2,3$, 令 $R_j$ 表示属于情况 $j$ 的 $X_2^{\perp}\cap O_2$ 中 $\langle M\rangle$ 的个数.

情况 **1.** 矩阵 $M$ 的其中一行为 $(0,0,0)$, 剩余两行线性无关.

根据定理 3.10对该种情况的说明可知, 这时 $M=\begin{pmatrix}0 & 0 & 0\\ \gamma & 0 & 0\\ b & \overline{\gamma} & 0\end{pmatrix}$ 满足 $\gamma\in\mathbb{F}_{q^2}^*$ 使得 $\overline{\gamma}=-\gamma, b\in\mathbb{F}_q$; 或 $M=\begin{pmatrix}0 & \beta & c\\ 0 & 0 & \overline{\beta}\\ 0 & 0 & 0\end{pmatrix}$ 满足 $\beta\in\mathbb{F}_{q^2}^*, c\in\mathbb{F}_q$. 则我们有

$$\begin{aligned}R_1&=\frac{1}{q-1}\big(q(q-1)+q(q^2-1)\big)\\&=q^2+2q.\end{aligned}\tag{3.36}$$

情况 **2.** 矩阵 $M$ 中没有行 $(0,0,0)$ 但 $M$ 中存在两行线性相关.

同样地, 根据定理 3.10对该种情况的说明, 我们有

$$\begin{aligned}R_2&=\frac{1}{q-1}\#\{(\lambda,\gamma,b):\ \lambda,\gamma\in\mathbb{F}_{q^2}^*,\ b\in\mathbb{F}_q|\lambda+\overline{\lambda}=0,\ \gamma^q=-\gamma\}\\&=\frac{1}{q-1}(q-1)(q-1)q\\&=(q-1)q.\end{aligned}\tag{3.37}$$

情况 **3.** 矩阵 $M$ 的任意两行线性无关, 且其中一行是另外两行的线性组合.

由定理 3.10的证明再加上 $\gamma^q=-\gamma$ 的条件可知, 该情况等价于 $\lambda_2+\overline{\lambda_2}=\lambda_1^{q+1}$ 且 $-\gamma^2\neq ab$, 这里 $a=-(\lambda_1\gamma-\overline{\lambda_1}\gamma+\lambda_1^{q+1}b)$. 则我们有

$$\begin{aligned}R_3=&\frac{1}{q-1}\#\{(\lambda_1,\lambda_2,\gamma,b):\ \lambda_1,\lambda_2\in\mathbb{F}_{q^2}^*,\gamma\in\mathbb{F}_{q^2},\ b\in\mathbb{F}_q|\lambda_2+\overline{\lambda_2}=\lambda_1^{q+1},\\&\qquad b(\lambda_1\gamma-\overline{\lambda_1}\gamma+\lambda_1^{q+1}b)\neq\gamma^2,\ \gamma^q=-\gamma\}\\=&\frac{q}{q-1}\#\{(\lambda_1,\gamma,b):\ \lambda_1\in\mathbb{F}_{q^2}^*,\gamma\in\mathbb{F}_{q^2},\ b\in\mathbb{F}_q|b(\lambda_1\gamma-\overline{\lambda_1}\gamma+\lambda_1^{q+1}b)-\gamma^2\neq 0,\\&\qquad\gamma^q=-\gamma\}\\=&\frac{q(q^2-1)q^2}{q-1}-\frac{q}{q-1}T_0,\end{aligned}\tag{3.38}$$

这里

$$T_0 = \#\{(\lambda_1, \gamma, b) : \lambda_1 \in \mathbb{F}_{q^2}^*, \gamma \in \mathbb{F}_{q^2}, b \in \mathbb{F}_q | b(\lambda_1\gamma - \overline{\lambda_1}\gamma + \lambda_1^{q+1}b) - \gamma^2 = 0, \gamma^q = -\gamma\}.$$

我们采用与定理 3.10相同的步骤和方法来计算 $T_0$ 的值. 同样地, 分为特征 $p$ 为奇数和偶数的情况分别进行计算.

情况 **3.1.** 特征 $p$ 为奇数, 我们取 $\mathbb{F}_{q^2}$ 在 $\mathbb{F}_q$ 上的一组基 $1, \delta$ 使得 $\delta \in \mathbb{F}_{q^2}^*$ 且 $\delta^q + \delta = 0$; 我们设 $\lambda_1 = x_1 + x_2\delta$ 和 $\gamma = r_1\delta$ 其中 $x_1, x_2, r_1 \in \mathbb{F}_q$, 使其满足 $\gamma^q = -\gamma$. 则我们有

$$T_0 = \#\{(x_1, x_2, r_1, b) \in \mathbb{F}_q^4 : \{x_1, x_2\} \neq \{0\}, (x_1^2 - \delta^2 x_2^2)b^2 + 2x_2\delta^2 r_1 b - r_1^2\delta^2 = 0\}.$$

我们进一步细分为以下两种情况来计算 $T_0$ 的值:

情况 **3.1.1.** $x_2 = 0$; 这时, 令

$$T_1 = \#\{(x_1, r_1, b) \in \mathbb{F}_q^3 : x_1 \neq 0, x_1^2 b^2 - r_1^2\delta^2 = 0\}.$$

在 $T_1$ 的表达式中, 由于 $x_1 \neq 0$ 且 $\delta^2$ 是 $\mathbb{F}_q$ 的非平方元. 则由 $x_1^2 b^2 = r_1^2\delta^2$ 可得 $r_1 = 0$, $b = 0, x_1 \in \mathbb{F}_q^*$. 从而

$$T_1 = q - 1.$$

情况 **3.1.2.** $x_2 \neq 0$; 这时, 令

$$T_2 = |\#\{(x_1, x_2, r_1, b) \in \mathbb{F}_q^4 : x_2 \neq 0, (x_1^2 - \delta^2 x_2^2)b^2 + 2x_2\delta^2 r_1 b - r_1^2\delta^2 = 0\}.$$

通过指数和计算, 我们有

$$\begin{aligned}
T_2 &= \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{x_2\in\mathbb{F}_q^*}\sum_{x_1,r_1,b\in\mathbb{F}_q}\psi\left(\lambda\left((x_1^2 - \delta^2x_2^2)b^2 + 2x_2\delta^2 br_1 - r_1^2\delta^2\right)\right)\\
&= \frac{(q-1)q^3}{q} + \frac{1}{q}\sum_{\lambda,\, x_2\in\mathbb{F}_q^*}\sum_{x_1,\, b\in\mathbb{F}_q}\psi\left(\lambda(x_1^2 - \delta^2x_2^2)b^2\right)\sum_{r_1\in\mathbb{F}_q}\psi(-\lambda\delta^2(r_1^2 - 2x_2br_1))\\
&= q^2(q-1) + \frac{1}{q}\sum_{\lambda,\, x_2\in\mathbb{F}_q^*}\sum_{x_1,\, b\in\mathbb{F}_q}\psi\left(\lambda(x_1^2 - \delta^2x_2^2)b^2\right)\psi(\lambda\delta^2x_2^2b^2)G(\eta,\psi)\eta(-\lambda\delta^2)\\
&= q^2(q-1) + \frac{1}{q}\sum_{\lambda,\, x_2\in\mathbb{F}_q^*}G(\eta,\psi)\eta(-\lambda\delta^2)\sum_{x_1,\, b\in\mathbb{F}_q}\psi\left(\lambda x_1^2b^2\right)\\
&= q^2(q-1) + \frac{1}{q}\sum_{\lambda,\, x_2\in\mathbb{F}_q^*}G(\eta,\psi)\eta(-\lambda\delta^2)\left(q + \sum_{x_1\in\mathbb{F}_q^*}G(\eta,\psi)\eta(\lambda x_1^2)\right)\\
&= q^2(q-1) + 0 - \frac{1}{q}\sum_{\lambda,\, x_2,\, x_1\in\mathbb{F}_q^*}G(\eta,\psi)^2\eta(-1).
\end{aligned}$$

从而, 我们有

$$\begin{aligned} T_2 &= q^2(q-1) + 0 - \frac{1}{q}(q(q-1)^3) \\ &= (q-1)(2q-1). \end{aligned}$$

因此, 在特征为奇数的情形下, 我们得到

$$T_0 = T_1 + T_2 = 2q(q-1).$$

情况 **3.2.** 特征 $p$ 为偶数, 我们取 $\mathbb{F}_{q^2}$ 在 $\mathbb{F}_q$ 上的一组基 $1, \delta$ 使得 $\delta \in \mathbb{F}_{q^2}^*$ 且 $\delta^q + \delta = 1$; 我们设 $\lambda_1 = x_1 + x_2\delta$, 其中 $x_1, x_2 \in \mathbb{F}_q$. 在该种情况下, 由于 $\gamma^q = -\gamma = \gamma$, 从而 $\gamma \in \mathbb{F}_q$. 则我们有

$$T_0 = \#\{(x_1, x_2, \gamma, b) \in \mathbb{F}_q^4 : \{x_1, x_2\} \neq \{0\}, (x_1^2 + x_1x_2 + x_2^2\delta^{q+1})b^2 + x_2\gamma b + \gamma^2 = 0\}.$$

我们进一步细分为以下两种情况来计算 $T_0$:

情况 **3.2.1.** $x_2 = 0$; 这时, 令

$$T_1 = \#\{(x_1, \gamma, b) \in \mathbb{F}_q^3 : x_1 \neq 0, x_1^2b^2 + \gamma^2 = 0\}.$$

在 $T_1$ 的表达式中, 由于 $x_1 \neq 0$, 则我们有 $b = x_1^{-1}\gamma$, 可见 $b$ 是由 $x_1$ 和 $\gamma$ 唯一确定的, 其中 $x_1 \in \mathbb{F}_q^*$, 所以我们有

$$T_1 = (q-1)q.$$

情况 **3.2.2.** $x_2 \neq 0$; 这时, 令

$$T_2 = \#\{(x_1, x_2, \gamma, b) \in \mathbb{F}_q^4 : x_2 \neq 0, (x_1^2 + x_1x_2 + x_2^2\delta^{q+1})b^2 + x_2\gamma b + \gamma^2 = 0\}.$$

现进行指数和计算, 我们有

$$\begin{aligned} T_2 &= \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{x_2\in\mathbb{F}_q^*}\sum_{x_1,\gamma,b\in\mathbb{F}_q}\psi\left(\lambda\left((x_1^2 + x_1x_2 + x_2^2\delta^{q+1})b^2 + x_2\gamma b + \gamma^2\right)\right) \\ &= \frac{(q-1)q^3}{q} + \frac{1}{q}\sum_{\lambda,\, x_2\in\mathbb{F}_q^*}\sum_{x_1,\, b\in\mathbb{F}_q}\psi\left(\lambda(x_1^2 + x_1x_2 + x_2^2\delta^{q+1})b^2\right)\sum_{\gamma\in\mathbb{F}_q}\psi(\lambda(\gamma^2 + x_2b\gamma)) \\ &= q^2(q-1) + \sum_{\lambda,\, x_2\in\mathbb{F}_q^*}\sum_{x_1\in\mathbb{F}_q}\psi\left(x_2^{-2}x_1^2 + x_2^{-1}x_1 + \delta^{q+1}\right) \\ &= q^2(q-1) - \sum_{\lambda,\, x_2\in\mathbb{F}_q^*}\sum_{x_1\in\mathbb{F}_q}\psi(0) \\ &= q^2(q-1) - q(q-1)^2 = q(q-1) \end{aligned}$$

进一步地, 在特征为偶数的情况下, 我们同样有

$$T_0 = T_1 + T_2 = 2q(q-1).$$

综合特征为奇数和偶数两种情况, 我们有

$$T_0 = 2q(q-1).$$

由等式(3.38)可得,

$$\begin{aligned} R_3 &= (q+1)q^3 - \frac{q}{q-1}T_0 \\ &= q^4 + q^3 - 2q^2. \end{aligned} \tag{3.39}$$

结合等式(3.36), (3.37)和(3.39), 我们有

$$\begin{aligned} |X_2^{\perp} \cap O_2| &= R_1 + R_2 + R_3 \\ &= q^4 + q^3 + q. \end{aligned} \tag{3.40}$$

由于 $O(\langle X_1\rangle)$ 和 $O(\langle X_2\rangle)$, (即, $O_1$ 和 $O_2$) 为 $\mathrm{PGU}_3(q)$ 的轨道, 则对于任意的 $M_1, M_2 \in O_1$, 我们有 $|M_1^{\perp} \cap O_2| = |M_2^{\perp} \cap O_2|$. 同理, 对于 $O_2$ 来讲也有同样的结论. 通过用两种方式重复计算集合

$$S_0 = \{(X, Y) : X \in O_1, Y \in O_2, X \in Y^{\perp}\}$$

的大小. 我们可以得到, 对任意的 $X \in O_1, Y \in O_2$, 有

$$|O_1||X^{\perp} \cap O_2| = |O_2||Y^{\perp} \cap O_1|$$

成立. 由定理 3.10可知, $|O_1| = q^3 + 1$, $O_2 = (q^2+q)(q^3+1)$. 由于 $O_1$ 是 $Q^+(7,q)$ 的一个 ovoid, 由定义, 则有

$$|Y^{\perp} \cap O_1| = q^2 + 1.$$

对任意的 $Y \in O_2$ 都成立. 从而, 对任意的 $X \in O_1$, 有

$$|X^{\perp} \cap O_2| = (q^2+q)(q^2+1). \tag{3.41}$$

对于任意的 $X \in Q^+(7,q)$, 我们有

$$|X^{\perp} \cap Q^+(7,q)| = (q^2+q+1)(q^2+1)q + 1.$$

因此, 对于任意的 $X \in O_2$, 我们有

$$\begin{aligned} |X^{\perp} \cap O_3| &= |X^{\perp} \cap Q^+(7,q)| - |X^{\perp} \cap O_1| - |X^{\perp} \cap O_2| \\ &= (q^2+1)q^3. \end{aligned}$$

同样地, 通过用两种方式重复计算集合

$$S_1 = \{(Y, X) : Y \in O_2, X \in O_3, X \in Y^{\perp}\}$$

的大小, 我们推得对任意的 $X \in O_3$, 有

$$|X^{\perp} \cap O_2| = (q^2 + q)(q^2 + 1). \tag{3.42}$$

由等式(3.40), (3.41)和(3.42), 我们有 $O_2$ 是 $Q^+(7, q)$ 的一个 $(q^2 + q)$-ovoid. 因此, $O_3$ 作为 $O_1 \cup O_2$ 在 $Q^+(7, q)$ 中的补, 构成了 $Q^+(7, q)$ 的一个 $q^3$-ovoid. 证毕. □

**注 3.12**：当 $q = 2$ 时, 我们通过 Magma 验证得到, 群 $\mathrm{PGU}_3(q)$ 作用在 $Q^+(7, q)$ 上恰有 3 个轨道, 它们仍分别构成 $Q^+(7, q)$ 的 $1, q^2 + q$ 和 $q^3$-ovoid. 因此, 本小节的结论对所有的 $q \equiv 2 (\mathrm{mod}\ 3)$ 成立.

## 3.3 $Q(6, q)$ 中自同构群为 ${}^2G_2(q)$ 的 $m$-ovoids

Ree 群是 Ree 在 1960-1961 年构造的有限域上的一个 Lie 型群, 它是由 Dynkin 图的一种特殊性质的自同构所构成的群, 它推广了 Suzuki 使用不同的方法得到的构造, 它们是有限单群中最后一个被发现的无穷类. 具有重要的研究意义和价值. Ree 在 1960 年引入了 ${}^2G_2(3^{2k+1})$ 型的 Ree 群. 他证明了除了 ${}^2G_2(3) \cong \mathrm{SL}_2(8)$ 外, 其余该类型的 Ree 群都是单群. Wilson 在 2010 年给出了 Ree 群的简化构造, 详情可参见文献[76] 和[77]. 令 $q = p^{2k+1}$ 使得 $p = 3$ 且 $k > 0$, 型为 ${}^2G_2(q)$ 的 Ree 群也被称为 small Ree 群. 该群 ${}^2G_2(q)$ 的阶为 $q^3(q^3 + 1)(q - 1)$. 它的外自同构群是一个 $2k + 1$ 阶的循环群. 令空间 $V = \mathbb{F}_q^7$ 为 $\mathbb{F}_q$ 上的 7 维向量空间, 对于 $x \in V$, 定义二次型如下:

$$Q(x) = x_1x_7 + x_2x_6 + x_3x_5 - x_4^2. \tag{3.43}$$

事实上, 群 ${}^2G_2(q)$ 是作为典型群 $\mathrm{PGO}_7(q)$ 的子群作用在 $\mathbb{F}_q$ 上的 7 维向量空间 $V$ 上的. 长时间以来, 群 ${}^2G_2(q)$ 是作为有限极空间 $Q(6, q)$ 中 Ree-Tits ovoid 的自同构群为人们所熟知, 但很少有人关心 small Ree 群 ${}^2G_2(q)$ 作用在 $Q(6, q)$ 中除去 Ree-Tits ovoid 之外的点有怎样的性质和结构. 在本小节, 我们给出了 $Q(6, q)$ 中自同构群为 ${}^2G_2(q)$ 的 $m$-ovoids. 其中, 我们引用文献[3] 中 $Q(6, q)$ 的模型, 即等式(3.43)所定义的二次型和群 ${}^2G_2(q)$ 的生成方式来进行具体的研究与刻画. 关于 small Ree 群的刻画, 更常见的是用 Octonions 的语言进行描述, 由于该种描述方式相对繁琐, 限于文章篇幅, 我们这里不多作介绍. 下面我们主要采用文献[3] 和[45] 中的矩阵形式作为生成元来对 ${}^2G_2(q)$ 进行刻画.

令 $t=p^k$. 对于 $y\in\mathbb{F}_q$ 和 $\lambda\in\mathbb{F}_q^*$, 定义矩阵

$$\alpha(y)=\begin{pmatrix}1&y^t&0&0&-y^{3t+1}&-y^{3t+2}&y^{4t+2}\\0&1&y&y^{t+1}&-y^{2t+1}&0&-y^{3t+2}\\0&0&1&y^t&-y^{2t}&0&y^{3t+1}\\0&0&0&1&y^t&0&0\\0&0&0&0&1&-y&y^{t+1}\\0&0&0&0&0&1&-y^t\\0&0&0&0&0&0&1\end{pmatrix},$$

$$\beta(y)=\begin{pmatrix}1&0&-y^t&0&-y&0&-y^{t+1}\\0&1&0&y^t&0&-y^{2t}&0\\0&0&1&0&0&0&y\\0&0&0&1&0&y^t&0\\0&0&0&0&1&0&y^t\\0&0&0&0&0&1&0\\0&0&0&0&0&0&1\end{pmatrix},$$

$$\gamma(y)=\begin{pmatrix}1&0&0&-y^t&0&-y&-y^{2t}\\0&1&0&0&-y^t&0&y\\0&0&1&0&0&y^t&0\\0&0&0&1&0&0&-y^t\\0&0&0&0&1&0&0\\0&0&0&0&0&1&0\\0&0&0&0&0&0&1\end{pmatrix},$$

$$h(\lambda)=\text{diag}(\lambda^t,\lambda^{1-t},\lambda^{2t-1},1,\lambda^{1-2t},\lambda^{t-1},\lambda^{-t}),$$

以及矩阵

$$\gamma_0=\text{antidiag}(-1,-1,-1,-1,-1,-1,-1).$$

在此基础上, small Ree 群为

$${}^2G_2(q)=\left\langle\alpha(y),\,\beta(y),\,\gamma(y),\,h(\lambda),\gamma_0|y\in\mathbb{F}_q,\,\lambda\in\mathbb{F}_q^*\right\rangle.$$

群 ${}^2G_2(q)$ 保持 $V$ 上矩阵表示为

$$J_0=\text{antidiag}(1,1,1,-1,1,1,1,). \tag{3.44}$$

的对称双线性型, 从而 ${}^2G_2(q)$ 保持等式(3.43)所定义的二次型 $Q$. 即在该模型下, 群 ${}^2G_2(q)$ 作为典型群 $\text{PGO}_7(q)$ 的子群作用在抛物二次曲面 $Q(6,q)$ 的点集上.

群 ${}^2G_2(q)$ 的两个分别由以下上三角和对角矩阵构成的子群定义为:

$$U(q)=\langle\alpha(y),\,\beta(y),\,\gamma(y)|y\in\mathbb{F}_q\rangle,$$

$$H(q) = \left\langle h(\lambda) | \lambda \in \mathbb{F}_q^* \right\rangle \cong \mathbb{F}_q^*.$$

由文献[48] 可知, 每个 $U(q)$ 中的元素可以唯一表示为 $S(a,b,c) = \alpha(a)\beta(b)\gamma(c)$, 也可参考文献[3]. 因此, $U(q) = \{S(a,b,c) | a,b,c \in \mathbb{F}_q\}$, 从而有 $|U(q)| = q^3$.

令 $Q(6,q)$ 表示由等式 3.43定义的二次型对应的二次曲面. 接下来我们对 ${}^2G_2(q)$ 在 $Q(6,q)$ 上的作用进行研究. 取 $Q(6,q)$ 中的 3 个奇异点, 分别为:

$$e_7 = \langle (0,0,0,0,0,0,1) \rangle,$$

$$e_6 = \langle (0,0,0,0,0,1,0) \rangle,$$

$$e_5 = \langle (0,0,0,0,1,0,0) \rangle.$$

很容易确定点 $e_7, e_6, e_5$ 在 ${}^2G_2(q)$ 中的稳定子群, 他们分别为

$$\text{Stab}_{{}^2G_2(q)}(e_7) = U(q)H(q) \text{ 阶为} q^3(q-1),$$

$$\text{Stab}_{{}^2G_2(q)}(e_6) = \left\langle \beta(y),\, \gamma(y),\, h(\lambda) | y \in \mathbb{F}_q,\, \lambda \in \mathbb{F}_q^* \right\rangle \text{ 阶为} q^2(q-1),$$

$$\text{Stab}_{{}^2G_2(q)}(e_5) = \left\langle \gamma(y),\, h(\lambda) | y \in \mathbb{F}_q,\, \lambda \in \mathbb{F}_q^* \right\rangle \text{ 阶为} q(q-1).$$

已知 $|{}^2G_2(q)| = q^3(q^3+1)(q-1)$, 然后我们就可以计算这 3 个轨道的长度, 它们分别为

$$|O(e_7)| = q^3 + 1,$$

$$|O(e_6)| = q(q^3+1),$$

$$|O(e_5)| = q^2(q^3+1).$$

已知 $|Q(6,q)| = (q^2+q+1)(q^3+1)$, 因此 $Q(6,q)$ 中的所有奇异点恰好被群 ${}^2G_2(q)$ 划分成 3 个轨道, 即 $O(e_7), O(e_6)$ 和 $O(e_5)$. 其中, 轨道 $O(e_7)$ 恰好构成了 $Q(6,q)$ 中自同构群为 ${}^2G_2(q)$ 的 Ree-Tits ovoid.

**定理 3.13：** *采用本节的定义和符号, 我们有 $O(e_6)$ 和 $O(e_5)$ 分别构成 $Q(6,q)$ 的一个 $q$-ovoid 和 $q^2$-ovoid.*

*证明.* 采用本节中的上述定义, 令 $\alpha(y)$, $\gamma_0$, $\alpha(a)$, $\beta(b)$, $\gamma(c)$ 作用在 $e_6$ 上. 我们得到 $O(e_6)$ 的一个子集 $O_2$, 这里 $O_2 = U_1 \cup U_2 \cup U_3$. 其中

$$U_1 = \{\left\langle (0,0,0,0,0,1,-y^t) \right\rangle : y \in \mathbb{F}_q\},$$

$$U_2 = \{\langle v \rangle = \langle (0,1,a,v_4,v_5,v_6,v_7) \rangle : a,b,c \in \mathbb{F}_q\},$$

这里 $v_4 = b^t + a^{t+1}, v_5 = -(c^t + a^{2t+1}), v_6 = ac^t - b^{2t} + a^{t+1}b^t$ 和 $v_7 = c - (b^t + a^{t+1})c^t + ab - a^{2t+1}b^t - a^{3t+2}$;

$$U_3 = \{\langle u\rangle = \langle(1, u_2, u_3, u_4, u_5, u_6, u_7)\rangle : y \in \mathbb{F}_q^*, a, b, c \in \mathbb{F}_q\},$$

这里 $u_2 = a^t - y^{-t}, u_3 = -b^t - ay^{-t}, u_4 = -c^t + u_2b^t - a^{t+1}y^{-t}, u_5 = -u_2(c^t + a^{2t+1}) - b$, $u_6 = -c + u_3c^t - u_2b^{2t} - a^{t+1}(b^ty^{-t} + a^{2t+1})$ 和 $u_7 = -c^{2t} + u_2c - (u_2b^t - y^{-t}a^{t+1})c^t + bu_3 - a^{2t+1}b^tu_2 + a^{3t+2}(a^t + y^{-t})$.

显然 $|U_1| = q, |U_2| = q^3$. 我们现在往证 $|U_3| = (q-1)q^3$.

根据 $U_3$ 的表达式进行计算, 我们得到两个等式:

$$(u_5 - u_2(u_4 + u_2u_3))^t - u_3 = -(a - y^{-1})u_2 + y^{-(t+1)}, \tag{3.45}$$

$$\left(u_6 + u_4u_3 - u_2u_3^2\right)^t - u_4 - u_2u_3 = -(a - y^{-1})u_2^2 - y^{-(t+1)}(a^t + y^{-t}). \tag{3.46}$$

令 $\phi$ 表示一个从 $\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^*$ 到 $\mathrm{PG}(7, q)$ 的映射使得 $\phi(a, b, c, y) = u$, 其中 $a$, $b$, $c$, $y$ 和 $u$ 是与 $U_3$ 中的点的定义相同. 我们只需证明映射 $\phi$ 是单射即可. 现假设 $\phi(a_1, b_1, c_1, y_1) = \phi(a_2, b_2, c_2, y_2)$. 由

$$a_1^t - y_1^{-t} = a_2^t - y_2^{-t}, \tag{3.47}$$

我们有 $a_1 - y_1^{-1} = a_2 - y_2^{-1}$. 结合等式(3.45)和 (3.46), 我们推得 $y_1^{-(t+1)} = y_2^{-(t+1)}$ 和

$$a_1^t + y_1^{-t} = a_2^t + y_2^{-t}. \tag{3.48}$$

由等式(3.47)和(3.48)可得 $a_1 = a_2$ 和 $y_1 = y_2$. 由 $u_3$ 和 $u_4$ 的表达式, 我们有 $b_1 = b_2$ 和 $c_1 = c_2$. 从而我们证明了该论断, 因此 $|O_2| = |O(e_6)|$, 即, $O_2 = O(e_6)$.

令 $B$ 表示等式(3.43)定义的二次型所对应的双线性型. 对于任意的 $x \in \mathrm{PG}(6, q)$, 定义 $x^\perp = \{z \in \mathrm{PG}(6, q) : B(x, z) = 0\}$. 容易看出

$$e_6^\perp = \{x \in \mathrm{PG}(6, q) : x_2 = 0\}.$$

现在我们计算 $|e_6^\perp \cap O(e_6)|$. 显然, $U_1 \subseteq e_6^\perp$ 且 $e_6^\perp \cap U_2 = \emptyset$. 由以上关于 $U_3$ 的分析, 我们有

$$e_6^\perp \cap U_3 = \{\phi(a, b, c, a^{-1}) : a \in \mathbb{F}_q^*, b, c \in \mathbb{F}_q\}$$

我们知道 $\phi$ 是双射从而 $|e_6^\perp \cap U_3| = (q-1)q^2$. 因此,

$$\begin{aligned} |e_6^\perp \cap O(e_6)| &= q + (q-1)q^2 \\ &= q(q^2+1) - (q^2+1) + 1. \end{aligned} \tag{3.49}$$

由于 $O(e_7)$ 是 $Q(6,q)$ 的一个 ovoid, 则有 $|z^\perp \cap O(e_7)| = q^2+1$ 对任意的 $z \in O(e_6)$ 成立. 通过用两种方式重复计算集合 $\{(x,z) : x \in O(e_7), z \in O(e_6), x \in z^\perp\}$ 的大小, 我们推得对任意的 $x \in O(e_7)$,

$$|x^\perp \cap O(e_6)| = q(q^2+1). \tag{3.50}$$

对任意的 $x \in Q(6,q)$, 我们有

$$|x^\perp \cap Q(6,q)| = (q^2+1)(q+1)q+1.$$

从而, 对任意的 $x \in O(e_6)$, 我们有

$$\begin{aligned} |x^\perp \cap O(e_5)| &= |x^\perp \cap Q(6,q)| - |x^\perp \cap O(e_7)| - |x^\perp \cap O(e_6)| \\ &= (q^2+1)q^2. \end{aligned}$$

进一步地, 通过用两种方式重复计算集合 $\{(x,z) : x \in O(e_5), z \in O(e_6), x \in z^\perp\}$ 的大小, 我们得出, 对任意的 $x \in O(e_5)$,

$$|x^\perp \cap O(e_6)| = q(q^2+1). \tag{3.51}$$

根据等式(3.49), (3.50)和(3.51), 我们有 $O(e_6)$ 是一个 $Q(6,q)$ 的 $q$-ovoid. 因此, $O(e_5)$ 作为 $O(e_6) \cup O(e_7)$ 在 $Q(6,q)$ 中的补, 是 $Q(6,q)$ 的一个 $q^2$-ovoid. 证毕. □

## 3.4 小结

在本章中, 我们在第 3.1节对于 $q \equiv 1 (\mathrm{mod}\ 4)$, $q > 5$ 的情形构造了 $Q(4,q)$ 中的 $\frac{q-1}{2}$-ovoids. 再结合文献[7] 和[35] 中的结果, 说明了对所有的奇素数幂 $q$, 广义四边形 $Q(4,q)$ 中都存在 $\frac{q-1}{2}$-ovoids. 我们的方法与文献[35] 中的相类似, 我们的主要贡献是找到了合适的自同构群, 以使得文献[35] 中的技术手段适用于我们所研究的情形. 由于 PGO$(5,q)$ 具有丰富的子群结构, 因此找到合适的自同构群确实是一个很大的挑战. 而确定 $Q(4,q)$ 中 $m$-ovoids 的谱, 即确定对于哪些 $m$ 在 $Q(4,q)$ 中存在 $m$-ovoids, 似乎目前还无法实现. 我们在第 3.2节给出了 $q \equiv 2 (\mathrm{mod}\ 3)$ 时, $Q^+(7,q)$ 中自同构群为 $\mathrm{PGU}_3(q)$ 的 $(q^2+q)$-ovoid 和 $q^3$-ovoid 的结构和证明. 我们在第 3.3节给出了 $q = 3^{2k+1}$ 且 $k \geq 1$ 时, $Q(6,q)$ 中自同构群为 ${}^2G_2(q)$ 的 $q$-ovoid 和 $q^2$-ovoid 的结构和证明.

# 4 由偏差集构造极小线性码

## 4.1 极小线性码及本章主要结果

令 $q$ 是一个素数幂, $\mathbb{F}_q$ 是一个有 $q$ 个元素的有限域. 令 $\mathcal{C}$ 是有限域 $\mathbb{F}_q$ 上的一个 $[n,k]$ 线性码, 即, 一个 $\mathbb{F}_q^n$ 的 $k$ 维子空间. 码字 $c=(c_1,c_2,\ldots,c_n)\in\mathcal{C}$ 的支撑 (support) 定义为

$$\mathrm{supp}(c)=\{1\le i\le n:\ c_i\neq 0\}.$$

码字 $c$ 的 Hamming 重量为 $wt(c):=|\mathrm{supp}(c)|$, 即为 $\mathrm{supp}(c)$ 的大小. 对于两个码字 $u,\ v\in\mathcal{C}$, 如果 $\mathrm{supp}(u)\subseteq\mathrm{supp}(v)$, 那么我们称 $v$ 覆盖 (covers) $u$ 并记作 $u\preceq v$. 显然, 如果 $u\preceq v$, 则 $au\preceq v$ 对所有的 $a\in\mathbb{F}_q$ 成立. 一个码字 $c\in\mathcal{C}$ 如果满足 $c$ 只覆盖码字 $\lambda c$, 这里 $\lambda\in\mathbb{F}_q$, 而不覆盖 $\mathcal{C}$ 中的其他码字, 则我们称 $c$ 是极小的 (minimal). 一个线性码 $\mathcal{C}$ 若满足每个码字 $c\in\mathcal{C}$ 都是极小的, 则我们称 $\mathcal{C}$ 是极小的 (minimal).

Ashikhmin 和 Barg 在文献[2] 中给出了线性码 $\mathcal{C}$ 是否是极小的一个简单有效的判据, 该判别方法在文献[12] 中被称为 AB 条件.

**引理 4.1：**[2] 令 $\mathcal{C}$ 是 $\mathbb{F}_q$ 上的线性码. 设 $\omega_{\min}$ 和 $\omega_{\max}$ 分别为 $\mathcal{C}$ 的最小和最大的非零重量. 如果

$$\frac{\omega_{\min}}{\omega_{\max}}>\frac{q-1}{q},\tag{4.1}$$

那么 $\mathcal{C}$ 是一个极小线性码.

这个条件对于判别极小线性码是充分而非必要条件. Heng 等人在文献[42] 中给出了如下的充分必要的条件:

**引理 4.2：**[42] 一个 $\mathbb{F}_q$ 上的线性码 $\mathcal{C}\subseteq\mathbb{F}_q^n$ 是极小的当且仅当对于 $\mathcal{C}$ 的任意两个 $\mathbb{F}_q$-线性无关的码字 $c$ 和 $c'$, 都满足

$$\sum_{a\in\mathbb{F}_q^*}wt(c'+ac)\neq(q-1)wt(c')-wt(c).$$

在文献[42] 中, 作者运用引理 4.2构造了不满足 AB 条件的三元线性码. 迄今为止, 已经有许多不满足 AB 条件的极小线性码被构造出来. 一些已知的构造可参考绪论中的表 1.2以及表中相应的参考文献.

在文献[12] 中, Bonini 和 Borello 利用切块集 (cutting blocking set) 构造了极小线性码. 一个仿射 $k$-分块集 (blocking set) 是 $n$ 维仿射空间中与所有 $(n-k)$ 维仿射子空间都相交的子集. 仿射 1-分块集也称为仿射分块集 (affine blocking set). 一个向量 $k$-分

块集 (vectorial $k$-blocking set) 是 $n$ 维仿射空间的一个子集, 不包含原点, 并且与所有通过原点 $(n-k)$ 维仿射子空间相交. 向量 1-分块集也被称为向量分块集 (vectorial blocking set). 向量 $(k,s)$-分块集 (vectorial $(k,s)$-blocking set) 是一个向量 $k$-分块集, 它不包含通过原点的 $s$ 维仿射子空间. 如果向量 $k$-分块集与每个通过原点的 $(n-k)$ 维仿射子空间的交集不包含在任何其他过原点的 $(n-k)$ 维仿射子空间中, 则称之为切割的 (cutting).

**引理 4.3：**[12] 令 $f:\mathbb{F}_q^m\to\mathbb{F}_q$ 是一个非线性函数。如果

1) $V(f)^*=\{\mathbf{x}\in\mathbb{F}_q^m\setminus\{\mathbf{0}\}:f(\mathbf{x})=0\}$ 是仿射空间 $\mathbb{F}_q^m$ 中的一个 $m$ 维切向量 $(1,m-1)$-分块集 (cutting vectorial $(1,m-1)$-blocking set);

2) 对于每个非 0 向量 $\mathbf{v}$, 若存在 $\mathbf{x}$ 使得 $f(\mathbf{x})+\mathbf{v}\cdot\mathbf{x}=0$ 并且 $f(\mathbf{x})$ 不等于 0,

则 $\mathcal{C}(f)=\{(uf(\mathbf{x})+\mathbf{v}\cdot\mathbf{x})_{\mathbf{x}\in\mathbb{F}_q^m\setminus\{0\}}:u\in\mathbb{F}_q,\mathbf{v}\in\mathbb{F}_q^m\}$ 是 $\mathbb{F}_q$ 上的一个 $[q^m-1,m+1]$ 极小线性码.

令 $m$ 是一个正整数且 $\mathbb{F}_{q^m}^*$ 是有限域 $\mathbb{F}_{q^m}$ 的乘法群. 注意本章此处的符号 $m$ 仅表示一个正整数, 与第 3 章中的术语 $m$-ovoids 中的 $m$ 无关. 取 $\mathbb{F}_{q^m}^*$ 的真子集 $D$ 定义它的特征函数为

$$f_D(x)=\begin{cases}1, & \text{如果}x\in D,\\ 0, & \text{如果}x\in\mathbb{F}_{q^m}^*\setminus D.\end{cases}$$

我们定义线性码

$$\mathcal{C}(f_D)=\left\{\left(uf_D(x)+\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(vx)\right)_{x\in\mathbb{F}_{q^m}^*}:(u,v)\in V\right\},\tag{4.2}$$

这里 $V=\mathbb{F}_q\times\mathbb{F}_{q^m}$ 表示 $\mathbb{F}_q$ 上的 $m+1$ 维向量空间, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ 表示从 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_q$ 的迹函数.

以下是本章主要结果的一个简要总结. 我们在定理 4.9中给出了 $\mathcal{C}(f_D)$ 是极小线性码的一个充要条件. 通过取 $D$ 作为 $\mathbb{F}_q^*$-不变的偏差集, 我们在定理 4.12中给出了关于 $D$ 的参数的充分条件以使得 $\mathcal{C}(f_D)$ 是极小线性码. 我们还表明, 如果 $D$ 的参数满足某些条件, 则码 $\mathcal{C}(f_D)$ 不满足 AB 条件. 我们的构造方法所得到的极小线性码不是由切块集产生的, 请参见例 4.20, 和例 4.21. 在 $D$ 是 $\mathbb{F}_q^*$-不变的偏差集的情况下, 我们确定了 $\mathcal{C}(f_D)$ 的重量分布. 在 4.3.3小节中, 我们展示了集合 $D$ 的每个自同构会诱导码 $\mathcal{C}(f_D)$ 的自同构. 特别地, 在某些情况下, 我们获得具有较大自同构群的极小线性码 $\mathcal{C}(f_D)$, 这可能使得 $\mathcal{C}(f_D)$ 具有快速的译码算法.

本章的结构如下. 在 4.2节, 我们回顾了有关特征与多项式的一些基本结果. 在 4.3节, 我们利用偏差集构造极小线性码, 并研究其性质. 在 4.4节中, 我们介绍了由我

们的构造方法得到的极小线性码在秘密共享方案中的应用. 最后, 我们在 4.5节对本章进行总结.

## 4.2 关于有限域的一些基本事实

在本节中, 我们仍令 $q$ 是一个素数幂, $m$ 是一个正整数. 令 $\mathbb{F}_q$ 和 $\mathbb{F}_{q^m}$ 分别表示有 $q$ 个元素和 $q^m$ 个元素的有限域. 令 $\mathbb{F}_q^*$ (对应.$\mathbb{F}_{q^m}^*$) 为 $\mathbb{F}_q$ (对应. $\mathbb{F}_{q^m}$) 的非 0 元素构成的乘法群. 对于 $\mathbb{F}_{q^m}$ 的任一子集 $S$, 我们将由 $S$ 张成的 $\mathbb{F}_q$-线性子空间记为 $\langle S\rangle$. 如果对于每个 $\lambda \in \mathbb{F}_q^*$, $s \in S$ 都有 $\lambda s \in S$, 则我们称 $S$ 是 $\mathbb{F}_q^*$-不变的. 对于有限域 $\mathbb{F}$ 的次数为 $[\mathbb{E}:\mathbb{F}]$ 的有限扩张 $\mathbb{E}$, 我们用 $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}$ 来表示来表示从 $\mathbb{E}$ 到 $\mathbb{F}$ 的迹 (trace) 函数.

令 $G$ 为一个有限交换群. 回顾一下, 群 $(G,+)$ 的特征 $\phi$ 是一个群同态 $\phi: G \to \mathbb{C}^\times$, 这里 $\mathbb{C}^\times$ 表示非 0 复数构成的乘法群. 群 $G$ 的平凡特征 (trivial character) $\phi_0$ 定义为 $\phi_0(g) = 1$ 对所有的 $g \in G$ 成立. 群 $G$ 的特征集 $\widehat{G}$ 构成一个单位元为 $\phi_0$ 的交换群, 且 $\widehat{G}$ 与 $G$ 同构, 参考[51] 第 5 章. 群 $\widehat{G}$ 称为 $G$ 特征群.

一个 $\mathbb{F}_q$ 的加法特征 (additive character) $\psi$ 是加法群 $(\mathbb{F}_q,+)$ 的特征. 对于每个 $a \in \mathbb{F}_q$, 我们定义 $\mathbb{F}_q$ 的加法特征 $\psi_a$ 为

$$\psi_a(x) = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)},$$

这里 $\zeta_p = e^{\frac{2\pi i}{p}}$ 是一个 $p$ 次本元单位根. 特征 $\psi_1$ 被称为标准加法特征 (canonical additive character), 我们将其表示为 $\psi$. $(\mathbb{F}_q,+)$ 的特征群是由 $\widehat{(\mathbb{F}_q,+)} = \{\psi_a : a \in \mathbb{F}_q\}$ 给出. 对于 $\mathbb{F}_q$ 的扩张 $\mathbb{F}_{q^m}$, 它的标准加法特征 $\Psi$ 可由 $\psi$ 得到, 即,

$$\Psi(x) = \psi(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)).$$

群 $(\mathbb{F}_{q^m},+)$ 的特征群为 $\widehat{(\mathbb{F}_{q^m},+)} = \{\Psi_a : a \in \mathbb{F}_{q^m}\}$, 这里 $\Psi_a(x) = \Psi(ax)$ 对于每个 $x \in \mathbb{F}_{q^m}$ 成立. 关于加法特征有一个非常重要的性质, 参考[51]:

$$\sum_{\lambda\in\mathbb{F}_q} \Psi(\lambda x) = \sum_{\lambda\in\mathbb{F}_q} \psi(\lambda \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)) = \begin{cases} q, & \text{如果} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = 0, \\ 0, & \text{否则}. \end{cases} \tag{4.3}$$

对于每个 $a \in \mathbb{F}_{q^m}$ 和子集 $A \subseteq \mathbb{F}_{q^m}$, 我们定义

$$\Psi_a(A) := \sum_{x\in A} \Psi(ax). \tag{4.4}$$

我们将 $\mathbb{F}_{q^m}$ 看作一个 $m$ 维的 $\mathbb{F}_q$-线性的向量空间. 对于每个 $a \in \mathbb{F}_{q^m}^*$, 我们定义

$$L(a) := \{x \in \mathbb{F}_{q^m} : \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xa) = 0\},$$

这是一个 $\mathbb{F}_{q^m}$ 的 $m-1$ 维 $\mathbb{F}_q$-线性子空间. 对于 $\mathbb{F}_{q^m}^*$ 的子集 $S$, 我们定义

$$L(S) := \{x \in \mathbb{F}_{q^m} : \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xs) = 0, \forall\, s \in S\}. \tag{4.5}$$

由于 $L(S)$ 是所有使得 $s \in S$ 的 $L(s)$ 的交, 所以它也是一个 $\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$-线性子空间.

**引理 4.4：** 令 $L$ 为等式(4.5)所定义的运算. 令 $V_1$ 是一个 $\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$-线性子空间且 $U_1$ 是 $V_1$ 的子集. 则 $\langle U_1\rangle = V_1$ 当且仅当 $L(U_1) \subseteq L(V_1)$, 这里 $\langle U_1\rangle$ 是由 $U_1$ 张成的 $\mathbb{F}_q$-线性子空间.

证明. 对于任意的子集 $S \subseteq \mathbb{F}_{q^m}$, 可直接验证 $L(\langle S\rangle) = L(S)$ 并且通过比较它们的维数可知 $L(L(S)) = \langle S\rangle$. 因此, $V_1 \subseteq \langle U_1\rangle$ 当且仅当 $L(U_1) = L(\langle U_1\rangle) \subseteq L(V_1)$, 证毕. □

**引理 4.5：** 令 $a \in \mathbb{F}_{q^m}$ 并且 $A \subseteq \mathbb{F}_{q^m}$. 则有 $A \subseteq L(a)$ 当且仅当 $\Psi_{\lambda a}(A) = |A|$ 对所有的 $\lambda \in \mathbb{F}_q$ 成立, 这里 $\Psi_{\lambda a}(A)$ 由等式(4.4)所定义. 特别地, 如果 $A$ 是 $\mathbb{F}_q^*$-不变的, 则 $L(A) = \{a \in \mathbb{F}_{q^m} : \Psi_a(A) = |A|\}$.

证明. 假设 $A \subseteq L(a)$. 则有 $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xa) = 0$ 对所有的 $x \in A$ 成立, 因此 $\Psi_{\lambda a}(x) = \psi\left(\lambda \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(ax)\right) = 1$ 对所有的 $x \in A$ 和 $\lambda \in \mathbb{F}_q$ 成立. 由等式(4.4)所给出的 $\Psi_{\lambda a}(A)$ 的定义可得 $\Psi_{\lambda a}(A) = |A|$ 对所有的 $\lambda \in \mathbb{F}_q$ 成立. 反之, 假设 $\Psi_{\lambda a}(A) = |A|$ 对所有的 $\lambda \in \mathbb{F}_q$ 成立, 我们计算可得

$$\begin{aligned} q|A| &= \sum_{\lambda\in\mathbb{F}_q} \Psi_{\lambda a}(A) = \sum_{x\in A}\sum_{\lambda\in\mathbb{F}_q} \Psi(\lambda a x) \\ &= \sum_{x\in A}\sum_{\lambda\in\mathbb{F}_q} \psi\left(\lambda \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(ax)\right). \end{aligned}$$

由等式(4.3), 我们推得 $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(ax) = 0$ 对所有的 $x \in A$ 成立, 即, $A \subseteq L(a)$. 在 $A$ 是 $\mathbb{F}_q^*$-不变的情况下, 我们有 $\Psi_{\lambda a}(A) = \Psi_a(\lambda A) = \Psi_a(A)$ 对任意的 $\lambda \in \mathbb{F}_q^*$ 成立. 此外, 显然有 $\Psi_0(A) = |A|$. 从而

$$\begin{aligned} L(A) &= \{a \in \mathbb{F}_{q^m} : \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xa) = 0, \forall\, x \in A\} \\ &= \{a \in \mathbb{F}_{q^m} : A \subseteq L(a)\} \\ &= \{a \in \mathbb{F}_{q^m} : \Psi_a(A) = |A|\}. \end{aligned}$$

证毕. □

多项式 $f(X) \in \mathbb{F}_{q^m}[X]$ 如果满足其相应的函数 $f : a \mapsto f(a)$ 是从 $\mathbb{F}_{q^m}$ 到自身的一个置换, 则称该多项式为置换多项式. 一个形如 $f(X) = \sum_{i=0}^{n} a_i X^{q^i}$ 使得 $a_i \in \mathbb{F}_{q^m}$ 的多项式被称为 $\mathbb{F}_{q^m}$ 上的 $q$-多项式; 如果 $n \le m-1$, 则称其为约化的 (reduced).

在 $\mathbb{F}_{q^m}$ 上的约化 $q$-多项式和 $\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$-线性变换之间存在一一对应, 请参考[51]. 令 $f(X)=\sum_{i=0}^{m-1}a_iX^{q^i}$ 为 $\mathbb{F}_{q^m}$ 上的一个约化 $q$-多项式, 则 $f(X)$ 的迹对偶 (trace dual) 是唯一的约化的 $q$-多项式 $\tilde{f}(X)$ 使得 $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(x)y)=\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\tilde{f}(y)x)$ 对所有的 $x, y\in\mathbb{F}_{q^m}$ 成立. 直接计算可得

$$\tilde{f}(X)=\sum_{i=0}^{m-1}a_{m-i}^{q^i}X^{q^i}. \tag{4.6}$$

## 4.3 由偏差集构造极小线性码

设 $V=\mathbb{F}_q\times\mathbb{F}_{q^m}$, 并将其视作 $\mathbb{F}_q$ 上的 $m+1$ 维向量空间. 令 $B$ 是 $V$ 上的一个双线性型使得

$$B((u,v),(x,y))=ux+\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(vy) \tag{4.7}$$

对于 $(u,v),(x,y)\in V$ 成立. 对于 $(a,b)\in V$, 我们定义

$$(a,b)^{\perp}=\{(x,y)\in V: B((a,b),(x,y))=0\}.$$

相应地, 对于 $V$ 的任意子集 $S$, 我们有

$$S^{\perp}=\{(x,y)\in V:\ B((a,b),(x,y))=0,\ \forall\,(a,b)\in S\}.$$

取 $V$ 的一个子集 $M$, 我们可以通过 $M$ 构造如下的线性码:

$$\mathcal{C}(M):=\{c(u,v)=(B((u,v),(a_i,b_i)))_{1\le i\le n}:(u,v)\in V\}, \tag{4.8}$$

这里 $M=\{(a_1,b_1),(a_2,b_2),\ldots,(a_n,b_n)\}$ 称作码 $\mathcal{C}(M)$ 的定义集 (defining set).

令 $\mathcal{C}(f_D)$ 是由等式(4.2)所定义的线性码. 显然有

$$\mathcal{C}(f_D)=\{(B((u,v),(f_D(x),x)))_{x\in\mathbb{F}_{q^m}^*}:(u,v)\in V\}.$$

由等式(4.7)中 $B$ 的定义可知, 码 $\mathcal{C}(f_D)$ 可由定义集构造得到. 我们定义 $V$ 的子集如下:

$$M_D:=\{(1,r):r\in D\}\cup\{(0,r):r\in\overline{D}\}, \tag{4.9}$$

这里 $\overline{D}=\mathbb{F}_{q^m}^*\setminus D$. 容易验证 $\mathcal{C}(f_D)=\mathcal{C}(M_D)$. 如果 $f_D$ 是非线性的, 那么码 $\mathcal{C}(f_D)$, 即码 $\mathcal{C}(M_D)$, 的维数已经被确定了.

**引理 4.6:** [12] 令 $D$ 是 $\mathbb{F}_{q^m}^*$ 的真子集使得特征函数 $f_D$ 是非线性的. 那么由等式(4.2)所定义的 $\mathbb{F}_q$ 上的线性码 $\mathcal{C}(f_D)$ 的长度为 $q^m-1$, 维数为 $m+1$.

**引理 4.7:** 令 $D$ 是 $\mathbb{F}_{q^m}^*$ 的 $\mathbb{F}_q^*$-不变真子集, $f_D$ 是等式(4.2)中的特征函数. 如果 $q>2$, 则 $f_D$ 是非线性的.

证明. 假设 $f_D$ 是线性的, 即, $f_D(x+y) = f_D(x) + f_D(y)$ 对任意的 $x, y \in \mathbb{F}_{q^m}^*$ 成立. 我们取任意的 $x \in D$ 并选择 $\lambda \in \mathbb{F}_q$ 使得 $\lambda \notin \{0, -1\}$. 由于 $D$ 是 $\mathbb{F}_q^*$-不变的, 则 $\lambda x$ 和 $(\lambda+1)x$ 都落在 $D$ 中. 由 $f_D((\lambda+1)x) = f_D(\lambda x) + f_D(x)$ 可得在 $\mathbb{F}_q$ 中, $1+1=1$, 这是不可能的. 证毕. □

### 4.3.1 码 $\mathcal{C}(M_D)$ 为极小码的充要条件

对于 $\mathbb{F}_{q^m}^*$ 的一个子集 $D$, 设 $\overline{D} = \mathbb{F}_{q^m}^* \setminus D$. 对于 $\mathbb{F}_{q^m}^*$ 的一个子集 $S$, $L(S)$ 由等式(4.5)所定义. 对于 $y \in \mathbb{F}_q$, $z \in \mathbb{F}_{q^m}^*$, 我们定义

$$\overline{D}_z := \{x \in \overline{D} : \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz) = 0\}, \tag{4.10}$$

$$D_{(y,z)} := \{x \in D : \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz) = -y\}, \tag{4.11}$$

$$P_{(y,z)} := L\left(D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z\right), \tag{4.12}$$

这里 $D_{(y,z)} D_{(y,z)}^{(-1)} = \{d_i - d_j : d_i, d_j \in D_{(y,z)}\}$.

回顾一下对于 $\mathbb{F}_{q^m}$ 的一个子集 $S$, $\langle S \rangle$ 是一个由 $S$ 张成的 $\mathbb{F}_q$-线性空间. 事实上, 可以利用文献[52] 中的定理 3.2 和定理 3.3 直接得到下面的定理, 我们在这里用我们的语言再简要地给一下证明过程.

**定理 4.8:** *采用上述符号. 假设 $D$ 是 $\mathbb{F}_{q^m}^*$ 的一个子集, $M_D$ 的定义由等式(4.9)给出. 令 $\mathcal{C}(M_D)$ 为一个由等式(4.8)所给出的线性码使得其定义集为 $M_D$. 对于每个 $(y,z) \in V$ 使得 $(y,z) \neq (0,0)$, 码字 $c(y,z) \in \mathcal{C}(M_D)$ 是极小的当且仅当 $\langle (y,z)^\perp \cap M_D \rangle = (y,z)^\perp$. 特别地, $\mathcal{C}(M_D)$ 是极小码当且仅当 $\langle (y,z)^\perp \cap M_D \rangle = (y,z)^\perp$ 对所有的 $(y,z) \in V \setminus \{(0,0)\}$ 成立.*

证明. 对于任意两个码字 $c(y_1,z_1)$, $c(y_2,z_2) \in \mathcal{C}(M_D)$, 根据等式(4.8)中 $\mathcal{C}(M_D)$ 的定义, 我们有 $c(y_1,z_1) \preceq c(y_2,z_2)$, 即, $\mathrm{supp}(c(y_1,z_1)) \subseteq \mathrm{supp}(c(y_2,z_2))$, 当且仅当 $(y_2,z_2)^\perp \cap M_D \subseteq (y_1,z_1)^\perp \cap M_D$.

假设 $(y,z) \in V \setminus \{(0,0)\}$ 使得 $\langle (y,z)^\perp \cap M_D \rangle = (y,z)^\perp$, 我们证明 $c(y,z)$ 是极小的. 取 $(y_1,z_1) \in V$ 使得 $c(y_1,z_1) \preceq c(y,z)$, 我们有

$$(y,z)^\perp = \langle (y,z)^\perp \cap M_D \rangle \subseteq \langle (y_1,z_1)^\perp \cap M_D \rangle \subseteq (y_1,z_1)^\perp.$$

如果 $(y_1,z_1) \neq (0,0)$, 则 $\dim(y,z)^\perp = \dim(y_1,z_1)^\perp$, 因此 $(y,z)^\perp = (y_1,z_1)^\perp$. 如果 $(y_1,z_1) = (0,0)$, 那么有 $c(y_1,z_1) = \mathbf{0}$. 因此 $c(y_1,z_1) = \mu c(y,z)$ 对于某个 $\mu \in \mathbb{F}_q$ 成立.

反之, 假设对于某个 $(y,z) \in V \setminus \{(0,0)\}$, 码字 $c(y,z)$ 是极小的并且使得 $\langle (y,z)^\perp \cap M_D \rangle \neq (y,z)^\perp$. 则我们有 $\dim\langle (y,z)^\perp \cap M_D \rangle < \dim(y,z)^\perp$, 即,

$$\dim\langle (y,z) \rangle < \dim\langle (y,z)^\perp \cap M_D \rangle^\perp.$$

因此, 存在 $(y_1, z_1) \in \langle (y,z)^\perp \cap M_D \rangle^\perp$ 使得 $(y_1, z_1)$ 与 $(y, z)$ 线性无关. 从而有 $(y,z)^\perp \cap M_D \subseteq (y_1,z_1)^\perp \cap M_D$, 即, $c(y_1,z_1) \preceq c(y,z)$, 这与 $c(y,z)$ 的极小性矛盾. 因此, 如果 $c(y,z)$ 是极小的, 必然有 $\langle (y,z)^\perp \cap M_D \rangle = (y,z)^\perp$. 则第一个论断得证.

由于一个码是极小的当且仅当它的所有码字都是极小的, 则该定理的最后一个论断成立. □

**定理 4.9:** 采用与定理4.8相同的符号. 码 $\mathcal{C}(M_D)$ 是极小线性码当且仅当下列两个条件成立:

1. 集合 $\overline{D}$ 在 $\mathbb{F}_q$ 上张成 $\mathbb{F}_{q^m}$, 即, $\langle \overline{D} \rangle = \mathbb{F}_{q^m}$.
2. 对任意的 $y \in \mathbb{F}_q$ 和 $z \in \mathbb{F}_{q^m}^*$, 都有 $D_{(y,z)} \neq \emptyset$ 且 $P_{(y,z)} \subseteq \langle z \rangle$, 这里 $D_{(y,z)}$ 和 $P_{(y,z)}$ 分别由等式 (4.11)和等式(4.12)所定义.

证明. 由定理 4.8可知, 对于每个码字 $c(y,z) \in \mathcal{C}(M_D)$ 使得 $(y,z) \in V \setminus \{(0,0)\}$, 它是极小的当且仅当 $\langle (y,z)^\perp \cap M_D \rangle = (y,z)^\perp$. 根据 $z = 0$ 与否, 我们将证明分为下面两种情况.

情况 **1.** $y \in \mathbb{F}_q^*$ 且 $z = 0$; 在该种情形下, 我们计算

$$(y,0)^\perp = \{(u,v) \in V : uy + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(v \cdot 0) = 0\} = \{(0,v) : v \in \mathbb{F}_{q^m}\}.$$

从而 $(y,0)^\perp \cap M_D = \{(0,v) : v \in \overline{D}\}$. 因此, 码字 $c(y,0)$ 是极小的当且仅当 $\langle (y,0)^\perp \cap M_D \rangle = (y,0)^\perp$, 即, $\overline{D}$ 在 $\mathbb{F}_q$ 上张成 $\mathbb{F}_{q^m}$.

情况 **2.** $(y,z) \in V$ 使得 $z \neq 0$; 在该种情形下, 我们有

$$(y,z)^\perp = \{(u,v) \in V : uy + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(vz) = 0\}.$$

由于 $(y,z)^\perp$ 是 $m$ 维 $\mathbb{F}_q$-线性的, 则它有如下分解:

$$(y,z)^\perp = \langle (1,v_0) \rangle \oplus \langle \{(0,v) : v \in L(z)\} \rangle, \tag{4.13}$$

这里 $v_0 \in \mathbb{F}_{q^m}$ 满足 $y + \mathrm{Tr}_{\mathbb{F}_q^m/\mathbb{F}_q}(v_0 z) = 0$. 此外, 显然有

$$(y,z)^\perp \cap M_D = \{(1,r) : r \in D_{(y,z)}\} \cup \{(0,r) : r \in \overline{D}_z\}. \tag{4.14}$$

我们往证 $\langle (y,z)^\perp \cap M_D \rangle = (y,z)^\perp$ 当且仅当 $D_{(y,z)} \neq \emptyset$ 且 $\langle D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z \rangle = L(z)$. 假设 $\langle (y,z)^\perp \cap M_D \rangle = (y,z)^\perp$. 我们有 $D_{(y,z)} \neq \emptyset$, 否则 $(y,z)^\perp \cap M_D = \{(0,r) : r \in \overline{D}_z\}$ 且 $(1,v_0) \notin \langle (y,z)^\perp \cap M_D \rangle$, 这与等式(4.13)中 $(y,z)^\perp$ 的分解矛盾. 对于每个

$d_0 \in D_{(y,z)}$, 由于 $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(z(v_0 - d_0)) = -y + y = 0$, 我们有

$$(1, v_0) - (1, d_0) = (0, v_0 - d_0) \in \langle \{(0, v) : v \in L(z)\} \rangle.$$

必要时可用 $d_0$ 代替 $v_0$, 则分解式(4.13)可由

$$(y, z)^{\perp} = \langle (1, d_0) \rangle \oplus \langle \{(0, v) : v \in L(z)\} \rangle. \tag{4.15}$$

来代替. 因为 $(1, d_0) \in (y, z)^{\perp} \cap M_D$, 则 $\langle (y, z)^{\perp} \cap M_D \rangle = (y, z)^{\perp}$ 当且仅当

$$\langle \{(0, d_i - d_0) : d_i \in D_{(y,z)}\} \cup \{(0, d) : d \in \overline{D}_z\} \rangle = \langle \{(0, v) : v \in L(z)\} \rangle.$$

这对于 $D_{(y,z)}$ 中的所有 $d_0$ 都成立, 从而我们推得 $\langle D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z \rangle = L(z)$. 反之, 假设 $D_{(y,z)} \neq \emptyset$ 和 $\langle D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z \rangle = L(z)$ 成立, 我们取 $d_0 \in D_{(y,z)}$. 根据以上的论断, 我们可在分解式(4.13)中用 $d_0$ 代替 $v_0$, 从而得到分解式(4.15). 由 $(1, d_0) \in (y, z)^{\perp} \cap M_D$, 等式 (4.14), (4.15)和 $\langle D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z \rangle = L(z)$ 等条件可得, $\langle (y, z)^{\perp} \cap M_D \rangle = (y, z)^{\perp}$. 则该结论成立.

我们现在往证 $\langle D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z \rangle = L(z)$ 当且仅当 $P_{(y,z)} \subseteq \langle z \rangle$. 注意 $D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z$ 是 $L(z)$ 的一个子集. 通过运用引理 4.4 到 $U_1 = D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z$ 和 $V_1 = L(z)$, 我们推得 $\langle D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z \rangle = L(z)$ 当且仅当 $L(D_{(y,z)} D_{(y,z)}^{(-1)} \cup \overline{D}_z) \subseteq L(L(z))$. 由等式(4.12)中 $P_{(y,z)}$ 的定义和 $L(L(z)) = \langle z \rangle$ 的事实可知, 该结论成立.

综上所述, 我们结合以上两种情况完成了该定理的证明. □

假设 $D \subseteq \mathbb{F}_{q^m}^*$ 是 $\mathbb{F}_q^*$-不变的. 可直接验证 $\overline{D}, \overline{D}_z$ 和 $D_{0,z}$ 对于任意的 $z \in \mathbb{F}_{q^m}^*$ 也都是 $\mathbb{F}_q^*$-不变的. 将引理 4.5运用到等式 (4.12), 我们有

$$\begin{aligned} P_{(y,z)} &= L\left(D_{(y,z)} D_{(y,z)}^{(-1)}\right) \cap L\left(\overline{D}_z\right) \\ &= \{a \in \mathbb{F}_{q^m} : \Psi_a(\overline{D}_z) = |\overline{D}_z|, \Psi_{a\lambda}\left(D_{(y,z)} D_{(y,z)}^{(-1)}\right) = |D_{(y,z)}|^2, \forall \lambda \in \mathbb{F}_q^*\}. \end{aligned}$$

由于

$$\Psi_{a\lambda}\left(D_{(y,z)} D_{(y,z)}^{(-1)}\right) = \Psi_{a\lambda}\left(D_{(y,z)}\right) \overline{\Psi_{a\lambda}\left(D_{(y,z)}\right)} = |\Psi_{a\lambda}\left(D_{(y,z)}\right)|^2,$$

我们推得

$$P_{(y,z)} = \{a \in \mathbb{F}_{q^m} : \Psi_a(\overline{D}_z) = |\overline{D}_z|, |\Psi_{a\lambda}\left(D_{(y,z)}\right)| = |D_{(y,z)}|, \forall \lambda \in \mathbb{F}_q^*\}. \tag{4.16}$$

基于上述论断和定理 4.9, 我们可以得到下面的推论.

**推论 4.10**：采用和定理 4.9相同的符号, 设 $D \subseteq \mathbb{F}_{q^m}^*$ 是 $\mathbb{F}_q^*$-不变的. 则 $\mathcal{C}(M_D)$ 是极小线性码当且仅当下列两个条件成立:

1. 集合 $\overline{D}$ 在 $\mathbb{F}_q$ 上张成 $\mathbb{F}_{q^m}$, 即, $\langle \overline{D} \rangle = \mathbb{F}_{q^m}$.

2. 对于任意的 $y \in \mathbb{F}_q$ 和 $z \in \mathbb{F}_{q^m}^*$, 有 $D_{(y,z)} \neq \emptyset$ 和 $P_{(y,z)} \subseteq \langle z \rangle$ 成立, 这里 $D_{(y,z)}$ 和 $P_{(y,z)}$ 分别由等式(4.11)和等式 (4.16)所定义.

### 4.3.2 偏差集构造极小线性码的方法

在本小节中, 我们利用 $\mathbb{F}_q^*$-不变的偏差集来构造极小线性码. 假设 $D \subseteq \mathbb{F}_{q^m}^*$ 是 $\mathbb{F}_q^*$-不变的. 令 $\psi$ 和 $\Psi$ 分别为 $\mathbb{F}_q$ 和 $\mathbb{F}_{q^m}$ 的标准加法特征. 回顾一下, 对于性质 $\mathcal{X}$, Kronecker delta 函数 $[[\mathcal{X}]]$ 的定义如下:

$$[[\mathcal{X}]] = \begin{cases} 1, & \text{如果性质 } \mathcal{X} \text{ 成立,} \\ 0, & \text{否则.} \end{cases}$$

对于任意的 $(y,z) \in V$ 使得 $z \neq 0$, 我们现计算集合 $D_{(y,z)}$ 的大小:

$$\begin{aligned} |D_{(y,z)}| &= \sum_{x \in D} [[\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz) + y = 0]] = \frac{1}{q} \sum_{x \in D} \sum_{\lambda \in \mathbb{F}_q} \psi(\lambda(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz) + y)) \\ &= \frac{1}{q} \left( |D| + \sum_{\lambda \in \mathbb{F}_q^*} \psi(\lambda y) \Psi(\lambda z D) \right) = \begin{cases} \frac{1}{q} \left( |D| - \Psi(zD) \right), & \text{如果} y \neq 0, \\ \frac{1}{q} \left( |D| + (q-1)\Psi(zD) \right), & \text{如果} y = 0. \end{cases} \end{aligned} \tag{4.17}$$

最后一个等式成立是因为 $D$ 是 $\mathbb{F}_q^*$-不变的, 从而 $\Psi(\lambda z D) = \Psi(zD)$ 对于任意的 $\lambda \in \mathbb{F}_q^*$ 成立.

**引理 4.11**：令 $D$ 是 $\mathbb{F}_{q^m}^*$ 的一个 $\mathbb{F}_q^*$-不变的子集, 对于任一给定的 $(y,z) \in V$ 使得 $z \in \mathbb{F}_{q^m}^*$, 令 $P_{(y,z)}$ 由等式(4.16)所定义. 如果存在 $a \in P_{(y,z)}$ 使得 $a \notin \langle z \rangle$, 则

$$|D| = q^m + \sum_{\lambda_1 \in \mathbb{F}_q} \Psi\left((\lambda_1 z + a)D\right) - (q-1)\Psi(zD), \tag{4.18}$$

$$|D_{(y,z)}| = \frac{1}{q} \Big| \sum_{\lambda_1 \in \mathbb{F}_q} \psi(\lambda_1 y) \Psi\left((\lambda_1 z + a)D\right) \Big|, \tag{4.19}$$

这里 $\psi$ 和 $\Psi$ 分别为 $\mathbb{F}_q$ 和 $\mathbb{F}_{q^m}$ 的标准加法特征.

证明. 由等式(4.10)和 $\overline{D}$ 的定义可知

$$|\overline{D}_z| = q^{m-1} - 1 - |D_{(0,z)}|. \tag{4.20}$$

我们进一步计算

$$\begin{aligned}\Psi(a\overline{D}_z) =& \sum_{x\in\mathbb{F}_{q^m}^*} \Psi(ax)[[\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz)=0]] - \sum_{x\in D} \Psi(ax)[[\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz)=0]]\\ =&\frac{1}{q}\sum_{x\in\mathbb{F}_{q^m}^*} \Psi(ax) \sum_{\lambda_1\in\mathbb{F}_q} \psi\left(\lambda_1 \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz)\right) - \frac{1}{q}\sum_{x\in D} \Psi(ax) \sum_{\lambda_1\in\mathbb{F}_q} \psi\left(\lambda_1 \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz)\right)\\ =&\frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^m}^*} \Psi\left((a+\lambda_1 z)x\right) - \frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q} \Psi\left((a+\lambda_1 z)D\right)\end{aligned}$$

由于 $a \notin \langle z\rangle$, 则有 $a+\lambda_1 z \neq 0$ 对所有的 $\lambda_1 \in \mathbb{F}_q$ 都成立. 因此, 我们有

$$\frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^m}^*} \Psi\left((a+\lambda_1 z)x\right) = -1$$

从而

$$\Psi(a\overline{D}_z) = -1 - \frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q} \Psi\left((a+\lambda_1 z)D\right). \tag{4.21}$$

由等式(4.16)和 $a \in P_{(y,z)}$ 可知 $\Psi(a\overline{D}_z) = |\overline{D}_z|$. 我们运用等式(4.20)和等式(4.21)可得

$$|D_{(0,z)}| = q^{m-1} + \frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q} \Psi\left((a+\lambda_1 z)D\right). \tag{4.22}$$

结合等式(4.17)和等式(4.22), 我们推得等式(4.18)成立.

由于 $a \in P_{(y,z)}$, 我们有 $|D_{(y,z)}| = |\Psi(a\lambda D_{(y,z)})|$ 对任意的 $\lambda \in \mathbb{F}_q^*$ 成立. 不失一般性, 设 $\lambda = 1$. 从而有

$$\begin{aligned}|D_{(y,z)}| = |\Psi(aD_{(y,z)})| &= |\sum_{x\in D} \Psi(ax)[[\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xz)+y=0]]|\\ &= |\frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q}\sum_{x\in D} \Psi(ax)\psi(\lambda_1(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(zx)+y))|\\ &= \frac{1}{q}|\sum_{\lambda_1\in\mathbb{F}_q} \psi(\lambda_1 y)\Psi\left((\lambda_1 z+a)D\right)|.\end{aligned}$$

综上, 我们完成了该引理的证明. □

在上述准备的基础上, 我们现在利用 $\mathbb{F}_q^*$-不变的偏差集给出极小线性码的构造.

**定理 4.12：** 令 $D \subseteq \mathbb{F}_{q^m}^*$ 是一个参数为 $(q^m, k, \lambda, \mu)$ 的 $\mathbb{F}_q^*$-不变的偏差集. 令 $\theta_1, \theta_2$ 是凯莱图 $\mathrm{Cay}(\mathbb{F}_{q^m}, D)$ 的两个限制特征值使得 $\theta_1 > 0 > \theta_2$, 令 $\theta_0 = \max\{|\theta_1|, |\theta_2|\}$. 假设 $\mathcal{C}(M_D)$ 是由等式(4.8)所定义的线性码, 这里定义集 $M_D$ 由等式(4.9)给出. 如果 $\mathrm{Cay}(\mathbb{F}_{q^m}, D)$ 的特征值 $k, \theta_1$ 和 $\theta_2$ 满足:

1) $k - \theta_2 \neq q^m$;

2) $k > \theta_1$ 且 $k > -(q-1)\theta_2$;

和下列条件之一

3a) $k < q^m + q\theta_2 - (q-1)\theta_1$;

3b) $k > \max\{q\theta_0 + \theta_1,\ q\theta_0 - (q-1)\theta_2\}$;

3c) $q^{m-1} + \theta_2 - \theta_1 > \theta_0$.

则 $\mathcal{C}(M_D)$ 是一个极小线性码.

证明. 回顾 2.2小节, 我们有 $k = \Psi_0(D) = |D|$ 且对于任意的 $a \in \mathbb{F}_{q^m}^*$, 我们有 $\Psi_a(D) \in \{\theta_1, \theta_2\}$. 假设该定理的条件成立, 我们采用三个步骤来证明推论 4.10的两个条件成立, 从而得出 $\mathcal{C}(M_D)$ 是极小的.

步骤 **1:** 我们往证 $\overline{D}$ 在 $\mathbb{F}_q$ 上张成 $\mathbb{F}_{q^m}$. 采用反证法, 假设 $\langle \overline{D} \rangle \neq \mathbb{F}_{q^m}$, 即, $L(\overline{D}) \neq \{0\}$. 注意到 $\overline{D}$ 是 $\mathbb{F}_q^*$-不变的, 则对于 $a \in L(\overline{D}) \setminus \{0\}$, 我们可从引理 4.5中推得

$$|\overline{D}| = \Psi_a(\overline{D}) = \sum_{x \in \mathbb{F}_{q^m}^*} \Psi(ax) - \Psi(aD) = -1 - \Psi(aD).$$

结合 $|\overline{D}| = q^m - 1 - |D| = q^m - 1 - k$ 的事实, 我们有 $k - \Psi(aD) = q^m$. 由于 $k - \theta_1 < k < q^m$, 则 $\Psi(aD) = \theta_2$, 这与条件 1) 矛盾. 因此, $L(\overline{D}) = \{0\}$, 即 $\overline{D}$ 在 $\mathbb{F}_q$ 上张成 $\mathbb{F}_{q^m}$.

步骤 **2:** 我们往证 $|D_{(y,z)}| > 0$ 对任意的 $z \in \mathbb{F}_{q^m}^*$ 都成立. 由于 $z \neq 0$, 则 $\Psi(zD) = \theta_1$ 或 $\theta_2$. 由等式(4.17)和条件 2) 可知, 该结论成立.

步骤 **3:** 我们往证 $P_{(y,z)} \subseteq \langle z \rangle$ 对任意的 $y \in \mathbb{F}_q, z \in \mathbb{F}_{q^m}^*$ 都成立, 这里 $P_{(y,z)}$ 由等式(4.16)所定义. 我们通过反证法来证明. 假设对于某个给定的 $(y, z) \in V$ 使得 $z \in \mathbb{F}_{q^m}^*$, 存在 $a \in P_{(y,z)} \setminus \langle z \rangle$. 我们只需要证明三个条件 3a), 3b), 3c) 均不成立即可. 由于 $a \notin \langle z \rangle$, 则对所有的 $\lambda_1 \in \mathbb{F}_q$, 我们有 $\lambda_1 z + a \neq 0$, 从而 $\Psi\left((\lambda_1 z + a)D\right)$ 等于 $\theta_1$

或 $\theta_2$. 设 $\triangle = \frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q}\psi(\lambda_1 y)\Psi\left((\lambda_1 z+a)D\right)$. 由引理 4.11中的等式(4.18), (4.19)和三角不等式, 我们有

$$|D| = q^m + \sum_{\lambda_1\in\mathbb{F}_q}\Psi\left((\lambda_1 z+a)D\right) - (q-1)\Psi(zD) \geq q^m + q\theta_2 - (q-1)\theta_1, \quad (4.23)$$

$$|D_{(y,z)}| = |\triangle| \leq \frac{1}{q}\sum_{\lambda_1\in\mathbb{F}_q}|\Psi((\lambda_1 z+a)D)| \leq \theta_0. \quad (4.24)$$

由不等式(4.23)可知, 条件 3a) 不成立.

接下来考虑等式(4.17), 我们推得

$$|D| = \begin{cases} q|D_{(y,z)}| + \Psi(zD), & \text{如果} y\neq 0, \\ q|D_{(y,z)}| - (q-1)\Psi(zD), & \text{如果} y = 0. \end{cases} \quad (4.25)$$

将不等式(4.24)运用到等式(4.25)中, 根据 $y\neq 0$ 或 $y=0$ 可得

$$k \leq q\theta_0 + \theta_1 \text{ 或} k \leq q\theta_0 - (q-1)\theta_2.$$

因此, 条件 3b) 不成立.

通过比较等式(4.25)和等式(4.18), 我们有

$$|D_{(y,z)}| = \begin{cases} q^{m-1} + \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\Psi\left((a+\lambda z)D\right) - \Psi(zD), & \text{如果} y\neq 0, \\ q^{m-1} + \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\Psi\left((a+\lambda z)D\right), & \text{如果} y = 0. \end{cases} \quad (4.26)$$

将不等式(4.24)应用到等式(4.26)中, 根据 $y\neq 0$ 或 $y=0$ 可得

$$q^{m-1} + \theta_2 - \theta_1 \leq \theta_0 \text{ 或} q^{m-1} + \theta_2 \leq \theta_0.$$

则条件 3c) 不成立. 从而该结论得证.

综上所述, 我们已经确定推论 4.10的两个条件成立, 因此 $\mathcal{C}(M_D)$ 是极小线性码, 证毕. □

**注 4.13**：现在, 我们对定理 4.12的条件 2) 作进一步的说明. 为了使 $\mathcal{C}(M_D)$ 为极小线性码, $D$ 必须满足对任意的 $y\in\mathbb{F}_q$ 和 $z\in\mathbb{F}_{q^m}^*$, 都有 $|D_{(y,z)}|\geq 1$, 请参阅推论 4.10. 因此, 定理 4.12的条件 2) 对于 $\mathcal{C}(M_D)$ 是极小线性码而言是必要的. 特别地, 由于 $|D_{(y,z)}|\geq 0$, 对于定理 4.12的条件 2), 只需验证 $k\neq\theta_1$ 和 $k\neq -(q-1)\theta_2$ 即可.

**定理 4.14**：采用与定理 4.12相同的符号和定义. 令 $m_1$ 和 $m_2$ 分别为两个限制特征值 $\theta_1$ 和 $\theta_2$ 的重数. 则码 $\mathcal{C}(M_D)$ 的重量分布如表 4.1所示.

表 4.1　码 $\mathcal{C}(M_D)$ 的重量分布

| 重量 | 个数 |
|---|---|
| 0 | 1 |
| $k$ | $q-1$ |
| $q^m-q^{m-1}$ | $q^m-1$ |
| $q^m-q^{m-1}+\theta_1$ | $m_1(q-1)$ |
| $q^m-q^{m-1}+\theta_2$ | $m_2(q-1)$ |

证明. 对于每个 $u \in \mathbb{F}_q$, $v \in \mathbb{F}_{q^m}$, 我们用 $\omega_{u,v}$ 来表示码字 $c(u,v)$ 的重量. 由等式(4.8)和等式 (4.9), 我们可算得

$$\omega_{u,v} =(q^m-1)-|\{x\in D:\, u+\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(vx)=0\}|-|\{x\in \overline{D}:\, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(vx)=0\}|.$$

情况 **1.** 如果 $u=v=0$, 则 $\omega_{0,0}=(q^m-1)-(|D|+|\overline{D}|)=0$, 重量为 0 的码字个数为 1.

情况 **2.** 如果 $u\neq 0$ 且 $v=0$, 则

$$\omega_{u,0}=(q^m-1)-|\overline{D}|=|D|=k,$$

这样的码字的个数为 $q-1$.

情况 **3.** 如果 $u=0$ 且 $v\neq 0$, 则

$$\begin{aligned}\omega_{0,v}&=(q^m-1)-|\{x\in\mathbb{F}_{q^m}^*:\, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(vx)=0\}|\\&=(q^m-1)-(q^{m-1}-1)=q^m-q^{m-1},\end{aligned}$$

这样的码字个数为 $q^m-1$.

情况 **4.** 如果 $u\neq 0$ 且 $v\neq 0$, 我们通过计算可得

$$\begin{aligned}\omega_{u,v}&=(q^m-1)-|D_{(u,v)}|-\left((q^{m-1}-1)-|D_{(0,v)}|\right)\\&=(q^m-q^{m-1})-\frac{1}{q}\left(|D|-\Psi(vD)\right)+\frac{1}{q}\left(|D|+(q-1)\Psi(vD)\right)\\&=q^m-q^{m-1}+\Psi(vD),\end{aligned}$$

回顾一下, 这里 $\Psi$ 是 $\mathbb{F}_{q^m}$ 的标准加法特征. 在情况 4 的第二个等式处我们运用了等式(4.17). 回顾一下, 凯莱图 $\mathrm{Cay}(\mathbb{F}_{q^m},D)$ 的两个限制特征值 $\theta_1$ 和 $\theta_2$ 的重数分别为 $m_1$ 和 $m_2$, 它们在引理 2.3中已经被确定了. 由 2.2小节关于强正则图的描述可知, 对任意的 $v\in\mathbb{F}_{q^m}^*$, $\Psi(vD)=\theta_1$ 或 $\theta_2$, 它们的重数分别为 $m_1$ 或 $m_2$. 由于 $\omega_{u,v}$ 与第一个坐标 $u$ 无关, 我们有

$$\omega_{u,v}=\begin{cases}q^m-q^{m-1}+\theta_1, & \text{个数为}m_1(q-1),\\ q^m-q^{m-1}+\theta_2, & \text{个数为}m_2(q-1),\end{cases}\quad \text{这里}u\in\mathbb{F}_q^*,\, v\in\mathbb{F}_{q^m}^*.$$

综上, 我们确定了码 $\mathcal{C}(M_D)$ 的重量分布, 如表 4.1所示. □

**推论 4.15：**采用与定理4.12相同的符号并假设$\mathcal{C}(M_D)$是极小线性码. 如果$k \in \{q^m - q^{m-1}, q^m - q^{m-1} + \theta_1, q^m - q^{m-1} + \theta_2\}$, 则$\mathcal{C}(M_D)$是三重码; 否则, $\mathcal{C}(M_D)$是四重码.

证明. 我们首先证明$q^m - q^{m-1} + \theta_2 \neq 0$. 取$z \in \mathbb{F}_{q^m}^*$使得$\Psi(zD) = \theta_2$. 由等式(4.17), 我们得到$k = q|D_{(y,z)}| + \theta_2$对所有的$y \in \mathbb{F}_q^*$都成立. 根据注4.13, 定理4.12的条件2)对于$\mathcal{C}(M_D)$是极小码而言是必要条件, 从而我们有$k > -(q-1)\theta_2$. 因此，对每个$y \in \mathbb{F}_q^*$, 有$-\theta_2 < |D_{(y,z)}|$成立. 由等式(4.11)可得$|D_{(y,z)}| \leq q^{m-1}$. 因为$q^m - q^{m-1} \geq q^{m-1}$, 所以得到了我们想要的$q^m - q^{m-1} + \theta_2 \neq 0$.

再结合表4.1可以看出$\mathcal{C}(M_D)$恰有3个非零重量当且仅当$k \in \{q^m - q^{m-1}, q^m - q^{m-1} + \theta_1, q^m - q^{m-1} + \theta_2\}$. 证毕. □

**推论 4.16：**假设定理4.12中的条件1), 2)成立, 且条件3a), 3b), 3c)中的至少一个成立. 如果$k \leq (q-1)^2 q^{m-2}$且集合$D$的特征函数$f_D$是非线性的, 则$\mathcal{C}(M_D)$是一个$[q^m - 1, m+1]$极小线性码且不满足AB条件.

证明. 在本节的开头我们展示了$\mathcal{C}(M_D) = \mathcal{C}(f_D)$, 这里$\mathcal{C}(f_D)$是由等式(4.2)所定义的. 在我们的假设条件下, 由引理4.6和定理4.12可得: $\mathcal{C}(f_D)$是$[q^m - 1, m+1]$极小线性码. 令$\omega_{\min}$和$\omega_{\max}$分别表示$\mathcal{C}(M_D)$的最小和最大的非零重量. 因为$k \leq (q-1)^2 q^{m-2} < q^m - q^{m-1}$, 根据定理4.14, 我们有$\omega_{\min} \leq k < q^m - q^{m-1} \leq \omega_{\max}$. 从而$\frac{\omega_{\min}}{\omega_{\max}} \leq \frac{k}{q^m - q^{m-1}} \leq \frac{q-1}{q}$. 证毕. □

在接下来, 我们将关注拉丁方和负拉丁方型的偏差集, 并考虑由它们得到的极小线性码.

**定理 4.17：**令$p$是素数, $q = p^e$且$\mathbb{F}_{q^m}$为$q^m$个元素的有限域, 它们满足$m \geq 4$, $(m, q) \neq (4, 2)$且2整除$em$. 假设$D \subsetneq \mathbb{F}_{q^m}^*$是一个$\mathbb{F}_q^*$-不变的偏差集, 并且它的参数为

$$(q^m, r(\sqrt{q^m} - \epsilon), \epsilon\sqrt{q^m} + r^2 - 3\epsilon r, r^2 - \epsilon r).$$

当$\epsilon = 1$时, 它是拉丁方型的; 当$\epsilon = -1$时, 它是负拉丁方型的. 令$\mathcal{C}(M_D)$是等式(4.8)中定义的线性码. 如果下列条件之一成立, 则$\mathcal{C}(M_D)$是极小线性码.

1. $\epsilon = 1, r \neq \sqrt{q^m}$且$r > 1$;

2. $\epsilon = -1, r \neq \sqrt{q^m} - 1$且$r > \frac{(q-1)\sqrt{q^m}}{\sqrt{q^m} + q}$.

证明. 根据引理 2.3, 图 Cay$(\mathbb{F}_{q^m}, D)$ 的特征值如下:

$$\begin{aligned} k &= r(\sqrt{q^m}-\epsilon), \\ \theta_1 &= \frac{1}{2}\left(\epsilon\sqrt{q^m}-2\epsilon r+\sqrt{q^m}\right), \\ \theta_2 &= \frac{1}{2}\left(\epsilon\sqrt{q^m}-2\epsilon r-\sqrt{q^m}\right). \end{aligned} \tag{4.27}$$

回顾一下, 我们设 $\theta_0 = \max\{|\theta_1|, |\theta_2|\}$. 在这种情形下, 我们有

$$\theta_0 = \frac{1}{2}\left(|\sqrt{q^m}-2r|+\sqrt{q^m}\right). \tag{4.28}$$

现在我们证明, 在我们的假设下, 定理 4.12的三个条件 1), 2) 和 3c) 成立.

步骤 **1:** 我们首先证明 $k-\theta_2 \neq q^m$ 成立. 经计算得

$$\begin{aligned} k-\theta_2-q^m &= r\sqrt{q^m}+\frac{1}{2}(1-\epsilon)\sqrt{q^m}-q^m \\ &= \sqrt{q^m}\left(r+\frac{1}{2}(1-\epsilon)-\sqrt{q^m}\right). \end{aligned}$$

很容易看出在 $\epsilon=1$ 或 $-1$ 两种情况下, 该值都是非零的.

步骤 **2:** 接下来我们证明 $k>\theta_1$ 和 $k>-(q-1)\theta_2$ 成立. 经计算, 我们有

$$k-\theta_1 = \left(r-\frac{1}{2}\epsilon-\frac{1}{2}\right)\sqrt{q^m} = \begin{cases} (r-1)\sqrt{q^m}, & \text{当}\epsilon=1\text{时}, \\ r\sqrt{q^m}, & \text{当}\epsilon=-1\text{时}. \end{cases}$$

和

$$\begin{aligned} k+(q-1)\theta_2 &= r(\sqrt{q^m}-\epsilon)+\frac{q-1}{2}(\epsilon\sqrt{q^m}-2\epsilon r-\sqrt{q^m}) \\ &= \begin{cases} r(\sqrt{q^m}-q), & \text{当}\epsilon=1\text{时}, \\ r(\sqrt{q^m}+q)-\sqrt{q^m}(q-1), & \text{当}\epsilon=-1\text{时}. \end{cases} \end{aligned}$$

可直接验证在我们的假设下, 这两个值均为正数.

步骤 **3:** 最后, 我们证明 $q^{m-1}+\theta_2-\theta_1-\theta_0>0$. 由等式 (4.27), 我们推得 $\theta_1-\theta_2=\sqrt{q^m}$. 再结合等式 (4.28), 我们有

$$\begin{aligned} q^{m-1}+\theta_2-\theta_1-\theta_0 &= q^{m-1}-\sqrt{q^m}-\frac{1}{2}(|\sqrt{q^m}-2r|+\sqrt{q^m}) \\ &= \begin{cases} q^{m-1}-2\sqrt{q^m}+r, & \text{如果 } \sqrt{q^m}\geq 2r; \\ q^{m-1}-\sqrt{q^m}-r, & \text{否则}. \end{cases} \end{aligned}$$

由于 $D$ 是 $\mathbb{F}_{q^m}^*$ 的一个真子集, 我们有 $0<k<q^m-1$, 则 $0<r<\sqrt{q^m}+\epsilon$. 再由 $m\geq 4$ 可得 $q^{m-1}-2\sqrt{q^m}+r>0$. 因为 $r<\sqrt{q^m}+\epsilon\leq\sqrt{q^m}+1$, 根据 $(m,q)\neq(4,2)$

的假设, 我们有 $q^{m-1}-\sqrt{q^m}-r>q^{m-1}-2\sqrt{q^m}-1>0$. 从而定理 4.12的条件 3c) 成立.

综上, 我们证明了定理 4.12中的条件 1), 2) 和 3c) 在我们的假设下成立, 由定理 4.12可知, 码 $\mathcal{C}(M_D)$ 是极小的. □

**定理 4.18:** 令 $p$ 是素数, $q=p^e, \mathbb{F}_{q^m}$ 为 $q^m$ 个元素的有限域, 它们满足 $m\geq 4, (m,q)\neq(4,2)$ 且 2 整除 $em$. 采用与引理 2.6相同的符号, 取大小为 $u$ 的真子集 $J\subset\mathbb{Z}_N$. 如果 $q$ 是奇数, 我们进一步假设 $N|\frac{q^m-1}{2}$ 并且 $J+\frac{q^m-1}{2}=J(\text{mod } N)$. 令 $D=\bigcup_{j\in J}C_j$, 令 $\mathcal{C}(M_D)$ 是等式(4.8)所定义的线性码, 其中 $M_D$ 由等式(4.9)给出. 如果 $J$ 在映射 $\rho: j\to j+\frac{q^m-1}{q-1}\ (\text{mod } N)$ 下是不变的, 且下列条件之一成立, 则 $\mathcal{C}(M_D)$ 是极小线性码.

1. $t$ 是奇数, $u\neq\frac{\sqrt{q^m}N}{\sqrt{q^m}+1}$ 且 $u>\frac{N}{\sqrt{q^m}+1}$;
2. $t$ 是偶数, $u>\frac{(q-1)\sqrt{q^m}N}{(\sqrt{q^m}+q)(\sqrt{q^m}-1)}$.

证明. 由引理 2.6可知, 强正则凯莱图 $\text{Cay}(\mathbb{F}_{q^m}, D)$ 的参数为

$$(q^m, r(\sqrt{q^m}-\epsilon), \epsilon\sqrt{q^m}+r^2-3\epsilon r, r^2-\epsilon r),$$

这里 $\epsilon=(-1)^{t+1}$ 且 $r=\frac{u}{N}(\sqrt{q^m}+\epsilon)$. 当 $t$ 是奇数时, 它是拉丁型的; 当 $t$ 是偶数时, 它是负拉丁型的. 由于 $J$ 在 $\rho$ 下是不变的, 根据引理 2.7可知: $D$ 是 $\mathbb{F}_q^*$-不变的. 则由定理 4.17可得该结论成立. □

**注 4.19:** 在定理 4.18中, 我们考虑 $m$ 是偶数且 $t$ 是奇数的情形. 在该情形下, $\sqrt{q^m}=p^{\ell_1 t}\equiv -1(\text{mod } N)$, 从而 $N|(\sqrt{q^m}+1)$. 由于 $\frac{q^m-1}{q-1}=\frac{\sqrt{q^m}-1}{q-1}\cdot(\sqrt{q^m}+1)$, 则有 $N|\frac{q^m-1}{q-1}$. 进而有 $\mathbb{Z}_N$ 的任一子集 $J$ 在映射 $\rho: j\to j+\frac{q^m-1}{q-1}\ (\text{mod } N)$ 下都是不变的. 由引理 2.7可知, $D$ 是 $\mathbb{F}_q^*$-不变的. 如果 $q$ 是奇数, 那么在上述定理中的条件 $N|\frac{q^m-1}{2}$ 和 $J+\frac{q^m-1}{2}\equiv J(\text{mod } N)$ 自动成立. 因此, 在定理 4.18中, 集合 $J$ 在该情况下只需满足 $|J|\neq\frac{\sqrt{q^m}N}{\sqrt{q^m}+1}$ 且 $|J|>\frac{N}{\sqrt{q^m}+1}$ 即可. 因为 $N|(\sqrt{q^m}+1)$, 我们有 $\frac{N}{\sqrt{q^m}+1}\leq 1$, 若 $|J|>1$, 就有条件 $|J|>\frac{N}{\sqrt{q^m}+1}$ 成立. 因此, 这种构造可得到许多极小线性码.

由定理 2.4可知有限极空间 $H(2r,q^2)$, $Q^-(2r-1,q)$ 和 $W(2r-1,q)$ 中的 $m$-ovoids 会产生负拉丁型强正则图, 其参数为 $(u^2, s(u+1), -u+s^2+3s, s^2+s)$. 当 $\mathcal{P}=H(2r,q^2), Q^-(2r-1,q)$ 或 $W(2r-1,q)$ 时, 分别有 $(u,s)=(q^{2r+1}, m(q^2-1)), (q^r, m(q-1))$ 或 $(q^r, m(q-1))$. 由于定理 4.17的条件较为宽松, 我们可以选取适当的 $r$, $q$ 和

$m$, 有很多 $H(2r,q^2)$, $Q^-(2r-1,q)$ 和 $W(2r-1,q)$ 中的 $m$-ovoids 可以用来进行极小线性码的构造, 可以参考文献[5–7,23,25,36] 等对这 3 类有限极空间中的 $m$-ovoids 的构造. 同样地, 由定理 2.5可知, 有限极空间 $H(2r-1,q^2)$, $Q^+(2r-1,q)$ 和 $W(2r-1,q)$ 中的 $i$-tight sets 会产生拉丁型强正则图, 其参数为 $(u^2,s(u-1),u+s^2-3s,s^2-s)$, 这里当 $\mathcal{P}=H(2r-1,q^2)$, $Q^+(2r-1,q)$ 或 $W(2r-1,q)$ 时, 分别有 $(u,s)=(q^{2r},i)$, $(q^r,i)$ 或 $(q^r,i)$. 同样根据定理 4.17, 我们可以选取适当的 $r$, $q$ 和 $i$, 有很多 $H(2r,q^2)$, $Q^-(2r-1,q)$ 和 $W(2r-1,q)$ 中的 $i$-tight sets 可以用来构造极小线性码, 可以参考文献[6,7,23,25,32,33,60,61] 等对这 3 类有限极空间中的 $i$-tight sets 的构造.

文献[12] 的作者提出了一种有效的方法, 可以根据引理 4.3, 通过向量切块集来得到极小线性码. 但是引理 4.3的条件 1) 对于线性码的极小性而言不是必要条件. 下列由定理 4.18得到的例子说明存在极小线性码 $\mathcal{C}(f_D)$ 使得 $\overline{D}$ 不是向量切块集. 从而说明了, 定理 4.18的构造不能被切块集的构造方法所涵盖.

**例 4.20：** 令 $p=2$, $e=2$, $q=p^e=4$, $m=4$. 设 $\gamma$ 是 $\mathbb{F}_{4^4}$ 的一个本原元. 取 $\ell_1=2$ 和 $N=p^{\ell_1}+1$, 则 $C_i=\{\gamma^{jN+i}:0\le j\le \frac{q^m-1}{N}-1\}$ 对于 $0\le i\le N-1$. 我们设 $J=\mathbb{Z}_N\setminus\{0\}$ 且 $D=D_J=\bigcup_{j\in J}C_j$. 则有 $\overline{D}=C_0$. 令 $\mathcal{C}(M_D)$ 是由等式(4.8)定义的线性码, 其中 $M_D$ 由等式(4.9)所给出. 经计算可得 $N=p^{\ell_1}+1=5$ 和 $t=em/(2\ell_1)=2$. 因为 $N$ 整除 $\frac{q^m-1}{q-1}$, 再根据引理 2.6和引理 2.7, 我们有 $D$ 是一个 $\mathbb{F}_q^*$-不变的偏差集. 由引理 4.7可知函数 $f_D$ 是非线性的. 可直接验证 $u=4>\frac{(q-1)\sqrt{q^m}N}{(\sqrt{q^m}+q)(\sqrt{q^m}-1)}$, $k=204$, $\theta_1=12$ 且 $\theta_2=-4$. 根据定理 4.18, 我们有 $\mathcal{C}(M_D)$ 是一个 $[255,5]$ 极小线性码. 容易验证 $q^m-q^{m-1}+\theta_1=k$, 由推论 4.15可知, $\mathcal{C}(M_D)$ 是一个三重码. 现考虑两个过原点的仿射超平面 $H_1=\{x\in\mathbb{F}_{4^4}:\mathrm{Tr}_{\mathbb{F}_{4^4}/\mathbb{F}_4}(x)=0\}$ 和 $H_2=\{x\in\mathbb{F}_{4^4}:\mathrm{Tr}_{\mathbb{F}_{4^4}/\mathbb{F}_4}(\gamma^7x)=0\}$. 通过计算可得 $\overline{D}\cap H_1=\{1,\gamma^{170},\gamma^{85}\}$ 和 $\overline{D}\cap H_2=\{1,\gamma^{170},\gamma^{85},\gamma^{190},\gamma^{20},\gamma^{105},\gamma^{145},\gamma^{230},\gamma^{60},\gamma^{180},\gamma^{10},\gamma^{95},\gamma^{45},\gamma^{130},\gamma^{215}\}$. 可以看出 $\overline{D}\cap H_1\subseteq\overline{D}\cap H_2$, 因此 $\overline{D}$ 不是 $(1,3)$-向量切块集.

关于 $\mathbb{F}_q^*$-不变的偏差集, 有许多的构造. 在表 4.2中, 我们列出了 5 个具体的例子, 这几个例子来自文献[64] 的表 1. 关于更多构造, 请参阅文献[34,37,39,53,62,64].

**例 4.21：** 令 $N$ 是 $q^m-1$ 的一个真因子, $\gamma$ 是 $\mathbb{F}_{q^m}$ 的一个给定的本原元, 设 $D=\{\gamma^{iN}:0\le i\le\frac{q^m-1}{N}-1\}$. 我们考虑表 4.2的每个例子. 很容易验证在每个例子中都有 $N|\frac{q^m-1}{q-1}$, 由引理 2.7可得 $D$ 是 $\mathbb{F}_q^*$-不变的. 根据引理 4.7可知, 特征函数 $f_D$ 是非线性的. 在表 4.2 的每个例子中, 我们验证定理 4.12的条件 1), 2), 3$a$) 成立, 从而每个例子对应的码 $\mathcal{C}(M_D)$ 是一个 $[q^m-1,m+1]$ 极小线性码. 在每个例子中, 我们验证

了 $k \le (q-1)^2 q^{m-2}$ 且 $k \notin \{q^m - q^{m-1},\, q^m - q^{m-1} + \theta_1,\, q^m - q^{m-1} + \theta_2\}$, 则由推论 4.15可知 $\mathcal{C}(M_D)$ 有四个非零重量; 由推论 4.16可知 $\mathcal{C}(M_D)$ 不满足 AB 条件.

根据文献[64], 在表 4.2的第一行, 我们有 $D = \{\gamma^{11i} : 0 \le i \le \frac{3^5-1}{11} - 1\}$, 这里 $\gamma$ 是 $\mathbb{F}_{3^5}$ 的一个给定的本原元. 设 $\overline{D} := \mathbb{F}_{q^m}^* \setminus D$, 它是 $\mathbb{F}_3^*$-不变的. 图 Cay$(\mathbb{F}_{q^m}, \overline{D})$ 的特征值分别为 $k = 220, \theta_1 = 4, \theta_2 = -5$. 由引理 4.7可知, 函数 $f_{\overline{D}}$ 是非线性的. 对于 $\overline{D}$, 我们验证了定理 4.12的条件 1), 2), 3b) 成立. 因此, $\mathcal{C}(M_{\overline{D}})$ 是一个 $[3^5 - 1, 6]$ 极小线性码. 我们还检验了 $k \notin \{q^m - q^{m-1},\, q^m - q^{m-1} + \theta_1,\, q^m - q^{m-1} + \theta_2\}$, 从而由推论 4.15得到 $\mathcal{C}(M_{\overline{D}})$ 有四个非零重量. 通过 Magma[13], 我们检验了 $D$ 不是一个 $(1, 4)$-向量切块集. 因此, 码 $\mathcal{C}(M_{\overline{D}})$ 并不是由引理 4.3得到.

表 4.2　一些偏差集 $D$ 的例子和 Cay$(\mathbb{F}_{q^m}, D)$ 的特征值

| No. | $q$ | $m$ | $N$ | $k$ | $\theta_1$ | $\theta_2$ |
|---|---|---|---|---|---|---|
| 1 | 3 | 5 | 11 | 22 | 4 | -5 |
| 2 | 5 | 9 | 19 | 102796 | 296 | -329 |
| 3 | 3 | 12 | 35 | 15184 | 118 | -125 |
| 4 | 7 | 9 | 37 | 1090638 | 584 | -1817 |
| 5 | 11 | 7 | 43 | 453190 | 650 | -681 |

### 4.3.3　码 $\mathcal{C}(M_D)$ 的自同构群

令 $D$ 是 $\mathbb{F}_{q^m}$ 的一个 $\mathbb{F}_q^*$-不变的真子集. 集合 $D$ 的自同构 (automorphism) 是 $\mathbb{F}_{q^m}$ 的一个 $\mathbb{F}_q$-线性变换 $g$ 使得 $g$ 是双射且保持集合 $D$ 不变, 即, $\{g(x) : x \in D\} = D$. 我们令 Aut$(D)$ 表示 $D$ 的所有自同构所构成的集合. 对于每个 $g \in$ Aut$(D)$ 和 $c(u, v) \in \mathcal{C}(M_D)$, 我们定义

$$c(u, v)^g := \big(u f_D(g(x)) + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(v g(x))\big)_{x \in \mathbb{F}_{q^m}^*}.$$

因为 $g \in$ Aut$(D)$, 我们有 $f_D(g(x)) = f_D(x)$ 对每个 $x \in \mathbb{F}_{q^m}^*$ 都成立. 回顾一下 $g$ 可以被看作 $\mathbb{F}_{q^m}$ 上的一个约化 $q$-多项式, 参考 4.2节. 取 $\tilde{g}$ 为 $g$ 的迹对偶. 从而 $c(u, v)^g = c(u, \tilde{g}(v))$. 很容易验证 $\tilde{g}$ 也是一个 $\mathbb{F}_{q^m}$ 上的 $\mathbb{F}_q$-线性变换, 且其为双射. 因此, $g$ 诱导了码 $\mathcal{C}(M_D)$ 的一个自同构.

当 |Aut$(D)$| 很大的情形, 所得到的码 $\mathcal{C}(M_D)$ 也会拥有一个大的自同构群. 因此, 在这种情况下 $\mathcal{C}(M_D)$ 可能具有快速的译码算法. 下面是一个示例, 其中 $D$ 拥有较大的自同构群, 并且对应的码 $\mathcal{C}(M_D)$ 是极小线性码.

**例 4.22：** 令 $Q : \mathbb{F}_q^m \to \mathbb{F}_q$ 是一个非退化的二次型使得 $m \ge 4$ 为偶数, $q = p^h$ 且 $(m, q) \ne (4, 2)$. 由文献[53] 的定理 2.6 可知, $D = \{\mathbf{x} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\} : Q(\mathbf{x}) = 0\}$ 是一个参数为 $(q^m, s(\sqrt{q^m} - \epsilon), \epsilon\sqrt{q^m} + s^2 - 3\epsilon s, s^2 - \epsilon s)$ 的 $\mathbb{F}_q^*$-不变偏差集. 如果

$Q$ 定义的是一个双曲二次曲面, 则 $\epsilon = 1$, $s = q^{m/2-1} + 1$ 并且 $D$ 是一个拉丁方型的偏差集. 在这种情况下, $D$ 的自同构群是 $\Gamma\mathrm{O}^+(m,q)$, 由注 2.9可知, 它的阶为 $2hq^{m(m-2)/4}(q-1)\Pi_{i=1}^{m/2}(q^{2i}-1)$; 如果 $Q$ 定义的是一个椭圆二次曲面, 则 $\epsilon = -1$, $s = q^{m/2-1} - 1$ 并且 $D$ 是一个负拉丁方型的偏差集. 在这种情况下, $D$ 的自同构群是 $\Gamma\mathrm{O}^-(m,q)$, 由注 2.9可知, 它的阶为 $2hq^{m(m-2)/4}(q-1)(q^{m/2}+1)\Pi_{i=1}^{m/2-1}(q^{2i}-1)$. 在这两种情形下, 由定理 4.17可知码 $\mathcal{C}(M_D)$ 是极小的.

## 4.4 极小线性码和秘密共享方案

在文献[54] 和文献[55] 中, Massey 证明了极小线性码可以用于构建秘密共享方案 (secret sharing scheme). 后来，Yuan 和 Ding 在文献[80] 中对基于线性码的秘密共享方案进行了更详细的描述, 我们将在下面进行简要介绍. 令 $\mathcal{C}$ 是一个 $[n,k,d;q]$ 线性码, 它的生成矩阵为 $G = (g_1, g_2, \ldots, g_n)$. 秘密 $s$ 是 $\mathbb{F}_q$ 中的一个元素. 在该方案中, 共有 $n-1$ 个参与者 $P_2, \ldots, P_n$ 和一个值得信赖的人作为分发者. 分发者随机选取一个向量 $\mathbf{u} \in \mathbb{F}_q^k$ 使得 $s = t_1 = \mathbf{u}g_1$, 并计算向量 $\mathbf{t} = (t_1, t_2, \ldots, t_n) = \mathbf{u}G$. 对于 $i \geq 2$, 分发者将每个 $t_i$ 分配给参与者 $P_i$ 作为共享. 我们称该方案为基于码 $\mathcal{C}$ 的秘密共享方案. 在这个方案中, 秘密 $s = t_1 = \mathbf{u}g_1$, 那么一个共享的集合 $\{t_{i_1}, t_{i_2}, \ldots, t_{i_\ell}\}$, 这里 $2 \leq i_1 < i_2 < \ldots < i_\ell \leq n$ 能够确定出这个秘密当且仅当 $g_1$ 是 $g_{i_1}, g_{i_2}, \ldots, g_{i_\ell}$ 的线性组合. 因此, 一个参与者的集合 $P = \{P_{i_1}, P_{i_2}, \ldots, P_{i_\ell}\}$, 这里 $2 \leq i_1 < i_2 < \ldots < i_\ell \leq n$ 能够确定出秘密当且仅当在对偶码 $\mathcal{C}^\perp$ 中存在码字 $(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_\ell}, 0, \ldots, 0)$. 详情请参阅文献[80] 中的命题 1 或文献[54]. 如果一组参与者中的所有参与者可以使用其共享恢复秘密, 但是任何该组参与者的真子集都无法恢复秘密, 则称该组参与者为最小访问集 (minimal access set). 显然, 如果 $\mathcal{C}^\perp$ 是极小线性码, 则最小访问集的集合与 $\mathcal{C}^\perp$ 中的第一个坐标为 1 的码字集之间存在一一对应关系. 如果每 $t$ ($t \geq 1$) 个参与者构成的组都具有相同数量的最小访问集, 则称该秘密共享方案为 $t$ 度民主 (democratic of degree $t$).

接下来, 我们考虑基于 $\mathcal{C}(M_D)^\perp$ 的秘密共享方案, 这里 $\mathcal{C}(M_D)$ 是 4.3节中得到的 $[q^m-1, m+1]$ 极小线性码. 这样的秘密共享方案有许多有趣的结构, 请参考文献[80] 的命题 2. 回顾一下, 码 $\mathcal{C}(M_D) = \mathcal{C}(f_D)$, 且 $\mathcal{C}(M_D)$ 的码字由 $c(u,v) = (H(x_j))_{j=1,\ldots,q^m-1}$ 给出, 这里 $H(x) = uf_D(x) + \mathrm{Tr}_{q^m/q}(vx)$ 且 $x_1, \cdots, x_{q^m-1}$ 是 $\mathbb{F}_{q^m}^*$ 中元素的有序集. 令 $P_i$ 是与由 $x_i, 2 \leq i \leq q^m - 1$ 标记的坐标相对应的参与者. 由上一段的内容可知, 最小访问集的数量 (即 $\mathcal{C}(M_D)$ 中使得 $H(x_1) = 1$ 的极小码字的数量) 为 $(q^{m+1} - q^m)/(q-1) = q^m$. 参与者 $P_i$ ($i \geq 2$) 所在的最小访问集的数量为

$$N_{x_i} = |\{(u,v) \in V : H(x_1) = 1, H(x_i) \neq 0\}|.$$

通过基本的线性代数计算, 我们得到

$$N_{x_i}=\begin{cases} q^m, \text{ 如果} x_1\in\overline{D},\ x_i\in\{ax_1: a\in\mathbb{F}_q^*\},\\ q^m-q^{m-1}, \text{否则}. \end{cases}$$

例如, 在 $x_1\in\overline{D}$ 和 $x_i\in\{ax_1: a\in\mathbb{F}_q^*\}$ 对于某个 $2\le i\le q^m-1$ 成立的情况下, 我们有 $N_{x_i}=|\{(u,v)\in V: \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(vx_1)=1\}|=q\cdot q^{m-1}=q^m$. 在其他情况下, 与该计算方法类似, 因此我们在这里省略细节. 事实上, 关于 $N_{x_i}$ 的结果与文献[80] 的命题 2 一致, 主要步骤是检验在哪种情况下 $(f_D(x_1),x_1)$ 和 $(f_D(x_i),x_i)$ 是 $\mathbb{F}_q$-线性相关的.

根据 $x_1$ 的选取, $\mathcal{C}(M_D)^\perp$ 会产生两种可能的方案类型. 如果我们取 $x_1\in\overline{D}$, 则满足 $x_i=ax_1$ 对某个 $a\in\mathbb{F}_q^*$ 成立的相应参与者 $P_i$ 会出现在每个最小访问集中, 这种参与者称为独裁者 (dictatorial). 这种方案在老板必须参与每个决策的情况下是很有效的. 如果我们选取 $x_1\in D$, 则在此方案中, 每个参与者 $P_i$, $2\le i\le q^m-1$ 位于 $q^m-q^{m-1}$ 个最小访问权限集中. 这样的方案是度至少为 1 的民主方案.

## 4.5 小结

在本节中, 我们介绍了由 $\mathbb{F}_q^*$-不变的偏差集得到极小线性码的一般性构造, 并研究了它们的性质. 我们的构造得到了许多不满足 AB 条件的极小线性码和一些不是通过切块集得到的极小线性码的例子. 我们还表明, 偏差集的自同构会引起相应的极小线性码的自同构. 在集合具有较大的自同构群的情况下, 相应的码也将具有较大的自同构群, 因此可能具有快速的译码算法. 最后, 我们根据我们得到的线性码的对偶码来考虑相应的秘密共享方案的性质.

# 5 讨论与展望

本章简要介绍一下作者在攻读博士学位期间的其它工作, 并列出与本文工作相关的一些展望和进一步可行的问题.

**LCD 码的构造**

一个线性码和其对偶码的交称为该码的包 (hull). 在确定线性码自同构群的计算复杂性方面, 包起着十分重要的作用[70]. 如果一个线性码的包的维数是 0, 则称该码为线性互补对偶码 (LCD 码). LCD 码被广泛应用于通信系统, 密码学, 数据存储等领域. 关于 LCD 码的构造和讨论的工作, 请参阅文献[19–21,49,50,57,65,71]. 我们关于这方面的工作主要是利用结合方案的工具对 LCD 码进行构造. 对于很多特定的结合方案, 如分圆结合方案, 它的第一特征矩阵 (first eigenmatrix) 已经由文献[10] 给出, 则对应 Bose-Mesner 代数中的矩阵的特征值也很容易计算, 从而可以利用其来进行 LCD 码的构造. 我们利用分圆结合方案得到的 LCD 码的构造结果推广了文献[19] 中通过计算高斯周期得出的 LCD 码的构造. 该部分成果被期刊《Advances in Mathematics of Communications》录用.

**Intriguing Sets 的构造**

在第 3章中, 我们对 $q \equiv 1 (\mathrm{mod}\ 4)$ 且 $q > 5$ 构造了 $Q(4,q)$ 的 $\frac{q-1}{2}$-ovoids 的无穷类. 而群 $\mathrm{PGO}(5,q)$ 有着丰富的子群结构, 在 $q$ 比较小的时候我们借助 Magma 得到了大量的例子, 如果可以将其中的一些例子推广成新参数的无穷类, 那将会是很有趣的结果. 此外, 在厄尔米特有限极空间 $H(n-1,q^2)$ 中, 我们运用 Singer 群的作用也得到了一些 $m$-ovoids 的例子, 能够利用这类群得到厄尔米特空间中新参数的 $m$-ovoids 的无穷类是值得挑战和研究的问题.

关于 $i$-tight sets, 最具典型的构造是双曲二次曲面 $Q^+(5,q)$ 中的 $i$-tight sets, 在克莱因对应法则下, $Q^+(5,q)$ 中的 $i$-tight set 与 $\mathrm{PG}(3,q)$ 上的 Cameron-Liebler 线有着一一对应关系. 关于这方面的构造性工作请参考文献[16,26,28,32,33] 等, 其中大部分结果都是利用典型群的子群作用在 $Q^+(5,q)$ 的点上得到的轨道所构造出的.

在高维情形下已知的 intriguing sets 的构造比较少, 比较典型的例子包括: 利用超平面进行的构造, 可参见文献[6] 的引理 7, 该种构造所对应的自同构群是可约子群 (reducible subgroups), 详见文献[46] 的 4.1 节; 利用域的扩张得到的构造[44], 该种构造所对应的自同构群是域扩张子群 (field extension subgroups), 详见文献[46] 的 4.3 节; 近期, 在文献[36] 中, 作者利用强正则图的方法得到了高维情形 $W(n-1,q)$ 中的 $m$-ovoids 的一些构造, 这篇文章中所用的群大多是可解群. 一般而言, 对于高维情形的

有限极空间, 点的个数太多, 而且典型群的阶非常大，受计算能力的影响, Magma 的搜索范围十分受限, 不能提供很多的例子. 所以在这种情况下, 从群的结构角度来分析并给出 intriguing sets 的无穷类的构造将会是很有意义的工作. 由于高维情形下, 对应的有限典型群有着丰富的子群结构, 同时也有着很多的对应不同类型自同构群的 intriguing sets. 而探索 intriguing sets 的代数表示和自同构群之间的联系可便于我们更好的去理解典型群的子群结构及相应的几何构型之间的联系, 这个工作是非常有意义而且十分有趣的.

**Intriguing Sets 的分类**

因为有限极空间中存在大量的 intriguing sets 的例子, 包括 $m$-ovoids 和 $i$-tight sets. 因此, 想要进行完全分类是非常困难的. 结合文献[7],[35] 和本文第 3.1节的结论可以知道, 对于每个奇素数幂 $q$, $Q(4,q)$ 中都存在 $\frac{q-1}{2}$-ovoids. 但对于 $q$ 是奇数时, 除 $\frac{q-1}{2}$ 和 $\frac{q+1}{2}$ 外, 其余参数的分类现在看来还是遥不可及. 最典型的情形之一, $Q(4,q)$ 中的 ovoid 的分类问题几十年都没有得到完全的解决. 此外, 正如 Bamberg 等人在文献[6] 中提到的一样, 当 $q>5$ 时, $Q(4,q)$ 中是否存在 2-ovoids 的无穷类仍然是未知的. 由此可见, 在更高维数的有限极空间的 $m$-ovoids 的分类工作是十分繁琐复杂的. 关于有限极空间中的 $i$-tight sets, 很显然有限极空间中的每个极大完全迷向或极大完全奇异子空间都是一个 1-tight set. 近些年, Klaus 和 Gavrilyuk 等人对 $Q^+(5,q)$ 中的 $i$-tight sets 的参数 $i$ 给出了具体的限制条件, 很大程度上推进了 $Q^+(5,q)$ 中 $i$-tight sets 的分类工作, 详情可参阅文献[38,58,59] 等. 此外, 他们对其他有限极空间中小参数的 tight sets 也做出了杰出的分类和构造工作, 具体请参阅文献[11,60,61] 等. 但对于高维情形参数较大的 tight sets 的分类还尚未有很好的结论. 需要特别提及的是, Aschbacher 在文献[1] 中给出了关于典型群的重要分类结论. 他证明了, 一个典型群的子群要么落在八类用几何方法定义的子群 $C_1-C_8$ 中, 要么是几乎单群 (almost simple group). Aschbacher 和有限单群的分类结果, 可以为我们从自同构群的角度分类 intriguing sets 奠定一个非常好的理论基础, 这也是我们下一阶段将要重点研究的问题.

其它在研工作目前仍处于初步阶段, 这里就不作介绍.

# 参考文献


[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[2] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inform. Theory*, 44(5):2010–2017, 1998.

[3] H. Bäärnhielm. Recognising the small Ree groups in their natural representations. *J. Algebra*, 416:139–166, 2014.

[4] S. Ball. *Finite geometry and combinatorial applications*, volume 82 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2015.

[5] J. Bamberg, M. Giudici, and G. F. Royle. Every flock generalized quadrangle has a hemisystem. *Bull. Lond. Math. Soc.*, 42(5):795–810, 2010.

[6] J. Bamberg, S. Kelly, M. Law, and T. Penttila. Tight sets and $m$-ovoids of finite polar spaces. *J. Combin. Theory Ser. A*, 114(7):1293–1314, 2007.

[7] J. Bamberg, M. Law, and T. Penttila. Tight sets and $m$-ovoids of generalised quadrangles. *Combinatorica*, 29(1):1–17, 2009.

[8] J. Bamberg, M. Lee, K. Momihara, and Q. Xiang. A new infinite family of hemisystems of the Hermitian surface. *Combinatorica*, 38(1):43–66, 2018.

[9] D. Bartoli and M. Bonini. Minimal linear codes in odd characteristic. *IEEE Trans. Inform. Theory*, 65(7):4152–4155, 2019.

[10] L. D. Baumert, W. H. Mills, and R. L. Ward. Uniform cyclotomy. *J. Number Theory*, 14(1):67–82, 1982.

[11] L. Beukemann and K. Metsch. Small tight sets of hyperbolic quadrics. *Des. Codes Cryptogr.*, 68(1-3):11–24, 2013.

[12] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *J. Algebr. Combin.*, 53(2):327–341, 2021.

[13] W. Bosma, J. Cannon, C Fieker, and et al. *Handbook of Magma Functions*. 2013.

[14] A.E. Brouwer and W.H. Haemers. *Spectra of graphs*. Universitext. Springer, New York, 2012.

[15] A.E. Brouwer, R.M. Wilson, and Q. Xiang. Cyclotomy and strongly regular graphs. *J. Algebr. Combin.*, 10(1):25–28, 1999.

[16] A. A. Bruen and Keldon Drudge. The construction of Cameron-Liebler line classes in PG$(3, q)$. *Finite Fields Appl.*, 5(1):35–45, 1999.

[17] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 18(2):97–122, 1986.

[18] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Trans. Inform. Theory*, 51(6):2089–2102, 2005.

[19] C. Carlet, C. Li, and S. Mesnager. Linear codes with small hulls in semi-primitive case. *Des. Codes Cryptogr.*, 87(12):3063–3075, 2019.

[20] C. Carlet, S. Mesnager, C. Tang, and Y. Qi. New characterization and parametrization of LCD codes. *IEEE Trans. Inform. Theory*, 65(1):39–49, 2019.

[21] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. *IEEE Trans. Inform. Theory*, 64(4, part 2):3010–3017, 2018.

[22] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In *Information security and cryptology—ICISC 2013*, volume 8565 of *Lecture Notes in Comput. Sci.*, pages 34–46. Springer, Cham, 2014.

[23] A. Cossidente, C. Culbert, G. L. Ebert, and G. Marino. On $m$-ovoids of $W_3(q)$. *Finite Fields Appl.*, 14(1):76–84, 2008.

[24] A. Cossidente and F. Pavese. Intriguing sets of quadrics in PG$(5, q)$. *Adv. Geom.*, 17(3):339–345, 2017.

[25] A. Cossidente and F. Pavese. On intriguing sets of finite symplectic spaces. *Des. Codes Cryptogr.*, 86(5):1161–1174, 2018.

[26] A. Cossidente and F. Pavese. Cameron-Liebler line classes of PG$(3, q)$ admitting PGL$(2, q)$. *J. Combin. Theory Ser. A*, 167:104–120, 2019.

[27] A. Cossidente and T. Penttila. Hemisystems on the Hermitian surface. *J. London Math. Soc. (2)*, 72(3):731–741, 2005.

[28] J. De Beule, J. Demeyer, K. Metsch, and M. Rodgers. A new family of tight sets in $\mathcal{Q}^+(5, q)$. *Des. Codes Cryptogr.*, 78(3):655–678, 2016.

[29] L.E. Dickson. *Linear groups: With an exposition of the Galois field theory*. Teubner, 1901.

[30] C. Ding, Z. Heng, and Z. Zhou. Minimal binary linear codes. *IEEE Trans. Inform. Theory*, 64(10):6536–6545, 2018.

[31] K. W. Drudge. *Extremal sets in projective and polar spaces*. ProQuest LLC, Ann Arbor, MI, 1998. Thesis (Ph.D.)–The University of Western Ontario (Canada).

[32] T. Feng, K. Momihara, M. Rodgers, Q. Xiang, and H. Zou. Cameron-liebler line classes with parameter $x = \frac{(q+1)^2}{3}$. *arXiv preprint arXiv:2006.14206*, 2020.

[33] T. Feng, K. Momihara, and Q. Xiang. Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$. *J. Combin. Theory Ser. A*, 133:307–338, 2015.

[34] T. Feng, K. Momihara, and Q. Xiang. Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes. *Combinatorica*, 35(4):413–434, 2015.

[35] T. Feng, K. Momihara, and Q. Xiang. A family of $m$-ovoids of parabolic quadrics. *J. Combin. Theory Ser. A*, 140:97–111, 2016.

[36] T. Feng, Y. Wang, and Q. Xiang. On $m$-ovoids of symplectic polar spaces. *J. Combin. Theory Ser. A*, 175:105279, 14, 2020.

[37] T. Feng and Q. Xiang. Strongly regular graphs from unions of cyclotomic classes. *J. Combin. Theory Ser. B*, 102(4):982–995, 2012.

[38] A. L. Gavrilyuk and K. Metsch. A modular equality for Cameron-Liebler line classes. *J. Combin. Theory Ser. A*, 127:224–242, 2014.

[39] G. Ge, Q. Xiang, and T. Yuan. Constructions of strongly regular Cayley graphs using index four Gauss sums. *J. Algebr. Combin.*, 37(2):313–329, 2013.

[40] C. Godsil and G. Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.

[41] L. C. Grove. *Classical groups and geometric algebra*. Amer. Math. Soc., 2002.

[42] Z. Heng, C. Ding, and Z. Zhou. Minimal linear codes over finite fields. *Finite Fields Appl.*, 54:176–196, 2018.

[43] W. M. Kantor. Ovoids and translation planes. *Canadian J. Math.*, 34(5):1195–1207, 1982.

[44] S. Kelly. Constructions of intriguing sets of polar spaces from field reduction and derivation. *Des. Codes Cryptogr.*, 43(1):1–8, 2007.

[45] G. Kemper, F. Lübeck, and K. Magaard. Matrix generators for the Ree groups ${}^2G_2(q)$. *Comm. Algebra*, 29(1):407–413, 2001.

[46] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*. Cambridge University Press, 1990.

[47] G. Korchmáros, G. P. Nagy, and P. Speziali. Hemisystems of the Hermitian surface. *J. Combin. Theory Ser. A*, 165:408–439, 2019.

[48] V. M. Levchuk and Ya. N. Nuzhin. The structure of Ree groups. *Algebra i Logika*, 24(1):26–41, 122, 1985.

[49] C. Li, C. Ding, and S. Li. LCD cyclic codes over finite fields. *IEEE Trans. Inform. Theory*, 63(7):4344–4356, 2017.

[50] S. Li, C. Li, C. Ding, and H. Liu. Two families of LCD BCH codes. *IEEE Trans. Inform. Theory*, 63(9):5699–5717, 2017.

[51] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[52] W. Lu, X. Wu, and X. Cao. The parameters of minimal linear codes. *arXiv preprint arXiv:1911.07648*, 2019.

[53] S.L. Ma. A survey of partial difference sets. *Des. Codes Cryptogr.*, 4(3):221–261, 1994.

[54] J. L. Massey. Minimal codewords and secret sharing. *Proc. 6-th Joint Swedish-Russian Workshop on Information Theory*, pages 276–279, Aug. 1993.

[55] J. L. Massey. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV, Esses England*, pages 33–47, 1995.

[56] S. Mesnager, Y. Qi, H. Ru, and C. Tang. Minimal linear codes from characteristic functions. *IEEE Trans. Inform. Theory*, 66(9):5404–5413, 2020.

[57] S. Mesnager, C. Tang, and Y. Qi. Complementary dual algebraic geometry codes. *IEEE Trans. Inform. Theory*, 64(4, part 1):2390–2397, 2018.

[58] K. Metsch. The non-existence of Cameron-Liebler line classes with parameter $2 < x \leqslant q$. *Bull. Lond. Math. Soc.*, 42(6):991–996, 2010.

[59] K. Metsch. An improved bound on the existence of Cameron-Liebler line classes. *J. Combin. Theory Ser. A*, 121:89–93, 2014.

[60] K. Metsch. Small tight sets in finite elliptic, parabolic and Hermitian polar spaces. *Combinatorica*, 36(6):725–744, 2016.

[61] K. Metsch and D. Werner. On the smallest non-trivial tight sets in Hermitian polar spaces $H(d, q^2)$, $d$ even. *Discrete Math.*, 342(5):1336–1342, 2019.

[62] K. Momihara. Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums. *European J. Combin.*, 34(4):706–723, 2013.

[63] K. Momihara, Q. Wang, and Q. Xiang. Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs, and related geometric substructures. *Combinatorics and Finite Fields. Difference Sets, Polynomials, Pseudorandomness and Applications*, pages 178–205, 2019.

[64] K. Momihara and Q. Xiang. Lifting constructions of strongly regular Cayley graphs. *Finite Fields Appl.*, 26:86–99, 2014.

[65] B. Pang, S. Zhu, and Z. Sun. On LCD negacyclic codes over finite fields. *J. Syst. Sci. Complex.*, 31(4):1065–1077, 2018.

[66] S. E. Payne. Tight pointsets in finite generalized quadrangles. volume 60, pages 243–260. 1987. Eighteenth Southeastern International Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, Fla., 1987).

[67] S. E. Payne and J. A. Thas. *Finite generalized quadrangles*. EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, second edition, 2009.

[68] T. Penttila and B. Williams. Ovoids of parabolic spaces. *Geom. Dedicata*, 82(1-3):1–19, 2000.

[69] R. Ree. A family of simple groups associated with the simple Lie algebra of type $(G_2)$. *Bull. Amer. Math. Soc.*, 66:508–510, 1960.

[70] N. Sendrier and G. Skersys. On the computation of the automorphism group of a linear code. In *:Proceedings of IEEE ISIT2001*. Washington, DC, 2001.

[71] X. Shi, Q. Yue, and S. Yang. New LCD MDS codes constructed from generalized Reed-Solomon codes. *J. Algebra Appl.*, 18(8):1950150, 23, 2019.

[72] Z. Shi and F. Fu. Several families of q-ary minimal linear codes with $w_{\min}/w_{\max} \leq (q-1)/q$. *Discrete Math.*, 343(6):111840, 2020.

[73] D. E. Taylor. *The geometry of the classical groups*. Heldermann, 1992.

[74] J. A. Thas. Ovoids and spreads of finite classical polar spaces. *Geom. Dedicata*, 10(1-4):135–143, 1981.

[75] J. A. Thas. Interesting pointsets in generalized quadrangles and partial geometries. *Linear Algebra Appl.*, 114/115:103–131, 1989.

[76] R. A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009.

[77] R. A. Wilson. Another new approach to the small Ree groups. *Arch. Math. (Basel)*, 94(6):501–510, 2010.

[78] G. Xu and L. Qu. Three classes of minimal linear codes over the finite fields of odd characteristic. *IEEE Trans. Inform. Theory*, 65(11):7067–7078, 2019.

[79] G. Xu, L. Qu, and X. Cao. Minimal linear codes from Maiorana-McFarland functions. *Finite Fields Appl.*, 65:101688, 19, 2020.

[80] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Trans. Inform. Theory*, 52(1):206–212, 2006.

[81] W. Zhang, H. Yan, and H. Wei. Four families of minimal binary linear codes with $w_{\min}/w_{\max} \leq 1/2$. *Appl. Algebra Engrg. Comm. Comput.*, 30(2):175–184, 2019.

# 作者简历

陶然, 女, 1994 年, 汉族, 黑龙江齐齐哈尔人. 2012 年考入中国海洋大学数学科学学院 (信息与计算科学专业), 2016 年本科毕业, 获得理学学士学位. 2016 年进入浙江大学数学科学学院 (应用数学专业), 研究生学习至今.

1. 通讯地址: 中国浙江省杭州市浙江大学玉泉校区数学科学学院，310027
2. 联系方式: rant@zju.edu.cn
3. 研究兴趣: 有限几何，代数编码，代数组合
4. 攻读博士学位期间主要研究成果

    - Tao Feng and Ran Tao. An infinite family of m-ovoids of Q(4,q), Finite Fields and Their Applications, vol. 63, pp. 101644, 16, 2020.
    - Ye Wang and Ran Tao. Constructions of linear codes with small hulls from association schemes, Advances in Mathematics of Communications, accepted.
    - Ran Tao, Tao Feng, and Weicong Li. A construction of minimal linear codes from partial difference sets, IEEE Transactions on Information Theory, accepted.