分类号：O157.2　　单位代码：10335
密　级：　　学　　号：11735031

浙江大学

博士学位论文

中文论文题目：关于几类有限几何结构及其自同构群的研究

英文论文题目：**On certain finite geometric structures and their automorphism groups**

申请人姓名：李伟聪
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：二〇二〇年六月

关于几类有限几何结构及其自同构群的研究

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：	李　方	教授	浙江大学
委员 1：	李　方	教授	浙江大学
委员 2：	吴志祥	教授	浙江大学
委员 3：	胡思煌	教授	山东大学
委员 4：	张一炜	教授	山东大学
委员 5：	冯　涛	研究员	浙江大学

答辩日期：二〇二〇年五月

On certain finite geometric structures and their automorphism groups

Author's signature: _____

Supervisor's signature: _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committe Chairperson:

Professor Fang Li,	Zhejiang University

Examining Committe Members:

Professor Fang Li,	Zhejiang University
Professor Zhixiang Wu,	Zhejiang University
Professor Sihuang Hu,	Shandong University
Professor Yiwei Zhang,	Shandong University
Visiting Professor Tao Feng,	Zhejiang University

Date of oral defence: May, 2020

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的导师冯涛教授. 从大三上学期开始, 冯老师手把手带我进入组合数学这领域, 让我从一个新手慢慢地学会如何做看文献, 解决科研上的问题. 冯老师的悉心教导和关怀一直激励着我不断努力, 并且他的言传身教让我获益匪浅. 更感谢他在我身上倾注大量的心血, 无论在科研上还是生活上他都给我很多指导和帮助。在攻读博士学位的五年中, 冯老师整理大量的笔记, 给我们讲授组合数学各领域的基础知识, 扩宽我们的研究领域和视野, 同时他一直鼓励我们多与国内外的专家学者交流学习. 冯老师一直叮嘱我们要重视细节, 教会我们在查阅文献时要学会如何用自己所学的工具去尝试证明文献的结果并养成记录笔记的科研习惯, 可惜我在这方面一直没有做好, 十分惭愧. 另一方面, 冯老师一直鼓励我们多看文献并寻找适合自己的题目, 积极与他讨论交流, 而且他也给我们很多出去交流学习的机会, 尽可能学会如何独立地思考和解决问题. 在今后的科研生涯中, 我将谨记冯老师的教诲并认真地做好每一件事, 不辜负冯老师对我的期望.

其次我要感谢南方科技大学的向青教授. 向老师在访问浙大期间给带来许多新课题和新方法，也在科研上给了我不少帮助和指导. 同时他在我人生未来的选择方向上给了不少的建议, 感谢他给予我去南科大继续科研学习的机会.

我还要感谢这五年中在学习和生活上给予过我指导和帮助的各位老师们, 特别是首都师范大学的葛根年教授, 国防科技大学的周悦教授. 在与他们交流的的过程中, 我得以拓宽研究视野, 体验科研的乐趣.

感谢和我一起学习的各位同门们：李抒行师兄、张一炜师兄、张韬师兄、汪馨师兄、Jerod Michel、丁报昆师兄、马景学师兄、钱昺辰师兄、林灯、戚立波、何智文、陶然、王野、奚元霄、徐子翔、周靖坤、孙秀芳、陆建兵、狄文帝等. 在这段学习与生活的时光里, 感谢他们对我的帮助和照顾, 很幸运能有机会跟他们在科研上相互讨论和学习. 在这短短的五年时间内, 他们给我带来很多美好的回忆.

感谢曾同我在浙大一起学习的朋友们：夏树灿、张仑、傅振滔、鲁思祈、陈世雷、霍归璟、朱凯伦、丁益彬、许佳攀、蓝朝祥等人. 感谢他们与我在攻读博士学位博期间探讨人生, 分享彼此对未来选择上的心得看法, 诉说彼此生活上的忧欢悲喜. 此外, 我还感谢几位高中好友: 姚炜健、肖景洋等, 谢谢他们在寒暑假期间跟我一起畅谈人生.

最后，我感谢我挚爱的父母和哥哥。他们一直在背后默默地支持和鼓励我，成为我克服科研和生活上种种困难的动力。谨此祝他们身体健康！

感谢所有曾经帮助过我的人。

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

有限几何是组合数学中有趣且令人兴奋的领域, 它往往会带来很多意想不到的结果, 而且它与组合数学的很多分支有着密切的联系, 如编码理论、设计理论、图论、密码学等等. 利用有限几何的结构能构造出很多有趣的代数几何码以及关联结构. 而且大部分几何对象的自同构群都是一些特别有意思的群, 如典型群, 其他有限单群. 本学位论文涉及有限几何中几类几何结构其自同构群的研究. 本文的主旨是用包括有限域、群环、指数和等现代的数学工具以及群论中一些结果去考察和研究问题。

在第 1 章中, 我们将简略介绍本文研究的几类几何结构的研究背景和本文的主要贡献。

在第 2 章中, 我们考虑 Budaghyan 和 Hellesecth 的 Budaghyan-Helleseth 交换半域, 并完全确定其 isotopism 类。

在第 3 章中, 我们证明 Desargusian 射影平面 PG$(2, q^2)$ 中所有非经典 Buekenhout-Metz untials 都存在 O'Nan 构型, 这个构型是由两两相交于一点的四条线组成的。

在第 4 章中, 我们考虑辛对称广义四边形 $W(q)$ 的 Payne 派生四边形的点正则群, 这是一类具有非经典参数 $(q-1, q+1)$ 的广义四边形. 我们将给出奇特征下点正则群的完整的分类, 也同时完全确定了偶特征下所有线性的点正则自同构群. 此外, 我们通过研究它们的群不变量说明有限广义四边形的点正则群可以有无限大的幂零类。

在第 5 章中, 我们对有限的 Hermitian 极空间中传递 ovoids 进行系统地分析. 在 Cossidente 和 Korchmáros[1] 的结果的基础上, 我们再结合 Bamberg 的结果[2] 对 Hermitian 极空间中传递 ovoids 进行完整的分类。

最后, 我们介绍这方向进一步的研究问题, 同时也简略地介绍作者攻读博士学位期间其他工作.

关键词： Budaghyan-Hellsseth 半域, Buekenhout-Metz unitals, O'Nan 构型, Payne 派生四边形, 点正则群, 传递 ovoids, Hermitian 极空间.

Abstract

Finite geometry is an interesting and exciting area in combinatorics with beautiful results, it further has a close connection with other branches of combinatorics, such as coding theory, design theory, graph theory, cryptology and so on. By applying some geometric structures, we obtain some interesting codes and incidence structures. Further, most of the geometric objects have an interesting automorphism group, likes classical group and other finite simple groups. This dissertation concerns with certain finite geometric structures and their automorphism groups. The substance is to investigate these structures by applying some results of group theory and some modern mathematical tools, including group ring, finite fields and exponential sums and so on.

In Chapter 1, we will briefly introduce the backgrounds of our concerned geometric structures, and summarize the main contributions to these problems.

In Chapter 2, we completely determined the isotopism classes of the Budaghyan-Helleseth commutative semifields constructed by Budaghyan and Helleseth[3].

In Chapter 3, we establish the existence of O'Nan configurations in all nonclassical Buekenhout-Metz unitals in Desargusian plane PG$(2, q^2)$.

In Chapter 4, we systematically study the point regular groups of Payne derived quadrangle of symplectic quadrangle $W(q)$, which is a finte generalized quadrangle with nonclassical parameters $(q-1, q+1)$. We completely determine all linear point regular automorphism group, and further give all nonlinear point regular automorphism groups in the odd characteristic case. In addition, by computing the group invariants of these groups, we show that the finite groups that act regularly on the points of a finite quadrangle can have unbounded nilpotency class.

In Chapter 5, we analysis the transitive ovoids of finite classical Hermitian polar space in details. Based on Bamberg et al's results[1,2], we use some combinatorial tools to give a complete classification of these ovoids.

In the end, we briefly introduce some further problems in finite geometry, and also give an introduction of some work under investigation.

Keywords: Budaghyan-Helleseth semifield, Buekenhout-Metz unitals, O'Nan con-

figuration, Payne derived quadrangles, Point regular groups, Transitive ovoids, Hermitian polar space.

图 目 录

表 目 录

目　次

1 绪论

有限几何是组合数学的一个重要分支, 它是研究有限域上的关联结构的科学. 最初对有限几何结构本身的研究并不流行, 但是随着计算机的发展和信息时代的来临, 离散结构的的研究在数学的其他分支和信息科学等其他领域有越来越多应用. 借用 Hirschfeld 和 Thas[4] 的话, 它是“an interesting and exciting area in combinatorics with beautiful results”. 有限几何中有不少有趣的的组合结构, 利用它们可以在编码和密码等领域中构造出某些具有优良性质的线性码和密码函数. 而且大部分几何对象的自同构群都是一些特别有意思的群, 如典型群, 其他有限单群. 本论文主要针对有限几何中某几类几何结构和它们的自同构群进行研究, 其中具体包括: Budaghyan-Helleseth 半域, O'Nan 构型, Payne 派生四边形的点正则群以及传递 ovoids. 下面将介绍研究课题的背景意义, 并对这些工作进行概括.

Budaghyan-Hellsseth 半域

半域是有乘法单位的非结合除环, 也被称为非结合除环或分配拟域. 由于有限半域和交换半域具有优良的性质, 一直是半域领域的研究热点. 半域的研究要追溯至 1900 年初, Dickson 构造出第一个非平凡的半域[5]. 1965 年 Knuth[6] 证明了每个半域的加法群都是初等阿贝尔群. 一个关键的突破是 2008 年 Coulter 和 Henderson 注意到在特定条件下 Dembowski-Ostrom 型线性化多项式和奇特征下交换半域是等价的, 之后这等价性的完全证明是 Zhou 在文献[7] 中给出的. 半域一直是学者的研究热点, 这不仅是与它自身的独特性质有关的, 还因为它跟各种各样的组合结构有着密切联系, 例如平面函数, 置换多项式和有限仿射平面等等。最近它能再次引起大家的兴趣是因为它能作为极大秩距离码的特殊例子。读者们可以通过查阅文献[8,9] 去了解半域与这些对象的联系, 目前最新的半域是从多项式除环中得到的[10].

对于半域的研究, 一个核心问题是确定半域的 isotopism 类. 由于两个 non-isotopic 半域会对应产生射影平面各不相同, 对应地也会产生不同的完全非线性函数, 因此确定半域的 isotopism 类对于研究半域具有重要的意义. 本文第 2 章主要针对 Budaghyan 和 Hellesecth[3,11] 构造的交换半域进行研究, 完全确定了 Budaghyan-Hellesecth 半域的 isotopsim 类. 特别地, 在奇特征情况下, 对于一个中心大小为 q 的 q^{2l} 阶 Budaghyan-Hellsseth 半域, 它们的 isotopism 类的大小如下所示:

(i) 在 $q \equiv 1 \pmod 4$ 且 $l > 2$ 偶数时, 大小为 $\phi(l)/2$;

(ii) 在 $q \equiv 3 \pmod 4$ 且 $l > 2$ 偶数时, 大小为 $\phi(l)$;

(iii) 在 l 是奇数时, 大小为 $\phi(l)/2$.

这里 ϕ 是欧拉函数. 这部分的工作已发表在《Finite fields and Their Applications》.

Unitals 和 O'Nan 构型

一个 n 阶 unital 是一个参数为 2-$(n^3+1, n+1, 1)$ 的区组设计. 当它恰好是某个射影平面的子集时, 我们称它为可嵌入该射影平面的 unitals. 一般而言, 存在很多能嵌入到射影平面 (Desargusian 和 non-Desarguesian) 的 unitals, 也有作为 2-$(n^3+1, n+1, 1)$ 区组设计不能嵌入于任何射影平面的 unitals. 其中 unitals 的经典的例子是 PG$(2, q^2)$ 的 Hermitian 曲线 $\mathcal{H}(2, q^2)$, 有时也被称为酉区组设计. 目前已知能嵌入到 Desarguesian 射影平面 PG$(2, q^2)$ 的 unitals 具体可以分成下面的几类：

(i) Classical(Hermitian) unitals：PG$(2, q^2)$ 中的 Hermitian 曲线.

(ii) Orthogonal-Buekenhout-Metz unitals：PG$(4, q)$ 中的椭圆椎体 (ellpitic cones)；

(iii) Buekenhout-Tits unitals：PG$(4, q)$ 中以 Tits ovoid 为基的 ovoidal cones；

(iv) Nonsingular-Buekenhout unitals: PG$(4, q)$ 中非退化的抛物线型二次型 (parabolic quadrics)；

它们都是 Buekenhout[12] 和 Metz[13] 在 q^2 阶 translation 平面中用 Bruck-Bose 表示法获得的, 统称它们为 Buekenhout unitals. 值得一提的是, 是否存在其他能嵌入到 PG$(2, q^2)$ 的 unital 依然是未解决的公开问题. 更多关于射影平面中的 unitals, 可以参考 Barwick 和 Ebert 的著作[14] 了解更多信息.

在 1972 年, O'Nan[15] 在研究经典的 unitals 的自同构群时发现它们不包含一种特殊构型 (4 线 6 点, 任意两线交于一点), 该构型后被人们称为 O'Nan 构型. 随后, Piper[16] 猜想这类特殊的构型是经典 unitals 的特征. 这个猜想至今都没有被完全解决, 只有一些相关结果在文献[17–20] 中给出. 在第 3章中, 我们解决了 Hirschfeld 和 Thas 在文献[21] 中列出的一个问题.

问题：非经典 *ovoidal Buekenhout-Metz unitals* 是否存在 *O'Nan* 构型*?*

答案是肯定的, 我们的主要想法是假定 O'Nan 构型是被某个对合所固定的或者包含某些特定的点和线, 再借助一些组合技巧和有限域的知识来确定此 O'Nan 构型的存在性. 这部分的工作已发表在《Discrete Mathematics》.

Payne 派生四边形和其点正则群

广义四边形的研究与数学的其他分支有着密切的联系, 其中与群论的关系特别大. 广义多边形的概念是 J.Tits[22] 为了更好地理解秩 2 的 Chevalley 群而引入的. 类似于有限射影平面 (广义三边形) 的研究, 人们主要通过几何论证和群论中深刻的结果对广义四边形进行分类. 所有目前已知的有限广义四边形在对偶等价意义下可以被分成四类：经典的的广义四边形, translation 广义四边形, flock 广义四边形以及参数为 $(q-1, q+1)$ 的广义四边形. 特别的是最后一类广义四边形都是用 Payne 派生法[23–25] 得到的, 人们往往把用这种方法获得的广义四边形称为 Payne 派生四边形. 除了具有非经典参数 $(q-1, q+1)$ 的广义四边形以外, 大部分已知的广义四边形都可以用 Kantor 的方法[26] 描述成 4-gonal family 形式的陪集几何 (coset geometry), 随后 Ghinelli 构造类似于 4-gonal family 的 AS-构型去描述 $(q-1, q+1)$ 阶广义四边形[27], 但是只有初等阿贝尔群才能构造出 AS-构型. 更多关于有限广义四边形的研究, 可查阅 Payne 和 Thas 的著作[28].

自 Singer 著名的论文[29] 以来, 有限几何结构的点正则自同构群 (Singer 群) 引起了人们的普遍关注. 对存在点正则群的广义四边形的研究最初是由 Ghinelli[30] 开始的, 她利用表示论和差集的理论去探究 s 是偶数时 (s, s) 阶广义四边形中是否存在点正则群的问题. 随后 20 年内, 人们对存在点正则群的广义四边形进行大量的研究, 详见文献[31–35], 但是依旧对这类具有点正则群的广义四边形了解甚少. 直至 2011 年, 该方向才出现一个重大的突破. Bamberg 和 Giudici[36] 对存在点正则群的的经典的广义四边形 $(s, t \geq 2)$ 进行分类, 这也导致他们发现 $W(q)$ 的 Payne 派生四边形拥有很多不同构的点正则群, 还给出一个新的非平凡的构造, 这恰恰包含 De.Winter 和 Thas 的猜想[33] 的反例. 此外, 他们的计算机搜索结果显示了 Payne 派生四边形的点正则群还有很多未知且有趣的构造. 受此启发, 我们对 Payne 派生四边形的点正则群进行了系统的研究. 这类广义四边形的自同构群已经在文献[32,37] 中得到很好的研究:

定理 1.1 (**推论** 2.4[37]). 令 q 是大于等于 5 的素数幂, 令是 $W(q)^P$ 是辛对称四边形 $W(q)$ 相对于正则点 P 的 Payne 派生四边形. 那么

$$\mathrm{Aut}(W(q)^P) = \mathrm{P\Gamma Sp}(4,q)_P = \mathrm{PGSp}(4,q)_P \rtimes \mathrm{Aut}(\mathbb{F}_q),$$

其中 $\mathrm{P\Gamma Sp}(4,q)_P$(resp. $\mathrm{PGSp}(4,q)_P$) 是射影点 P 在 $\mathrm{P\Gamma Sp}(4,q)$(resp. $\mathrm{PGSp}(4,q)$) 中的稳定子群.

基于 Bamberg 等人的计算机搜索结果[36], 我们运用群环以及有限域等工具给出下面的结果:

定理 1.2. 当 q 是奇素数幂且 $q \geq 5$, $W(q)$ 的 Payne 派生四边形 $\mathcal{Q}^P$ 的点正则群 G 是

与构造 4.16-4.19得到的某个点正则群相共轭的.

同时, 同样的方法也能完整地确定了偶特征下所有线性的点正则群. 特别地, 为了区分奇特征下的构造, 我们考虑点正则群的同构性问题. 通过计算他们的 exponents 和 Thompson 子群, 我们证明了这四个构造在普遍意义下是不同构的, 同时我们进一步通过研究这些点正则群的幂零类发现作用在有限广义四边形上的有限群可以有无穷大的幂零类. 这部分的工作已投稿至《Journal of Combinatorial Theory Series A》.

$\mathcal{H}(3,q^2)$ 的传递 ovoids

有限极空间 (秩大于 1) 的一个 ovoid 是一个点集使得它与该极空间上每个完全迷向 (奇异) 极大子空间只有一个公共点. Ovoids 一直以来都是有限几何中重点关注的研究对象. 特别值得一提的是, 它们与各种各样的几何对象以及组合学的其他分支有密切的联系, 详情可参考文献[38,39]. 关于有限极空间中 ovoids 的最新研究进展详见著作[4]. 对于有限极空间中的 ovoid $\mathcal{O}$ 的目前存在性, 我们在表 1中给出: 其中

有限极空间	$\mathcal{O}$ 的存在性
$W_3(q)$, q even	Yes
$W_3(q)$, q odd	No
$W_n(q)$, $n=2t+1$ and $t>1$	No
$Q(4,q)$	Yes
$Q(6,q)$, q prime, $q>3$	No
$Q(6,q)$, $q=3^h$	Yes
$Q(2n,q)$, $n>2$ and q even	No
$Q(2n,q)$, $n>3$ and q odd	No
$Q^+(3,q)$	Yes
$H(5,q)$	Yes
$Q^+(7,q)$, q odd with q prime or $q\equiv 0$ or $2 \pmod 3$	Yes
$Q^+(7,q)$, q even	Yes
$Q^+(2n+1,q), n>3, q=p^h$, p prime and $p^n > \binom{2n+p}{2n+1} - \binom{2n+p-2}{2n+1}$	No
$Q^-(2n+1,q), n>1$	No
$H(3,q^2)$	Yes
$H(2n,q^2), n\geq 2$	No
$H(2n+1,q^2), n>1, q=p^h$, p prime and $p^{2n+1} > \binom{2n+p}{2n+1}^2 - \binom{2n+p-1}{2n+1}^2$	No
$H(5,4)$	No

表 1.1　Ovoid 在有限极空间的存在性

对于 Hermitian 极空间 $H(n,q^2)$, 我们只在 $n=3$ 是奇数的情况下发现里面包含很多 ovoids, 而在 $n\geq 5$ 时, 目前只有一些不存在性的结果[40–42]. 发现新的 ovoids 一直是有限几何方向中最受关注的一类问题.

在第 5 章中, 我们主要研究 Hermitian 极空间 $H(n,q^2)$ 中的传递 ovoids. 令 O 是

$H(n,q^2)$ 中的一个 ovoid, 若存在 PΓU$(n+1,q^2)$ 中一个子群 H 固定 O 的点集并在 O 上的作用是传递的, 那么我们称该 ovoid 是传递的 (*transitive*). 当 H 是 PGU$(n+1,q^2)$ 的子群时, 那么该 ovoid 是线性的. 在 $H(3,q^2)$ 中, 所有经典的 ovoids(即 $H(3,q^2)$ 的非退化超平面的截面) 都是线性传递 ovoids, 它的全自同构群包含非阿贝尔群 PSU$(3,q^2)$. 当 $q>2$ 是偶数, Cossidente 和 Korchmáros[1] 借助文献[43] 中 $H(2,q^2)$ 的循环 spreads 并且运用几何论据以及一些群论的结果构造出 $H(3,q^2)$ 中的新一类传递的 ovoids, 即 Singer-type ovoids. 这类 ovoids 是 Hermitian 极空间中唯一已知的具有可解的自同构群的传递 ovoids. 在 2009 年, Bamberg 和 Penttila 运用典型群中深刻的结果对有限极空间中存在不可解的自同构群的传递 ovoids 进行分类. 因此, Hermitian 极空间中已知的传递 ovoids 都射影等价于下面其中一类

(1) 经典 ovoid $H(2,q^2)$, 其中它的全稳定子群是 ΓU$(3,q^2)$;

(2) Singer-type ovoid, 其中 q 是偶数且它的全稳定子群同构于 $\mathbb{Z}_2\times(\mathbb{Z}_3\times\mathrm{PSL}(2,7)):2$;

(3) $H(3,5^2)$ 中例外的 ovoid, 其中它的全稳定子群同构于 $\mathbb{Z}_2\times(\mathbb{Z}_3\times\mathrm{PSL}(2,7)):2$;

第 5 章的主要工作是对 Hermitian 极空间的传递 ovoids 进行完整的分类. 首先我们给出 $H(3,q^2)$ 的传递 ovoids 的一个完整的分类, 并且说明对于一个给定的奇整数 $n\geq 5$ 不存在任何 $H(n,q^2)$ 的传递 ovoid. 精确来说, 在 $H(3,q^2)$ 中的传递 ovoids 还可能射影等价于

(4) $H(3,8^2)$ 中的某个非线性的传递 ovoid, 其中它的全稳定子群同构于 $\mathbb{Z}_{57}:9$, 或

(5) $H(3,8^2)$ 中的某个非线性的传递 ovoid 其中它的全稳定子群同构于 $\mathbb{Z}_{57}:18$.

因此, Hermitian 极空间中所有传递 ovoids 会射影等价于以上 5 类 ovoids 的其中一类. 这部分的工作已投稿至《Combinatorica》.

2 Budaghyan-Helleseth 半域

2.1 背景

一个有限预半域 (*presemifield*) $\mathbb{S}$ 是一个满足左右分配律且不含零因子的有限环. 如果 $\mathbb{S}$ 拥有乘法单位, 我们就称它为半域 (*semifield*). 一个半域不一定满足交换律和结合律, 但是根据 *Wedderburn* 定理[44] 可知, 满足结合律在有限的情况下必然意味着满足交换律. 半域的研究是由 *Dickson*[5] 在可除代数的研究中提出的, 并且他也构造出第一个非平凡的交换半域 (*Dickson* 半域). *Knuth*[6] 证明了半域 $\mathbb{S}$ 的加法群是初等交换群. 因此任何有限预半域都可用 $(\mathbb{F}_{p^n}, +, *)$ 表示, 其中 $(\mathbb{F}_{p^n}, +)$ 是含 p^n 个元素的有限域 $\mathbb{F}_{p^n}$ 的加法群和 $x * y = \varphi(x, y)$, 这里 φ 是从 $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ 到 $\mathbb{F}_{p^n}$ 的双线性函数. 若想了解关于有限半域的最近的研究进展, 可参考文献[9]. 在本章中, 我们主要研究奇特征下的交换预半域, 这种半域可以等价地用 *Dembowski-Ostrom* 型的平面多项式来描述.

令 $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, *)$ 和 $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, *')$ 为两个预半域. 如果存在三个 $\mathbb{F}_{p^n}$ 上的线性置换 L, M, N 使得对所有 $x, y \in \mathbb{F}_{p^n}$ 均有 $L(x * y) = M(x) *' N(y)$, 那么我们称三元组 (M, N, L) 是 $\mathbb{S}_1$ 和 $\mathbb{S}_2$ 之间的 *isotopism*. 如果这个 *isotopism* 满足 $M = N$, 那么它是一个 *strong isotopism*, 并且称 $\mathbb{S}_1$ 和 $\mathbb{S}_2$ 是 *strongly isotopic*. 特别的是如果 $\mathbb{S}_1 = \mathbb{S}_2$, *(strong) isotopism* 又被称为 *(strong) autotopism*. *Isotopism* 和 *strong isotopism* 都是定义有在限半域之间的等价关系, 其中它们对应的等价类分别叫做 *isotopism* 类和 *strong isotopism* 类. 两个 *isotopic* 预半域被叫做各自的 *isotopes*. 对于预半域 $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$ 和它的非零元 e, 我们可以用 $(x * e) \star (e * y) = x * y$ 去定义新的乘法. 那么 $\mathbb{S}' = (\mathbb{F}_{p^n}, +, \star)$ 是有单位元 $e * e$ 的半域, 而且与 $\mathbb{S}$ 是 *strongly isotopic*.

在文献[3,11] 中, *Budaghyan* 和 *Helleseth* 从在 $\mathbb{F}_{p^{2k}}$ 上特定的 *Dembowski-Ostrom* 型平面函数中构造出两类 p^{2k} 阶交换预半域, 其中 p 是奇素数. 他们在 $p \neq 3$ 和 k 是奇数时证明第一类预半域与之前已知的半域是 *non-isotopic*, 并且在某些特殊情况下确定他们的 *middle nuclei*. 后来, *Bierbrauer*[45] 观察到这两类预半域实际上是同一类, 且该结论也独立地在文献[46] 中给出. 这一种半域在文献中通常被称为 *Budaghyan-Helleseth* 半域 (*Budaghyan-Helleseth* 类). 而且在同一篇论文[45] 中, *Bierbrauer* 对 *Budaghyan-Helleseth* 半域进行概括, 主要说明这类半域包含 *LMPT* 构造[47]. 因此这新一类半域有时也被称为 *LMPTB* 族半域, 并且它与以前任何已知的交换半域都是 *non-isotopic*, 但可能跟 *Budaghyan-Helleseth* 半域是 *isotopic*. 然而, *Marino* 和 *Polerino* 在文献[48] 中证明了 *Budaghyan-Helleseth* 半域包含 *LMPTB* 族半域, 并且他

们也在文献[49]中确定了 *Budaghyan-Helleseth* 半域的 *nuclei* 和 *middle nuclei*.

本章的主要结果就是完全确定了 *Budaghyan-Helleseth* 预半域的 *isotopism* 类. 本章的结构如下所示. 第 *2.2*节是先介绍一些预备知识和准备工作. 在第 *2.3*节中我们将确定 *Budaghyan-Helleseth* 预半域的 *strong isotopism* 类, 之后在第 *2.4*节中完全确定它们的 *isotopism* 类. 当 q 是奇数时, 对于中心大小为 q 的 q^{2l} 阶 *Budaghyan-Helleseth* 半域, 它们的 *isotopism* 类的大小如下所示：

(i) 在 $q \equiv 1 \pmod 4$ 且 $l > 2$ 偶数时, 大小为 $\phi(l)/2$;

(ii) 在 $q \equiv 3 \pmod 4$ 且 $l > 2$ 偶数时, 大小为 $\phi(l)$;

(iii) 在 l 是奇数时, 大小为 $\phi(l)/2$.

这里 ϕ 是欧拉函数. 值得注意的是当 $l = 2$ 时, *Budaghyan-Helleseth* 半域就与 *Dickson* 半域是 *isotopic*.

2.2 准备工作

我们首先介绍一些我们将在本章中使用的符号. 令 p 为奇素数, 以及令 l, h, d 都是满足以下条件的正整数：

$$1 < l, \quad 1 \le d \le 2lh - 1, \quad \gcd(l, d) = 1, \quad \text{并且 } l + d \text{ 是奇数}.$$

设 $q = p^h$, 以及固定 $\mathbb{F}_{q^{2l}}$ 中的非平方元 β 和非零元 $\omega \in \mathbb{F}_{q^{2l}}$ 使得 $\omega + \omega^{q^l} = 0$. 定义映射 $\mathrm{Tr} : \mathbb{F}_{q^{2l}} \to \mathbb{F}_{q^l}$ 为一个迹函数使得对所有 $x \in \mathbb{F}_{q^{2l}}$ 有 $\mathrm{Tr}(x) = x + x^{q^l}$. 我们定义以下乘法

$$x *_{(d,\beta)} y = x^{q^l} y + xy^{q^l} + \left(\beta(x^{q^d} y + xy^{q^d}) + \beta^{q^l}(x^{q^d} y + xy^{q^d})^{q^l}\right) \omega. \tag{2.1}$$

此时, $(\mathbb{F}_{q^{2l}}, +, *_{(d,\beta)})$ 就是 *Budaghyan-Helleseth* 半域. 这是在文献[49]中找到的简化形式. 易知 ω 的不同选取都会产生 *strongly isotopic* 预半域. 我们现在证明 β 的不同选取也同样会产生 *strongly isotopic* 预半域.

引理 2.1. 令 β 和 β' 是 $\mathbb{F}_{q^{2l}}$ 中的两个非平方元, 再设 d 是整数以致 $\gcd(d, l) = 1$ 且 $l + d$ 是奇数. 那么 $\gcd(q^d + 1, q^l + 1) = 2$, 并且存在非零元 $b_0, b_1 \in \mathbb{F}_{q^{2l}}$ 使得

$$\beta'\beta^{-1} b_0^{q^d+1} \in \mathbb{F}_{q^l}, \quad \beta^{1-q^{2l-d}} b_1^{q^{2l-d}+1} \in \mathbb{F}_{q^l}.$$

证明. $\gcd(q^d+1, q^l+1)=2$ 早已经在文献[49] 的引理 *3.1* 的 (ii) 中得到证明. 固定 $\mathbb{F}_{q^{2l}}$ 中的本原元 γ 以及记 $\log(\gamma^i) := i \pmod{q^{2l}-1}$. 那么引理中条件可转化为

$$\begin{aligned}\log(\beta') - \log(\beta) + (q^d+1)\log(b_0) &\equiv 0 \pmod{q^l+1},\\ (1-q^{2l-d})\log(\beta) + (q^{2l-d}+1)\log(b_1) &\equiv 0 \pmod{q^l+1}.\end{aligned}$$

因为 $\log(\beta')$ 和 $\log(\beta)$ 都是奇数, 所以引理需要的 b_0 和 b_1 总是存在的. □

取如引理 *2.1*中定义的 β, β', b_0 和 b_1. 令 $N_0(x)=b_0x$, $N_1(x)=b_1x$, 以及

$$\begin{aligned}L_0(x) &= \frac{1}{2}b_0^{q^l+1}(x+x^{q^l}) + \frac{1}{2}\beta'\beta^{-1}b_0^{q^d+1}(x-x^{q^l}),\\ L_1(x) &= \frac{1}{2}b_1^{q^l+1}(x+x^{q^l}) + \frac{1}{2}\beta^{1-q^{2l-d}}b_1^{q^{2l-d}+1}\omega^{1-q^{l-d}}(x-x^{q^l})^{q^{l-d}}.\end{aligned}$$

易证可得

$$\begin{aligned}L_0(x *_{(d,\beta)} y) =& b_0^{q^l+1}\mathrm{Tr}(x^{q^l}y) + \beta'\beta^{-1}b_0^{q^d+1}\mathrm{Tr}(\beta(x^{q^d}y + xy^{q^d}))\,\omega\\ =& b_0^{q^l+1}\mathrm{Tr}(x^{q^l}y) + \mathrm{Tr}(\beta' b_0^{q^d+1}(x^{q^d}y + xy^{q^d}))\,\omega\\ =& N_0(x) *_{(d,\beta')} N_0(y).\end{aligned}$$

因此对于乘法(2.1), β 的不同的取法产生 *strongly isotropic* 预半域. 遂我们固定 $\mathbb{F}_{q^{2l}}$ 中的非平方元 β, 为了便于表示, 我们将乘法记号 $*_{(d,\beta)}$ 替换成 $*_d$, 并且使用符号 $BH(q, l, d)$ 来表示 *Budaghyan-Helleseth* 半域 $(\mathbb{F}_{q^{2l}}, +, *_d)$. 如果 q 和 l 是固定的, 那么我们用记号 $\mathbb{S}_d := (\mathbb{F}_{q^{2l}}, +, \star_d)$ 表示对应的半域, 其中乘法 $\star_d$ 用下面的方式定义:

$$(1 *_d x) \star_d (1 *_d y) = x *_d y. \tag{2.2}$$

引理 2.2. 令 d 是满足 $0<d<2lh-1$ 的整数, 并且 $\gcd(l,d)=1$ 和 $l+d$ 是奇数. 预半域 $BH(q, l, d)$ 和 $BH(q, l, 2l-d)$ 属于同一个 strong isotopism 类.

证明. 从 $\omega+\omega^{q^l}=0$ 中我们能推出 $\omega^{1-q^{l-d}} \in \mathbb{F}_{q^l}$. 借助已经定义好的 (引理 *2.1*的证明结束下面的) 函数 L_1 和 N_1, 我们直接地计算

$$\begin{aligned}L_1(x *_d y) =& b_1^{q^l+1}\mathrm{Tr}(x^{q^l}y) + \beta^{1-q^{2l-d}}b_1^{q^{2l-d}+1}\omega^{1-q^{l-d}}\mathrm{Tr}\big((\beta^{q^{2l-d}}(x^{q^{l+d}}y^{q^l} + x^{q^l}y^{q^{l+d}})^{q^{l-d}}\big)\,\omega^{q^{l-d}}\\ =& b_1^{q^l+1}\mathrm{Tr}(x^{q^l}y) + \mathrm{Tr}\big(\beta b_1^{q^{2l-d}+1}(xy^{q^{2l-d}} + x^{q^{2l-d}}y)\big)\,\omega\\ =& N_1(x) *_{2l-d} N_1(y).\end{aligned}$$

于是三元组 (N_1, N_1, L_1) 是所需的 *strong isotopism.* □

令 $\mathbb{S}=(\mathbb{F}_{p^n}, +, \star)$ 是一个交换半域. 它的 *nucleus* $N(\mathbb{S})$ 和 *middle nucleus* $N_m(\mathbb{S})$

如下所示:

$$N(\mathbb{S}) = \{a \in \mathbb{F}_{p^n} : (a \star x) \star y = a \star (x \star y) \textit{ for all } x, y \in \mathbb{F}_{p^n}\},$$
$$N_m(\mathbb{S}) = \{a \in \mathbb{F}_{p^n} : (x \star a) \star y = x \star (a \star y) \textit{ for all } x, y \in \mathbb{F}_{p^n}\}.$$

易知它们都是有限域, 并且 $N(\mathbb{S})$ 也称为 $\mathbb{S}$ 的中心. 他们的大小在 *isotopism* 等价意义下是不变量. 并且半域 $\mathbb{S}_d$ 的 *nucleus* 和 *middle nucleus* 的显式表达式已经在文献[48]的定理 *4.1* 中给出.

定理 2.3 (Marino 和 Polverino[48]). 令 $\mathbb{S}_d := (\mathbb{F}_{q^{2l}}, +, \star_d)$ 具有乘法(2.2)的半域. 那么它的中心大小为 q, 并且它的 middle nucleus 大小为 q^2. 对于每个 $\alpha \in N_m(\mathbb{S}_d)$, 都存在 $a, b \in \mathbb{F}_q$ 使得 $(x *_d 1) \star_d \alpha = (ax + b\xi x^{q^l}) *_d 1$ 对所有 $x \in \mathbb{F}_{q^{2l}}$ 成立, 其中 ξ 是满足 $\beta^{1-q^l} = \xi^{q^{l+d}-1}$ 的常数.

在本章的余下部分中, 我们将记 $\alpha = \kappa(a, b)$, 其中 α, a, b 是在定理 *2.3*中定义的符号.

引理 2.4. 取定理 2.3中一样的符号. 那么 ξ^{q^l+1} 是 $\mathbb{F}_q^*$ 中的非平方元. 对于 $a, b \in \mathbb{F}_q$, $\alpha = \kappa(a, b)$ 是 $N_m(\mathbb{S}_d)$ 中的非平方元当且仅当 $a^2 - b^2\xi^{q^l+1}$ 是 $\mathbb{F}_q$ 中的非平方元. 特别地, 如果 α 是非平方元, 那么 $b \neq 0$.

证明. 我们先从条件 $\beta^{1-q^l} = \xi^{q^{l+d}-1}$ 中推出 $\xi^{(q^l+1)(q^{l+d}-1)} = 1$. 因为 $\gcd(q^{l+d}-1, q^l-1) = q^{\gcd(l+d,l)} - 1 = q - 1$, 所以 $\xi^{q^l+1} \in \mathbb{F}_q$. 进一步, 因为 β 是 $\mathbb{F}_{q^{2l}}$ 中的非平方元和 $l + d$ 是奇数, 所以

$$-1 = \xi^{(q^l+1)(q^{l+d}-1)/2} = \left(\xi^{(q^l+1)(q-1)/2}\right)^{(q^{l+d}-1)/(q-1)} = \xi^{(q^l+1)(q-1)/2}.$$

于是 ξ^{q^l+1} 是 $\mathbb{F}_q$ 中的非平方元. 这就证明了第一个命题.

在 $\alpha = \kappa(a, b) \in N_m(\mathbb{S}_d)$ 时, 如果存在 $\gamma = \kappa(a_1, b_1) \in N_m(\mathbb{S}_d)$ 以致 $\alpha = \gamma \star_d \gamma$, 那么对所有 $x \in \mathbb{F}_{q^{2l}}$ 均有 $((x *_d 1) \star_d \alpha) = ((x *_d 1) \star_d \gamma) \star_d \gamma$. 我们就能推出

$$\begin{aligned}(ax + b\xi x^{q^l}) *_d 1 &= \left((a_1x + b_1\xi x^{q^l}) *_d 1\right) \star_d \gamma \\ &= \left(a_1(a_1x + b_1\xi x^{q^l}) + b_1\xi(a_1x + b_1\xi x^{q^l})^{q^l}\right) *_d 1 \\ &= \left((a_1^2 + b_1^2\xi^{q^l+1})x + 2a_1b_1\xi x^{q^l}\right) *_d 1.\end{aligned}$$

于是就有 $a = a_1^2 + b_1^2\xi^{q^l+1}$ 和 $b = 2a_1b_1$. 因此, $\alpha = \kappa(a, b)$ 是 $N_m(\mathbb{S}_d)$ 中的非平方元当且仅当 $X^2 + Y^2\xi^{q^l+1} = a$, $2XY = b$ 在 $\mathbb{F}_q \times \mathbb{F}_q$ 中不存在解 (X, Y).

如果 $b=0$, 那么总存在一个解 (X,Y) 因为 ξ^{q^l+1} 是 $\mathbb{F}_q$ 中的非平方元. 因此我们现在假定 $b\neq 0$. 我们用 $Y=b/(2X)$ 去消去变量 Y, 于是就得到关于 X 的四次方程:$4X^4-4aX^2+b^2\xi^{q^l+1}=0$. 设 $D:=a^2-b^2\xi^{q^l+1}$. 我们考虑以下两种情况

(i) 如果 D 是 $\mathbb{F}_q$ 中的非平方元, 那么这四次方程在 $\mathbb{F}_q$ 上没有解.

(ii) 如果 D 是 $\mathbb{F}_q$ 中的平方元, 那么二次方程 $4T^2-4aT+b^2\xi^{q^l+1}=0$ 在 $\mathbb{F}_q$ 上有两个解且这两个解的乘积是 $\mathbb{F}_q$ 中的非平方元 $\frac{1}{4}b^2\xi^{q^l+1}$, 其中一个解是 $\mathbb{F}_q$ 中的平方元.

综上所述, 我们已经完成后面两个命题的证明. □

下面我们回忆一下 *Dickson* 半域的描述.

定理 2.5 **(定理** 1.1, Blokhuis **和** Lavrauw[50]**).** 令 $\mathbb{S}=(\mathbb{F}_{q^{2n}},+,*)$ 是具有中心 $\mathbb{F}_q$ 和 middle nucleus $\mathbb{F}_{q^n}$ 的交换半域, 其中 q 是奇数. 如果 $q\geq 4n^2-8n+2$, 那么 $\mathbb{S}$ 要么是一个 Dickson 半域或者是一个有限域.

将以上定理应用于 $n=2$ 的情况, 我们推出预半域必须跟一个 *Dickson* 半域是 *isotopic*. 因此, 我们以下将只考虑 $l>2$ 的情况. 此外, 根据引理 *2.2*, 我们可以不失一般性地假设 $0<d<l$.

2.3 Budaghyan-Helleseth 预半域的 *Strong isotopisms* 类

在这节中, 我们考虑 *Budaghyan-Helleseth* 预半域的 *strong isotopisms* 类, 其中该节中主要的结果如下所示.

定理 2.6. 如果 $0<d,\, d'\leq l-1$, 那么 $BH(q,\,l,\,d)$ 和 $BH(q,\,l,\,d')$ 是 strongly isotopic 当且仅当 $d=d'$. 而且 $BH(q,\,l,\,d)$ 的 strong autotopism 构成的群的阶是 $4lh(q^l-1)$.

我们把证明分成下面几个引理. 假设 $BH(q,l,d)$ 和 $BH(q,l,d')$ 是 *strongly isotopic*, 其中 $0<d,\,d'\leq l-1$. 那么存在 $\mathbb{F}_{q^{2l}}$ 上的线性化置换多项式 $L(x)$, $N(x)$ 使得

$$L(x*_d y)=N(x)*_{d'}N(y). \tag{2.3}$$

记 $L(x)=\sum_{i=0}^{2lh-1}a_ix^{p^i}$ 以及 $N(x)=\sum_{i=1}^{2lh-1}b_ix^{p^i}$, 其中它们的多项式系数都属于 $\mathbb{F}_{q^{2l}}$. 记得我们有 $q=p^h$. 我们将在 a_i 和 b_i 的下标中做加减法, 其中这些下标都取模 $2lh$. 令 C_L 和 C_R 分别是等式 (2.3)的左手边和右手边. 那么我们有

$$C_L=L\left(\mathrm{Tr}(x^{q^l}y)+\mathrm{Tr}\big(\beta(x^{q^d}y+xy^{q^d})\big)\,\omega\right),$$

以及

$$C_R = \mathrm{Tr}\left(N(x)^{q^l}N(y)\right) + \mathrm{Tr}\left(\beta(N(x)^{q^{d'}}N(y) + N(x)N(y)^{q^{d'}})\right)\omega.$$

于是我们推出

$$C_L + C_L^{q^l} = 2N(x)^{q^l}N(y) + 2N(x)N(y)^{q^l}, \tag{2.4}$$

$$C_L - C_L^{q^l} = 2\,\mathrm{Tr}\left(\beta\big(N(x)^{q^{d'}}N(y) + N(x)N(y)^{q^{d'}}\big)\right)\omega. \tag{2.5}$$

注意到这两个方程对所有 $x, y \in \mathbb{F}_{q^{2l}}$ 都成立. 因此我们将他们看作在多项式商环 $\mathbb{F}_{q^{2l}}[X,Y]/(X^{q^{2l}} - X, Y^{q^{2l}} - Y)$ 中的多项式恒等式. 在之后的讨论中, 我们需要理解以下符号:

$$x = \overline{X}, y = \overline{Y} \quad \text{和} \quad \mathrm{Tr}(x^{p^i}y^{p^j}) = \overline{X}^{p^i}\,\overline{Y}^{p^j} + \overline{X}^{p^iq^l}\,\overline{Y}^{p^jq^l},$$

所以我们讨论单项式 x^uy^v 的系数是有意义的, 其中 $0 \le u, v \le q^{2l} - 1$. 一个关键观察是如果 $j - i \pmod{2lh} \notin \{lh, dh, (2l-d)h\}$, 那么 $x^{p^i}y^{p^j}$ 在等式 (2.4), (2.5)中左手边的系数为零.

引理 2.7. 设 $b_i \neq 0$. 如果 $j - i \pmod{2lh} \notin \{0, (l+d)h, (l-d)h\}$, 那么 $b_j = 0$ 以及 $b_{j+(l-d')h} = 0$.

证明. 我们比较等式 (2.4), (2.5)中 $x^{p^i}y^{p^i}$ 的系数可得

$$4b_ib_{i+lh}^{q^l} = 0, \quad \beta b_{i-d'h}^{q^{d'}}b_i + \beta^{q^l}b_{i+(l-d')h}^{q^{d'+l}}b_{i+lh}^{q^l} = 0.$$

于是很容易得到 $b_{i+lh} = 0$ 和 $b_{i-d'h} = 0$. 令 j 是在本引理中给出的整数. 比较等式 (2.4), (2.5)中 $x^{p^i}y^{p^{j+lh}}$ 的系数, 我们可得

$$b_ib_j^{q^l} = 0 \text{和} \beta b_ib_{j+(l-d')h}^{q^{d'}} + \beta^{q^l}b_{i+(l-d')h}^{q^{l+d'}}b_j^{q^l} = 0.$$

于是就有 $b_j = 0$ 和 $b_{j+(l-d')h} = 0$. □

引理 2.8. 若存在满足 $j - i \pmod{2lh} \in \{(l+d)h, (l-d)h\}$ 的整数 i, j, 那么我们有 $N(x) = b_ix^{p^i} + b_jx^{p^j}$.

证明. 假设 $b_i \neq 0$. 根据引理 *2.7*, 只有 $j - i \pmod{2lh} \in \{0, lh + dh, lh - dh\}$ 时, 我们才有 $b_j \neq 0$. 于是通过 $\gcd(l, d) = 1$ 和 $l + d$ 是奇数的条件去直接验证 $(i + lh + dh) - (i + lh - dh) = 2dh \notin \{0, lh + dh, lh - dh\}$. 因此根据同一个引理可知 $b_{i+(l+d)h}$ 和 $b_{i+(l-d)h}$ 不全为零. □

引理 2.9. 我们有 $d = d'$, 并且 $N(x)$ 是单项式.

证明. 如果 $d' \neq d$, 那么 $d'h \notin \{lh, dh, (2l-d)h\}$, 且通过检查等式 (2.5)中 $x^{p^i q^{d'}} y^{p^i}$ 和 $x^{p^j q^{d'}} y^{p^j}$ 的系数, 我们可知 $\beta b_i^{q^{d'}+1} = \beta b_j^{q^{d'}+1} = 0$, 所以 $b_i = b_j = 0$ 和 $N(x) \equiv 0$: 这与 N 是置换多项式的假设相矛盾. 这就证明了 $d' = d$. 如果有必要的话就交换下标 i, j, 那么我们不失一般性地假设 $j = i + (d+l)h \pmod{2lh}$. 跟前面的叙述一样, 我们能验证

$$j + dh - i = (2d+l)h \pmod{2lh} \notin \{lh, dh, (2l-d)h\},$$

则等式 (2.5)中 $x^{p^{j+dh}} y^{p^i}$ 的系数就可推出 $\beta b_j^{q^d} b_i = 0$. 因此 $N(x)$ 是单项式. □

现在我们就可以完成主要定理的证明. 根据引理 *2.9*, 我们假设 $N(x) = bx^{p^i}$, 其中 $0 \leq i \leq 2lh - 1$. 通过展开等式 (2.3), 我们可得

$$L(\mathrm{Tr}(x^{q^l} y)) + L(\mathrm{Tr}(\beta(x^{q^d} y + x y^{q^d}))\omega) = b^{q^l+1}\mathrm{Tr}(x^{q^l} y) + \mathrm{Tr}(\beta b^{q^d+1}(x^{q^d} y + x y^{q^d}))\omega.$$

通过比较上式两边的系数, 我们可知该等式成立当且仅当

$$a_j + a_{j+lh} = \begin{cases} b^{q^l+1}, & \text{if } j = i, \\ b^{q^l+1}, & \text{if } j = i + lh, \\ 0, & \textit{otherwise.} \end{cases} \qquad a_j - a_{j+lh} = \begin{cases} b^{q^d+1}, & \text{if } j = i, \\ -b^{q^{d+l}+q^l} & \text{if } j = i + lh, \\ 0, & \textit{otherwise.} \end{cases}$$

于是在 $j \neq i \pmod{lh}$ 时 $a_j = a_{j+lh} = 0$, 且 $b^{q^d+1} = b^{q^{d+l}+q^l}$, 也就是 $b^{(q^d+1)(q^l-1)} = 1$. 接着我们通过解线性方程组可得

$$L(x) = \frac{1}{2} b^{q^l+1}(x + x^{q^l})^{p^i} + \frac{1}{2} b^{q^d+1}(x - x^{q^l})^{p^i}.$$

由引理 *2.1*可知 $\gcd(q^d+1, q^l+1) = 2$, 所以我们从 $b^{(q^d+1)(q^l-1)} = 1$ 中推出 $b^2 \in \mathbb{F}_{q^l}$. 注意到我们选定的 ω 满足 $\omega^{q^l} = -\omega$, 因此我们就能推出 $b \in \mathbb{F}_{q^l}^* \cup \mathbb{F}_{q^l}^* \omega$. 那么映射 $x \mapsto N(x)$ 是 $\mathbb{F}_{q^{2l}}$ 中的一个置换. 又因为等式 (2.3)成立, 所以 $x \mapsto L(x)$ 自然成为 $\mathbb{F}_{q^{2l}}$ 中的一个置换. 因此, 我们用这种方式得到所需要的 *strong isotopism* (N, N, L). 这就完成定理 *2.6*的证明.

2.4 Budaghyan-Helleseth 预半域的 *Isotopism* 类

本节致力于证明下面的定理.

定理 2.10. 如果 $0 < d, d' < l$, 那么预半域 $BH(q, l, d)$ 和 $BH(q, l, d')$ 是 isotopic 当且仅当以下其中一个条件成立.

(i) $d' = d$,

(ii) $q \equiv 1 \pmod 4$, $d' = l - d$ 且 l 是偶数.

我们再次把主要定理的证明分成几个引理. 我们首先介绍一些将在本节中使用的符号. 令 $\mathbb{S}_d = (\mathbb{F}_{q^{2l}}, +, \star_d)$ 是预半域 $BH(q, l, d)$ 对应的半域的 *isotope,* 其中乘法 $\star_d$ 如等式 (2.2)定义所示. 对于 $x \in \mathbb{F}_{q^{2l}}$, 定义符号 $K_d(x) = x *_d 1$. 令 $*_{d'}$, $\star_{d'}$, $\mathbb{S}_{d'}$ 和 $K_{d'}$ 是预半域 $BH(q, l, d')$ 对应的符号. 为了证明我们的结果, 我们再回忆以下结果

定理 2.11 ((定理 2.5, Coulter 和 Henderson[51])). 令 $\mathbb{S}_1 = (\mathbb{F}_q, +, \star_1)$ 和 $\mathbb{S}_2 = (\mathbb{F}_q, +, \star_2)$ 是 isotopicd 交换半域. 那么在 $\mathbb{S}_1$ 和 $\mathbb{S}_2$ 之间存在一个 isotopism(M, N, L) 以致以下其中一个条件成立:

(i) $M = N$;

(ii) $M(x) \equiv \alpha \star_1 N(x) \mod (X^q - X)$, 其中 $\alpha \in N_m(\mathbb{S}_1)$ 不可以写成 $N(\mathbb{S}_1)$ 的元素与 $N_m(\mathbb{S}_1)$ 的平方元的乘积.

假定两个预半域 $BH(q, l, d)$ 和 $BH(q, l, d')$ 是 *isotopic,* 所以对应的半域 $\mathbb{S}_d$ 和 $\mathbb{S}_{d'}$ 是 *isotopic.* 如果它们是 *strongly isotopic,* 那么我们根据定理 *2.6*可得 $d = d'$. 现在假设两个预半域是 *isotopic* 但不 *strongly isotopic.* 根据定理 *2.11,* 存在两个 $\mathbb{F}_{q^{2l}}$ 上的线性化置换多项式 $L(x)$, $N(x)$ 和 $N_m(\mathbb{S}_d)$ 中的非平方元使得对所有 $x, y \in \mathbb{F}_{q^{2l}}$ 有 $(N(x) \star_d \alpha) \star_d N(y) = L(x \star_{d'} y)$. 通过变量替换, 我们可以将上式改成

$$(K_d(x) \star_d \alpha) \star_d K_d(y) = L\left(N^{-1}(K_d(x)) \star_{d'} N^{-1}(K_d(y))\right). \tag{2.6}$$

因为 $K_{d'}(x) \star_{d'} K_{d'}(y) = x *_{d'} y$, 所以等式 (2.6)的右手边等于

$$L\left(K_{d'}^{-1}\left(N^{-1}(K_d(x))\right) *_{d'} K_{d'}^{-1}\left(N^{-1}(K_d(y))\right)\right).$$

那么定义符号 $L' := L^{-1}$ 和 $N' := K_{d'}^{-1} N^{-1} K_d$, 等式 (2.6)可变成以下形式:

$$L'\left((K_d(x) \star_d \alpha) \star_d K_d(y)\right) = N'(x) *_{d'} N'(y).$$

根据定理 *2.3*可知存在 $a, b \in \mathbb{F}_q$ 使得 $\alpha = \kappa(a, b)$ 且 $K_d(x) \star_d \alpha = K_d(ax + b\xi x^{q^l})$, 其中 ξ 是满足 $\xi^{q^{l+d}-1} = \beta^{1-q^l}$ 的常数. 由引理 *2.4*可得 $b \neq 0$. 于是将此代入上述等式, 我们得到

$$L'(a \cdot x *_d y) + L'(b \cdot (\xi x^{q^l}) *_d y) = N'(x) *_{d'} N'(y). \tag{2.7}$$

像第 *2.3*节的论证一样, 我们定义等式 (2.7)的左手边和右手边分别为 C_L 和 C_R. 通过

展开公式, 我们得到 C_L 的表达式, 如下所示：

$$L'\left(a\,\mathrm{Tr}(x^{q^l}y)\right)+L'\left(b\,\mathrm{Tr}(\xi^{q^l}xy)\right)+L'\left(a\,\mathrm{Tr}\big(\beta(x^{q^d}y+xy^{q^d})\,\omega\right)$$
$$+L'\left(b\,\mathrm{Tr}\big(\beta\xi(x^{q^d}y^{q^l}+x^{q^l}y^{q^d})\big)\,\omega\right).$$

在最后一项中, 我们使用了条件 $\xi^{q^{l+d}-1}=\beta^{1-q^l}$. 根据 $*_{d'}$ 的定义,

$$C_R=\mathrm{Tr}\left(N'(x)N'(y)^{q^l}\right)+\mathrm{Tr}\left(\beta(N'(x)^{q^{d'}}N'(y)+N'(x)N'(y)^{q^{d'}})\right)\,\omega.$$

从以上这些公式的表达式中我们可以计算出

$$C_L+C_L^{q^l}=2\,N'(x)^{q^l}N'(y)+2\,N'(x)N'(y)^{q^l}, \tag{2.8}$$
$$C_L-C_L^{q^l}=2\,\mathrm{Tr}\left(\beta(N'(x)^{q^{d'}}N'(y)+N'(x)N'(y)^{q^{d'}})\right)\,\omega. \tag{2.9}$$

因为 L' 和 N' 都是线性化多项式, 所以我们有

$$L'(x)=\sum_{i=0}^{2lh-1}a_ix^{p^i},\quad N'(x)=\sum_{i=0}^{2lh-1}b_ix^{p^i},$$

其中 a_i 和 $b_i,(0\le i\le 2lh-1)$ 是 $\mathbb{F}_{q^{2l}}$ 中的常数. 并且系数 a_i 和 b_i 的下标都是像第 *2.3*节的一样对下标取模 $2lh$. 通过使等式 (2.8)和(2.9)的两边取定的单项式的系数想等, 我们能推出关于 L 以及 N 的多项式系数的限制.

引理 2.12. 我们有 l 是偶数, 以及 d,d' 都是奇数. 而且如果对于某个 i 有 $b_i\neq 0$, 那么存在 $\gamma_i\in\mathbb{F}_{q^l}^*$ 使得 $\gamma_i^{p^{-i}}$ 是二次多项式 $\xi^{q^l+1}X^2-2(ab^{-1})X+1\in\mathbb{F}_q[X]$ 的根以及 $b_{i+lh}=b_i\xi^{p^i}\gamma_i\neq 0$.

证明. 因为 N' 是置换多项式, 所以至少有一个非零的多项式系数. 不妨假定 $b_i\neq 0$, 其中 $0\le i\le 2lh-1$. 我们在等式 (2.8)的两边中分别比较三个单项式 $x^{p^i}y^{p^i}$, $x^{p^iq^l}y^{p^i}$ 和 $x^{p^iq^l}y^{p^iq^l}$ 的系数, 于是得到

$$\mathrm{Tr}(a_i+a_{i+lh})\,(b\xi^{q^l})^{p^i}=4b_{i+lh}^{q^l}b_i \tag{2.10}$$
$$\mathrm{Tr}(a_i+a_{i+lh})\,a^{p^i}=2b_i^{q^l+1}+2b_{i+lh}^{q^l+1} \tag{2.11}$$
$$\mathrm{Tr}(a_i+a_{i+lh})\,(b\xi)^{p^i}=4b_i^{q^l}b_{i+lh}. \tag{2.12}$$

因为上述等式的右手边不全为零, 所以 $\mathrm{Tr}(a_i+a_{i+lh})\neq 0$. 由引理 *2.4*可得 $b\neq 0$, 故等式 (2.10)和(2.12)证明了对某个 $\gamma_i\in\mathbb{F}_{q^l}^*$ 有 $b_{i+lh}\neq 0$ 和 $b_{i+lh}=b_i\xi^{p^i}\gamma_i$. 这就证明引理的第二部分.

从等式 (2.10)-(2.12)中我们能推出

$$b_i^{-(q^l+1)}\cdot\mathrm{Tr}(a_i+a_{i+lh})=4b^{-p^i}\gamma_i=2a^{-p^i}(1+\xi^{p^i(q^l+1)}\gamma_i^2).$$

因此, $4b^{-p^i}\gamma_i = 2a^{-p^i}(1+\xi^{p^i(q^l+1)}\gamma_i^2)$, 而且它可简化为 $\xi^{q^l+1}(\gamma_i^{p^{-i}})^2 - 2ab^{-1}\gamma_i^{p^{-i}} + 1 = 0$. 这个方程 $\xi^{q^l+1}X^2 - 2ab^{-1}X + 1 = 0$ 的多项式系数都在 $\mathbb{F}_q$ 中, 并且根据引理 *2.4*可知它的判别式 $4((ab^{-1})^2 - \xi^{q^l+1})$ 是 $\mathbb{F}_q$ 中的非平方元. 因为 $\gamma_i^{p^{-i}}$ 是其中一个解, 所以我们有 $\gamma_i \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. 根据假设 $\gamma_i \in \mathbb{F}_{q^l}^*$, 故 l 必须是偶数. 回想一下, 我们有 $l+d$ 和 $l+d'$ 都是奇数, 于是 d 和 d' 也都是奇数. 证毕. □

注意到如果 C_L 中某一项 $x^{p^i}y^{p^j}$ $(0 \le i, j \le 2lh-1)$ 的系数非零, 那么 $i-j \pmod{2lh}$ 必须属于 $\{0, lh, dh, 2lh-dh, dh+lh, lh-dh\}$, 换言之, $i-j \pmod{lh} \in \{0, dh, lh-dh\}$. 对于 $C_L^{q^l}$ 也有同样的结论. 因此, 如果 $i-j \pmod{lh} \notin \{0, dh, lh-dh\}$, 那么等式 (2.8), (2.9)的右手边的 $x^{p^i}y^{p^j}$ 的系数全为零, 即

$$b_{i+lh}^{q^l}b_j + b_i b_{j+lh}^{q^l} = 0, \tag{2.13}$$

$$\beta(b_{i-d'h}^{q^{d'}}b_j + b_i b_{j-d'h}^{q^{d'}}) + \beta^{q^l}(b_{i-d'h+lh}^{q^{d'}}b_{j+lh} + b_{i+lh}b_{j-d'h+lh}^{q^{d'}})^{q^l} = 0. \tag{2.14}$$

引理 2.13. 令 (i, j) 满足以下条件:

$$0 \le i, j \le 2lh-1, \quad i-j \pmod{lh} \notin \{0, dh, lh-dh\}. \tag{2.15}$$

如果 $b_i \neq 0$, 那么 $b_j = 0$.

证明. 通过前面引理的证明, 等式 (2.13) 对 (i, j) 成立. 记 $i' = i + lh \pmod{2lh}$. 因为 (i', j) 也同样地满足条件(2.15), 所以我们将等式 (2.13)中的 i 替换为 i' 可得

$$b_i^{q^l}b_j + b_{i+lh}b_{j+lh}^{q^l} = 0. \tag{2.16}$$

假设 $b_j \neq 0$. 由引理 *2.12*可得存在 $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 中的 γ_i, γ_j 以致 $b_{i+lh} = b_i\xi^{p^i}\gamma_i$ 和 $b_{j+lh} = b_j\xi^{p^j}\gamma_j$ 成立. 我将它们分别代入等式 (2.13)和(2.16), 则得到

$$b_i^{q^l}b_j\xi^{p^iq^l}\gamma_i = -b_i b_j^{q^l}\xi^{p^jq^l}\gamma_j, \quad b_i^{q^l}b_j = -b_i b_j^{q^l}\xi^{p^i+p^jq^l}\gamma_i\gamma_j.$$

结果就是 $(b_ib_j^{-1})^{q^l-1}$ 跟 $-\xi^{p^jq^l-p^iq^l}\gamma_j\gamma_i^{-1}$ 和 $-\xi^{p^i+p^jq^l}\gamma_i\gamma_j$ 都相等. 利用后面两个数相等的事实, 我们可推出 $\xi^{q^l+1}\gamma_i^{2p^{-i}} - 1 = 0$. 同时根据引理 *2.12*, 我们有 $\xi^{q^l+1}\gamma_i^{2p^{-i}} - 2ab^{-1}\gamma_i^{p^{-i}} + 1 = 0$. 这样就有 $ab^{-1}\gamma_i^{p^{-i}} = 1$, 所以 $a \neq 0$ 且 $\gamma_i^{p^{-i}} \in \mathbb{F}_q$. 这与 $\gamma_i \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 相矛盾. 因此 b_j 必须等于 0. □

定义集合 Λ 如下:

$$\Lambda := \{0 \le i \le 2lh-1 : b_i \neq 0\}.$$

根据引理 *2.12*, $i \in \Lambda$ 当且仅当 $i+lh \pmod{2lh}$ 是属于 Λ. 对于 Λ 中任意两个不同的元素, 利用引理 *2.13*可知它们的差模 lh 后属于 $\{0, dh, lh-dh\}$. 于是我们声称：

$$\{i \pmod{lh} : i \in \Lambda\}\text{的大小最多为 } 2.$$

否则模 $2lh$ 后它包含一个公差为 dh 的等差数列. 注意到这两个不相邻的项之间的差值是 $2dh \pmod{lh}$, 并且该差值属于集合 $\{0, dh, lh-dh\}$. 而这种情况只有在 lh 整除 $2dh$ 或 $3dh$ 时才发生. 因为根据引理 *2.12*可知 l 是偶数和 d 是奇数, 所以我们必然有 $l = 2d$. 然而, 由 $\gcd(l, d) = 1$ 可知 $l = 2$ 和 $d = 1$, 这与假设 $l > 2$ 相矛盾. 于是这就完成我们的声称的证明.

令 i 是 Λ 中的最小元. 然后 $\Lambda \subseteq \{i, i+dh, i+lh, i+dh+lh\}$, 并且有

$$N'(x) = b_i x^{p^i} + b_{i+lh} x^{p^{i+lh}} + b_{i+dh} x^{p^{i+dh}} + b_{i+dh+lh} x^{p^{i+dh+lh}}. \tag{2.17}$$

此外, 由引理 *2.12*可知存在 $\gamma_j \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 使得对 $j \in \Lambda$ 均有 $b_{j+lh} = b_j \xi^{p^j} \gamma_j$ 和 $\gamma_j^{q+1} = \xi^{-p^j(q^l+1)}$. 接着我们从一个技术引理开始.

引理 2.14. *不存在奇整数 k 使得*

$$\beta b_i^{q^k+1} + \beta^{q^l} b_{i+lh}^{(q^k+1)q^l} = 0, \quad \beta b_i^{q^k} b_{i+lh} + \beta^{q^l} b_{i+lh}^{q^{k+l}} b_i^{q^l} = 0. \tag{2.18}$$

证明. 我们将 $b_{i+lh} = b_i \xi^{p^i} \gamma_i$ 代入以上方程, 经简化后可得

$$(\beta b_i^{q^k+1})^{q^l-1} \xi^{p^i(q^{k+l}+q^l)} \gamma_i^{q+1} = -1, \quad (\beta b_i^{q^k+1})^{q^l-1} \xi^{p^i(q^{k+l}-1)} \gamma_i^{q-1} = -1.$$

对它们二者作商后得 $\gamma_i^2 = \xi^{-p^i(q^l-1)}$. 根据前面的条件 $\gamma_i^{q+1} = \xi^{-p^i(q^l+1)}$, 我们能推出 $\gamma_i^{q-1} = 1$, 这与 $\gamma_i \notin \mathbb{F}_q$ 这事实相矛盾. □

引理 2.15. *我们有 $d' = d$ 或 $d' = l - d$.*

证明. 我们用反证法证明. 假设 $d' \neq d, l-d$. 因为我们有

$$i + d'h \notin \{i, i+dh, i+lh, i+dh+lh\},$$

所以 $b_{i+d'h} = b_{i+d'h+lh} = 0$. 考虑两对数 $(i+d'h, i)$, $(i+d'h, i+lh)$, 其中每个数都是取模 $2lh$, 于是它们就满足条件(2.15), 然后利用条件 $b_{i+d'h} = b_{i+d'h+lh} = 0$, 则等式(2.14)就取等式 (2.18)在 $k = d'$ 时的形式. 这与引理 *2.14*相矛盾. □

引理 2.16. *我们有 $b_{i+dh} = b_{i+dh+lh} = 0$, 于是 $N'(x) = b_i x^{p^i} + b_{i+lh} x^{p^{i+lh}}$.*

证明. 根据引理 *2.12*, 我们只需要证明 $b_{i+dh}=0$. 假设 $b_{i+dh}\neq 0$. 我们有 $i+2dh\notin\{i,\, i+lh,\, i+dh,\, i+dh+lh\}$, 所以 $b_{i+2dh}=b_{i+2dh+lh}=0$. 这个证明与引理 *2.15*的证明很相似, 接着我们需要把证明分成两种情况.

Case 1: $d'=d$. 在这种情况下, $(i+2dh,\, i)$ 和 $(i+2dh,\, i+lh)$ 满足条件(2.15), 其中每对数中的每一项都是取模 $2lh$. 再利用 $b_{i+2dh}=b_{i+2dh+lh}=0$ 可将等式 (2.14)转化为

$$\beta b_{i+dh}^{q^d}b_i+\beta^{q^l}b_{i+dh+lh}^{q^{d+l}}b_{i+lh}^{q^l}=0,\ \beta b_{i+dh}^{q^d}b_{i+lh}+\beta^{q^l}b_{i+dh+lh}^{q^{d+l}}b_i^{q^l}=0.$$

像引理 *2.15*的证明一样, 我们推出

$$(\beta b_{i+dh}^{q^d}b_i)^{q^l-1}\gamma_i\gamma_{i+dh}^{q}\xi^{p^i(q^{l+2d}+q^l)}=-1,\quad (\beta b_{i+dh}^{q^d}b_i)^{q^l-1}\gamma_i^{-1}\gamma_{i+dh}^{q}\xi^{p^i(q^{l+2d}-1)}=-1.$$

论证的剩余部分与引理 *2.15*的证明一样.

Case 2: $d'=l-d$. 在这种情况下, 通过考虑 $(i+d'h,\, i+dh)$ 和 $(i+d'h,\, i+dh+lh)$, 相同的论证会得到 $\gamma_{i+dh}\in\mathbb{F}_q$, 而事实上 $\gamma_{i+dh}\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$, 因此我们得到一个矛盾. □

引理 2.17. 我们有 $d'=l-d$.

证明. 根据引理 *2.15*有 $d'=d$ 或 $d'=l-d$, 于是我们相反地假设 $d=d'$. 我们比较在等式(2.7)中 $x^{p^{i+dh}}y^{p^i}$ 和 $x^{p^{i+dh}}y^{p^{i+lh}}$ 的系数, 则可得方程

$$\begin{aligned}(a_i-a_{i+lh})\,(a\beta\omega)^{p^i}&=(\beta b_i^{q^d+1}+\beta^{q^l}b_{i+lh}^{q^{d+l}+q^l})\,\omega,\\(a_i-a_{i+lh})\,(b\beta\xi\omega)^{p^i}&=(\beta b_i^{q^d}b_{i+lh}+\beta^{q^l}b_{i+lh}^{q^{d+l}}b_i^{q^l})\,\omega.\end{aligned}$$

如果 $a_i=a_{i+lh}$, 那么我们将得到与在 $k=d$ 时的引理 *2.14*矛盾的结论. 因此 $a_i-a_{i+lh}\neq 0$. 我们现在对以上两个等式作商并将 $b_{i+h}=b_i\xi^{p^i}\gamma_i$ 代入可得

$$(ab^{-1}\xi^{-1})^{p^i}=\frac{1+(\beta b_i^{q^d+1})^{q^l-1}\xi^{p^i(q^{d+l}-1)}}{\xi^{p^i}\gamma_i+(\beta b_i^{q^d+1})^{q^l-1}\xi^{p^iq^{d+l}}\gamma_i^q}.$$

在上述的计算过程中, 我们使用 $\gamma_i^{q+1}=\xi^{-p^i(q^l+1)}$. 定义符号 $t:=(\beta b_i^{q^d+1})^{q^l-1}\xi^{p^i(q^{l+d}-1)}$, 我们可将上述等式改写成 $((ab^{-1})^{p^i}\gamma_i^q-1)\,t=-(ab^{-1})^{p^i}\gamma_i+1$. 回忆 $\xi^{q^l+1}\in\mathbb{F}_q$, $\gamma_i\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ 和 l 是偶数. 将两边提到 (q^l+1) 次方, 我们推出 $(1-\gamma_i^q(ab^{-1})^{p^i})^2-(1-\gamma_i(ab^{-1})^{p^i})^2=0$. 于是就有 $(ab^{-1})^{p^i}\,(2-(ab^{-1})^{p^i}(\gamma_i+\gamma_i^q))=0$.

根据引理 *2.12*, 我们有 $\gamma_i+\gamma_i^q=2(ab^{-1})^{p^i}\xi^{-p^i(q^l+1)}$, 所以

$$\begin{aligned}2-(ab^{-1})^{p^i}\,(\gamma_i+\gamma_i^q)&=2-2(ab^{-1})^{2p^i}\xi^{-p^i(q^l+1)}\\&=-2b^{-2p^i}\xi^{-p^i(q^l+1)}(a^2-b^2\xi^{q^l+1})^{p^i}.\end{aligned}$$

这个数是非零的, 这是因为 $a^2 - b^2\xi^{q^l+1}$ 是 $\mathbb{F}_q$ 中的非平方元. 所以我们必须有 $a = 0$, 且 $t = 1$. 回忆一下, 我们有 $\beta^{q^l-1} = \xi^{1-q^{l+d}}$, 因此由该等式可得 $b_i^{(q^d+1)(q^l-1)}\xi^{(p^i-1)(q^{l+d}-1)} = -1$. 将它提到 $\frac{q^l+1}{2}$ 次方, 它的左手边就等于 1. 但是因为 l 是偶数, 则我们有 $q^l \equiv 1 \pmod 4$ 和 $\frac{q^l+1}{2}$ 是奇数, 所以右手边依旧等于 -1, 这显然是一个矛盾. □

我们就可以完成主要定理的证明. 通过比较等式 (2.7)中 $x^{p^iq^{l-d}}y^{p^iq^l}$ 和 $x^{p^iq^{2l-d}}y^{p^iq^l}$ 的系数, 我们可得

$$(a_{i+lh-dh} - a_{i+2lh-dh})\,(a\beta\omega)^{p^iq^{l-d}} = (\beta b_i^{q^{l-d}}b_{i+lh} + \beta^{q^l}b_{i+lh}^{q^{2l-d}}b_i^{q^l})\,\omega,$$
$$(a_{i+lh-dh} - a_{i+2lh-dh})\,(b\beta\xi\omega)^{p^iq^{l-d}} = (\beta b_{i+lh}^{q^{l-d}+1} + \beta^{q^l}b_i^{q^{2l-d}+q^l})\,\omega.$$

利用跟引理 *2.17*中一样的论证, 我们推出 $a = 0$. 而 $a^2 - b^2\xi^{q^l+1}$ 是 $\mathbb{F}_q$ 中的非平方元这个事实暗示着 $(-\xi^{q^l+1})^{(q-1)/2} = -1$, 也就是说, $\xi^{(q^l+1)(q-1)/2} = (-1)^{(q+1)/2}$. 记得 $\xi^{q^l+d-1} = \beta^{1-q^l}$, β 也是 $\mathbb{F}_{q^{2l}}$ 的非平方元, 所以

$$-1 = \beta^{(q^{2l}-1)/2} = \xi^{(q^l+1)(q^{l+d}-1)/2} = (-1)^{(q+1)(l+d)/2} = (-1)^{(q+1)/2}.$$

在上述计算的过程中, 我们使用事实 $l+d$ 是奇数. 因此我们推出结论 $q \equiv 1 \pmod 4$.

于是在 $q \equiv 1 \pmod 4$ 以及 l 是大于 2 的偶数的情况下, 我们可以显式地构造 $BH(q, l, d)$ 和 $BH(q, l, l-d)$ 之间具有特定形式的 *isotopism*. 在这种情况下, ω 是 $\mathbb{F}_{q^{2l}}$ 中的非平方元, 其中 ω 是在等式 (2.1)中定义的元素并且满足 $\omega + \omega^{q^l} = 0$. 由引理 *2.2*, 我们可以在不改变 *isotopism* 类的意义下取 $\beta := w^{-1}$. 取定 $\xi \in \mathbb{F}_{q^2}^*$ 以致 $\xi^q + \xi = 0$ 成立. 那么就有 $\beta^{q^l-1} = \xi^{1-q^{l+d}} = -1$. 我们现在取 $a = 0$, $b = 1$, $\alpha = \kappa(a, b)$, 以及

$$L'(x) = \xi^{(q-3)/2}(x + x^{q^l}) + \xi^{-1}(x - x^{q^l})^{q^{l-d}}, \quad N'(x) = x + \xi^{(q-1)/2}x^{q^l}$$

易证 L' 和 N' 都是 $\mathbb{F}_{q^{2l}}$ 上的置换多项式, $a^2 - b^2\xi^{q^l+1} = -\xi^{q^l+1}$ 是 $\mathbb{F}_q$ 中的非平方元, 以及等式(2.7) 成立. 借助条件 $L' = L^{-1}$ 和 $N' = K_{d'}^{-1}N^{-1}K_d$, 我们能重新构造 L 和 N 使得 $(N, \alpha \star_d N, L)$ 是半域 $\mathbb{S}_d$ 和 $\mathbb{S}_{l-d}$ 之间的一个 *isotopism*. 这就完成定理 *2.10*的证明.

由定理 *2.10*的证明可知 $BH(q, l, d)$ 的 *autotopisms* 必须是 *strong autotopism*, 因此我们从定理 *2.3*和定理 *2.6*中推出预半域 $BH(q, l, d)$ 的 *autotopism* 构成的群的阶数为 $2lh(q^l - 1)(q^2 - 1)$. 并且根据定理 *2.10*也可以得到以下结果: 对于固定的 q 和 $l > 2$, *Budaghyan-Helleseth* 族的 *isotopism* 类的大小是以下两种情况的之一:

(i) 在 $q \equiv 1 \pmod 4$ 以及 l 是偶数时, 大小为集合 $\{0 < d < l : \gcd(l, d) = 1\}$ 的大小的一半;

(ii) 在其他情况下, 大小为集合 $\{0 < d < l : \gcd(l, d) = 1, \quad l + d \text{ 是奇数}\}$ 的大小.

也就是说,

(1) 在 $q \equiv 1 \pmod 4$ 以及 l 是偶数时, 大小为 $\phi(l)/2$;

(2) 在 $q \equiv 3 \pmod 4$ 以及 l 是偶数时, 大小为 $\phi(l)$;

(3) 在 l 是奇数时, 大小为 $\phi(l)/2$, 这是因为在 $l - d$ 和 d 中只有一个是偶数.

其中 ϕ 是著名的欧拉函数.

3 PG$(2,q^2)$ 中非经典 *unitals* 的 *O'Nan* 构型

3.1 介绍

一个 n 阶 *unital* 是一个包含 n^3+1 个点的关联结构并且满足以下两个性质;

(1) 每个区组上有 $n+1$ 个点;

(2) 任意两个相异的点恰好在同一个区组上.

用设计的语言来说, 一个 *n* 阶 *unital* 实际上是一个参数为 2-$(n^3+1,n+1,1)$ 的设计. 除了一个阶为 6 的特殊例子[52,53] 以外, 所有已知的 *unital* 都是素数幂阶的. 当 q 是素数幂时, 经典 *q* 阶 *unital* 是由 *Desarguesian* 平面 PG$(2,q^2)$ 中酉极性 *(unitary polarity)* 定义的 *absolute* 点和 *nonabsolute* 线构成的. 令 $\mathcal{U}$ 是一个 q 阶 *unital*, 假如它能嵌入到一个 q^2 阶射影平面, 那么 $\mathcal{U}$ 是一个包含 q^3+1 个点的点集, 并且使得射影平面的每条线都恰好交 $\mathcal{U}$ 于 1 或 $q+1$ 个点. 对于 PG$(2,q^2)$ 中的线而言, 那些交 $\mathcal{U}$ 于一个点的线叫切线, 而交 $\mathcal{U}$ 于 $q+1$ 个点的线叫割线, 并且割线和 $\mathcal{U}$ 的交集就是 $\mathcal{U}$ 的区组 *(block)*.

在 *1976* 年, *Buekenhout*[12] 使用 *Bruck-Bose* 模型去证明每个二维 *translation* 平面包含一个 q 阶 *unital*, 随后人们将这种方式构造出来的 *unitals* 叫做 *Buekenhout unitals*. *Metz*[13] 指出在任意素数幂 $q>2$ 的情况下 PG$(2,q^2)$ 中存在非经典 *Buekenhout unitals*. 特别值得注意的是, 所有能嵌入到在有限 *Desarguesian* 射影平面的 *unitals* 都是 *Buekenhout unitals*. 若需要更多信息, 读者们请参考 *Barwick* 和 *Ebert* 的著作[14].

在 *1972* 年, *O'Nan*[15] 观察到经典 *unitals* 中不存在一类由四条两两交于一个点的线组成的构型, 而这类构型叫做 *O'Nan* 构型. 在文献[16] 中, *Piper* 猜想 *"O'Nan* 构型的不存在性是经典 *unitals* 的特征". 为了解决这一猜想, 学者们做了不少相关研究. *Wilbrink* 在文献[17] 中用 *O'Nan* 构型的不存在性和两个额外的条件得到经典 *unitals* 的内蕴式刻画. 在文献[19], *Hui* 等人对能嵌入到射影平面的 *unitals* 给出了一个充分必要条件, 并且以文献[17,54] 的结果为基础进一步加强 *Wilbrink* 的结果. 另一方面, 对于某些嵌入到 *non-Desarguesian* 射影平面的特定的 *unitals*, 其 *O'Nan* 构型的存在性已经在文献[18,20] 中给出.

在本章中, 我们主要考察在 *Desarguesian* 射影平面 PG$(2,q^2)$ 中 *Buekenhout unitals* 的 *O'Nan* 构型的存在性问题. 本章结构如下：第 *3.2*节介绍一些必要的背景知识和初步结果. 在第 *3.3*节中, 我们证明了每个非经典正交 *Buekenhout-Metz unital* $\mathcal{U}$ 都存在 *O'Nan* 构型, 而且这类构型是被 PΓL$(3,q^2)$ 中 $\mathcal{U}$ 的稳定子群的一个对合固定的.

在第 *3.4*节中, 我们同样地确定 *Buekenhout-Tits unitals* 中某类特殊的 *O'Nan* 构型的存在性, 这种构型包含一条固定的 *Baer* 子线.

3.2 准备工作

在介绍本章的主要工作前, 我们先固定一些符号. 令 p 为素数和 m 为正整数使得 $q := p^m$ 是大于 2 的素数幂. 对于 m 的因子 d, 我们定义迹函数如下

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^d}}(x) = x + x^{p^d} + \cdots + x^{p^{m-d}}, \forall x \in \mathbb{F}_q.$$

对于三维 $\mathbb{F}_q$-线性空间 $\mathbb{F}_q^3$ 中的一个非零向量 u, 我们定义

$$[u] := \{x \in \mathrm{PG}(2,q) : x \cdot u = 0\},$$

其中 $\cdot$ 是一般的欧几里得内积. 很明显, $[u]$ 是 $\mathrm{PG}(2,q)$ 中的一条直线.

为了更好地描述 *Buekenhout* 的构造, 我们先介绍几个相关几何结构的定义.

定义 3.1. $\mathrm{PG}(3,q)$ 中的一个 *ovoid* 是含有 q^2+1 个点的点集, 且使得其中任意三点不共线. 一个在 $\mathrm{PG}(4,q)$ 上的 *ovoidal* 椎体 *(ovoidal cone)* 是以 P 为顶点, 且以不过 P 的超平面中的 ovoid 为基的椎体 (cone). 其中椭圆椎体是以椭圆二次型 (elliptic quadratic) 为基的椎体.

定义 3.2. $\mathrm{PG}(3,q)$ 中的一个 *spread* $\mathcal{S}$ 是划分 $\mathrm{PG}(3,q)$ 中所有点的 q^2+1 条线的线集. 一个在 $\mathrm{PG}(3,q)$ 上的 *regulus* 是 $q+1$ 条线的线集且满足条件: 如果 $\mathrm{PG}(3,q)$ 中任意一条线跟这个 regulus 的某三条线相交, 则它与 regulus 中所有线都相交. 当在 $\mathcal{S}$ 上每三条相互不交的线都唯一地属于 S 中的一个 regulus 时, 这个 spread $\mathcal{S}$ 是正则的 (regular).

现在让我们简短地回顾从 *ovoidal* 椎体获得 *unitals* 的 *Buekenhout* 构造. 令 Σ_∞ 为 *4* 维射影空间 $\mathrm{PG}(4,q)$ 的一个超平面, 并且假定 Σ_∞ 包含一个 *spread* $\mathcal{S}$. 于是我们能定义关联结构 Π, 如下所示: Π 的点是在 $\mathrm{PG}(4,q) \setminus \Sigma_\infty$ 上的仿射点和属于 $\mathcal{S}$ 的线, Π 的线就是所有 $\mathrm{PG}(4,q)$ 上只交超平面 Σ_∞ 于 $\mathcal{S}$ 中某一条线的平面和 Σ_∞, 而关联关系是根据包含关系而来的. 这样的关联结构 Π 就是一个 *translation* 平面, 并被称为 *Bruck-Bose* 模型[55,56]. 取 $\mathrm{PG}(4,q)$ 中一个 *ovoidal* 椎体 U 使得它交超平面 Σ_∞ 于 $\mathcal{S}$ 的一条线 ℓ. 令 $\mathcal{U}$ 为 U 在 Π 中对应的像, 也就是所有仿射点和一个特殊点 ℓ 组成的点集. $\mathcal{U}$ 就成为了 Π 中的一个 *unital*, 这种 *unital* 被称为 *ovoidal Buekenhout-Metz unital*. 特别地, ℓ 就是 $\mathcal{U}$ 的特殊点. 当 U 是一个椭圆椎体 *(elliptic cone)* 时, 对应的 *unital* $\mathcal{U}$ 是一个正交 *Buekenhout-Metz unital;* 而当 U 是一个以 *Tits ovoid* 为基的椎体时, 对应

的 *unital* $\mathcal{U}$ 是一个 *Buekenhout-Tits unital*. 在本章接下来的讨论中, 我们将只考虑 Π 是 *Desarguesian* 射影平面 PG$(2,q^2)$ 的情况, 也就是说, $\mathcal{S}$ 是一个正则的 *spread*. 此外, 将以上 *ovoidal* 椎体替换成一个 PG$(4,q)$ 中非退化二次型也有类似的 *unital* 构造. *Barwick* 在文献[57] 中使用计数方法去说明这种用 PG$(4,q)$ 的非退化二次型的构造出不能得到 PG$(2,q^2)$ 中 *unitals* 的新例子, 换句话说, 这种方法得到的 *unital* 同构于经典 *unital*.

在文献[58,59] 中, *Baker* 和 *Ebert* 推出 $q>2$ 时 PG$(2,q^2)$ 中 *ovoidal Buekenhout-Metz unitals* 的具体表达式. 当 $q>2$ 时, PG$(2,q^2)$ 中每个正交 *Buekenhout-Metz unital* 都射影等价于以下形式

$$\mathcal{U}_{\alpha,\beta}=\{(x,\alpha\, x^2+\beta x^{q+1}+r,1):r\in\mathbb{F}_q\,,x\in\mathbb{F}_{q^2}\}\cup\{(0,1,0)\},\tag{3.1}$$

其中 α,β 是 $\mathbb{F}_{q^2}$ 中满足下列性质的元素:

1) 当 q 是奇数时, $d=(\beta-\beta^q)^2+4\alpha^{q+1}$ 是 $\mathbb{F}_q$ 中的非平方元;

2) 当 q 是大于 2 的偶数时, $\beta\notin\mathbb{F}_q$ 以及 $d=\frac{\alpha^{q+1}}{(\beta+\beta^q)^2}$ 的绝对迹是 0.

上述定义的参数 d 被称为 $\mathcal{U}_{\alpha,\beta}$ 的判别式. 当且仅当 $\alpha=0$ 时, $\mathcal{U}_{\alpha,\beta}$ 才是经典的. 这些 *unitals* 之间的等价性可以用下面的方式决定.

定理 3.3 (Baker 和 Ebert[58,59]). 令 $\mathcal{U}_{\alpha,\beta}$ 和 $\mathcal{U}_{\alpha',\beta'}$ 是 PG$(2,q^2)$ 中两个 unitals, 其中 $q>2$. 那么这两个 unitals 是射影等价的当且仅当存在 $f\in\mathbb{F}_q^*$, $s\in\mathbb{F}_{q^2}^*$, $u\in\mathbb{F}_q$ 和 $\sigma\in$ Aut$(\mathbb{F}_{q^2})$ 使得

$$\alpha'=\alpha^\sigma s^2 f \text{ 和 } \beta'=\beta^\sigma s^{q+1}f+u.$$

我们接下来描述一下 *Buekenhout-Tits unitals* 的表达式. 令 $q=2^m$, 其中 $C\,m$ 为一个大于 *1* 的奇数. 定义函数如下所示

$$f(x_0,x_1)=x_0^{\tau+2}+x_0x_1+x_1^\tau,\quad \text{其中}\tau:=2^{(m+1)/2}.$$

通过一个类似于文献[60] 的推导过程以及一些详细分析, 我们可以说明在 PG$(2,q^2)$ 中一个 *Buekenhout-Tits unital* 一定射影等价于以下形式:

$$\mathcal{U}_T=\{(0,1,0)\}\cup\{(x_0+x_1\delta,r+f(x_0,x_1)\delta,1):x_0,x_1,r\in\mathbb{F}_q\},\tag{3.2}$$

其中 δ 是 $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ 中一个元素, 并且 δ 的不同选取都会产生射影等价的 *unitals*. 特别地, PG$(2,q^2)$ 中 *Buekenhout-Tits unital* 在射影等价意义下是唯一的. 这里我们没有

找到任何参考文献包含这唯一性结果的证明, 但是因为它与文献[60] 中的证明非常相似, 故我们在本章中没有给出证明.

以下结果就是文献[61] 中的定理 *12.8.7.*

引理 3.4. 如果对 $\mathbb{F}_q$ 中 x, y 满足 $f(x,y) = x^{\tau+2} + xy + y^{\tau} \neq 0$, 那么

$$\frac{1}{f(x,y)} = f\left(\frac{y}{f(x,y)}, \frac{x}{f(x,y)}\right).$$

证明. 先直接通过运算可验证下面的公式

$$f(x,y)^{\tau+1} = y^{\tau+2} + xy(f(x,y))^{\tau} + x^{\tau}(f(x,y))^2.$$

接着在上述的公式两边同时除去 $f(x,y)^{\tau+2}$ 则得到引理的结论. □

我们也需要下面关于 *O'Nan* 构型的结果.

引理 3.5. (引理 7.42, Barwick 和 Ebert[14]) 令 $\mathcal{U}$ 为在 $\mathrm{PG}(2,q^2)$ 中一个 ovoidal Buekenhout-Metz unital, 其中 $q > 2$. 那么不存在包含 $\mathcal{U}$ 中特殊点的 O'Nan 构型.

3.3 正交 *Buekenhout-Metz unitals* 的 *O'Nan* 构型

在本节中, 我们主要证明下面的结果.

定理 3.6. $\mathrm{PG}(2,q^2)$ 中每个非经典正交 Buekenhout-Metz unital 都有一个 O'Nan 构型, 其中 $q > 2$.

令 $\mathcal{U}_{\alpha,\beta}$ 是 $\mathrm{PG}(2,q^2)$ 中如等式 (3.1)所定义的一个非经典正交 *Buekenhout-Metz unital,* 其中 $q > 2$. 在这里, 我们有 $\alpha \neq 0$, 并且记 d 为它的判别式. 设 $\mathcal{N}$ 为 $\mathcal{U}_{\alpha,\beta}$ 中一个假定的 *O'Nan* 构型. 根据文献[14] 中的定理 *4.12* 和 *4.23,* $\mathrm{P\Gamma L}(3,q^2)$ 中有一个子群保持 $\mathcal{U}_{\alpha,\beta}$ 不变还固定特殊点 $P_\infty = (0,1,0)$, 而且它传递地作用在点集 $\mathcal{U}_{\alpha,\beta}\backslash\{P_\infty\}$ 上. 因此, 我们可以不失一般性地假设这个 *O'Nan* 构型 $\mathcal{N}$ 具有一个固定的点 $P = (0,0,1)$. 我们的策略是让假定的 *O'Nan* 构型 $\mathcal{N}$ 被 $\mathrm{P\Gamma L}(3,q^2)$ 中 $\mathcal{U}_{\alpha,\beta}$ 的稳定子群的一个对合固定. 这将就大大减少问题的复杂度.

本节的剩下部分将致力于证明定理 *3.6.* 我们将分别处理奇特征和偶特征的情况. 下面先从一些技术引理开始.

引理 3.7. 令 $\mathcal{U}_{\alpha,\beta}$ 是 $\mathrm{PG}(2,q^2)$ 中一个非经典正交 Buekenhout-Metz unital, 如等式

(3.1)所示, 其中 $q>2$. 那么对所有的 $\lambda\in\mathbb{F}_q$ 和 $y\in\mathbb{F}_{q^2}^*$, 我们有

$$\alpha^{q+1}\neq(\lambda-\beta)^{q+1}\text{ 和}\alpha^q y+(\lambda-\beta)y^q\neq 0.$$

证明. 假定对某个 $\lambda\in\mathbb{F}_q$ 和 $y\in\mathbb{F}_{q^2}^*$ 有 $\alpha^q y+(\lambda-\beta)y^q=0$. 那么通过对 $\alpha^q y=-(\lambda-\beta)y^q$ 取 $(q+1)$ 次方, 我们推出 $\alpha^{q+1}y^{q+1}=(\lambda-\beta)^{q+1}y^{q+1}$, 也就是说, $\alpha^{q+1}=(\lambda-\beta)^{q+1}$. 接着我们考虑 q 是奇数或偶数的情况.

当 q 是奇数时, $\mathcal{U}_{\alpha,\beta}$ 的判断式 d 等于

$$d=(\beta-\beta^q)^2+4\alpha^{q+1}=(\beta-\beta^q)^2+4(\lambda-\beta)^{q+1}=(\beta+\beta^q-2\lambda)^2,$$

这与 d 是 $\mathbb{F}_q^*$ 中的非平方元的事实相矛盾.

当 q 是偶数时, 记 $\beta=b_0+b_1\delta$ 其中 $b_0,b_1\in\mathbb{F}_q$ 且 $\delta\in\mathbb{F}_{q^2}^*$ 满足 $\delta+\delta^q=1$. 根据文献[14] 的引理 *4.21* 可知 $v=\delta^2+\delta=\delta^{q+1}$ 的绝对迹为 1. 那么 $\mathcal{U}_{\alpha,\beta}$ 的判断式 d 等于

$$d=\frac{(\beta+\lambda)^{q+1}}{(\beta+\beta^q)^2}=\frac{(b_0+\lambda+b_1\delta)^{q+1}}{b_1^2}=\frac{(b_0+\lambda)^2}{b_1^2}+\frac{b_0+\lambda}{b_1}+v.$$

对两边取绝对迹, 我们得到 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(d)=1$, 这又是一个矛盾. 证毕. □

当 $y\in\mathbb{F}_{q^2}^*$ 时, 令 ℓ_y 为 PG$(2,q^2)$ 中一条线, 具体表达式如下所示

$$[y,1,0]=\{x\in\mathrm{PG}(2,q^2):x\cdot(y,1,0)=0\},$$

其中 $\cdot$ 是一般欧几里得内积. 易知这条线经过 $\mathcal{U}_{\alpha,\beta}$ 中一个点 $P=(0,0,1)$. 因为 $\mathcal{U}_{\alpha,\beta}$ 中过 P 的切线是 $[0,1,0]$, 所以 $B_y:=\ell_y\cap\mathcal{U}_{\alpha,\beta}$ 恰好包含 $q+1$ 个点, 而且是对应的 *unital* 中一个区组. 此外, 线 $\ell_\infty=[1,0,0]$ 与区组 $B_\infty=\{(0,r,1):r\in\mathbb{F}_q\}\cup\{(0,1,0)\}$ 相互对应.

引理 3.8. 对每个 $y\in\mathbb{F}_{q^2}^*$, 我们有

$$B_y=\left\{(x_\lambda,-x_\lambda y,1):x_\lambda=-\frac{\alpha^q y+(\lambda-\beta)y^q}{\alpha^{q+1}-(\lambda-\beta)^{q+1}},\ \lambda\in\mathbb{F}_q\right\}\cup\{(0,0,1)\}.$$

证明. 当 $x\neq 0$ 和 $r\in\mathbb{F}_q$ 时, $(x,\alpha x^2+\beta x^{q+1}+r,1)$ 属于 B_y 当且仅当 $yx+\alpha x^2+\beta x^{q+1}+r=0$. 记 $\lambda:=-rx^{-(q+1)}\in\mathbb{F}_q$, 于是我们有 $y+\alpha x+\beta x^q=\lambda x^q$. 对方程两边同时取 q 次方, 我们得到 $y^q+\alpha^q x^q+\beta^q x=\lambda^q x$. 现在就可以按常规方法推出 $x=-\frac{\alpha^q y+(\lambda-\beta)y^q}{\alpha^{q+1}-(\lambda-\beta)^{q+1}}$. 于是命题成立. □

3.3.1 奇特征的情况

考虑 PGL$(3,q^2)$ 中一个 *involutionary central collineation,* 如下所示:

$$\sigma:(x,y,z)\mapsto(-x,y,z).$$

它不但保持 $\mathcal{U}_{\alpha,\beta}$ 不变, 而且固定 B_∞ 中每一个点, 同时也把 B_y 映射到 B_{-y}, 其中 $y \in \mathbb{F}_{q^2}^*$. 现在我们假设 $\mathcal{U}_{\alpha,\beta}$ 具有一个特定的 *O'Nan* 构型使得它包含两条过点 $P = (0,0,1)$ 的线 ℓ_1 和 ℓ_{-1}. 设 ℓ' 和 $\ell'' = \sigma(\ell')$ 为 $\mathcal{N}$ 中另外两条线, 并且假设对于一个有待确定的元素 $r \in \mathbb{F}_q$ 有 $\ell' \cap \ell'' = (0,r,1) \in \mathcal{U}_{\alpha,\beta}$. 那么我们正在寻找的 *O'Nan* 构型会被 σ 固定, 如图 *3.1*所示. 由引理 *3.8*可知两条线 ℓ_1 和 ℓ' 的交点是

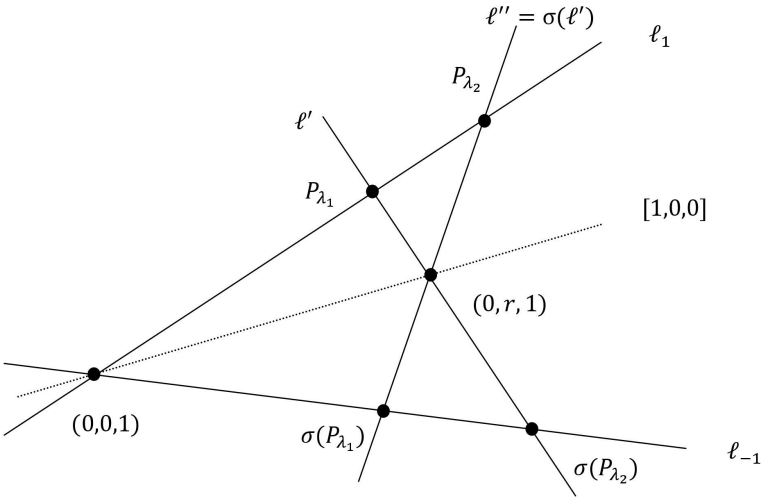

图 3.1　当 q 是奇数时 $\mathcal{U}_{\alpha,\beta}$ 中假定的 O'Nan 构型

$$P_{\lambda_1} = (x_{\lambda_1}, -x_{\lambda_1}, 1), \quad x_{\lambda_1} = -\frac{\alpha^q + \lambda_1 - \beta}{\alpha^{q+1} - (\lambda_1 - \beta)^{q+1}}$$

其中 $\lambda_1 \in \mathbb{F}_q$. 相似地, $\mathcal{N}$ 中剩下两条线 ℓ_1 和 ℓ'' 的交点是

$$P_{\lambda_2} = (x_{\lambda_2}, -x_{\lambda_2}, 1), \quad x_{\lambda_2} = -\frac{\alpha^q + \lambda_2 - \beta}{\alpha^{q+1} - (\lambda_2 - \beta)^{q+1}},$$

其中 $\lambda_2 \in \mathbb{F}_q$ 且 $\lambda_1 \neq \lambda_2$. 由此断定 $\sigma(P_{\lambda_1})$ 和 $\sigma(P_{\lambda_2})$ 分别是 ℓ'' 和 ℓ' 与线 $\ell_{-1} = \sigma(\ell_1)$ 的交点. 因此,

$$\ell' = \langle (x_{\lambda_1}, -x_{\lambda_1}, 1), (-x_{\lambda_2}, -x_{\lambda_2}, 1) \rangle, \quad \ell'' = \langle (x_{\lambda_2}, -x_{\lambda_2}, 1), (-x_{\lambda_1}, -x_{\lambda_1}, 1) \rangle.$$

在该节的余下部分中, 我们将确定参数 $\lambda_1, \lambda_2 \in \mathbb{F}_q$ 和 $r \in \mathbb{F}_q$ 的存在性使得如图 *3.1*所示的构型 $\mathcal{N}$ 形成一个 *O'Nan* 构型. 我们先直接地计算得到 $\ell' \cap \ell'' = (0,r,1)$ 和

$$r = -\frac{2x_{\lambda_1}x_{\lambda_2}}{x_{\lambda_1} + x_{\lambda_2}}. \tag{3.3}$$

为了让 $\mathcal{N}$ 是 *O'Nan* 构型, 只需要 $r \in \mathbb{F}_q$, 也就是说, $r = r^q$. 这等同于 $x_{\lambda_1}^{q+1}(x_{\lambda_2} - x_{\lambda_2}^q) + (x_{\lambda_1} - x_{\lambda_1}^q)\, x_{\lambda_2}^{q+1} = 0$. 将 x_{λ_1} 和 x_{λ_2} 的表达式代入以上等式, 我们即可推出

$$(h(\lambda_1)g(\lambda_2) + h(\lambda_2)g(\lambda_1))\,(\alpha^q - \alpha + \beta - \beta^q) = 0, \tag{3.4}$$

其中 $g(X) = -X^2 + \alpha^{q+1} - \beta^{q+1}$ 和 $h(X) = (X + \alpha^q - \beta)^{q+1}$. 因此现在问题简化为寻找 $\mathbb{F}_q$ 中不同元素 λ_1, λ_2 满足等式 (3.4), 而 r 的值由等式 (3.3)决定.

因为 $d = (\beta - \beta^q)^2 + 4\alpha^{q+1}$ 是 $\mathbb{F}_q$ 中的非平方元, 所以我们能得到 $\alpha^q - \alpha + \beta - \beta^q \neq 0$; 不然由此推出 $d = (\alpha + \alpha^q)^2$ 是平方元, 这是一个矛盾. 我们因此可以消去等式 (3.4)的左手边第二个因子. 代入 $y = 1$ 到引理 *3.7*, 我们观察到对任何 $x \in \mathbb{F}_q$ 均有 $g(x) \neq 0$ 和 $h(x) \neq 0$. 于是现在我们定义

$$\kappa(x) := \frac{h(x)}{g(x)}, \quad x \in \mathbb{F}_q.$$

注意到, 对每个 $x \in \mathbb{F}_q$ 均有 $\kappa(x)$ 是 $\mathbb{F}_q$ 中的非零元. 于是等式 (3.4)简化为

$$\kappa(\lambda_1) + \kappa(\lambda_2) = 0. \tag{3.5}$$

注意到如果等式 (3.5)成立, 那么必定有 $\lambda_1 \neq \lambda_2$: 否则我们能推出 $\kappa(\lambda_1) = \kappa(\lambda_2) = 0$, 这是不可能的.

综上所述, 我们已经证明下面的结果.

引理 3.9. 设 $\alpha \neq 0$ 以及 q 是奇数. 如果存在元素 $\lambda_1, \lambda_2 \in \mathbb{F}_q$ 以致 $\kappa(\lambda_1) + \kappa(\lambda_2) = 0$ 成立, 那么非经典 unital $\mathcal{U}_{\alpha,\beta}$ 存在一个 O'Nan 构型, 如图 3.1所示.

根据定理 *3.3*可知, 对于任何 $u \in \mathbb{F}_q$, 两个 *unitals* $\mathcal{U}_{\alpha,\beta}$ 和 $\mathcal{U}_{\alpha,\beta+u}$ 是射影等价的. 因此, 如果有必要将 β 替换为 $\beta + u$, 其中 $u \in \mathbb{F}_q$, 那么我们能假设

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha - \beta) \neq 0. \tag{3.6}$$

引理 3.10. 在假设(3.6)的前提下, 存在 $\lambda_1, \lambda_2 \in \mathbb{F}_q$ 满足等式 (3.5).

证明. 设 $K := \{\kappa(x) : x \in \mathbb{F}_q\}$. 对每个 $k \in K$, 我们考虑方程 $h(X) - kg(X) = 0$, 再展开化简可得,

$$(1+k)X^2 - \big(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha - \beta)\big)X + (\alpha^q - \beta)^{q+1} - k(\alpha^{q+1} - \beta^{q+1}) = 0. \tag{3.7}$$

根据 K 和 κ 的定义可知, 等式(3.7)在 $\mathbb{F}_q$ 上至少有一个解. 另一方面, 根据假设(3.6), 这是 $\mathbb{F}_q$ 上一个 1 次或 2 次多项式. 因此在映射 $x \mapsto \kappa(x)$ 下的像集 K 中, 每个元素在 $\mathbb{F}_q$ 中有 1 或 2 个原像. 由此可得 $|K| \geq \lceil \frac{q}{2} \rceil = \frac{q+1}{2}$, 于是就有

$$|K \cap -K| \geq |K| + |-K| - q \geq 1,$$

其中 $-K = \{-k : k \in K\}$. 证毕. □

综上所述, 我们已经证明以下结果.

推论 3.11. 在 q 是奇数和 $\alpha \neq 0$ 的情况下,$\mathcal{U}_{\alpha,\beta}$ 存在一个 O'Nan 构型.

3.3.2 偶特征的情况

我们现在考虑 q 是偶数的情况, 其中 $q > 2$. 取 $\delta \in \mathbb{F}_{q^2}^*$ 满足 $\delta + \delta^q = 1$, 再设 $\delta + \delta^q = 1$, 由文献[14] 的引理 *4.21* 可得 v 的绝对迹是 1. 注意到 δ 的选取有一定的自由度, 我们将在后面对这个选取进行进一步探讨. 根据前面的叙述可知, $\mathcal{U}_{\alpha,\beta}$ 是非经典的意味着它的参数 α, β 满足 $\alpha \neq 0$ 和 $\beta \notin \mathbb{F}_q$. 易知存在元素 $s \in \mathbb{F}_{q^2}^*$, $f \in \mathbb{F}_q^*$ 和 $u \in \mathbb{F}_q$ 以致 $\alpha' = \alpha s^2 f \in \mathbb{F}_q^*$ 和 $\beta' = (\beta s^{q+1} + u)f = \delta$ 成立. 根据定理 *3.3*, 我们可以不失一般性地假设 $\mathcal{U}_{\alpha,\beta}$ 的参数满足 $\alpha = a \in \mathbb{F}_q^*$, $\beta = \delta$.

引理 3.12. 对固定的 $a \in \mathbb{F}_q^*$, 存在 $\eta \in \mathbb{F}_{q^2}$ 使得 $\eta + \eta^q = 1$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{a^2}{\eta+\eta^2}\right) = 1$.

证明. 易知 $\{x + x^2 : x \in \mathbb{F}_{q^2}, x + x^q = 1\}$ 大小为 $q/2$ 并且不含 0. 同时, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a^2 X) = 0$ 只有 $q/2 - 1$ 个非零解, 再通过比较大小可得结论. □

取定 $\mathbb{F}_{q^2}$ 中一个 δ 满足 $\delta' + \delta'^q = 1$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{a^2}{\delta'+\delta'^2}\right) = 1$. 那么 δ' 和 δ 之间只差一个 $\mathbb{F}_q$ 中的元素, 故根据定理 *3.3*可知 $\mathcal{U}_{a,\delta}$ 与 $\mathcal{U}_{a,\delta'}$ 是同构的. 因此, 我们只需要考虑这个 *unital* 的参数 α 和 β 满足

$$\alpha = a \in \mathbb{F}_q^*, \quad \beta = \delta$$

并且有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{a^2}{v}\right) = 1$, 其中 $v = \delta^{q+1} = \delta^2 + \delta$.

取 $\mathrm{P\Gamma L}(3, q^2)$ 中一个对合, 如下所示:

$$\phi : (x, y, z) \mapsto (x^q, y^q, z^q).$$

这个对合不但保持 $\mathcal{U}_{\alpha,\beta}$ 不变, 而且固定区组 B_∞ 中每一个点以及把 B_y 映射到 B_{y^q}, 其中 $y \in \mathbb{F}_{q^2}^*$. 类似奇特征的情况, 我们假设 $\mathcal{U}_{\alpha,\beta}$ 具有一个 *O'Nan* 构型以致它具有两条过 $P = (0, 0, 1)$ 的线, 并且 $\mathcal{N}$ 中另外两条线 ℓ', ℓ'' 满足条件

$$\ell' = \phi(\ell'),\ \ell'' = \phi(\ell'') \text{ 以及} \ell' \cap \ell'' = (0, r, 1) \in \mathcal{U}_{\alpha,\beta},$$

其中 r 是 $\mathbb{F}_q \setminus \{0\}$ 中某个元素, 具体参考图 *3.2*. 请注意奇偶特征下使用对合 ψ, ϕ 的区别: 在 q 是偶数时, 对合 ϕ 只有在 α 和 β 满足特定条件下才保持 $\mathcal{U}_{\alpha,\beta}$ 不变, 因此我们在 q 是奇数时不能使用该对合.

令 $P_\lambda = (x_\lambda, \delta x_\lambda, 1)$ 是 B_δ 中的一个点, 其中 λ 是 $\mathbb{F}_q$ 的某个元素并且

$$x_\lambda = \frac{a\delta + (\lambda + \delta)\delta^q}{a^2 + (\lambda + \delta)^{q+1}} = \frac{\lambda + v + (a + \lambda)\delta}{a^2 + \lambda^2 + \lambda + v}.$$

应用引理 *3.7*并取 $y=1$ 则可知以上等式分母非零, 故 x_λ 是良定义的. 易得点 $\phi(P_\lambda)$ 属于 $B_{\delta^q}=\phi(B_\delta)$. 于是我们推出两条线 ℓ_∞ 和 $P_\lambda\phi(P_\lambda)$ 的交点是

$$\left(0,\frac{x_\lambda^{q+1}}{x_\lambda+x_\lambda^q},1\right)=\left(0,\frac{\lambda^2v+\lambda(a+v)+av+v^2+a^2v}{(a^2+\lambda^2+\lambda+v)(\lambda+a)},1\right).$$

如果我们能找到两个不同的解 $\lambda_1,\lambda_2\in\mathbb{F}_q$ 满足以下方程

$$r^{-1}=G(X):=\frac{(a^2+X^2+X+v)(X+a)}{X^2v+X(a+v)+av+v^2+a^2v}, \tag{3.8}$$

其中 r 是 $\mathbb{F}_q^*$ 中某个元素, 那么这四条线 ℓ_δ, ℓ_{δ^q}, $\ell'=P_{\lambda_1}\phi(P_{\lambda_1})$ 和 $\ell''=P_{\lambda_2}\phi(P_{\lambda_2})$ 组成 $\mathcal{U}_{a,\beta}$ 中具有规定形式的 *O'Nan* 构型, 具体参考图 *3.2*.

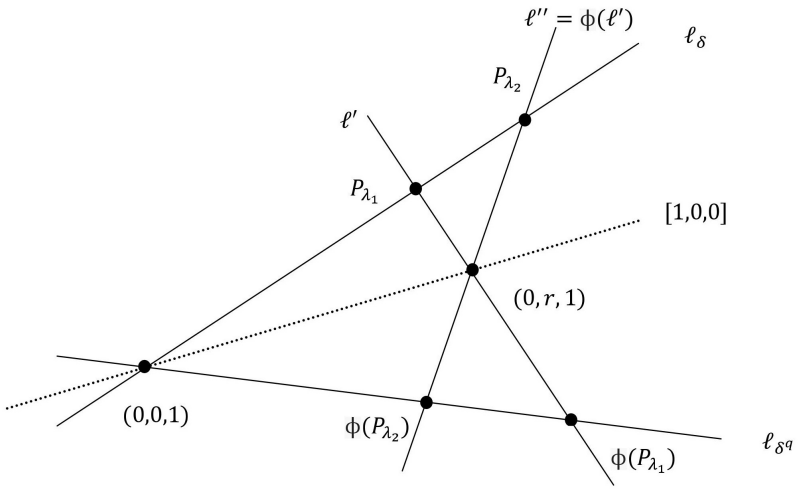

图 3.2　当 q 是奇数时 $\mathcal{U}_{\alpha,\beta}$ 中假定的 O'Nan 构型

综上所述, 我们有以下结果.

引理 3.13. 假定 q 是大于 2 的偶数且 $\alpha\in\mathbb{F}_q^*$. 如果存在 $r\in\mathbb{F}_q^*$ 使得等式 (3.8)在 $\mathbb{F}_q$ 上有两个不同的解, 那么非经典 unital $\mathcal{U}_{\alpha,\beta}$ 存在一个 O'Nan 构型 $\mathcal{N}$, 如图 3.2所示.

我们接下来要说明存在 $r\in\mathbb{F}_q^*$ 使得上述引理的条件成立. 回想一下, 我们有 $v=\delta^{q+1}=\delta+\delta^2$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\frac{a^2}{v})=1$：参考引理 *3.12*下面句子的证明. 我们观察到 $a=v$ 不可能发生, 不然判别式 $d=a$ 的绝对迹为 0, 这就与取定的 v 绝对迹为 1 相矛盾.

引理 3.14. 当 $r=\frac{v}{a+v}$ 时, 等式 (3.8)在 $\mathbb{F}_q$ 上有两个不同的解.

证明. 因为 $G(x)$ 中所有系数都属于 $\mathbb{F}_q$, 所以对所有 $x \in \mathbb{F}_q$ 均有 $G(x) \in \mathbb{F}_q$. 我们直接计算 $G(v) = r^{-1}$, 而且等式 $G(Z+a) = G(v)$ 简化为

$$(Z+a+v)\left(Z^2+Z+\frac{a^2}{v}+v\right)=0.$$

因为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{a^2}{v}+v\right)=1+1=0$, 所以以上公式第二个因子有两个不同的解. 因此在 $r=\frac{v}{a+v}$ 时, $r^{-1}=G(X)$ 至少有两个不同的解. 证毕. □

结合引理 *3.12*的论证, 我们有下面的结果

推论 3.15. 在 q 是大于 2 的偶数和 $\alpha \neq 0$ 的情况下, $\mathcal{U}_{\alpha,\beta}$ 存在一个 O'Nan 构型.

综上所述, 我们用推论 *3.11*和推论 *3.15*证明本节的主要定理 *(*定理 *3.6).*

3.4 Buekenhout-Tits unitals 的 *O'Nan* 构型

我们在这节中主要建立下面的结果.

定理 3.16. $\mathrm{PG}(2,q^2)$ 中每个 Buekenhout-Tits unital 都有一个 O'Nan 构型, 其中 $q=2^m$, m 是大于 1 的奇数.

令 $\mathcal{U}_T$ 是 $\mathrm{PG}(2,q^2)$ 中如等式 (3.2)所定义的 *Buekenhout-Tits unital,* 其中 $q=2^m$ 且 m 是大于 1 的奇数. 取定 $\delta \in \mathbb{F}_4$ 以致 $\delta^2+\delta+1=0$. 于是因为 m 是奇数, 所以 $1,\delta$ 在 $\mathbb{F}_q$ 上构成 $\mathbb{F}_{q^2}$ 的一组基. 如等式 (3.2)所示, 我们选用以上取定的 δ 去给出 $\mathcal{U}_T$ 的定义. 回想一下,

$$f(x,y)=x^{\tau+2}+xy+y^{\tau}, \quad \tau=2^{(m+1)/2}.$$

对 $y \in \mathbb{F}_{q^2}^*$ 以致线 $\ell_y := [y,1,0]$ 是 $\mathcal{U}_t$ 的割线, 我们记区组 B_y 为 $\mathcal{U}_T$ 和 ℓ_y 的交集. 此外, 很容易知道线 $\ell_\infty=[1,0,0]$ 与区组 $B_\infty=\{(0,r,1):r\in\mathbb{F}_q\}\cup\{(0,1,0)\}$ 相对应.

自然地, 我们也尝试使用第 *3.3*节中一样的想法, 尽可能寻找被 $\mathrm{P\Gamma L}(3,q^2)$ 中 $\mathcal{U}_T$ 的稳定子群中某一个对合固定的 *O'Nan* 构型. 然而经过一些简单分析后发现这是不可能的. 因此我们改变策略. 回忆一下, 根据引理 *3.5*可知不存在过特殊点 $P_\infty=(0,0,1)$ 的 *O'Nan* 构型.

引理 3.17. 假定 $q=2^m$ 和 m 是大于 1 的奇数. 那么存在 $c\in\mathbb{F}_q^*$ 使得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{\tau+2}+c+1)=0$.

证明. 通过直接的验证, 二次型 $Q(x)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x^{\tau+2})$ 在 $\mathbb{F}_2$-线性空间 $\mathbb{F}_q$ 上是非退化的. 于是二次曲面 $Q(x)=0$ 不可能包含在超平面 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)=0$ 中. 因此存在 $c\in\mathbb{F}_q$

使得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{\tau+2})=0$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c)=1$, 从而 c 具有所需的性质. □

令 $\mathcal{N}$ 为 $\mathcal{U}_T$ 中一个假定的 *O'Nan* 构型且它包含 $(0,0,1)$, ℓ_∞ 和过 $(0,0,1)$ 的 ℓ_c, 其中 $c\in\mathbb{F}_q^*$ 是选定的且满足

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{\tau+2}+c+1)=0.$$

由之前的引理可知, 这样的 c 是存在. 进一步假设 $\mathcal{N}$ 中另外两条线 ℓ 和 ℓ' 交于 $P=(1,v+\delta,1)$, 其中 $v=\frac{1}{c^\tau+1}(c^2+c^{1-\tau}+c^{\tau+1})$. 记

$$\ell\cap\ell_\infty=(0,r_1,1),\quad \ell'\cap\ell_\infty=(0,r_2,1),$$

其中 r_1, r_2 是 $\mathbb{F}_q^*$ 中不同的元素. 这两点都落在区组 B_∞ 中. 那么假定的 *O'Nan* 构型如图 *3.3*所示. 为了构造一个具有上述规定形式的 *O'Nan* 构型 $\mathcal{N}$, 我们需要找 $\mathbb{F}_q^*$ 中两个不同的元素 r_1, r_2 使得对应两条线 ℓ, ℓ' 均交 ℓ_c 于 $\mathcal{U}_T$ 中同一个点.

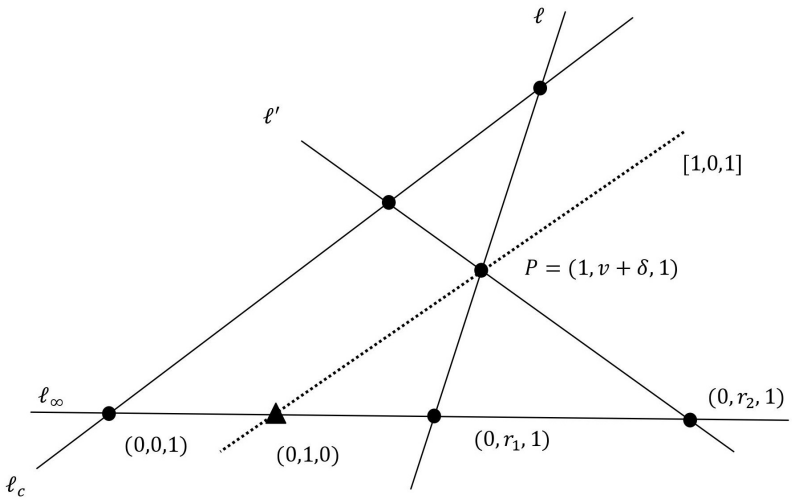

图 3.3 Buekenhout-Tits unital $\mathcal{U}_T$ 中假定的 O'Nan 构型

引理 3.18. 定义 $H(x,y):=x^2+xy+y^2$ 以及 $v=\frac{1}{c^\tau+1}(c^2+c^{1-\tau}+c^{\tau+1})$. 如果

$$\frac{X^\tau}{c^\tau}+\frac{c+1}{c^2}X+\left(\frac{1}{c^{\tau+2}}+\frac{v+1}{c^2}+1+\frac{v^\tau+1}{c^\tau}\right)+\frac{H(c+v,1)}{Xc}=0 \tag{3.9}$$

在 $\mathbb{F}_q$ 上有两个非零解, 那么我们得到 $\mathcal{U}_T$ 中一个 O'Nan 构型, 如图 3.3所示.

证明. 取定 $r\in\mathbb{F}_q^*$, 接着考虑一条经过 $(0,r,1)$ 和 $P=(1,v+\delta,1)$ 的线 $\ell''=[r+v+\delta,1,r]$, 则我们可以推出 ℓ'' 和 ℓ_c 的交点 P' 为

$$P'=(r,rc,r+c+v+\delta).$$

对两个不全为零的元素 $x, y \in \mathbb{F}_q$, 我们有 $(x+y\delta)^{-1} = \frac{(x+y)+y\delta}{H(x,y)}$, 其中 $H(x,y) = x^2+xy+y^2$. 因此我们将 P' 改写成

$$P' = \left(\frac{r(r+c+v+1+\delta)}{H(r+c+v,1)}, \frac{rc(r+c+v+1+\delta)}{H(r+c+v,1)}, 1 \right).$$

这点落在这个 *unital* $\mathcal{U}_T$ 当且仅当

$$f\left(\frac{r(r+c+v+1)}{H(r+c+v,1)}, \frac{r}{H(r+c+v,1)} \right) = \frac{rc}{H(r+c+v,1)}. \tag{3.10}$$

将 $x = \frac{r(r+c+v+1)}{H(r+c+v,1)}$ 和 $y = \frac{r}{H(r+c+v,1)}$ 代入引理 *3.4*, 我们知道等式 (3.10)的左手边等于 $f\left(c^{-1}, c^{-1}(r+c+v+1)\right)^{-1}$. 因此, 条件(3.10)等价于

$$f\left(\frac{1}{c}, \frac{r+c+v+1}{c} \right) = \frac{H(r+c+v,1)}{rc}.$$

将它展开并进行简化, 我们得到等式 (3.9), 其中 $X = r$. 在引理的假设前提下, 取 r_1, r_2 为等式 (3.9)中两个解, 我们就得到如图 *3.3*所示的 *O'Nan* 构型 $\mathcal{N}$. □

回顾 $v = \frac{1}{c^\tau+1}(c^2 + c^{1-\tau} + c^{\tau+1})$. 现在我们定义

$$f_1(X) := \frac{X^\tau}{c^\tau} + \frac{X}{c^2} + \left(\frac{1}{c} + 1 \right)^{\tau+2} + \frac{v}{c^2} + \frac{v^\tau}{c^\tau} + \frac{1}{c^{\tau+1}}.$$

经过繁琐但常规的检查, 等式 (3.9)可以改写成以下形式

$$f_1(r) + \frac{c}{r}\left(\big(f_1(r)\big)^\tau + \frac{1}{c^\tau} f_1(r) \right) = 0.$$

引理 3.19. 多项式 $f_1(X) = 0$ 在 $\mathbb{F}_q$ 上有两个非零解, 等式 (3.9) 也是一样.

证明. 令 $Y := c^\tau X$, 则我们可以将 $c^{\tau+2} f_1(X) = 0$ 改写为如下形式

$$Y^\tau + Y + A = 0,$$

其中 $A = (1+c)^{\tau+2} + c + c^\tau v + c^2 v^\tau$. 因为该线性映射 $y \mapsto y^\tau + y$ 的 *kernel* 恰好是有限域 $\mathbb{F}_2$, 所以以上方程有 0 或 2 个解. 注意到方程 $Z^2 + Z + A = 0$ 有解当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A) = 0$. 如果对某个 $z \in \mathbb{F}_q$ 有 $z^2 + z + A = 0$, 那么 $Y = z^\tau + z$(或 $z^\tau + z + 1$) 是 $Y^\tau + Y + A = 0$ 的其中一个解. 因此我们计算

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A) &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left((1+c)^{\tau+2} + c + c^\tau v + c^2 v^\tau \right) \\ &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1 + c^{\tau+2} + c) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{\tau+1} + c + 1) = 0. \end{aligned}$$

在这个计算过程中我们使用事实 $\tau^2 \equiv 2 \pmod{q-1}$. 剩下只需要证明 $A \neq 0$, 我们用反证法证明. 将 v 的值代入 $A = 0$, 我们得到

$$(1+c)^{\tau+2} + \frac{c^{\tau+2}}{c^\tau+1} + c^{\tau+1} + c + \frac{c^{2\tau+2}}{c^2+1} + c^{\tau+2} + c^\tau = 0. \tag{3.11}$$

再通过两边乘以 $\frac{(1+c)^{\tau+2}}{c^{\tau+2}}$, 我们得到

$$c^{-\tau-2}+c^{2-\tau}+c^{-2}+c^{-1}+1+c+c^{\tau-1}+c^{\tau}+c^{\tau+1}+c^{2\tau}=0.$$

接着在两边取绝对迹函数并且利用条件 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{\tau+1}+c+1)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{\tau+1}+c^2+c)$, 我们得到 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{-\tau-2})=0$. 相似地, 通过在等式 (3.11)两边乘以 $\frac{(1+c)^{\tau+2}}{c^{2\tau+2}}$ 推出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{-\tau-2}+1)=0$, 这就与前面结果矛盾. 证毕. □

综上所述, 我们已经完成定理 *3.16*的证明.

3.5 小结

最近 *Korchmáros, Siciliano* 和 *Szőnyi*[62] 证明在 PG$(2,q^2)$ 中经典 *unital* 存在唯一的嵌入方式. 他们的基本想法就是利用包含某些点和区组的特别构型的存在性说明区组的同构性. 在本章中, 我们受他们这样的想法所启发, 去寻找能嵌入到 PG$(2,q^2)$ 的 *Buekenhout unitals* 中具有特别形式的 *O'Nan* 构型. 在正交 *Buekenhout-Metz unitals* 的情况下, 只有经过特别点 *(*对应 *Buekenhout* 构造中 *cone* 的顶点*)* 的线才是 *Baer* 子线, 遂我们能确定某一种 *O'Nan* 构型的存在性, 该构型是被 PΓL$(3,q^2)$ 中取定的 *unital* 的稳定子群中一个对合固定的. 而在 *Buekenhout-Tits unital* 的情况下, 我们需要确定一个包含固定 *Baer* 子线的 *O'Nan* 构型的存在性. 本章的主要贡献是给 *Piper* 的猜想 *(O'Nan* 构型的不存在性是经典 *unital* 的特征*)* 提供强有力的证据.

4 $W(q)$ 中的 *Payne* 派生四边形的点正则自同构群

4.1 介绍

一个 (s,t) 阶有限广义四边形 *(generalized quadrangle)* $\mathcal{Q}$ 是一个具有以下性质的点-线关联结构：

1. 每个点与 $t+1$ 条线关联；
2. 每条线包含 $s+1$ 个点；
3. 对于不关联的点线对 (P,ℓ), 即 $P\notin\ell$, 存在唯一与 ℓ 关联的点 Q 使得 P,Q 两点共线.

若这个四边形 $\mathcal{Q}$ 的参数 s 和 t 均大于 1, 则称它是厚的 *(thick)*. 如果交换一个 (s,t) 阶广义四边形中的点和线的角色, 那么就得到一个 (t,s) 阶对偶四边形. 经典广义四边形是以秩为 2 的有限经典极空间的点-线关联结构的形式来出现. 关于有限广义四边形的标准的参考书是经典著作[28].

广义四边形的研究与群论和数学中其他分支有着密切的联系. *J. Tits*[22] 为了更好地理解秩 2 的 *Chevalley* 群而提出广义多边形 *(generalized polygon)* 的概念. 一个广义 3 边形 *(generalized 3-gon)* 是一个射影平面, 而广义 4 角形 *(generalized 4-gon)* 就是广义四边形. 与有限射影平面的研究相似, 学者们利用一些几何论据和群论中深刻的结果对一些具有高度对称性的广义四边形进行大量的分类研究. 请参考专著[63,64]了解这一领域的历史和最新发展.

除了经典的例子和它们的对偶以外, 所有目前已知的有限广义四边形在对偶等价意义下还能分成三类：*translation* 广义四边形, *flock* 广义四边形以及 $(q-1,q+1)$ 阶广义四边形. 值得一提的是除了阶数为 $(q-1,q+1)$ 的例子以外, 大多数已知的广义四边形都可以用它们各自对应的 *Kantor* 族或 *4-gonal* 族的子群结构来描述, 这是 *Kantor* 在文献[26] 中第一次提出的概念. 第一个 $(q-1,q+1)$ 阶广义四边形的例子 *(*q 是素数幂*)* 应归功于 *Ahrens* 和 *Szekeres*[65], 同时 *M. Hall, Jr.*[66] 也独立地发现偶特征下的例子. 后来, *Payne* 对此进行推广并给出了一般化的构造方法, 现在被人们称为 *Payne* 派生法 *(Payne derivation)*, 这种方法是从具有一个 *regular* 点 P 的 (q,q) 阶广义四边形 $\mathcal{Q}$ 中得到新的 $(q-1,q+1)$ 阶广义四边形, 这部分工作具体可参考文献[23–25]. 由此产生的广义四边形 $\mathcal{Q}^P$ 被称为 *Payne* 派生四边形 *(Payne derived quadrangle)*. 所有已知的 $(q-1,q+1)$ 阶广义四边形都是以 *Payne* 派生四边形的形式出现. 从外, 文献[32,37] 对 *Payne* 派生四边形的自同构群进行了研究.

人们也对广义四边形的点正则自同构群做了大量的研究. *Ghinelli*[30] 是第一个对存在点正则自同构群的广义四边形进行研究的学者, 其中她主要是用表示论和差集等工具去对 (s,s) 阶广义四边形中的点正则群进行研究, 这里 s 是偶数. 后来, 这方面的研究在文献[35,67] 中取得新的进展. 值得一提的是 *Yoshiara* 在文献[35] 中证明了 (t^2,t) 阶广义四边形不可能存在任何点正则自同构群. 结合文献[27,35] 的结果, 文献[68] 指出任何 (q,q) 阶 *skew-translation* 广义四边形在 q 为奇数的情况下与经典辛对称四边形 $W(q)$ 同构. 最近 *Swartz*[67] 针对某一类特定广义四边形进行研究, 其中这类四边形具有一个正则作用在点和线上的自同构群. 在 *2011* 年之前, 所有已知的存在点正则群的有限广义四边形都是通过 *Payne* 派生法从一个 (s,s) 阶 *elation* 广义四边形 $\mathcal{Q}$ $(s\geq 2)$ 中产生的, 而且它们的点正则群都是从 $\mathcal{Q}$ 的 *elation* 群中诱导得到的. *De Winter, K. Thas* 和 *Shult* 受这些观察所启发, 遂尝试用一系列文献[31–34] 中去证明不存在点正则群的其他例子.

直至 *2011* 年, 这个方向上的研究才出现一个重大的突破：存在点正则群的经典广义四边形 $(s,t\geq 2)$ 得到了一个完整的分类, 从而发现三个稀疏的例子以及辛对称四边形 $W(q)$ 的 *Payne* 派生四边形中新的点正则群的构造, 具体可查阅文献[36]. 同时这也修正了文献[34] 中的一个小错误并给出文献[33] 中猜想的反例. 在同一篇参考文献[36] 中, 作者们还借助计算机软件 *Magma*[69] 进行计算机搜索, 并列出对于小参数 $(q\leq 25)$ 的 $W(q)$ 的 *Payne* 派生四边形中的所有点正则自同构群. 根据结果显示“这个问题是很宽泛的”. 在 q 是奇数的情况下, *Chen*[70], *K. Thas* 和 *De Winter*[71] 分别独立地完成线性情况的分类, 换言之, 他们得到的群都是从 $W(q)$ 的环绕射影空间的线性群中诱导出来的. 此外, 后者更在文献[71] 中列出 q 是偶数时一些线性的构造. 除了阶数较小的群以外, 目前所有已知能正则作用在有限广义四边形上的有限群都有不大于 3 的幂零类. *Payne* 派生四边形的点正则群在 $\widetilde{C}_2$*-buildings* 中 *uniform lattices* 的构造上也有相关的应用, 详情请见文献[71,72].

在本章中, 我们将对辛对称四边形 $\mathcal{Q}=W(q)$ 相对于 *regular* 点 P 所得到的 *Payne* 派生四边形 $\mathcal{Q}^P$ 的点正则自同构群进行系统的研究. $W(q)$ 中每个点都是 *regular,* 并且 P 的不同选取都会产生同构的 *Payne* 派生四边形. 根据文献[37] 中的推论 *2.4, Payne* 派生四边形 $\mathcal{Q}^P$ 的全自同构群在 $q\geq 5$ 时恰好是 $\mathrm{P\Gamma Sp}(4,q)$ 中点 P 的稳定子群. 如果 $\mathcal{Q}^P$ 的点正则群 G 是 $\mathrm{P\Gamma Sp}(4,q)$ 的子群, 那么我们称 G 是线性的；否则称它是非线性的. 本章的主要结果是一方面给出了 q 是奇数时 $\mathcal{Q}^P$ 的所有点正则群, 另一方面是给出 q 是偶数时所有线性点正则群. 具体而言, 就是分别得到奇特征下四个不同的构造以及偶特征下两个不同的构造. 特别地, 在 q 是奇数时我们确定了从这些构造中得到的群的幂零类的上下界, 并且这上下界是相对禁的. 这些结果有助

于解决具有什么结构的有限群能正则作用在有限广义四边形上的基本问题. 特别地, 我们发现这些点正则群可以有无限大的幂零类.

本章的结构安排如下. 在第 *4.2*节中, 我们将列出一些关于有限域 $\mathbb{F}_q$ 的运算结果和基本事实以及引入 *Payne* 派生四边形 $\mathcal{Q}^P$ 的点正则群的模型. 在第 *4.3*节中, 我们将对本章的主要结果进行一个简短的概述, 其中包括了奇特征情况下点正则群的分类结果以及这些点正则群的幂零类的上下界. 同时我们也简短地介绍一下对这些点正则群分类的思路. 在第 *4.4*节中, 我们给出了 $q \geq 5$ 时 *Payne* 派生四边形 $\mathcal{Q}^P$ 的线性点正则群的完整的分类结果. 在 *4.5*节中, 我们分析了 $\mathcal{Q}^P$ 中假定的非线性的点正则群的群结构, 这就导致我们能得到第 *4.6*节中奇特征情况下完整的分类结果. 而在第 *4.7*节中, 我们首先简化第 *4.6*节中获得的构造, 然后通过计算这些点正则群中各种各样的群不变量去解决这些群的同构性问题. 最后, 第 *4.8*节是对本章的内容的总结.

4.2 准备工作

本章中我们使用的群论术语都是标准的, 具体可参考文献[73–75]. 令 G 是一个有限群. G 的 *exponent*（记为 $\exp(G)$）是最小正整数 n 使得对所有 $g \in G$ 有 $g^n = 1$. 当 $g, h \in G$ 时, 他们的交换子是 $[g,h] = g^{-1}h^{-1}gh$. 对 $g \in G$, 它的中心化子 $C_G(g)$ 是 G 中所有满足 $[g,h] = 1$ 的元素 h's. G 的中心为 $Z(G) = \{g \in G : [g,h] = 1, \forall\, h \in G\}$. 对 G 中两个子群 H_1, H_2, 我们用记号 $[H_1, H_2]$ 表示子群 $\langle [h_1,h_2] : h_1 \in H_1,\, h_2 \in H_2\rangle$. 特别地, G 的导群是交换子群 $[G,G]$. 我们用记号 $\gamma_i(G)$ 来表示 G 的下中心序列的第 i 项. 归纳地, 我们对每个 $i \geq 1$ 有 $\gamma_1(G) = G$ 和 $\gamma_{i+1}(G) = [\gamma_i(G), G]$. 当对某个整数有 $\gamma_{c+1}(G) = 1$ 则称群 G 是幂零的, 我们称满足这条件最小的整数是该群的幂零类 *(nilpotency class)*. 相似地, 我们用记号 $Z_i(G)$ 来表示 G 的上中心序列的第 i 项, 其中 $Z_0(G) = 1$ 并且 $Z_{i+1}(G)$ 是由性质 $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ 来定义的, $i \geq 0$. 幂零群的上中心序列和下中心序列具有相同的长度. 令 d 为有限 p 群 G 中阿贝尔子群的阶的最大值. 该群 G 的 *Thompson* 子群是由所有 d 阶阿贝尔子群生成的, 并被记为 $J(G)$.

4.2.1 有限域 $\mathbb{F}_q$ 的运算

令 $\mathbb{F}_q$ 为具有 q 个元素的有限域, 其中 $q = p^m$ 且 p 是素数. 再令 $\mathrm{Aut}(\mathbb{F}_q)$ 为有限域 $\mathbb{F}_q$ 的伽罗华群, 其中包含 *Frobenius* 映射 $x \mapsto x^{p^i}$, $0 \leq i \leq m-1$. 对于 $g \in \mathrm{Aut}(\mathbb{F}_q)$, 我们均记 x^g 和 $g(x)$ 为 g 在 $x \in \mathbb{F}_q$ 上的作用. 对于 m 的因子 d, 从 $\mathbb{F}_q$ 到子域 $\mathbb{F}_{p^d}$ 的迹函数为

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^d}}(x) := x + x^{p^d} + \cdots + x^{p^{m-d}}, \quad x \in \mathbb{F}_q.$$

以上定义的迹函数是满射的, 即 $\{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^d}(x)} : x \in \mathbb{F}_q\} = \mathbb{F}_{p^d}$. 读者们可参考文献[76]去了解一些关于有限域 $\mathbb{F}_q$ 的基本事实.

引理 4.1 (定理 2.25, Lidl 和 Niederreiter[76]). 令 d 是正整数 m 的因子. 当 $\alpha \in \mathbb{F}_{p^m}$ 时, 则 $\mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_{p^d}}(\alpha) = 0$ 当且仅当对某个 $\beta \in \mathbb{F}_{p^m}$ 有 $\alpha = \beta^{p^d} - \beta$.

根据文献[76]中的定理 *2.23* 可知迹函数 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ 是 $\mathbb{F}_p$-线性的, 并且对所有 $x \in \mathbb{F}_q$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x^p) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)$. 于是对每个 $\beta \in \mathbb{F}_q$, 定义:

$$L_\beta : \mathbb{F}_q \to \mathbb{F}_p, \quad x \mapsto \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta x). \tag{4.1}$$

引理 4.2 (定理 2.24, Lidl 和 Niederreiter[76]). 每个从 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的 $\mathbb{F}_p$-线性变换等于 L_β, 其中 β 是 $\mathbb{F}_q$ 中某个元素, 并且 $L_\beta = L_\gamma$ 当且仅当 $\beta = \gamma$.

作为推论, 当且仅当 $\beta = 0$ 时, 才对所有 $x \in \mathbb{F}_q$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta x) = 0$.

引理 4.3. 对 $\alpha, \beta \in \mathbb{F}_q$ 且 $\beta \neq 0$, 如果 $\ker(L_\alpha)$ 包含一个 $\mathbb{F}_p$-线性子空间 $K = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta x) = 0\}$, 那么对某个 $\lambda \in F$ 有 $\alpha = \lambda\beta$.

证明. 我们有 $K = \ker(L_\beta)$. 取 $u \in \mathbb{F}_q \setminus K$ 使得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta u) = 1$. 那么 $\mathbb{F}_q = K \oplus \mathbb{F}_p \cdot u$. 因为 $K \subseteq L_\alpha$, 所以我们对 $x \in K$ 和 $\lambda \in \mathbb{F}_p$ 有 $L_\alpha(x + \lambda u) = \lambda L_\alpha(u)$. 换言之, $L_\beta(x + \lambda u) = \lambda$, 因此对所有 $z \in \mathbb{F}_q$ 均有 $L_\alpha(z) = L_\alpha(u)L_\beta(z)$. 因为 $L_\alpha(u)$ 属于 $\mathbb{F}_p$ 且 $L_\alpha(u)L_\beta = L_{L_\alpha(u)\beta}$, 所以通过引理 *4.2*即可证明所需的结果. □

引理 4.4. 假定 p 是素数并令 $q = p^m$, 再设 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 的阶为 p^r, 其中 $r \geq 0$. 如果 $K = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu x) = 0\}$ 是 g-不变的, 即 $g(K) = K$, 那么 $g(\mu) = \mu$.

证明. $r = 0$ 和 $\mu = 0$ 的情况都是平凡的, 所以我们假设 $r \geq 1$ 和 $\mu \neq 0$. 令 L_β 是用某个 $\beta \in \mathbb{F}_q$ 在等式(4.1)中定义的 $\mathbb{F}_p$-线性变换. 易知 $g(K) = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(g(\mu)x) = 0\}$, 即 $g(K) = \ker(L_{g(\mu)})$. 因为 $g(K) = K$, 所以我们从引理 *4.3*中推断出对某个 $\lambda \in \mathbb{F}_p^*$ 有 $g(\mu) = \lambda\mu$. 对上式取到被 g 固定的子域的相对范数, 我们就得到 $\lambda^{p^r} = 1$, 即 $\lambda = 1$. 证毕. □

一个 $\mathbb{F}_q$ 上的线性化多项式是一个具有以下形式的多项式 f: $f(X) = \sum_{i=0}^{n} a_i X^{p^k}$, 其中 $a_i \in \mathbb{F}_q$. 当 $n \leq m-1$ 时该多项式被称为简化的 *(reduced)*, 其中 $q = p^m$. $\mathbb{F}_q$ 中的 $\mathbb{F}_p$-线性变换与 $\mathbb{F}_q$ 上简化的线性化多项式之间有一个双射. 令 $L(X)$ 是 $\mathbb{F}_q$ 上简化的线性化多项式. 那么它的迹对偶多项式是唯一的简化的线性化多项式 $\widetilde{L}(X)$ 使得

对 $x, y \in \mathbb{F}_q$ 都有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(L(x)y) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\widetilde{L}(y)x)$. 如果 $L(X) = \sum_{i=0}^{m-1} s_i X^{p^i}$, 那么我们就有

$$\widetilde{L}(X) = \sum_{i=0}^{m-1} s_{m-i}^{p^i} X^{p^i}. \tag{4.2}$$

一个映射 $B : \mathbb{F}_q \times \mathbb{F}_q \mapsto \mathbb{F}_p$ 是一个双线性型只要 $B(x, y)$ 关于 x, y 都是可加的. 而当对所有 $x, y \in \mathbb{F}_q$ 有 $B(x, y) = B(y, z)$ 时它是对称的. 在接下来的引理中, 我们建立 $\mathbb{F}_q$ 上双线性型与线性化多项式之间的联系.

引理 4.5. 假定 $B : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_p$ 是一个双线性型. 那么存在 $\mathbb{F}_q$ 上一个简化的线性化多项式 L 使得 $B(x, y) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xL(y))$.

证明. 根据引理 *4.2*可知对每个 $y \in \mathbb{F}_q$ 存在一个元素 $L(y) \in \mathbb{F}_q$ 使得 $B(x, y) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xL(y))$. 对 $y, z \in \mathbb{F}_q$, 我们有 $B(x, y+z) = B(x, y)+B(x, z)$, 即 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x(L(y+z) - L(y) - L(z))) = 0$. 这是对所有 $x \in \mathbb{F}_q$ 都成立, 因此 $L(y + z) - L(y) - L(z) = 0$, 也就是说, L 在 $\mathbb{F}_q$ 上是加性的. 证毕. □

我们需要下面关于线性化多项式以及双线性型的技术引理, 这在后面我们对点正则群的推导有很大帮助.

引理 4.6. 令 $x \mapsto L(x)$ 是 $\mathbb{F}_q$ 中一个 $\mathbb{F}_p$-线性变换, 并对某个 $\eta \in \mathbb{F}_q$ 设 $K = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x) = 0\}$. 如果 $\mathrm{Im}(L|_K) = \mathbb{F}_p \cdot \omega$, 那么存在 $u, \mu \in \mathbb{F}_q^*$ 使得

$$L(x) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu x) + u\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x), \quad \forall x \in \mathbb{F}_q.$$

证明. $\eta = 0$ 的情况（即 $K = \mathbb{F}_q$）可通过应用引理 *4.2*到 $\mathbb{F} = \mathbb{F}_q$ 直接推出结论, 所以我们下面假设 $\eta \neq 0$. 取 $\beta \in \mathbb{F}_q$ 使得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta\beta) = 1$, 并且定义 $M(x) := L(x) - L(\beta) \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x)$. 那么 M 是 $\mathbb{F}_p$-线性的, 且对 $a \in K$ 和 $\lambda \in \mathbb{F}_p$ 有 $M(a+\lambda\beta) = L(a)$, 所以 $\mathrm{Im}(M) = \mathbb{F}_p \cdot \omega$. 相似地通过应用引理 *4.2*到 *M* 上, 我们即可推出 $M(X) = \omega\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu X)$. 证毕. □

引理 4.7. 令 $q = p^m$ 是素数幂并且有 $m = p^e l$, 再取 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x) = x^{p^l}$. 取 $\eta \in \mathbb{F}_{p^l}$, 并定义 $K := \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x) = 0\}$. 如果 L 是 $\mathbb{F}_q$ 中一个 $\mathbb{F}_p$-线性变换使得对 $x \in K$ 都有 $g(L(g^{-1}(x))) = L(x)$, 那么存在一个 $\mathbb{F}_q$ 上简化的线性化多项式 $L_1(X)$ 使得它的多项式系数都属于 $\mathbb{F}_{p^l}$, 并且对 $x \in K$ 有 $L(x) = L_1(x)$.

证明. 假定对 $x \in \mathbb{F}_q$ 有 $L(x) = \sum_{i=0}^{m-1} d_i x^{p^i}$. 于是我们有

$$D(x) := g(L(g^{-1}(x))) - L(x) = \sum_{i=0}^{m-1} (g(d_i) - d_i)\, x^{p^i}, \tag{4.3}$$

易知它在 $x \in K$ 时取值为零. 由此断定 $\dim_{\mathbb{F}_p}(\mathrm{Im}(D)) \leq 1$. 如果 $\mathrm{Im}(D) = 0$, 那么我们对 $0 \leq i \leq m-1$ 有 $g(d_i) = d_i$, 即 $d_i \in \mathbb{F}_{p^l}$, 于是此时引理成立. 因此, 我们下面假设 $\mathrm{Im}(D)$ 在 $\mathbb{F}_p$ 上的维数是 1; 特别地, 我们从 $\mathrm{Im}(D_K) = \{0\}$ 可得 $K \neq \mathbb{F}_q$, 即 $\eta \neq 0$. 也就是说, 根据引理 *4.6*, 我们断定存在某个 $u \in \mathbb{F}_q^*$ 使得 $D(x) = u\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x)$. 因此我们有以下多项式方程 $\sum_{i=0}^{m-1}(g(d_i)-d_i)X^{p^i} = \sum_{i=0}^{m-1} u\eta^{p^i} X^{p^i}$. 通过比较两边的多项式系数我们就可推出 $g(d_i) - d_i = u\eta^{p^i}$, $0 \leq i \leq m-1$. 根据假设我们有 $g(\eta) = \eta$, 所以 $\eta\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(g(d_0) - d_0) = 0$. 由引理 *4.1*可知存在某个 $v \in \mathbb{F}_q$ 使得 $u = g(v) - v$. 于是我们从 $g(d_i) - d_i = u\eta^{p^i}$ 中推断出 $f_i := d_i - v\eta^{p^i}$ 是被 g 固定的, 即属于 $\mathbb{F}_{p^l}$. 现在定义一个线性化多项式 $L_1(X) := \sum_{i=0}^{m-1} f_i X^{p^i}$. 当 $x \in K$ 时, 我们有

$$L(x) - L_1(x) = \sum_{i=0}^{m-1} v\eta^{p^i} x^{p^i} = v\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x) = 0,$$

故 L_1 是引理所需的多项式. 证毕. □

引理 4.8. 假定 p 是素数并且令 $q = p^m$. 令 $L(X) = \sum_{i=0}^{m-1} s_i X^{p^i}$ 是 $\mathbb{F}_q$ 上一个简化的线性化多项式以及 $\widetilde{L}$ 是该多项式的迹对偶. 取 $\mu \in \mathbb{F}_q$. 假定 $B(c, z) := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu c L(z))$ 是在 $\mathbb{F}_p$-线性子空间 $K = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x) = 0\}$ 上一个对称的双线性型, 其中 η 是 $\mathbb{F}_q$ 中的某个元素. 那么存在 $u \in \mathbb{F}_q$ 使得对所有 $x \in \mathbb{F}_q$ 有 $\widetilde{L}(\mu x) = \mu L(x) - \eta\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ux) + u\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x)$ 以及

$$\mu s_i - s_{m-i}^{p^i} \mu^{p^i} = \eta u^{p^i} - u\eta^{p^i}, \quad 0 \leq i \leq m-1. \tag{4.4}$$

而且如果 q 是偶数和 $K = \mathbb{F}_q$, 那么当且仅当 $\mu s_0 = 0$ 时, 才对所有 $c \in \mathbb{F}_q$ 有 $B(c, c) = 0$.

证明. $\eta = 0$ 的情况和 $\eta \neq 0$ 的情况的证明是相似的, 于是我们这里只证明更复杂的情形 $\eta \neq 0$. 如果 $\mu = 0$, 那么我们可以取 $u = 0$, 而此时结论成立. 我们接下来假设 $\mu \neq 0$. 由引理的假设可知我们有 $B(c, z) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\widetilde{L}(\mu c)z)$, 其中 $\widetilde{L}$ 是 L 的迹对偶. 因为 B 在 K 上是对称的, 所以对 $c, z \in K$ 有 $B(c, z) = B(z, c)$, 因此 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((\mu L(c) - \widetilde{L}(\mu c))z) = 0$, $c, z \in K$. 于是由引理 *4.3*可得对 $c \in K$ 有 $\mu L(c) - \widetilde{L}(\mu c) \in \mathbb{F}_p \cdot \eta$. 由引理 *4.6*可知存在 $u, v \in \mathbb{F}_q^*$ 使得 $\mu L(c) - \widetilde{L}(\mu c) = \eta\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(uc) + v\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x)$. 引理的第一部分就是通过比较多项式等式 $\mu L(X) - \widetilde{L}(\mu X) = \sum_{i=0}^{m-1} \eta u^{p^i} X^{p^i} + \sum_{i=0}^{m-1} v\eta^{p^i} X^{p^i}$

中对应的系数得到的. 此外, 我们通过比较 X 项的系数和利用其左手边等于 0 的事实推出 $v = -u$.

现在假设 q 是偶数以及 $K = \mathbb{F}_q$, 即 $\eta = 0$. 我们只需要处理 m 是偶数的情况, 这是因为 m 是奇数的情况是类似的. 在这种情况下, 我们通过在等式(4.4)取 $i = m/2$ 得到 $\mu s_{m/2} \in \mathbb{F}_{2^{m/2}}$. 这样我们就可以计算出

$$\begin{aligned} B(c,c) &= \mathrm{Tr}(\mu s_0 c^2) + \mathrm{Tr}(\mu s_{m/2} c^{2^{m/2}+1}) + \sum_{i=1}^{m/2-1} \mathrm{Tr}(\mu s_i c^{2^i+1} + \mu s_{m-i} c^{2^{m-i}+1}) \\ &= \mathrm{Tr}(\mu s_0 c^2), \end{aligned}$$

其中 $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}$. 由于 $\mu s_{m/2} c^{2^{m/2}+1} \in \mathbb{F}_{2^{m/2}}$ 可知第二项为零, 并且在第三项中每个被加数都是通过等式(4.4)和 $\mathrm{Tr}(\mu s_{m-i} c^{2^{m-i}+1}) = \mathrm{Tr}((\mu s_{m-i})^{2^i} c^{2^i+1})$ 而被消去的. 于是引理的第二部分成立. □

对于 $\mathbb{F}_q$ 中两个子集 A 和 B, 我们定义 $A \cdot B := \{xy : x \in A, y \in B\}$, 并且也记由 A 生成 $\mathbb{F}_p$-线性子空间为 $\langle A \rangle_{\mathbb{F}_p}$.

引理 4.9. *假定 p 是素数和 $q = p^m$, $m > 2$, 再令 A, B 是 $\mathbb{F}_q$ 中两个余维数为 1 的 $\mathbb{F}_p$-线性子空间. 那么 $\langle A \cdot A \rangle_{\mathbb{F}_p} = \langle A \cdot B \rangle_{\mathbb{F}_p} = \mathbb{F}_q$.*

证明. 我们不失一般性地假设 $1 \in A \cap B$. 记 $W = \langle A \cdot A \rangle_{\mathbb{F}_p}$, 同时假设 $W \neq \mathbb{F}_q$. 因为 $A \leq W \leq \mathbb{F}_q$ 且 A 的余维数是 1, 所以我们有 $W = A$. 子空间 A 在域乘法下是封闭的, 我们推出 A 是有限域 $\mathbb{F}_q$ 的真子域, 因此有 $q \geq |A|^2$. 另一方面, 根据假设 A 的余维数为 1, 即 $q = p \cdot |A|$. 于是我们推断出 $(|A|, q) = (p, p^2)$ 或 $(|A|, q) = (1, p)$, 这两个结论都与假设 $m > 2$ 矛盾. 概括而言, 我们已经证明 $\langle A \cdot A \rangle_{\mathbb{F}_p} = \mathbb{F}_q$.

现在我们考虑证明另外一个等式, 假设 $A \neq B$. 记 $U = \langle A \cdot B \rangle_{\mathbb{F}_p}$. 根据 $1 \in A \cap B$ 可知它包含 A 和 B, 于是它也包含子空间 $A + B = \mathbb{F}_q$. 证毕. □

我们分类的关键因素是 $\mathbb{F}_q$ 中 $\mathrm{Aut}(\mathbb{F}_q)$ 模的结构. 假设 $m = p^e l$ 且 $e \geq 1$. 取 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得对 $x \in \mathbb{F}_q$ 有 $g(x) = x^{p^l}$. 记 $G := \langle g \rangle \leq \mathrm{Aut}(\mathbb{F}_q)$, 于是就有 $|G| = p^e$. 令 $\mathbb{F}$ 是有限域 $\mathbb{F}_q$ 的子域. 这里我们记录一些群环 $\mathbb{F}[G]$ 的基本事实, 详见文献[77,78].

(i) 群环 $\mathbb{F}[G]$ 是一个单链局部环. 它的理想集 $(1-g)^i\mathbb{F}[G]$, $0 \leq i \leq p^e$ 是它所有理想的集合, 并且它们用包含关系构成了一个理想链. $(1-g)^i\mathbb{F}[G]$ 在 $\mathbb{F}$ 上的维数是 $p^e - i$; 特别地, $(1-g)^{p^e} = 1 - g^{p^e} = 0$.

(ii) 通过二项式展开可得 $(1-g)^{p-1}=1+g+\cdots+g^{p-1}$, 并且用归纳法可得

$$(1-g)^{p^i-1}=1+g+\cdots+g^{p^i-1},\quad 1\le i\le e. \tag{4.5}$$

作为推论, 对 $x\in\mathbb{F}_q$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(x)=\sum_{i=0}^{p^e-1}g^i(x)=(1-g)^{p^e-1}(x)$.

引理 4.10. 使用以上定义的符号. 如果 $1\le i\le p^e-1$ 且 $\gcd(i,p)=1$, 那么 $1+g+\cdots+g^{i-1}$ 在群环里是可逆的.

证明. 群环 $\mathbb{F}[G]$ 是一个含有极大理想 $I=(1-g)\mathbb{F}[G]$ 的局部环, 且 $\mathbb{F}[G]$ 中的元素 a 是可逆的当且仅当它在商环 $\mathbb{F}[G]/I\cong\mathbb{F}$ 里的像是可逆的. 因为 $1+g+\cdots+g^{i-1}=i \bmod (1-g)$, 所以我们从 $\gcd(i,p)=1$ 中推断出 $1+g+\cdots+g^{i-1}$ 不可能落在极大理想 I. □

从现在开始, 设 $R'=\mathbb{F}_{p^l}[G]$, $R=\mathbb{F}_p[G]$, 并且对 $0\le i\le p^e$ 定义 $R_i:=(1-g)^iR$. 我们有下面 R 中的理想链:

$$R=R_0\supseteq R_1\supseteq\cdots\supseteq R_{p^e-1}\supseteq R_{p^e}=0, \tag{4.6}$$

其中对每个 $0\le i\le p^e-1$ 有 $\dim_{\mathbb{F}_p}(R_i/R_{i+1})=1$. 特别地, $\dim_{\mathbb{F}_p}(R_i)=p^e-i$.

根据文献[76] 中的定理 *2.35* 可知存在 $\mathbb{F}_q$ 中的一组 $\mathbb{F}_{p^l}$-线性正规基, 其形式为 $\{g^i(\eta):0\le i\le p^e-1\}$, 这里 $\eta\in\mathbb{F}_q$. 故 $\mathbb{F}_q$ 是具有生成元 η 的自由 $\mathbb{F}_{p^l}[G]$ 模, 即 $\mathbb{F}_q=R'\cdot\eta$, 其中 $R'=\mathbb{F}_{p^l}[\langle g\rangle]$. 取 $\xi_1,\xi_2,\cdots,\xi_l$ 为 $\mathbb{F}_{p^l}$ 中的一组 $\mathbb{F}_p$-线性基. 那么 $R'=\xi_1R\oplus\xi_2R\oplus\cdots\oplus\xi_lR$ 和

$$\mathbb{F}_q=R\cdot\xi_1\eta\oplus R\cdot\xi_2\eta\oplus\cdots\oplus R\cdot\xi_l\eta. \tag{4.7}$$

因此每个 $R\cdot\xi_i\eta$ 是以 $\xi_i\eta$ 为生成元的自由 R 模. $R\cdot\xi_i\eta$ 的子模是 $R_k\cdot\xi_i\eta$, $0\le k\le p^e-1$, 并且这些子模组成类似于等式(4.6)中所示的子模链. 特别地, $R\cdot\xi_i\eta$ 中每个子模都有唯一对应的维数, 而且这些子模也用包含关系构成类似于等式(4.6)中所示的子模链.

引理 4.11. 假定 $q=p^{p^el}$, 并且 $e\ge1$, 再取 $g\in\mathrm{Aut}(\mathbb{F}_q)$ 使得对 $x\in\mathbb{F}_q$ 有 $g(x)=x^{p^l}$. 那么存在 (W,t) 使得

(1) W 是 $\mathbb{F}_q$ 中的一个 g 不变和余维数为 h 的 $\mathbb{F}_p$-线性子空间, 其中 $0<h\le e$;

(2) t 是 $\mathbb{F}_q$ 中的元素使得 $W_i:=W+t_i$, $0\le i\le p^h-1$ 两两不相交, 其中 $t_0=0$ 和 $t_i=(1+\cdots+g^{i-1})(t)$, $1\le i\le p^h-1$;

当且仅当 $h\ge p^{h-1}$, 即当 p 是奇数时 $h=1$, 而当 $p=2$ 时 $h=1$ 或 2.

证明. 如果 (W, t) 是引理所需的, 那么根据条件 (1) 可知 W 是 $\mathbb{F}_q$ 的 R 子模, 其中 $G = \langle g\rangle$, $R = \mathbb{F}_p[G]$. 记得我们有 $R_i = (1-g)^i R$, 其中 $0 \le i \le p^e$.

我们现在证明条件 (2) 可以简化为一个单独条件 $t_{p^{h-1}} \notin W$. 对 $0 \le i < j \le p^h - 1$, 我们有 $t_j - t_i = g^i(t_{j-i})$. 因为 W 是 g 不变的, 所以 $W + t_i \cap W + t_j = \emptyset$ 当且仅当 $t_{j-i} \notin W$. 如果 $j - i = p^k u$ 并且有 $\gcd(u, p) = 1$, 那么

$$t_{j-i} = (1 + g_k + \cdots + g_k^{u-1})(t_{p^k}), \quad g_k := g^{p^k}.$$

根据引理 *4.10*可知 $1+g_k+\cdots+g_k^{u-1}$ 在 R 上是可逆的, 故 $t_{j-i} \notin W$ 当且仅当 $t_{p^k} \notin W$. 这就只需要证明对 $0 \le k \le h-1$ 有 $t_{p^k} \notin W$. 根据等式(4.5)可知 $t_{p^k} = (1-g)^{p^k-1}(t)$, 注意到 $R_{p^k-1} \cdot t = R \cdot t_{p^k}$, 这是该子模的生成元. 通过把子模链(4.6)应用到 t 上, 问题就转化为证明 $t_{p^{h-1}} \notin W$. 这就证明我们的说法.

由等式(4.5)可知 $t_{p^{h-1}} = (1-g)^{p^{h-1}-1}(t)$. 满足 $(1-g)^{p^{h-1}-1}(t) \notin W$ 的 t 的存在性等价于 $W^* \not\le W$,

$$W^* := (1-g)^{p^{h-1}-1}(\mathbb{F}_q) = R_{p^{h-1}-1} \cdot \xi_1\eta \oplus \cdots \oplus R_{p^{h-1}-1} \cdot \xi_l\eta,$$

其中 η 和 $\xi_i, 1 \le i \le l$ 是 $\mathbb{F}_q$ 中的元素使得等式(4.7)成立. W^* 中的每个组成部分 $W_i^* = R_{p^{h-1}-1} \cdot \xi_i\eta$ 在 $\mathbb{F}_p$ 上的维数是 $p^e - p^{h-1} + 1$.

利用上述的准备, 我们就可以开始证明引理. 如果 $h \ge p^{h-1}$, 那么我们就取 W 是 $R \cdot \xi_2\eta \oplus \cdots \oplus R \cdot \xi_l\eta$ 和一个 $R \cdot (\xi_1\eta)$ 的 R 子模组成的直和, 其中该 R 子模具有维数

$$p^e l - h - p^e(l-1) = p^e - h < \dim_{\mathbb{F}_p}(W_1^*).$$

由此断定 W_1^* 不可能是选定的 W 的子模. 接着取 $t \in \mathbb{F}_q$ 使得 $(1-g)^{p^{h-1}-1}(t) \in W_1^* \setminus W$, 于是 (W, t) 就是引理所需的.

相反地, 如果 $h < p^{h-1}$, 那么

$$\begin{aligned}\dim_{\mathbb{F}_p}(W \cap (R \cdot \xi_i\eta)) &\ge \dim_{\mathbb{F}_p} W + \dim_{\mathbb{F}_p}(R \cdot \xi_i\eta) - \dim_{\mathbb{F}_p}(\mathbb{F}_q) \\ &= p^e l - h + p^e - p^e l = p^e - h \ge \dim_{\mathbb{F}_p}(W_i^*).\end{aligned}$$

又因为 $R \cdot \xi_i\eta$ 是一个单列 R 模, 所以 W 包含 W_i^*. 于是就有 $W^* \le W$, 因此不可能存在 (W, t) 使得引理的条件成立. 证毕. □

4.2.2 $\mathcal{Q} = W(q)$ 的 *Payne* 派生四边形 $\mathcal{Q}^P$

我们将使用广义四边形的标准概念, 这些概念都可以在著作[28] 中找到. 令 $q = p^m$ 是素数幂, 其中 p 是素数. 令 $\perp$ 是 $\mathrm{PG}(3, q)$ 中固定的辛极性 *(symplectic polarity)*. 经典的辛对称四边形 $\mathcal{Q} = W(q)$ 具有跟 $\mathrm{PG}(3, q)$ 一样的点集, 而它的线集包含 $\mathrm{PG}(3, q)$

中辛极性下的完全迷向线. $\mathcal{Q}$ 中关于点 P 的 *Payne* 派生四边形 $\mathcal{Q}^P$ 以 $\mathrm{PG}(3,q)\setminus P^\perp$ 为点集, 而它的线集包含两类线: 所有不过点 P 的完全迷向线以及所有过不属于 $P^\perp$ 的点 Q 的线 $\langle P, Q\rangle$. 这样的四边形 $\mathcal{Q}^P$ 的阶是 $(q-1, q+1)$. 因为 $\mathcal{Q}$ 的自同构群作用在它的点集上是传递的, 所以 P 的不同选取都会产生同构的派生四边形. 根据文献[37] 中的推论 *2.4*, 点 P 在 $\mathrm{P\Gamma Sp}(4,q)$ 中的稳定子群在 $q\geq 5$ 时是 $\mathcal{Q}^P$ 的全自同构群.

令 $V:=\mathbb{F}_q^4$ 为在 $\mathbb{F}_q$ 上赋有 *alternating* 型 $(x,y):=x_1y_4-x_4y_1+x_2y_3-x_3y_2$ 的向量空间. 记 $\delta:=\mathit{diag}(\gamma,\gamma,1,1)$, 其中 γ 是 $\mathbb{F}_q$ 中的本原元. 对每个 $\sigma\in\mathrm{Aut}(\mathbb{F}_q)$, 定义 $x^\sigma=(x_1^\sigma,\cdots,x_4^\sigma)$. 那么我们根据文献[79] 中的第 *1.7.1* 节可知 $\Gamma\mathrm{SP}(4,q)=\langle\mathrm{Sp}(4,q),\delta\rangle\rtimes\mathrm{Aut}(\mathbb{F}_q)$. 注意到 $\Gamma\mathrm{SP}(4,q)$ 中每个元素可以写成 $x\mapsto x^\sigma A$, 其中 $A\in\mathrm{GL}(4,q)$ 和 $\sigma\in\mathrm{Aut}(\mathbb{F}_q)$, 于是我们记这个元素为 (A,σ). 我们分别将元素 (A,σ) 中的 A 称为矩阵部分以及 σ 称为 *Frobenius* 部分.

取一个固定的射影点 $P:=\langle(1,0,0,0)\rangle$. 点 P 在 $\mathrm{Sp}(4,q)$ 中的稳定子群 $\mathrm{Sp}(4,q)_P$ 由以下矩阵组成:

$$\begin{pmatrix}\lambda & 0 & 0\\ -HJ\boldsymbol{v}^T & H & 0\\ z & \boldsymbol{v} & \lambda^{-1}\end{pmatrix},\ H\in\mathrm{SL}(2,q),\ \boldsymbol{v}\in\mathbb{F}_q^2,\ z\in\mathbb{F}_q,\ \lambda\in\mathbb{F}_q^*,$$

其中 $J=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$. 那么 $\mathrm{Sp}(4,q)_P$ 连同 σ 和 δ 生成 $\Gamma Sp(4,q)_P$. 此时模去 $\Gamma\mathrm{Sp}(4,q)$ 的中心, 我们就得到 $\mathrm{P\Gamma Sp}(4,q)_P$. 这里为了便于表示, 我们依旧分别记 δ 和 σ 分别是他们在 $\mathrm{P\Gamma Sp}(4,q)_P$ 中的像. 特别地, 我们观察到 δ 的阶是 $q-1$.

令 G 为 $\mathrm{P\Gamma Sp}(4,q)_P$ 中的子群, 并且它正则地作用在 $\mathcal{Q}^P$ 的点上. 对每个 $g\in\mathrm{P\Gamma Sp}(4,q)_P$, g 保持 $\mathcal{Q}^P$ 不变, $g^{-1}Gg$ 也是 $\mathcal{Q}^P$ 的点正则群. 因此, 我们可以不失一般性地假设 G 包含于 $\mathrm{P\Gamma Sp}(4,q)_P$ 的某个特定 *Sylow* p-子群, 该群是由 $\mathrm{Aut}(\mathbb{F}_q)$ 中 *Sylow* p-子群和 $\mathrm{Sp}(4,q)_P$ 中所有对角元为 *1* 的下三角矩阵组合, 其中后者具体形式如下所示:

$$E(a,b,c,t):=\begin{pmatrix}1&0&0&0\\ -c&1&0&0\\ b-ct&t&1&0\\ a&b&c&1\end{pmatrix},\quad a,\,b,\,c,\,t\in\mathbb{F}_q. \tag{4.8}$$

Payne 派生四边形 $\mathcal{Q}^P$ 的点集恰好是 $\{\langle(a,b,c,1)\rangle:\ a,\,b,\,c\in\mathbb{F}_q\}$. 为了让 G 是点正则的, 对每个三元组 (a,b,c), 都应该恰好存在一个 G 中的元素使得它将 $\langle(0,0,0,1)\rangle$ 映射到 $\langle(a,b,c,1)\rangle$ 上, 也就是说, 该元素的矩阵部分的最后一行恰好是 $(a,b,c,1)$. 于是我们记这样的元素为 $\mathfrak{g}_{a,b,c}=(\mathcal{M}_{a,b,c},\theta_{a,b,c})$, 其中 $\theta_{a,b,c}\in\mathrm{Aut}(\mathbb{F}_q)$ 和 $\mathcal{M}_{a,b,c}:=E\left(a,b,c,T(a,b,c)\right)$. 这里 T 是把 $\mathbb{F}_q^3$ 映射到 $\mathbb{F}_q$ 的函数. 对应地, G 中的群乘法 $\circ$ 定义

为

$$\mathfrak{g}_{a,b,c} \circ \mathfrak{g}_{x,y,z} = (\mathcal{M}_{a,b,c}^{\theta_{x,y,z}} \cdot \mathcal{M}_{x,y,z},\, \theta_{a,b,c}\theta_{x,y,z}), \tag{4.9}$$

其中 $\mathcal{M}^{\theta}$ 是将 θ 作用在矩阵 $\mathcal{M}$ 中每一项而获得的矩阵, 并且 $\cdot$ 是一般的矩阵乘法. 综上所述, 在 $\mathrm{P\Gamma Sp}(4,q)_P$ 中的共轭等价意义下 $\mathcal{Q}^P$ 的一个点正则子群 G 形式为 $G = \{\mathfrak{g}_{a,b,c} : a, b, c \in \mathbb{F}_q\}$, 其中 T 和 θ 是下面定义的某些函数

$$T : \mathbb{F}_q^3 \to \mathbb{F}_q, \quad \theta : \mathbb{F}_q^3 \to \mathrm{Aut}(\mathbb{F}_q),$$

这里记 $\theta(x,y,z) = \theta_{x,y,z}$.

定理 4.12. 令 $T : \mathbb{F}_q^3 \to \mathbb{F}_q$ 和 $\theta : \mathbb{F}_q^3 \to \mathrm{Aut}(\mathbb{F}_q)$ 为两个函数. 设 $\mathcal{M}_{a,b,c} := E(a,b,c,T(a,b,c))$, $\theta_{a,b,c} := \theta(a,b,c)$, 以及 $\mathfrak{g}_{a,b,c} := (\mathcal{M}_{a,b,c}, \theta_{a,b,c})$. 定义 $G := \{\mathfrak{g}_{a,b,c} : a, b, c \in \mathbb{F}_q\}$. 那么 G 是 Payne 派生四边形 $\mathcal{Q}^P$ 的一个点正则群当且仅当对任何三元组 (a,b,c) 和 (x,y,z) 有 $\mathfrak{g}_{a,b,c} \circ \mathfrak{g}_{x,y,z} = \mathfrak{g}_{u,v,w}$, 也就是说,

$$\theta_{a,b,c}\theta_{x,y,z} = \theta_{u,v,w}, \tag{4.10}$$

$$T(a,b,c)^{\theta_2} + T(x,y,z) = T(u,v,w), \tag{4.11}$$

其中 $\theta_2 = \theta_{x,y,z}$, $w = c^{\theta_2} + z$ 和

$$u = a^{\theta_2} + x - b^{\theta_2}z + c^{\theta_2}y - c^{\theta_2}zT(x,y,z),$$
$$v = b^{\theta_2} + y + c^{\theta_2}T(x,y,z).$$

证明. 易知群元素 $\mathfrak{g}_{a,b,c}$ 将 $(0,0,0,1)$ 映射到 $(a,b,c,1)$, 故只需要证明 G 是一个群, 那么 G 作用在 $\mathcal{Q}^P$ 的点集就是传递的. 因为 G 是有限的, 所以只要保证 G 在等式(4.9)中定义的乘法 $\circ$ 下是封闭的. 通过直接的计算, 我们就推出 $\mathfrak{g}_{a,b,c} \circ \mathfrak{g}_{x,y,z}$ 中矩阵部分的最后一行是 $(u,v,w,1)$, 其中 u,v,w 是如定理中叙述的元素. 因此我们只需要验证 $\mathfrak{g}_{a,b,c} \circ \mathfrak{g}_{x,y,z} = \mathfrak{g}_{u,v,w}$. 定理中叙述的等价条件是通过比较上式两边的 *Frobenius* 部分和矩阵部分的第 (3, 2) 项获得的. □

一般而言, 定理 *4.12*中的条件是十分复杂的. 故我们考虑一些特殊情况从而简化定理 *4.12*中的条件. 我们接着引入下面一些符号, 其中它们将在这章的余下部分一直使用.

符号 4.2.1. 定义 $\sigma_c := \theta_{0,0,c}$ 以及

$$L(x) := T(x,0,0),\ M(y) := T(0,y,0),\ S(z) := T(0,0,z).$$

而且, 定义 $G_A := \{\mathfrak{g}_{a,0,0} : a \in \mathbb{F}_q\}, G_B := \{\mathfrak{g}_{0,b,0} : b \in \mathbb{F}_q\}$ 和 $G_{A,B} := \{\mathfrak{g}_{a,b,0} : a, b \in \mathbb{F}_q\}$.

推论 4.13. 取如定理 4.12中一样的符号, 并且假设 G 是 Payne 派生四边形 $\mathcal{Q}^P$ 的一个点正则群. 那么对 $\mathbb{F}_q$ 中的 a, b, c, x, y, z, 以下条件成立:

(1) $\theta_{a,0,0}\theta_{x,0,0} = \theta_{(a^{\theta_{x,0,0}}+x),0,0}$ 和 $L(a)^{\theta_{x,0,0}} + L(x) = L(a^{\theta_{x,0,0}} + x)$;

(2) $\theta_{0,b,0}\theta_{0,y,0} = \theta_{0,(b^{\theta_{0,y,0}}+y),0}$ 和 $M(b)^{\theta_{0,y,0}} + M(y) = L(b^{\theta_{0,y,0}} + y)$;

(3) $\sigma_c\sigma_z = \theta_{u,v,w}$ 和 $S(c)^{\sigma_z} + S(z) = T(u, v, w)$, 其中 $u = -\sigma_z(c)zS(z)$, $v = \sigma_z(c)S(z)$ 以及 $w = \sigma_z(c) + z$;

(4) $\theta_{a,0,0}\theta_{0,b,0} = \theta_{a^{\theta_{0,b,0}},b,0}$ 和 $L(a)^{\theta_{0,b,0}} + M(b) = T(a^{\theta_{0,b,0}}, b, 0)$;

(5) $\theta_{0,b,0}\theta_{a,0,0} = \theta_{a,b^{\theta_{a,0,0}},0}$ 和 $L(a) + M(b)^{\theta_{a,0,0}} = T(a, b^{\theta_{a,0,0}}, 0)$;

(6) $\mathfrak{g}_{a,b,c} = \mathfrak{g}_{a',b',0} \circ \mathfrak{g}_{0,0,c}$, 或等价地, $\theta_{a,b,c} = \theta_{a',b',0}\theta_{0,0,c}$ 且 $T(a, b, c) = T(a', b', 0)^{\sigma_c} + S(c)$, 其中 $a' = \sigma_c^{-1}(a + bc), b' = \sigma_c^{-1}(b)$;

(7) $\sigma_c\theta_{a,b,0} = \theta_{u,v,0}\sigma_w$ 和 $S(c)^{\theta_{a,b,0}} + T(a, b, 0) = T(u, v, 0)^{\sigma_w} + S(w)$, 其中 $w = c^{\theta_{a,b,0}}$, $v = \sigma_w^{-1}\left(b + c^{\theta_{a,b,0}}T(a, b, 0)\right)$ 以及 $u = \sigma_w^{-1}\left(a + 2bc^{\theta_{a,b,0}} + c^{2\theta_{a,b,0}}T(a, b, 0)\right)$.

证明. 条件 (1)-(5) 都是定理 *4.12*的特殊情况. 条件 (6) 中的第一个方程可以通过检查其两边在点 $\langle(0, 0, 0, 1)\rangle$ 的作用来直接验证, 而第二部分可从定理 *4.12*中得到. 这只待证明条件 (7). 先固定一个三元组 (a, b, c). 由条件 (6) 可知存在一个三元组使得

$$\mathfrak{g}_{0,0,c} \circ \mathfrak{g}_{a,b,0} = \mathfrak{g}_{u,v,0} \circ \mathfrak{g}_{0,0,w}. \tag{4.12}$$

由定理 *4.12*可知道上式左边等于 $\mathfrak{g}_{x,y,w}$, 其中

$$(x, y, w) = (a + bc^{\theta_{a,b,0}}, b + c^{\theta_{a,b,0}}T(a, b, 0), c^{\theta_{a,b,0}}).$$

我们通过条件 (6) 推出如条件 (7) 中所示的 u, v 的表达式. 接着我们直接计算等式(4.12)的两边, 于是条件 (7) 在通过比较等式两边的 *Frobenius* 部分和矩阵部分的第 (3, 2) 项后得到 *(*或者, 通过使用定理 *4.12*验证 $\mathfrak{g}_{x,y,w} = \mathfrak{g}_{u,v,0} \circ \mathfrak{g}_{0,0,w}$*)*. □

推论 4.14. 取如定理 4.12中一样的符号, 并且假设 G 是 Payne 派生四边形 $\mathcal{Q}^P$ 的一个点正则群. 那么 $G_A := \{\mathfrak{g}_{a,0,0} : a \in \mathbb{F}_q\}, G_B := \{\mathfrak{g}_{0,b,0} : b \in \mathbb{F}_q\}$ 和 $G_{A,B} := \{\mathfrak{g}_{a,b,0} : a, b \in \mathbb{F}_q\}$ 都是 G 的子群.

证明. 证明是通过直接验证这些子集在群乘法(4.9)下封闭来实现的. 这里我们只证明 G_A 的部分. 根据定理 *4.12*可知对 $x, a \in \mathbb{F}_q$ 存在某个 $u \in \mathbb{F}_q$ 使得 $\mathfrak{g}_{a,0,0} \circ \mathfrak{g}_{x,0,0} = \mathfrak{g}_{u,0,0}$, 所以 G_A 在群乘法(4.9)下是封闭的. 又因为 G 是有限的, 所以我们推出 G_A 是一个群. 对于 G_B 和 $G_{A,B}$ 的证明也是如此的. □

注 4.15. 令 E 是如等式(4.8)中定义的矩阵. 我们将在本章中大量地使用下列计算方法:

$$E(a,b,c,t)\cdot E(x,y,z,w) = E(a+x-bz+cy-czw, b+y+cw, c+z, t+w),$$
$$E(a,b,c,t)^{-1} = E(-a,-b+ct,-c,-t).$$

在上述的每个方程中最后的两个坐标, 即矩阵部分的第 $(4,3)$ 项和第 $(3,2)$ 项, 它们在右手边均有相对简单的表达式. 这个观察将在很多情况下是特别有用的, 这是因为我们在推导过程中只关心这两个坐标.

4.3 q 是奇数时 $\mathcal{Q}^P$ 的所有点正则群的总结

我们首先列出本章在奇特征情况下关于 $\mathcal{Q}^P$ 的点正则群的所有构造, 但是具体验证每个构造所需要的元素的存在性的过程将会在后面的章节中给出.

构造 4.16. 对于素数幂 $q = p^m$, 设 $\theta_{a,b,c} \equiv 1$, 并存在 $\mathbb{F}_q$ 上一个简化的线性化多项式 S_1 使得 $T(a,b,c) := S_1(c)$. 当 T 和 θ 是具有以上规定形式的函数时, 如定理 4.12中定义的集合 G 就是 $\mathcal{Q}^P$ 的一个点正则群.

构造 4.17. 假定 $q = p^{pl}$ 其中 p 是奇素数和 l 是正整数. 再令 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x) = x^{p^l}$. 令 $S_1(X)$ 为简化的线性化多项式, 其每项多项式系数都落在 $\mathbb{F}_{p^l}$ 中. 取 $\mu_C \in \mathbb{F}_{p^l}^*$. 对 a, b, $c \in \mathbb{F}_q$, 令 $\theta_{a,b,c} := g^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C c)}$ 和 $T(a,b,c) := S_1(c)$. 当 T 和 θ 是具有以上规定形式的函数时, 如定理 4.12中定义的集合 G 就是 $\mathcal{Q}^P$ 的一个点正则群.

构造 4.18. 假定 $q = p^{pl}$, 其中 p 是奇素数和 l 是正整数. 再令 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x) = x^{p^l}$. 取 $\mu_B \in \mathbb{F}_{p^l}^*$, $\alpha \in \mathbb{F}_{p^l}$ 以及 pl 元组 $(s_0, s_1, \cdots, s_{pl-1})$, 其中 pl 元组中每个元素都属于 $\mathbb{F}_{p^l}$ 且满足对 $1 \le i \le pl-1$ 有 $\mu_B s_i - s_{pl-i}^{p^i} \mu_B^{p^i} = 0$. 设 $S_1(x) := \sum_{i=0}^{pl-1} s_i x^{p^i}$, 再令 $Q(x) := -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B x S_1(x))$, 其中 $x \in \mathbb{F}_q$. 接着取

$$\theta_{a,b,c} := g^{\frac{1}{2}Q(c)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B b+\alpha c)}, \quad T(a,b,c) := S_1(c) \text{ for } a,\ b,\ c \in \mathbb{F}_q.$$

当 T 和 θ 是具有以上规定形式的函数时, 如定理 4.12中定义的集合 G 就是 $\mathcal{Q}^P$ 的一个点正则群.

构造 4.19. 假定 $q=3^{9l}$ 且 l 是正整数, 再取 $g\in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x)=x^{3^l}$. 设 $g_1:=g^3$.

(i) 取 $u\in\mathbb{F}_{3^{3l}}$ 使得 $\mu_C:=u-u^g\in\mathbb{F}_{3^l}^*$;

(ii) 取 $t_C\in\mathbb{F}_q^*$ 使得 $\lambda_C:=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_C t_C)\neq 0$;

(iii) 取 $\mu_B\in\mathbb{F}_{3^l}^*$;

(iv) 取 $9l$ 元组 $(s_0, s_1,\cdots, s_{9l-1})$, 其中每个元素都属于 $\mathbb{F}_{3^l}$ 并满足

$$-\mu_B s_i+s_{9l-i}^{3^i}\mu_B^{3^i}=\mu_C u^{3^i}-u\mu_C^{3^i},\ 1\le i\le 9l-1;$$

(v) 取 $\alpha\in\mathbb{F}_{3^{3l}}, \lambda\in\mathbb{F}_3$ 使得 $g(\alpha)-\alpha=\lambda_C u+\lambda\mu_C$.

设 $S_1(x):=\sum_{i=0}^{9l-1}s_i x^{3^i}, Q(x):=-\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_B x S_1(x))$, 其中 $x\in\mathbb{F}_q$. 再令 $K:=\{z\in\mathbb{F}_q:\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_C z)=0\}$. 当 $a, b\in\mathbb{F}_q$ 和 $c\in K$ 时, 定义

$$\mathcal{M}_{a,b,c}=E(a,b,c,S_1(c)),\quad \theta_{a,b,c}:=g_1^{\frac{1}{2}Q(c)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\alpha c+\mu_B b)},$$

和 $\mathfrak{g}_{a,b,c}=(\mathcal{M}_{a,b,c},\theta_{a,b,c})$. 那么 $G_K:=\{\mathfrak{g}_{a,b,c}: a, b\in\mathbb{F}_q, c\in K\}$ 是一个阶为 $q^3/3$ 的群. 设 $\mathfrak{g}_{0,0,t_C}:=(\mathcal{M}_{0,0,t_C}, g)$, 其中 $\mathcal{M}_{0,0,t_C}:=E(0,0,t_C,S_1(t_C))$. 于是 $G:=\langle G_K, \mathfrak{g}_{0,0,t_C}\rangle$ 是 $\mathcal{Q}^P$ 的一个点正则群.

本章的主体部分将致力于完成对奇特征情形下的分类定理的证明.

定理 4.20. 假定 q 是奇数且 $q\ge 5$ 时. 令 G 是辛对称四边形 $\mathcal{Q}=W(q)$ 的 Payne 派生四边形 $\mathcal{Q}^P$ 的一个点正则自同构群. 那么 G 跟构造 4.16-4.19其中一个构造产生的群相共轭.

这里我们简略地描述一下我们是如何证明定理 *4.20*. 线性的情况将在第 *4.4*节中处理, 方法是通过探究推论 *4.13*中的条件, 值得注意的是在这种情况下这些条件迫使函数 T,θ 表现出简单的形式. 这些论证也适用于 q 是偶数的情形, 因此诱导出一个新的构造, 即构造 *4.26*. 而非线性的情况也依赖于对推论条件的详细分析, 但需要考虑的内容的范围要比线性的复杂得多. 第一个主要步骤是借助引理 *4.11*来约束 G 的 *Frobenius* 部分的阶, 具体做法参考定理 *4.28*和 *4.31*. 这一步是至关重要的, 因为它将暗示着 G 实际上几乎是线性的, 换言之, 从 G 到 $\mathrm{Aut}(\mathbb{F}_q)$ 的群同态的核 H*(*将元素映射到它的 *Frobenius* 部分*)* 在 G 中有很小的 *index*. 同时这一步在 q 是偶数时也是有效的. 与在线性的情况一样, 我们可以通过检查推论 *4.13*中的条件来很好地描述 H 的群结构. 取一个元素 $g\in G$ 使得该元素的 *Frobenius* 部分具有尽可能大的阶

$b = [G : H]$. 那么我们就有 $G = \langle H, g\rangle$, $g^b \in H$ 以及 $H \trianglelefteq G$. 然后, 我们进一步推导出 H 和 g 的参数的限制条件, 具体是考虑 $H^g \leq H$, g^bH 和 g 在 $\mathcal{Q}^P$ 上的传递性, 但是实际的分析会上面的描述复杂, 不过它们的本质是一样的. 这就将非线性的情况分为三个构造. 在第 *4.7*节中, 我们进一步简化了 $\mathrm{P\Gamma Sp}(4, q)$ 中的结构, 从而完成了定理的证明.

注 4.21. 构造 4.24是以隐式的方法在文献[70] 和文献[71] 中给出. 令 $q = p^m$, 其中 p 是素数. 对于 $\alpha \in \mathbb{F}_q$, 定义 $\theta_\alpha := E(0, 0, \alpha, \alpha)$ 和 $t_{0,0,\alpha} := E(0, 0, \alpha, 0)$, 其中 E 是在等式(4.8)中定义的矩阵. 令 $\{\alpha_1, \cdots, \alpha_m\}$ 是 $\mathbb{F}_q$ 的一组 $\mathbb{F}_p$-线性基. 取 $\{\beta_1, \cdots, \beta_m\}$ 为它的对偶基, 即若 $i = j$ 就有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_i\beta_j) = 1$, 否则 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_i\beta_j) = 0$. 对 $1 \leq k \leq m-1$, 设 $T_k(x, y, z) := \sum_{i=1}^{k} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta_i z)\alpha_i$. 再令 G_k 是来自构造 4.24的点正则群, 其中 $T = T_k$. 于是我们在 G_K 中观察到 $\mathfrak{g}_{0,0,\alpha_i} = \theta_{\alpha_i}$, $\mathfrak{g}_{0,0,\alpha_j} = t_{0,0,\alpha_j}$, 其中 $1 \leq i \leq k$ 和 $k+1 \leq j \leq m$. 使用文献[36] 中一样的符号, 群 G_k 是用 $U = \langle \alpha_1, \cdots, \alpha_k\rangle_{\mathbb{F}_p}$ 和 $W = \langle \alpha_{k+1}, \cdots, \alpha_m\rangle_{\mathbb{F}_p}$ 来生成的群 $S_{U,W}$.

在第 *4.7*节中, 我们将来证明从构造 *4.16-4.19*中产生的点正则群在一般意义下是不同构的, 具体方法是计算它们的群不变量, 如 *exponents* 和 *Thompson* 子群等. 对构造 *4.17-4.19*产生的群, 我们将在定理 *4.54*中证明这些群在 $l \geq 1$ 条件下对应的幂零类落在范围 $[2p^e, 3p^e]$ 中, 其中 $p^e = o(g)$. 在表 *4.1*中, 我们列出构造 *4.17*在 $\mu_C = 1$ 时和构造 *4.18* 在 $\alpha = 0$, $\mu_B = 1$ 时的群在某些特殊情况下幂零类的具体值. 特别地, 在这两种情况中我们均假设 $l > 1$. 从表中我们可以看出 G 的幂零类一般会随着 $\ker(S_1)$ 变小而逐渐变大. 表 *4.1*中数据的具体计算是比较复杂, 我们在这里将其省略, 但是它们遵循的方法跟第 *4.7*节中的方法是一样的.

4.4 $\mathcal{Q}^P$ 在 $\mathbf{PGL}(4, q)$ 中的线性点正则群的分类结果

令 G 是 *Payne* 派生四边形 $\mathcal{Q}^P$ 的一个点正则群, 其中 $\mathcal{Q} = W(q)$, $P = \langle(1, 0, 0, 0)\rangle$. 在这节中, 我们考虑群 G 是线性的情况, 即 G 是 $\mathrm{PGL}(4, q)$ 中的一个子群. 在文献*[2]* 中, *Bamberg* 和 *Gudicci* 通过 *Magma*[69] 列出 $q \leq 25$ 时 $\mathcal{Q}^P$ 的所有点正则群, 所以我们下面只需要考虑 $q \geq 5$ 的情况. 本节的主要结果是下面的定理, 值得注意的是奇特征情况下的线性的分类结果是分别由 *Chen*[70] 和 *De Winter ,Thas*[71] 独立地完成.

定理 4.22. 令 G 是 $\mathrm{PGL}(4, q)$ 中的一个子群, 并且它正则地作用在 $\mathcal{Q} = W(q)$ 的 Payne 派生四边形 $\mathcal{Q}^P$ 的点集上. 于是 G 跟下面构造 4.24和构造 4.26中产生的某个群相共轭.

表 4.1　点正则群 G 的幂零类：假设 $l>1$, 在构造 4.17中取 $\mu_C=1$；而在构造 4.18取 $\alpha=0$, $\mu_B=1$

构造	$S_1(z)$	幂零类	条件
4.17	0	$2p$	
	z^{p^k}	$3p$	$l\nmid k$
	z^{p^k}	$3p-1$	$l\mid k$
	$(1-g)^k(z)$	$3p-k$	$1\le k\le p-1$
4.18	0	$2p$	
	z	$3p-1$	
	$z^{p^k}+z^{p^{pl-k}}$	$3p$	$1\le k\le pl-1$
	$(1-g)^{2k}(z^{p^{pl-kl}})$	$3p-2k$	$2\le 2k\le p-1$

本节将致力于完成定理 *4.22*的证明. 根据第 *4.2.2*节中的分析, 我们在共轭等价意义下可以假设 G 是在定理 *4.12*中由函数 T 和 θ 定义的群. 采用与定理 *4.12*一样的符号, 并且记 $q=p^m$, 其中 p 是素数. 在这种情况下, G 是线性的等价于 $\theta_{a,b,c}\equiv 1$. 回忆我们定义了符号 $L(x)=T(x,0,0)$, $M(y)=T(0,y,0)$. 根据推论 *4.13*中的 $(1),(2),(4)$ 和 (5) 可知映射 L 和 M 均是可加的, 并且对所有 $a,b\in\mathbb{F}_q$ 有 $T(a,b,0)=L(a)+M(b)$. 此外, 由同一推论中的 (7) 可知对所有 $a,b,c\in\mathbb{F}_q$ 有

$$L\left(2bc+c^2L(a)+c^2M(b)\right)+M\left(cL(a)+cM(b)\right)=0. \tag{4.13}$$

通过在上述等式分别取 $b=0$ 和 $a=0$, 我们就能得到

$$L(c^2L(a))+M(cL(a))=0,\quad \forall a,\,c\in\mathbb{F}_q, \tag{4.14}$$

$$L(2bc+c^2M(b))+M(cM(b))=0,\quad \forall b,\,c\in\mathbb{F}_q. \tag{4.15}$$

引理 4.23. 使用以上定义的符号. 如果 q 是奇数, 那么 $L(x)\equiv 0$ 和 $M(y)\equiv 0$. 如果 q 是偶数, 那么存在 $\omega,\,\mu\in\mathbb{F}_q$ 使得

$$L(x)=\omega\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu^2\omega x),\quad M(y)=\omega\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu y). \tag{4.16}$$

证明.　记 $q=p^m$ 且 p 是素数. 令 $L(X):=\sum_{i=0}^{m-1}u_iX^{p^i}$, $M(X):=\sum_{i=0}^{m-1}v_iX^{p^i}$ 分别是加法映射 $x\mapsto L(x)$ 和 $y\mapsto M(y)$ 对应的简化的线性化多项式, 其中它们的多项式系数 u_i's 和 v_j's 的下标都是取模 m.

首先假设 q 是奇数. 因为 $2p^{m-1}\le q-1$, 所以我们从等式(4.14)中推断出

$$L(X^2L(a))+M(XL(a))=0.$$

通过比较 X^{2p^i} 该项在两边中的系数, 我们推出对 $0 \leq i \leq m-1$ 和 $a \in \mathbb{F}_q$ 有 $u_i L(a)^{p^i} = 0$. 如果对所有 $a \in \mathbb{F}_q$ 都有 $L(a) = 0$, 那么 $L(X) = 0$; 否则取 $a \in \mathbb{F}_q$ 使得 $L(a) \neq 0$, 于是我们推出对每个 i 都有 $u_i = 0$, 即 $L(X) = 0$: 矛盾. 因此我们总有 $L(X) = 0$. 于是等式(4.15)就简化为 $M(XM(b)) = 0$, 同理可得 $M(X) = 0$.

接着我们考虑 q 是偶数的情况. 如果 $L(X) = 0$, 那么我们从等式(4.15)中使用上一段中一样的方法推出 $M(X) = 0$, 此时我们可以取 $\omega = \mu = 0$, 所以我们下面不妨地假设 $L(X) \neq 0$. 取一个固定的 $a \in \mathbb{F}_q$ 使得 $L(a) \neq 0$. 通过将等式(4.14)转化为简化的线性化多项式的形式并比较它们的系数, 我们可知对每个 $0 \leq i \leq m-1$ 有 $u_i L(a)^{2^i} + v_{i+1} L(a)^{2^{i+1}} = 0$, 即 $u_i = v_{i+1} L(a)^{2^i}$. 于是 $\mathrm{Im}(L)$ 只有一个非零元, 记作 ω. 由引理 *4.6*可知存在 $\mu_A \in \mathbb{F}_q^*$ 使得 $L(x) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu_A x)$, 即 $L(x) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu_A x)$. 由此断定 $v_{i+1} = \omega^{1-2^i} \mu_A^{2^i}$ 以及 $M(X) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\omega^{-1/2} \mu_A^{1/2} X)$. 通过取 $\mu = \omega^{-1/2} \mu_A^{1/2}$ 我们即可得到具有规定形式的 L 和 M. □

我们接下来分别考虑引理 *4.23*中的两种情况. 首先考虑对所有 $a, b \in \mathbb{F}_q$ 都有 $L(a) = M(b) = 0$ 的情况. 在这种情况下, 易从推论 *4.13*的 (6) 中可知 $T(a, b, c) = S(c)$, 其中 $S(c) = T(0, 0, c)$. 由推论 *4.13*的 (3) 可知 S 是可加的. 于是定理 *4.12*的条件在这种情况下平凡地成立. 因此我们得到下面的构造, 其中这个构造在文献[70] 和文献[71] 以其它方式出现.

构造 4.24. 对于素数幂 q, 设 $\theta_{x,y,z} := 1$, 并对 $\mathbb{F}_q$ 上一个可加映射 S, 设 $T(x, y, z) := S(z)$. 于是对于指定函数 T 和 θ, 在定理 4.12中定义的集合 G 是 Payne 派生四边形 $\mathcal{Q}^P$ 的一个点正则群.

接着我们考虑引理 *4.23*的另一种情况, 即 $q = 2^m$ 是偶数并且存在某些非零元 ω, μ 使得等式(4.16)成立. 设

$$B(c, z) := S(c + z) + S(c) + S(z),$$

易知该函数关于 c, z 是对称的. 根据推论 *4.13*中 (6) 和 (3) 可知我们有 $S(c) + S(z) = T(czS(z), cS(z), c + z)$ 和 $T(u, v, w) = T(u + vw, v, 0) + S(w)$, 所以

$$\begin{aligned} B(c, z) =& S(c + z) + T(czS(z), cS(z), c + z) \\ =& T\left(czS(z) + cS(z)(c + z), cS(z), 0\right) \\ =& L(c^2 S(z)) + M(cS(z)) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\mu^2 c^2 (\omega S(z) + S(z)^2)\right). \end{aligned} \tag{4.17}$$

易知上式既关于 c 是可加的, 也关于 z 是可加的. 设 $F(z) := (\omega S(z) + S(z)^2)^{q/2}$, 于是就有 $B(c, z) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu c F(z))$. 由于对所有 $c \in \mathbb{F}_q$ 有 $B(c, z_1 + z_2) = B(c, z_1) +$

$B(c,z_2)$, 所以我们从中推断映射 $z \mapsto F(z)$ 是可加的. 注意到 $B(c,c) = S(2c) + 2S(c) = 0$. 令 $F(X) = \sum_{i=0}^{m-1} f_i X^{2^i}$ 是该映射 $z \mapsto F(z)$ 对应的简化的线性化多项式. 由引理 *4.8*可知我们有 $f_0 = 0$, 且

$$\mu f_i + (\mu f_{m-i})^{2^i} = 0,\ 1 \le i \le m-1. \tag{4.18}$$

我们现在定义一个辅助函数 $H(x) := \sum_{0\le i<j\le m-1} \mu^{2^i} f_{j-i}^{2^i} x^{2^i+2^j}$. 它的赋值均落在 $\mathbb{F}_2$, 这是因为

$$\begin{aligned} H(x) + H(x)^2 &= \sum_{0\le i<j\le m-1} \mu^{2^i} f_{j-i}^{2^i} x^{2^i+2^j} + \sum_{1\le i<j\le m} \mu^{2^i} f_{j-i}^{2^i} x^{2^i+2^j} \\ &= \sum_{1\le j\le m-1} \mu f_j x^{1+2^j} + \sum_{1\le i\le m-1} (\mu f_{m-i})^{2^i} x^{2^i+1} = 0, \end{aligned}$$

这里我们通过等式(4.18)去获得最后一个等式. 于是 $H(c+z) + H(c) + H(z)$ 等于

$$\begin{aligned} &\omega \cdot \sum_{i<j} \mu^{2^i} f_{j-i}^{2^i} \left((c+z)^{2^i+2^j} + c^{2^i+2^j} + z^{2^i+2^j} \right) \\ =&\omega \cdot \sum_{i<j} \mu^{2^i} f_{j-i}^{2^i} c^{2^i} z^{2^j} + \omega \cdot \sum_{i<j} \mu^{2^i} f_{j-i}^{2^i} z^{2^i} c^{2^j} \\ =&\omega \cdot \sum_{i<j} (\mu f_{j-i})^{2^i} c^{2^i} z^{2^j} + \omega \cdot \sum_{i<j} (\mu f_{i-j})^{2^j} c^{2^j} z^{2^i} \\ =&\omega \cdot \sum_{i,j} (\mu f_{j-i})^{2^i} c^{2^i} z^{2^j} = \omega \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu c F(z)). \end{aligned} \tag{4.19}$$

这里所有多项式系数的下标都取模 m. 我们在第二个等式中使用等式(4.18)导出的条件 $\mu f_{j-i} = (\mu f_{i-j})^{2^{j-i}}$, 并且在第三个等式中交换最后一个求和项的 i, j 和使用条件 $f_0 = 0$.

现在我们设 $S_1(z) := S(z) + \omega \cdot H(z)$. 于是通过等式(4.17), (4.19)从而推出 $S_1(c+z) + S_1(c) + S_1(z)$ 等于 $B(c,z) + \omega \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu c F(z)) = 0$. 因此 S_1 是可加的. 令 $S_1(X) := \sum_{i=0}^{m-1} s_i X^{2^i}$ 为对应简化的线性化多项式. 总而言之, 我们有 $S(x) = S_1(x) + \omega \cdot H(x)$, 即

$$S(x) = \sum_{i=0}^{m-1} s_i x^{2^i} + \omega \cdot \sum_{0\le i<j\le m-1} \mu^{2^i} f_{j-i}^{2^i} x^{2^i+2^j}. \tag{4.20}$$

观察到这个表达式只涉及 $S_1(X)$ 和 $F(X)$ 的多项式系数. 我们现在考虑关系 $F(x)^2 = \omega S(x) + S(x)^2$. 该式的左手边等于 $\sum_{i=0}^{m-1} f_{i-1}^2 x^{2^i}$, 而右手边等于 $\sum_{i=0}^{m-1} (\omega s_i + s_{i-1}^2) x^{2^i}$. 因为两边表示的多项式次数都不超过 $q-1$, 所以它们作为多项式而言是相等的. 通过比较两边的多项式系数, 我们得到 $\omega s_{i+1} + s_i^2 = f_i^2$, 其中 $0 \le i \le m-1$. 于是我们

归纳地推出

$$s_{i+1} = \sum_{j=1}^{i} \omega^{-2^j+1} f_{i+1-j}^{2^j} + w^{-2^{i+1}+1} s_0^{2^{i+1}}, \quad 0 \le i \le m-1. \tag{4.21}$$

这样我们就用系数 f_i's 和 s_0 取表示 s_i, $1 \le i \le m-1$, 并且 $s_m = s_0$ 得到一个限制条件.

$$\sum_{1 \le j \le m-1} \omega^{-2^j+1} f_{m-j}^{2^j} = 0. \tag{4.22}$$

引理 4.25. 对固定的非零元 ω, μ, 满足 $f_0 = 0$ 和等式(4.18), (4.22)中的所有条件的 $(m+1)$ 元组 $(f_0, \cdots, f_{m-1}, s_0)$ 的个数是 $2q^{(m-1)/2}$.

证明. 首先, 假设 m 是奇数. 根据等式(4.18)我们可以用 $f_1, \cdots, f_{(m-1)/2}$ 去表示 $f_{(m+1)/2}, \cdots, f_{m-1}$, 具体如下所示:

$$f_{m-i} = \mu^{2^{m-i}-1} f_i^{2^{m-i}}, \ (m+1)/2 \le i \le m-1.$$

将这些等式代入等式(4.22)中并在等式的两边除以 $\omega^2\mu$, 于是我们得到

$$\beta + \beta^2 = \sum_{i=2}^{(m-1)/2} (\mu^{-2^i} \omega^{-1-2^i} f_i + \mu^{-1} \omega^{-1-2^{m-i}} f_i^{2^{m-i}}),$$

其中 $\beta = \mu^{-1}\omega^{-1-2^{m-1}} f_1^{2^{m-1}}$. 易知该式的右手边的绝对迹函数取值为零. 因此, 由引理 *4.1*可知对任何选定的 $(f_2, \cdots, f_{(m-1)/2})$ 都存在两个可能的解 β's. 此时引理的结论成立.

接着考虑 m 是偶数的情况. 这个证明基本跟奇数的情况是一样的, 但唯一的不同之处是在证明等式的右手边的绝对迹函数为零时我们需要利用 $f_{m/2}\mu$ 属于子域 $\mathbb{F}_{2^{m/2}}$ 这个观察. 证毕. □

根据推论 *4.13*中的 (4) 和 (6), 我们有

$$T(a,b,c) = T(a+bc, b, 0) + S(c) = L(a+bc) + M(b) + S(c). \tag{4.23}$$

函数 L 和 M 是如等式(4.16)中定义的, 并且 ω 和 μ 是它们对应的参数. 而函数 S 是如等式(4.20)中定义的, 其中参数 s_i's 和 f_i's 满足等式(4.18), (4.21)和(4.22). 因此, 我们现在已经推出的条件是充分的. 于是我们得到下面的构造.

构造 4.26. 假定 $q = 2^m$ 且 $m > 1$. 再令 ω, μ 是 $\mathbb{F}_q$ 中的两个非零元. 取任意满足引理 4.25中的条件的 $m+1$ 元组 $(f_0, \cdots, f_{m-1}, s_0)$, 并且通过等式(4.21)去定义

$s_1, \cdots, s_{m-1}$. 设 $\theta_{a,b,c} \equiv 1$ 以及

$$T(a,b,c) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\mu^2\omega(a+bc)+\mu b\right) + \sum_{i=0}^{m-1} s_i c^{2^i} + \omega \sum_{0\le i<j\le m-1} \mu^{2^i} f_{j-i}^{2^i} c^{2^i+2^j}.$$

于是定理4.12中具有规定形式的函数 T 和 θ 的集合 G 是 Payne 派生四边形 $\mathcal{Q}^P$ 的点正则群.

证明. 令 L, M 是等式(4.16)中定义的函数, 再令 S 是等式(4.20)中定义的函数. 我们就能通过直接的计算去验证等式(4.23)成立. 设 $F(x) := \sum_{i=0}^{m-1} f_i x^{2^i}$, $B(c,z) := S(c+z)+S(c)+S(z)$. 因为对 $0 \le i \le m-1$ 有 $\omega s_{i+1}+s_i^2 = f_i$, 所以 $F(x)^2 = \omega S(x)+S(x)^2$. 再考虑等式(4.19)中的计算, 我们就得到 $B(c,z) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu c F(z))$.

根据定理 *4.12*可知我们现在只需要验证 $T(a,b,c)+T(x,y,z) = T(u,v,w)$, 其中 $w = c+z$, $v = b+y+cT(x,y,z)$ 和 $u = a+x+bz+cy+czT(x,y,z)$. 易知 $v+b+y = T(x,y,z)$ 以及

$$(u+vw)+(a+bc)+(x+yz) = c^2 T(x,y,z).$$

我们就可以从等式(4.20)中得到 $T(u,v,w)+T(a,b,c)+T(x,y,z)$ 等于 $L(c^2T(x,y,z))+M(cT(x,y,z))+B(c,z)$. 通过代入 L, M, T 和 B 的表达式, 我们即可推出上式可以简化为 $\omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu^2c^2(S(z)^2+\omega S(z)))+B(c,z)$. 又因为 $F(x)^2 = \omega S(x)+S(x)^2$ 和 $B(c,z) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu c F(z))$, 所以它是等于 0. 证毕. □

综上所述, 我们现在已经完成定理 *4.22*的证明.

注 4.27. 假设 q 是偶数, 并假定 G 是从构造4.24或构造4.26中获得的 $\mathcal{Q}^P$ 的点正则群. 如果 $T(a,b,c) \equiv 0$, 那么 G 是初等阿贝尔群, 因此我们假设 $T(a,b,c) \not\equiv 0$. 我们可以用常规的方法计算出 G 的 exponent 等于 4 以及它的幂零类等于 2, 特别的是, 无论 G 是来自构造4.24还是构造4.26, 它的中心都是 $Z(G) = \{\mathfrak{g}_{a,b,0} : a, b \in \mathbb{F}_q, T(a,b,0) = 0\}$. 当 G 来自于构造4.24时, $T(a,b,0) \equiv 0$, 也就是说, $Z(G)$ 的大小是 q^2; 而当 G 来自于构造4.26时, $T(a,b,0) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mu^2\omega a+\mu b)$, 则 $Z(G)$ 的大小是 $q^2/2$. 这就说明了两个构造在偶特征情况下会产生不同构的自同构群.

4.5 $\mathcal{Q}^P$ 中的非线性点正则群 G 的群结构

在本节中, 我们将假设 G 是 *Payne* 派生四边形 $\mathcal{Q}^P$ 中的一个非线性点正则群, 其中 T 和 θ 是在定理 *4.12*中它对应的两个函数, 也就是说, 存在 $a,b,c \in \mathbb{F}_q$ 使得 $\theta_{a,b,c} \neq 1$. 本节的主要目标是得到一些关于群 G 的群结构的性质和定理. 我们首先介

绍一些将在本节以及下一节用到的符号.

符号 4.5.1. 令 $\sigma_c, L, M, S, G_A, G_B, G_{A,B}$ 是在符号 4.2.1中定义的符号. 对 G 中的子群 G_A, 我们定义 $r_A := \log_p(\max\{o(\theta_{a,0,0}) : a \in \mathbb{F}_q\})$. 我们固定一个阶为 p^{r_A} 的域自同构 $g_A \in \mathrm{Aut}(\mathbb{F}_q)$, 再令 t_A 是 $\mathbb{F}_q$ 中的元素以致 $\theta_{t_A,0,0} = g_A$. 同样地用符号 r_B, g_B, t_B 和 $t_{B,i}$'s 来表示 G_B 中相应的概念, 以及用同一种方式去定义 g_C, t_C 和 $t_{C,i}$'s. 记得 $\sigma_c = \theta_{0,0,c}$, 设 $r_C := \log_p(\max\{o(\sigma_c) : c \in \mathbb{F}_q\})$. 定义

$$r_{A,B} := \max\{r_A, r_B\}, \quad s := \max\{0, r_C - r_{A,B}\}.$$

此外, 定义 $\mathcal{K}_0^* := \{z \in \mathbb{F}_q : \sigma_z^{p^{r_{A,B}}} = 0\}$.

因为 G 是非线性的, 所以根据推论中的 (4) 和 (6), 我们必须有 $r_{A,B} > 0$ 或 $r_C > 0$. 在接下来的讨论中, 我们将分别推出一些关于群 G 的 *Frobenius* 部分和矩阵部分的结构性定理.

4.5.1 点正则群 G 的 *Frobenius* 部分

由推论 *4.14*可知 G_A 和 G_B 都是 G 的子群. 定义群同态

$$\psi_A : G_A \mapsto \mathrm{Aut}(\mathbb{F}_q), \quad \mathfrak{g}_{a,0,0} \mapsto \theta_{a,0,0}.$$

于是 $\ker(\psi_A)$ 是 G_A 的正规子群. 再根据 r_A 的定义, 我们有 $|\mathrm{Im}(\psi_A) = p^{r_A}|$, 因此 $|G_A : \ker(\psi_A)| = p^{r_A}$. 当这些符号的下标 A 替换成 B 时, 同样的结果依旧成立. 我们在接下来的定理中探讨这些事实里面隐藏的信息.

定理 4.28. 采用在符号 4.5.1中定义的符号, 并且取一个 p 阶元 $g_2 \in \mathrm{Aut}(\mathbb{F}_q)$.

(1) 子集 $G_{A,K} := \{\theta_{a,0,0} : a \in K_A\}$ 是 G_A 中一个 index 为 p^{r_A} 的正规子群, 并且

$$G_A = \langle G_{A,K}, \mathfrak{g}_{t_A,0,0}\rangle = \cup_{i=0}^{p^{r_A}-1} G_{A,K} \circ \mathfrak{g}_{t_A,0,0}^i. \tag{4.24}$$

(2) 子集 K_A 是 $\mathbb{F}_q$ 中一个 g_A 不变和余维数为 r_a 的 $\mathbb{F}_p$-线性子空间, 对 $a \in K_A$ 有 $L(a)^{g_A} = L(g_A(a))$, 并且映射 $L : x \mapsto L(x)$ 在 K_A 上是可加的.

(3) 如果 q 是奇数 (或偶数), 那么 $r_{A,B} \leq 1 (r_{A,B} \leq 2)$.

(4) 如果 $r_A \leq 1$, 那么存在 $\mu_A \in \mathbb{F}_q$ 使得 $g_2(\mu_A) = \mu_A$ 和 $\theta_{a,0,0} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A a)}$.

当上述符号的下标 A 全部替成 B 并且映射 L 替换成 M 时, 上述的结论依旧成立.

证明. 因为对 G_A 和 G_B 的证明都是一样的, 所以我们在下面的讨论中只需要考虑关于 G_A 的部分. 先考虑 $r_A = 0$ 的情况, 我们有 $K_A = \mathbb{F}_q$, 并且由推论 ***4.13***中的 (1) 可知映射 L 是可加的. 于是所有结论在这种情况下都是平凡的, 而对于结论 (4) 我们只需要取 $\mu_A = 0$. 在接下来的讨论我们不妨地假设 $r_A \geq 1$. 为了便于表示, 我们记 $r = r_A$. 对每个 $i \geq 0$, 我们定义 $t_i = (1 + g_A + \cdots + g_A^{i-1})(t_A)$, $K_i := \{a \in \mathbb{F}_q : \theta_{a,0,0} = g_A^i\}$. 特别地, 这里我们有 $t_0 = 0$, $t_A \in K_1$ 和 $K_i = K_{i+p^r}$.

(1). 因为集合 $G_{A,K}$ 是前面定义的群同态 $\psi_A : G_A \to \mathrm{Aut}(\mathbb{F}_q)$, $\mathfrak{g}_{a,0,0} \mapsto \theta_{a,0,0}$ 的 ***kernel***, 所以 (1) 的第一部分成立. 再根据 t_A 在符号 ***4.5.1***中的选取, 我们就有 $\mathrm{Im}(\psi_A) = \langle\theta_{t_A,0,0}\rangle$, 于是 (1) 的余下部分的结论成立.

(2). 我们定义一个映射 $\theta^* : \mathbb{F}_q \to \mathrm{Aut}(\mathbb{F}_q)$, $a \mapsto \theta_{a,0,0}$. 根据推论 ***4.13***中的 (1), 我们有 $L(a)^{\theta^*(x)} + L(x) = L(a^{\theta^*(x)} + x)$, 以及

$$\theta^*(a)\theta^*(x) = \theta^*(a^{\theta^*(x)} + x) \text{ for } a,\ x \in \mathbb{F}_q. \tag{4.25}$$

如果 $a, x \in K_A$, 那么 n $\theta^*(a) = \theta^*(x) = 1$, 于是就有 $L(a) + L(x) = L(a + x)$, $\theta^*(a + x) = 1$. 由此断定 $a + x \in K_A$. 我们从而得出 K_A 是加法封闭的, 即它是 $\mathbb{F}_q$ 中一个 $\mathbb{F}_p$ 线性子空间, 并且 L 在 K_A 上是线性的.

我们接下来探究 $G_{A,K}$ 是 G_A 的正规子群. 当 $a \in K_0$ 时, 我们考虑群元素 $\mathfrak{g}_{t_1,0,0}^{-1} \circ \mathfrak{g}_{a,0,0} \circ \mathfrak{g}_{t_1,0,0} = (\mathcal{M}_{-t_1,0,0} \cdot \mathcal{M}_{a,0,0}^{g_1} \cdot \mathcal{M}_{t_1,0,0}, 1)$. 因为它的矩阵部分的最后一行是 $(g_1(a), 0, 0, 1)$, 所以它等于 $\mathfrak{g}_{g_1(a),0,0}$. 通过比较它们的矩阵部分的第 $(3, 2)$ 项, 我们有 $L(a)^{g_1} = L(g_1(a))$. 于是它的 ***Frobenius*** 部分是平凡的, 故 $g_1(a) \in K_0$. 这就完成 (2) 的证明.

(3). 我们研究在等式(4.24)中 G_A 的陪集划分. 对 $a \in K_A$ 以及 $i \geq 1$, 定义符号 $\mathfrak{g}_i := \mathfrak{g}_{a,0,0} \circ \mathfrak{g}_{t_A,0,0}^i$. 我们接着通过归纳法计算 $\mathfrak{g}_i$ 的矩阵部分的最后一行为 $(g_1^i(a) + t_i, 0, 0, 1)$, 所以 $\mathfrak{g}_i$ 等于 $\mathfrak{g}_{g_1^i(a)+t_i,0,0}$.

- (a) 由于 $\mathfrak{g}_i$ 的 ***Frobenius*** 部分是 g_1^i, 因此 $K_0 + t_i \subseteq K_i$, 其中 $i \geq 1$; 特别地, 当 $i = p^r$ 时我们由 $g_1^{p^r} = 1$ 可知 $K_0 + t_{p^r} = K_0$. 于是就有 $t_{p^r} \in K_0$.

- (b) 取 $x \in K_1$, $a \in K_i$, 我们从等式(4.25)中可推出对每个 i 都有 $t_1 + g_1(K_i) \subseteq K_{i+1}$, 遂 $|K_i| = |g_1(K_i)| \leq |K_{i+1}|$. 由此断定所有集合 K_i's 都有同样的大小. 作为一个推论, 从 (a) 中可知 $K_0 + t_i = K_i$. 于是就有 $G_A = \cup_{i=0}^{p^r-1} G_{A,K} \circ \mathfrak{g}_{t_A,0,0}^i$, 也就是说, G_A 是由 $G_{A,K}$ 和 $\mathfrak{g}_{t_A,0,0}$ 生成的.

根据 (1) 可知 K_A 是 $\mathbb{F}_q$ 中一个余维数为 r_A 的 $\mathbb{F}_p[\langle g_A\rangle]$ 子模. 因为 $K_i = K_A + t_i$ 并且

它们形成 $\mathbb{F}_q$ 的分割, 所以对 (K_A, t_A) 且令 $e = h = r_A$, 引理 *4.11*中所有条件都是满足的. 于是就有 $r_A \geq p^{r_A-1}$, 换言之, 当在 p 是奇数时 $r_A \leq 1$, 而在 $p = 2$ 时 $r_A \leq 2$.

(4). 记得我们在定理的证明开始前已经假设 $r \geq 1$, 根据 (3) 可知我们只需要考虑 $r = 1$ 的情况. 在这种情况下, 对某个 d, $1 \leq d \leq p-1$ 有 $g_A = g_2^d$.

我们首先利用 K_A 的 g_A 不变性推出 $g_A(t_A) \equiv t_A \pmod{K_A}$, 以及对 $0 \leq i \leq p-1$ 有 $t_i \equiv it_A \pmod{K_A}$. 因为 $\mathbb{F}_p$-线性子空间 K_A 在 $\mathbb{F}_q$ 中的余维数为 1 以及 $t_A \notin K_A$, 所以我们有下面的分割 $\mathbb{F}_q = \cup_{\lambda\in\mathbb{F}_p} K_A + \lambda t_A$. 又因为 $K_A + g_A(t_A)$ 是 K_A 的陪集, 所以存在 $\lambda \in \mathbb{F}_p^*$ 使得 $K_A + g_A(t_A) = K_A + \lambda t_A$. 注意到 K_A 是 g_A 不变的, 于是我们通过归纳法得到 $K_A + g_A^i(t_A) = K_A + \lambda^i t_A$. 因此在商空间 $\mathbb{F}_q/K_A$ 中, 我们发现 $i \geq 0$ 时 $g_A^i(\overline{t_A}) = \lambda^i \overline{t_A}$. 我们从 (a) 的 $t_p = \sum_{i=0}^{p-1} g_A^i(t_A) \in K_A$ 中推出 $\sum_{i=0}^{p-1} \lambda^i \cdot \overline{t_A} = 0$, 这就得到所需的结果 $\lambda = 1$.

因为 K_0 是 $\mathbb{F}_q$ 中一个 g_1 不变和余维数为 1 的 $\mathbb{F}_p$-线性子空间以及 $t_A \notin \mathbb{F}_q$, 所以存在 $\mu_A \in \mathbb{F}_q^*$ 使得对 $x \in K_A$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A x) = 0$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A t_A) = 1$. 那么对 $i \geq 0$ 有 $K_i = K_A + it_A = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A x) = i\}$. 根据陪集 K_i 的定义, 我们因此推出对每个 $a \in \mathbb{F}_q$ 有 $\theta_{a,0,0} = g_A^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A a)} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(d\mu_A a)}$. 因为 K_A 是 g_A 不变的, 所以我们从引理 *4.4*中可知 $g_A(\mu_A) = \mu_A$. 这就证明 (4). □

推论 4.29. *采用如上面所示的符号, 并且假设 q 是奇数. 令 g_2 是 $\mathrm{Aut}(\mathbb{F}_q)$ 中的 p 阶元. 那么在 $\mathbb{F}_q$ 中存在 g_2 不变的 μ_A 和 μ_B 使得 $\theta_{a,b,0} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A a + \mu_B b)}$.*

证明. 因为 q 是奇数, 所以我们从定理 *4.28*中可知 $r_A \leq 1$, $r_B \leq 1$, 并且根据同一定理既可推出存在 g_2 不变的 μ_A, $\mu_B \in \mathbb{F}_q$ 使得 $\theta_{a,0,0} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A a)}$, $\theta_{0,b,0} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B b)}$. 这里我们在 $r_A = 0$ 时取 $\mu_A = 0$, 而在 $r_B = 0$ 时取 $\mu_B = 0$. 于是根据推论 *4.13*中的 (4) 可知, 我们有 $\theta_{a,b,0} = \theta_{\theta_{0,b,0}^{-1}(a),0,0} \cdot \theta_{0,b,0} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A a + \mu_B b)}$. 我们在第二个等式中使用 $\theta_{0,b,0} \in \langle g_2 \rangle$ 这个事实, 这就意味着 g_2 保持 μ_A 不变. □

我们需要用到下面的引理, 其中一部分结果早已经在定理 *4.28*中给出.

引理 4.30. *采用如上面所示的符号. 对 $i \geq 0$, 设 $t_{A,i} := (1 + g_A + \cdots + g_A^{i-1})(t_A)$. 于是我们有 $t_{A,p^{r_A}} \in K_A$. 而且对 $x \in K_A$ 有*

$$L(g_A^i(x) + t_{A,i}) = g_A^i(L(x)) + \sum_{j=0}^{i-1} g_A^j(L(t_A)), \quad i \geq 1. \tag{4.26}$$

如果我们将上述符号中下标 A 替换成 B 以及 L 替换成 M, 那么结论依旧成立.

证明. 我们已经在定理 *4.28*的证明中说明了 $t_{A,p^{r_A}} \in K_A$, 而且当 $i \geq 1$ 时有 $\mathfrak{g}_{x,0,0} \circ \mathfrak{g}^i_{t_A,0,0} = \mathfrak{g}_{g_A^i(x)+t_{A,i},0,0}$. 通过比较这个方程的两边的矩阵部分的第 $(3,2)$ 项, 我们就有等式(4.26). □

定理 4.31. 采用如上面所示的符号, 并且设 $\mathcal{K}_i^* := \{z \in \mathbb{F}_q : \sigma_z^{p^{r_{A,B}}} = g_C^{ip^{r_{A,B}}}\}$.

(1) 如果 q 是偶数, 那么 $r_C \leq r_{A,B} + 2$.

(2) 如果 q 是奇数, 那么 $r_C \leq r_{A,B} + 1$, 且 $\mathcal{K}_0^*$ 是一个 g_C 不变且余维数为 $s = \max\{0, r_C - r_{A,B}\}$ 的 $\mathbb{F}_p$-线性子空间, 还有 $\mathcal{K}_i^* = (1 + g_C + \cdots + g_C^{i-1})t_C + \mathcal{K}_0^*$, 其中 $i \geq 1$.

证明. 在 $r_C \leq r_{A,B}$ 情况下, 对每个 $i \geq 0$ 有 $\mathcal{K}_i^* = \mathbb{F}_q$, 此时结论都是平凡地成立. 因此, 我们在下面的讨论中假设 $r_C \geq r_{A,B} + 1$, 即 $s = \max\{0, r_C - r_{A,B}\} \geq 1$.

设 $H_0^* := \{x \in \mathbb{F}_q : x + \mathcal{K}_0^* \subseteq \mathcal{K}_0^*\}$, 这显然是一个 $\mathbb{F}_p$-线性子空间. 因为 $0 \in \mathcal{K}_0^*$, 所以我们有 $H_0^* \subseteq \mathcal{K}_0^*$. 为了便于表示, 我们在下面的证明中记

$$r := r_{A,B} = \max\{r_A, r_B\},\ g := g_C,\ g_0 := g_C^{p^r},\ g_1 := g_C^{p^s}.$$

并且对 $i \geq 0$, 定义 $\mathcal{K}_i := \{z \in \mathbb{F}_q : \sigma_z = g_C^i\}$, $t_i := (1 + g_C + \cdots + g_C^{i-1})(t_C)$. 特别地, 我们有 $t_0 = 0$, 以及 $t_{i+j} = t_i + g^i(t_j)$. 我们从 t_C 的选取中得知得 $t_1 = t_C \in \mathcal{K}_1$.

我们首先证明对非负整数 i, j, k 有 $\mathcal{K}_i^* = t_i + g^i(\mathcal{K}_0^*)$, $t_{p^s i} \in \mathcal{K}_0^*$ 以及 $\mathcal{K}_i^* = t_i + g^i(\mathcal{K}_0^*)$, $t_{p^s i} \in \mathcal{K}_0^*$. 结合推论 *4.13*中的 (3) 和 (6), 我们有 $\sigma_c\sigma_z = \theta_{-c^{\sigma_z}zS(z),c^{\sigma_z}S(z),c'} = \theta_{a,b,0}\sigma_{c'}$, 其中 $c' = c^{\sigma_z} + z$, $a = \sigma_{c'}^{-1}(c^{2\sigma_z}S(z))$ 和 $b = \sigma_{c'}^{-1}(c^{\sigma_z}S(z))$. 将等式的两边提到 p^r 次方, 我们就能推出

$$g^{i+p^s k}(c) + z \in \mathcal{K}_{i+j}^*,\ c \in \mathcal{K}_j^*,\ z \in \mathcal{K}_{i+p^s k}. \tag{4.27}$$

因此我们从等式(4.27) 中推出 $\mathcal{K}_{i+p^s k} + g^{i+p^s k}(\mathcal{K}_j^*) \subseteq \mathcal{K}_{i+j}^*$; 特别地, $|\mathcal{K}_j^*| \leq |\mathcal{K}_{i+j}^*|$. 注意到这是对所有非负整数 i, j, k 都成立. 显然可知 $\mathcal{K}_i^* = \mathcal{K}_{i+p^s}^*$ 以及这些陪集 $\mathcal{K}_i^*$ 组成 $\mathbb{F}_q$ 的分割, 这意味着所有陪集 $\mathcal{K}_i^*$'s 有同样的大小 q/p^s. 通过在等式(4.27)中取 $i = 1$, $k = 0$, $z = t_C$, 我们获知当 $c \in \mathcal{K}_j^*$ 时 $g(c) + t_C \in \mathcal{K}_{j+1}^*$. 再通过比较大小, 我们就有 $g(\mathcal{K}_j^*) + t_C = \mathcal{K}_{j+1}^*$. 这时我们用归纳法就可以推出对 $i \geq 0$ 有 $\mathcal{K}_i^* = t_i + g^i(\mathcal{K}_0^*)$. 在 $i = p^s k$ 这种情况下, 我们从 $0 \in \mathcal{K}_0^*$ 和 $\mathcal{K}_{p^s k}^* = \mathcal{K}_0^*$ 中推出对每个整数 k 有 $t_{p^s k} \in \mathcal{K}_0^*$. 这就证明我们声称的结论.

我们接着去证明对非负整数 j, k 有 $\mathcal{K}_{p^s k} - t_{p^s k} \subseteq g^j(H_0^*)$. 根据 $\mathcal{K}_{p^s k} + g^{p^s k}(\mathcal{K}_j^*) =$

$\mathcal{K}_j^*$ 和 $\mathcal{K}_j^* = g^j(\mathcal{K}_0^*) + t_j$ 这些事实, 我们就有

$$\mathcal{K}_{p^sk} + g^j(g^{p^sk}(\mathcal{K}_0^*)) + g^{p^sk}(t_j) = g^j(\mathcal{K}_0^*) + t_j.$$

进一步使用 $g^{p^sk}(\mathcal{K}_0^*) = \mathcal{K}_0^* - t_{p^sk}$ 和 $-g^j(t_{p^sk}) + g^{p^sk}(t_j) - t_j = -t_{p^sk}$, 即

$$-\sum_{l=j}^{p^sk+j-1} g^l(t_1) + \sum_{l=p^sk}^{p^sk+j-1} g^l(t_1) - \sum_{l=0}^{j-1} g^l(t_1) = -\sum_{l=0}^{p^sk-1} g^l(t_1),$$

于是我们就有 $\mathcal{K}_{p^sk} - t_{p^sk} + g^j(\mathcal{K}_0^*) = g^j(\mathcal{K}_0^*)$. 我们所需的结论就直接从 H_0^* 的定义中推出.

我们现在定义集合 $W := \cap_{i=0}^{p^{r+s}-1} g^i(H_0^*)$. 因为 H_0^* 是 $\mathbb{F}_q$ 中的一个 $\mathbb{F}_p$-线性子空间, 所以 W 是 $\mathbb{F}_q$ 中的一个 g 不变的 $\mathbb{F}_p$-线性子空间. 根据之前的说法, 对每个 $k \geq 0$ 有 $\mathcal{K}_{p^sk} \subseteq W + t_{p^sk}$. 从 $\mathcal{K}_0 \subseteq W$, $\mathcal{K}_{p^{r+s}} \subseteq W + t_{p^{r+s}}$ 和 $0 \in \mathcal{K}_0 = \mathcal{K}_{p^{r+s}}$ 中我们推出 $t_{p^{r+s}} \in W$. 因为 $W \subseteq H_0^* \subseteq \mathcal{K}_0^*$ 和 $t_{p^sk} \in \mathcal{K}_0^*$, 所以我们有

$$\mathcal{K}_0^* = \cup_{i=0}^{p^r-1} \mathcal{K}_{p^si} \subseteq \cup_{i=0}^{p^r-1} (W + t_{p^si}) \subseteq \mathcal{K}_0^*. \tag{4.28}$$

值得注意的是, 上式中的每个等式都成立.

令 d 是最小的正整数以致 $t_{p^sd} \in W$. 我们刚才已经证明了 $t_{p^{r+s}} \in W$, 故 $d \leq p^r$. 从 $g(W) = W$, $t_{p^sd} \in W$ 以及 $t_{p^sd(i+1)} = t_{p^sdi} + g^{p^sdi}(t_{p^sd})$ 中我们用归纳法推出 $t_{p^sdi} \in W$. 很容易验证这 d 个陪集 $W + t_{p^si}$, $0 \leq i \leq d-1$ 都是两两不交的. 根据等式(4.28)我们得到 $\mathcal{K}_0^*$ 的分割：

$$\mathcal{K}_0^* = \cup_{i=0}^{d-1} (W + t_{p^si}). \tag{4.29}$$

我们将分割(4.29)代入 $\mathcal{K}_i^* = g^i(\mathcal{K}_0^*) + t_i$, 并利用 $t_{i+p^sj} = t_i + g^i(t_{p^sj})$ 去简化得到 $\mathcal{K}_i^* = \cup_{j=0}^{d-1}(W + t_{i+p^sj})$, $0 \leq i \leq p^s - 1$. 因此, 从 $\mathbb{F}_q = \cup_{i=0}^{p^s-1} \mathcal{K}_i^*$ 中我们得到一个分割 $\mathbb{F}_q = \cup_{i=0}^{p^s-1} \cup_{j=0}^{d-1} (W + t_{i+p^sj})$, 这也意味着 $\mathbb{F}_q$ 可以被分割成 p^sd 个不同的 W 的陪集. 于是存在某个非负整数 d_0 使得 $d = p^{d_0}$. 我们从 $d \leq p^r$ 中推出 $0 \leq d_0 \leq r$. 在引理 *4.11*中取 $h = d_0 + s$ 和 $e = r_C = r + s$, 因为在引理 *4.11*中取 $h = d_0 + s$ 和 $e = r_C = r + s$ 时 (W, t_C) 满足引理 *4.11*中所有的条件, 所以我们有 $p^{d_0+s-1} \leq d_0 + s$, 因此在 q 是奇数时 $d_0 + s \leq 1$, 而在 q 是偶数时 $d_0 + s \leq 2$. 特别地, 在 q 是奇数时, 根据假设 $s \geq 1$, 我们必然有 $d_0 = 0$, $s = 1$, 此时从等式(4.29)中推出 $\mathcal{K}_0^* = W$. 证毕. □

推论 4.32. 采用如上面所示的符号, 并且假设 q 是奇数. 集合

$$G_{\mathcal{K}_0^*} := \{\mathfrak{g}_{a,b,c} : a, b \in \mathbb{F}_q, c \in \mathcal{K}_0^*\} \tag{4.30}$$

是 G 中 index 为 p^s 的正规子群, 并且 $G = \cup_{i=0}^{p^s-1} G_{\mathcal{K}_0^*} \circ \mathfrak{g}_{0,0,t_C}^i$, 其中 $s = \max\{0, r_C - r_{A,B}\}$.

证明. 如果 $s = 0$, 那么 $\mathcal{K}_0^* = \mathbb{F}_q$, 此时结论就平凡地成立. 故我们在接下来的证明中假设 $s > 0$. 特别地, $r_C = s + r_{A,B}$. 为了便于表示, 记 $g = g_C$, $r = r_{A,B}$. 定义群同态 $\psi_r : G \to \mathrm{Aut}(\mathbb{F}_q), \quad \mathfrak{g}_{a,b,c} \mapsto \theta_{a,b,c}^{p^r}$.

我们先证明 $G_{\mathcal{K}_0^*}$ 是群同态 ψ_r 的 *kernel* 的子集. 根据推论 *4.13*中的 (4) 和 (5), 我们推出 $\langle \theta_{a,b,0} : a, b \in \mathbb{F}_q \rangle$ 是 p^r 阶群. 根据推论 *4.13*中的 (6) 可知 $\theta_{a,b,c} = \theta_{\sigma_c^{-1}(a+bc),\sigma_c^{-1}(b),0}\sigma_c$, 注意到当 $c \in \mathcal{K}_0^*$ 时它的 p^r 次方等于 1. 命题成立.

根据定理 *4.31*, 我们推出子群 $G_{\mathcal{K}_0^*}$ 的大小是 $q^2 \cdot |\mathcal{K}_0^*| = q^3/p^s$, 这也就意味着 $|\ker(\psi_r)| \geq q^3/p^s$. 另一方面, 因为 $\theta_{0,0,t_C}^{p^r} = g^{p^r}$ 的阶是 p^s, 所以 $|\mathrm{Im}(\psi_r)| \geq p^s$. 又因为 $|G| = |\ker(\psi_r)| \cdot |\mathrm{Im}(\psi_r)|$, 所以我们就有 $G_{\mathcal{K}_0^*} = \ker(\psi_r)$. 此时我们很容易发现 $\psi_r(\mathfrak{g}_{0,0,t_C})$ 可以由 $\mathrm{Im}(\psi_r)$ 生成, 于是引理中所有的结论成立. □

4.5.2 奇特征情况下的点正则群 G 的矩阵部分

在这一子节中, 我们继续使用在符号 *4.5.1*中引入的符号, 并假设 q 是奇数. 根据定理 *4.28*和定理 *4.31*, 我们有 $r_{A,B} = \max\{r_A, r_B\} \leq 1$ 和 $s = \max\{0, r_C - r_{A,B}\} \leq 1$.

令 g_2 是 $\mathrm{Aut}(\mathbb{F}_q)$ 中的 p 阶元, 再定义

$$K_A := \{a \in \mathbb{F}_q, \theta_{a,0,0} = 1\}, \quad K_B := \{b \in \mathbb{F}_q, \theta_{0,b,0} = 1\}. \tag{4.31}$$

我们现在收集一些已知的事实, 为了方便后面的引用.

(F1) 由推论 *4.29*可知对 $a, b \in \mathbb{F}_q$ 有 $\theta_{a,b,0} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A a + \mu_B b)}$, 其中 μ_A 和 μ_B 都是在 $\mathbb{F}_q$ 中 g_2 不变的. 特别地, $K_A = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A x) = 0\}$, 并且 $r_A = 0$ 当且仅当 $\mu_A = 0$; 如果这些符号的下标 A 被代替成 B, 同样的结果也成立.

(F2) 根据推论 *4.13*中的 (1), (2), (4) 和 (5) 可知在 $a \in K_A$ 或 $b \in K_B$ 时有 $T(a, b, 0) = L(a) + M(b)$, 并且 L 和 M 分别在 K_A 和 K_B 上是可加的.

(F3) 由推论 *4.13*中的 (7), 我们有

$$\sigma_c\, \theta_{a,b,0} = \theta_{a',b',0}\, \sigma_{c'}; \tag{4.32}$$

$$S(c)^{\theta_{a,b,0}} + T(a, b, 0) = T(a', b', 0)^{\sigma_{c'}} + S(c'); \tag{4.33}$$

其中 $c' = \theta_{a,b,0}(c)$, $b' = \sigma_{c'}^{-1}\left(b + c^{\theta_{a,b,0}} T(a, b, 0)\right)$ 和

$$a' = \sigma_{c'}^{-1}\left(a + 2bc^{\theta_{a,b,0}} + c^{2\theta_{a,b,0}} T(a, b, 0)\right).$$

本子节的主要结果是下面的定理.

定理 4.33. 假定 q 是奇数. 采用在符号 4.5.1中定义的符号, 令 μ_A, μ_B 是在推论 4.29中定义的元素, 再令 K_A, K_B 是在等式(4.31)中定义的集合. 那么 $\mu_A = 0, r_A = 0, L \equiv 0$, $g_C(\mu_B) = \mu_B$, 并且对 $b \in K_B$ 有 $M(b) = 0$. 特别地, 当 $r_B = 1$ 时, 我们有 $(1 + g_B + \cdots + g_B^{p-1})(M(t_B)) = 0$, 以及

$$M(y) = (1 + g_B + \cdots + g_B^{i-1})(M(t_B)),$$

其中 $\theta_{0,y,0} = g_B^i$, $1 \le i \le p-1$.

证明. 我们通过观察而发现在 $c \in \mathcal{K}_0^*$ 时 $\sigma_c \in \langle g_2 \rangle$, 这是因为 $r = r_{A,B} \le 1$. 由定理 *4.31*的 *(2)* 可知 $\mathcal{K}_0^*$ 是 $\mathbb{F}_q$ 中一个 g 不变和余维数为 $s \le 1$ 的 $\mathbb{F}_p$-线性子空间. 由引理 *4.4*可知存在一个 g 不变的 $\mu_C \in \mathbb{F}_q$ 使得 $\mathcal{K}_0^* = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C x) = 0\}$. 又因为当 $c \in \mathcal{K}_0^*$ 时 $\sigma_c \in \langle g_2 \rangle$, 所以 g 也保持 μ_A 和 μ_B 不变. 我们现在把证明分成 *5* 个步骤, 这涉及在某些特殊情况下 *(F3)* 中的两个方程的重复使用. 为了便于表示, 我们在证明中记 $g = g_C$, $r = r_{A,B}$.

Step 1 : 我们将在这步骤中证明 $\mu_A = 0$, 于是有 $K_A = \mathbb{F}_q$. 在 *(F3)* 中, 取 $a = 0, b \in K_B$ 以及 $c \in \mathcal{K}_0^*$, 我们有 $c' = c^{\theta_{0,b,0}} = c$, 而且通过比较幂指数可知等式(4.32)简化为

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\mu_A(2bc + c^2 M(b)) + cM(b))\right) = 0. \tag{4.34}$$

对在 $c = c_1, c_2 \in \mathcal{K}_0^*$ 时的等式(4.34)作差, 我们得到

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left((2\mu_A b + \mu_B M(b)) \cdot v\right) = -2\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\mu_A M(b) uv\right), \tag{4.35}$$

其中 $u = \frac{1}{2}(c_1 + c_2)$, $v = c_1 - c_2$. 我们观察到 (u, v) 遍历 $\mathcal{K}_0^* \times \mathcal{K}_0^*$, 这是因为 c_1, c_2 的取值范围是 $\mathcal{K}_0^*$. 再同样地对在 $u = u_1, u_2 \in \mathcal{K}_0^*$ 时的等式(4.35)的两边作差, 我们推出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_A M(b) vv') = 0$, 其中 v 和 $v' = u_1 - u_2$ 都属于 $\mathcal{K}_0^*$. 因为引理 *4.9* 证明了 $\{vv' : v, v' \in \mathcal{K}_0^*\}$ 在 $\mathbb{F}_p$ 上张成 $\mathbb{F}_q$, 所以我们从而推出 $b \in K_B$ 时 $\mu_A M(b) = 0$. 注意到此时等式(4.35)的左手边等于 0, 这就意味着 $\dim_{\mathbb{F}_p}\langle 2\mu_A b + \mu_B M(b) : b \in K_B\rangle_{\mathbb{F}_p} \le s \le 1$. 因为 K_B 的大小至少是 q/p 并且 $q \ge p^p$, 所以这只有在 $\mu_A = 0$ 时才有可能发生. 这就证明 *Step* 1 的结论.

Step 2 : 我们在这步骤中要证明如果 $\mu_B \ne 0$, 那么 $g(\mu_B) = \mu_B$, $M(b) = 0$, 其中 $b \in K_B$. 假设 $\mu_B \ne 0$. 在 *(F3)* 中, 取 $b \in K_B$ 和 $c \in \mathbb{F}_q$, 然后通过比较幂指数, 等式(4.32)就有更简单的形式:

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\mu_B^{\sigma_c}(b + cM(b))\right) = 0, \quad b \in K_B, c \in \mathbb{F}_q. \tag{4.36}$$

如果 $\mathcal{K}_0^* = \mathbb{F}_q$, 那么 $\mu_B^{\sigma_c} = \mu_B$, 而且等式(4.36)可简化为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c M(b)) = 0$, 其中 $c \in \mathbb{F}_q$, 这就有 $b \in K_B$ 时 $M(b) = 0$. 所以我们接下来假设 $\mathcal{K}_0^* \neq \mathbb{F}_q^*$. 在这种情况下, $r = 1$, $s = 1$, 并且我们有 $\langle g_2 \rangle = \langle g^{p^s} \rangle$. 根据定理 *4.31*可知对 $i \geq 0$ 有 $\mathcal{K}_i^* = t_{C,i} + \mathcal{K}_0^*$, 其中 $\mathcal{K}_i^* := \{z \in \mathbb{F}_q : \sigma_z^{p^r} = g_C^{ip^r}\}$. 如果 $c \in \mathcal{K}_i^*$, 那么我们由 $g_2(\mu_B) = \mu_B$ 可知 $\mu_B^{\sigma_c} = g^i(\mu_B)$. 通过将在 $c = c_1, c_2 \in \mathcal{K}_i^*$ 时等式(4.36)的两个等式作差, 我们即可推出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(g^i(\mu_B)M(b)u) = 0$, 其中 $u = c_1 - c_2 \in \mathcal{K}_0^*$ 和 $b \in K_B$. 根据引理 *4.3*, 我们有 $g^i(\mu_B)M(b) \in \mathbb{F}_p \cdot \mu_C$. 注意到这等式对任意 $b \in K_B$ 和 $i \geq 0$ 都成立. 有了以上的准备, 我们现在可以证明本步骤的结论.

(1) 我们首先证明 $b \in K_B$ 时 $M(b) = 0$. 假设存在 $b_0 \in K_B$ 使得 $M(b_0) \neq 0$. 那么我们从 $\mathbb{F}_p \cdot g(\mu_B)M(b_0) = \mathbb{F}_p \cdot \mu_B M(b_0) = \mathbb{F}_p \cdot \mu_C$ 中推出对某个 $\lambda \in \mathbb{F}_p^*$ 有 $g(\mu_B) = \lambda \mu_B$. 取到被 g 固定的子域的相对范数, 我们即可推出 $\lambda = 1$, 也就是说, $g(\mu_B) = \mu_B$. 此时等式(4.36)可简化为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B M(b)c) = 0$, 其中 $c \in \mathbb{F}_q$, 接着我们从中推出 $b \in K_B$ 时 $M(b) = 0$：矛盾. 因此 $b \in K_B$ 时 $M(b) = 0$.

(2) 然后我们证明 $g(\mu_B) = \mu_B$. 等式(4.36)现在简化为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B^{\sigma_c} b) = 0$, 其中 $b \in K_B$. 于是对 $c \in \mathbb{F}_q$ 有 $\sigma_c(\mu_B) \in \mathbb{F}_p \cdot \mu_B$, 故 $g(\mu_B) \in \mathbb{F}_p \cdot \mu_B$. 我们需要用跟 (1) 一样的方法可推出我们想要的结果.

Step 3: 我们将在这步骤中证明对 $a \in \mathbb{F}_q$ 有 $L(a) = 0$. 我们考虑两种情况.

(1) 如果 $\mu_B \neq 0$, 在等式(4.32)中取 $a \in K_A = \mathbb{F}_q$, $b \in K_B$ 和 $c \in \mathbb{F}_q$, 再通过比较幂指数, 那么我们就有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c L(a)) = 0$. 此时该步骤的结论成立.

(2) 如果 $\mu_B = 0$, 那么 $\theta_{a,b,0} \equiv 1$, 并且 $r = r_{A,B} = 0$. 在这种情况下, $s = 1$, 也就是说, $\mathcal{K}_0^*$ 的余维数为 1 并且 L 和 M 在 $\mathbb{F}_q$ 上都是可加的. 在等式 (4.33)中取 $b = 0$, $c \in \mathcal{K}_0^*$, 我们就能推出 $L(c^2 L(a)) = -M(cL(a))$. 在取 $c = c_1, c_2 \in \mathcal{K}_0^*$ 并对其对应的两个等式作差, 我们推出 $L(uvL(a)) = -M(vL(a))$, 其中 $u, v \in \mathcal{K}_0^*$. 观察到右手边与 u 无关, 因此等式两边都等于 $L(0 \cdot vL(a)) = 0$. 于是 $L \equiv 0$, 这是因为根据引理 *4.9*可知 $\{uv : u, v \in \mathcal{K}_0^*\}$ 张成 $\mathbb{F}_q$.

Step 4: 我们将在这步骤中证明如果 $\mu_B = 0$, 那么对 $b \in \mathbb{F}_q$ 有 $M(b) = 0$. 假设 $\mu_B = 0$ 并且 M 恒为零. 在这种情况下, 我们从 G 是非线性的中可知此时必须有 $s = 1$, 也就是说, $o(g) = p$. 而且我们有 $\theta_{a,b,0} \equiv 1$, 并且由事实 *(F1)* 和 *(F2)* 可知 M 在 $K_B = \mathbb{F}_q$ 上是可加的. 再在等式(4.33)中取 $b \in \mathbb{F}_q$ 和 $c \in \mathbb{F}_q$, 我们就有

$$M(\sigma_c^{-1}(b))^{\sigma_c} - M(b) + M(\sigma_c^{-1}(cM(b)))^{\sigma_c} = 0. \tag{4.37}$$

取 $c = c_1, c_2 \in \mathcal{K}_i^*$ 并对相应的两个等式作差, 我们推出 $M(g^{-i}(vM(b))) = 0$ 和其中 $v \in \mathcal{K}_0^*, i \geq 0$. 这就意味着 $i \geq 0$ 时 $\mathcal{K}_0^* \cdot g^i(M(b)) \subseteq \ker(M)$. 通过比较两边集合的大小, 我们可以看出只要 $M(b) \neq 0$ 就有 $\mathcal{K}_0^* \cdot g^i(M(b)) \subseteq \ker(M)$. 因此 $\mathrm{Im}(M)$ 的维数是 1, 也就是说, $\mathrm{Im}(M) = \mathbb{F}_p \cdot \omega$, 其中 $\omega \neq 0$. 那么 $\ker(M)$ 等于 $\mathcal{K}_0^* \cdot \omega$, 而且它是 g 不变的. 记得由定理 *4.31*可知 $\mathcal{K}_0^*$ 也是 g 不变的. 根据引理 *4.4*, 我们就推出 $g(\omega) = \omega$.

我们现在已经证明了 M 在 $\mathbb{F}_q$ 上是 $\mathbb{F}_p$-线性的, $\ker(M) = \mathcal{K}_0^* \cdot \omega$ 以及 $\mathrm{Im}(M) = \mathbb{F}_p \cdot \omega$. 通过应用引理 *4.6*到 $K = \mathbb{F}_q$ 上, 我们就有存在 $\eta \in \mathbb{F}_q^*$ 使得 $M(x) = \omega \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta x)$. 将这等式代入等式(4.37)中并化简, 我们推出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\Delta b) = 0$, 其中 $\Delta = \sigma_c(\eta) - \eta + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\sigma_c(\eta)c\omega)\eta$. 因为 b 是任意的, 所以我们对 $c \in \mathbb{F}_q$ 有 $\Delta = 0$. 这就意味着 $\sigma_c(\eta)\eta^{-1} = 1 - \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\sigma_c(\eta)c\omega) \in \mathbb{F}_p$. 我们通过取绝对范数就推出 $\sigma_c(\eta)\eta^{-1} = 1$. 现在 $\Delta = 0$ 简化为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta c\omega) = 0$, 其中 $c \in \mathbb{F}_q$, 故 $\omega\eta = 0$：矛盾. 这就证明该步骤的结论.

Step 5: 假定 $r_B = 1$. 我们现在需要证明 $(1 + g_B + \cdots + g_B^{p-1})(M(t_B)) = 0$, 以及当 $\theta_{0,y,0} = g_B^i$, $1 \leq i \leq p-1$ 时 $M(y) = (1 + g_B + \cdots + g_B^{i-1})(M(t_B))$. 在这种情况下, $\mu_B \neq 0$. 根据引理 *4.30*可知 $(1 + g_B + \cdots + g_B^{p-1})(t_B) \in K_B$. 因为 *Step* 2 说明了 M 在 K_B 上赋值为零, 所以我们从等式(4.26) 的 (B, M) 形式和 $x = 0$ 中推出 $(1 + g_B + \cdots + g_B^{p-1})(M(t_B)) = 0$. 令 y 为 $\mathbb{F}_q$ 中的某个元素以致 $\theta_{0,y,0} = g_B^i$. 于是 $y \in K_i$, 其中 $K_i = \{b \in \mathbb{F}_q : \theta_{0,b,0} = g_B^i\}$. 在定理 *4.28*的证明中, 我们已经证明了 $K_i = K_B + (1 + g_B + \cdots + g_B^{i-1})(t_B)$. 因此存在 $x \in K_B$ 使得 $y = g_B^i(x) + (1 + g_B + \cdots + g_B^{i-1})(t_B)$. 于是结果是从等式(4.26)的 (B, M) 版本中得到的.

综上所述, 我们已经完成了定理的证明. □

4.6 奇特征下的非线性点正则群

这一节致力于证明 q 是奇数时的非线性点正则群的分类结果.

定理 4.34. 令 G 是正则地作用在 $\mathcal{Q} = W(q)$ 的派生四边形 $\mathcal{Q}^P$ 的点集上的群, 其中 q 是奇数并且 $q \geq 5$. 如果 G 不是 $\mathrm{PGL}(4, q)$ 的子群, 那么 G 是与构造 4.37, 4.42和 4.46中产生的某一个群共轭.

在本节中, 我们假设 G 是定理 *4.12*中定义的 *Payne* 派生四边形 $\mathcal{Q}^P$ 的一个非线性点正则群, 其中 T 和 θ 是 G 中对应的函数. 使用在符号 *4.5.1*中定义的符号, 故存在整数 l 使得 $q = p^{r^{+s}l}$. 取 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x) = x^{p^l}$, 并且设 $g(x) = x^{p^l}$. 令 g_2 是 $\mathrm{Aut}(\mathbb{F}_q)$ 中的 p 阶元, 特别注意的是在 $r_{A,B} = 1$ 时我们取它为 g_1. 根据定理 *4.33*, 我

们有 $r_A = 0$, 也就是说, $r_{A,B} = r_B$. 如果 $r_{A,B} = 1$, 那么 $g_B = g_1$ 和 t_B 是选定的元素使得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B t_B) = 1$, 如符号 *4.5.1*中定义的一样. 根据定理 *4.31*和引理 *4.4*可知存在 $\mu_C \in \mathbb{F}_q$ 使得

$$\mathcal{K}_0^* = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C x) = 0\},$$

并且 $g_C(\mu_C) = \mu_C$, 其中 $\mathcal{K}_0^* = \{c \in \mathbb{F}_q : \sigma_c^{p^r} = 1\}$.

我们现在根据 $r_{A,B} = 0$ 和 $r_{A,B} = 1$ 把定理 *4.34*的证明分成两种情况在前一种情况下, 我们必须有 $r_C = 1$, 这是因为 G 是非线性的. 而在后者, 我们由定理 *4.31*的 (2) 可知 $r_C = 1$ 或 2.

我们现在通过定理 *4.33*的结果将第 *4.5.2*小节中 *(F1)-(F3)* 重新表述一下.

(F4) $\theta_{a,b,0} = g_2^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B b)}$, 其中 $g_C(\mu_B) = \mu_B$. 作为一个推论, 对 $a, b \in \mathbb{F}_q$ 有 $\theta_{a,g_C(b),0} = \theta_{0,b,0}$, 并且 $\theta_{0,b,0}$ 关于 b 是可加的. 特别地, 当 $r_{A,B} = 1$ 时 $g_2 = g_1$.

(F5) 对 a, $b \in \mathbb{F}_q$ 有 $T(a, b, 0) = M(b)$, 并且 M 在 $K_B = \{b : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B b) = 0\}$ 上取值为零. 当 $r_{A,B} = 0$ 时, 我们有 $M \equiv 0$; 而当 $r_{A,B} = 1$ 时, 令 $\nu_B := M(t_B)$, 我们有 $(1 + g + \cdots + g^{p-1})(\nu_B) = 0$ 以及 $M(b) = N_C(\theta_{0,b,0})$, 其中

$$N_C(g_1^i) := \begin{cases} 0, & \text{if } i = 0, \\ (1 + g_1 + \cdots + g_1^{i-1})(\nu_B), & \text{if } 1 \le i \le p-1|. \end{cases} \tag{4.38}$$

于是我们从 $\theta_{0,g_C(b),0} = \theta_{0,b,0}$ 中推出 $M(g_C(b)) = M(b)$. 易证

$$g_1^j(N_C(g_1^i)) + N_C(g_1^j) = N_C(g_1^{i+j}), \quad 0 \le i, j \le p-1. \tag{4.39}$$

(F6) 当 b, $c \in \mathbb{F}_q$ 时, 设 $c' = \theta_{0,b,0}(c)$, 我们有

$$\sigma_c = \sigma_{c'}\theta_{0,c'M(b),0}, \tag{4.40}$$

$$(S(c) - N_C(\sigma_c))^{\theta_{0,b,0}} = S(c') - N_C(\sigma_{c'}). \tag{4.41}$$

我们这里简述一下证明过程. 从等式(4.32)中得到 $\sigma_c\theta_{0,b,0} = \sigma_{c'}\theta_{0,b+c'M(b),0}$, 然后等式(4.40) 就从 *(F4)* 中得到. 根据 *(F5)* 可知等式(4.33) 可以取下面的形式 $S(c)^{\theta_{0,b,0}} + N_C(\theta_{0,b,0}) = N_C(\theta_{0,b',0})^{\sigma_{c'}} + S(c')$. 因此等式(4.41)等价于 $N_C(\theta_{0,b,0}) + N_C(\sigma_c)^{\theta_{0,b,0}} = N_C(\theta_{0,b+c'M(b),0})^{\sigma'_c} + N_C(\sigma'_c)$, 这是根据等式(4.39)以及 $\sigma_c\theta_{0,b,0} = \sigma_{c'}\theta_{0,b+c'M(b),0}$ 得到的结果. 证毕.

引理 4.35. 采用上述定义的符号. 对 $\mathbb{F}_q$ 中的 a, b, c, x, y, z 以及 $v = \sigma_z(c)S(z)$, $w = \sigma_z(c) + z$, 下面等式成立:

$$\theta_{a,b,c} = \theta_{0,b,0}\sigma_c, \tag{4.42}$$

$$T(a,b,c) = M(b)^{\sigma_c} + S(c), \tag{4.43}$$

$$\sigma_c\sigma_z = \theta_{0,v,0}\sigma_w, \tag{4.44}$$

$$S(c)^{\sigma_z} + S(z) = M(v)^{\sigma_w} + S(w). \tag{4.45}$$

证明. 前面两个等式是利用 *(F4)* 和 *(F5)* 对推论 *4.13*的内容进行重新表述. 后面的两个等式是从推论 *4.13*的 (3) 中推出. □

4.6.1 $r_{A,B} = 0, r_C = 1$ 的情况下的分类结果

在这子节中, 我们考虑 $r_{A,B} = 0$, $r_C = 1$ 的情况. 在这种情况下, $s = 1$, $q = p^{pl}$ 以及 $o(g) = p$. 根据符号 *4.5.1*中的一些符号的定义, 我们可以取 g_C 使得 $g_C = g$. 因为 $g_C(\mu_C) = \mu_C$, 所以我们有 $\mu_C \in \mathbb{F}_{p^l}^*$. 于是我们从 *(F5)* 中推出 $T(a,b,0) \equiv 0$, 由等式(4.45)可知 S 在 $\mathcal{K}_0^*$ 上是可加的, 并且由等式(4.43)可知 $T(a,b,c) = S(c)$. 特别地, 我们有

$$\mathfrak{g}_{0,0,t_C} = (\mathcal{M}_{0,0,t_C}, g), \quad \mathcal{M}_{0,0,t_C} = E(0,0,t_C,S(t_C)).$$

引理 4.36. 我们有 $\mathbb{F}_{p^l} \subseteq \mathcal{K}_0^*$.

证明. 因为 $q = p^{pl}$, 所以我们对 $z \in \mathbb{F}_{p^l}$ 有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(z) = \mathrm{Tr}_{\mathbb{F}_{p^l}/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(z)) = 0$. 于是结论直接从 $\mu_C \in \mathbb{F}_{p^l}^*$ 中得到. □

根据推论 *4.32*, $G_{\mathcal{K}_0^*}$ 是 G 个 *index* 为 p 的正规子群. 现在我们通过探究这个事实从而推出一些参数的限制条件. 记 $\nu_C := S(t_C)$.

(1) 我们有 $\mathfrak{g}_{0,0,t_C}^{-1} \circ \mathfrak{g}_{a,b,c} \circ \mathfrak{g}_{0,0,t_C} \in G_{\mathcal{K}_0^*}$, 其中 a, $b \in \mathbb{F}_q$, $c \in \mathcal{K}_0^*$. 根据群乘法(4.9), 它就等于 $(\mathcal{M}', 1)$, 其中 $\mathcal{M}' = \mathcal{M}_{0,0,t_C}^{-1} \cdot \mathcal{M}_{a,b,c}^g \cdot \mathcal{M}_{0,0,t_C}$. 于是我们利用注 *4.15*的计算可知 $\mathcal{M}'$ 的第 $(4,3)$ 项和第 $(3,2)$ 项分别是 c^g 和 $S(c)^g$. 于是就从 $T(a,b,c) = S(c)$ 中得到 $S(c^g) = S(c)^g$, 其中 $c \in \mathcal{K}_0^*$. 根据引理 *4.7*可知存在一个简化的线性化多项式 $S_1(X) \in \mathbb{F}_{p^l}[X]$ 使得对 $c \in \mathcal{K}_0^*$ 有 $S(c) = S_1(c)$.

(2) 我们有 $\mathfrak{g}_{0,0,t_C}^p \in G_{\mathcal{K}_0^*}$. 相似地, 我们可以验证它的矩阵部分的第 $(4,3)$ 项和第 $(3,2)$ 项分别是 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu_C)$ 和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(t_C)$. 于是就从 $T(a,b,c) = S(c)$ 中得到 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu_C) = S(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(t_C))$. 我们由引理 *4.36*可得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(t_C) \in \mathcal{K}_0^*$, 所以

$S(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(t_C)) = S_1(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(t_C))$. 又因为 S_1 是可加的并且它的多项式系数都属于 $\mathbb{F}_{p^l}$, 所以它等于

$$\sum_{i=0}^{p-1} S_1(t_C^{p^{il}}) = \sum_{i=0}^{p-1} S_1(t_C)^{p^{il}} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(S_1(t_C)).$$

因此, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu_C - S_1(t_C)) = 0$.

结果是我们目前推出的条件也是充分的. 这就得到下面的构造.

构造 4.37. 假定 $q = p^{pl}$, 其中 p 是奇素数以及 l 是正整数, 再令 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x) = x^{p^l}$. 取 $\mu_C \in \mathbb{F}_{p^l}^*$, 并定义 $K := \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C x) = 0\}$. 取一个元素 $t_C \in \mathbb{F}_q \setminus K$ 以及一个线性化多项式 $S_1(X) \in \mathbb{F}_{p^l}[X]$. 令 ν_C 是 $\mathbb{F}_q$ 中的元素以致 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu_C - S_1(t_C)) = 0$.

对 $a, b \in \mathbb{F}_q, c \in K$ 有 $\mathcal{M}_{a,b,c} = E(a, b, c, S_1(c))$, 并且设 $\mathcal{M}_{0,0,t_C} := E(0, 0, t_C, \nu_C)$, 其中 E 是等式(4.8)中定义的矩阵. 那么 $G_K := \{\mathfrak{g}_{a,b,c} : a, b \in \mathbb{F}_q, c \in K\}$ 是一个 q^3/p 阶群, 其中 $\mathfrak{g}_{a,b,c} = (\mathcal{M}_{a,b,c}, 1)$. 令 G 是由 G_K 和 $\mathfrak{g}_{0,0,t_C} := (\mathcal{M}_{0,0,t_C}, g)$ 生成的群. 于是 G 是 Payne 派生四边形 $\mathcal{Q}^P$ 的点正则群.

证明. 验证过程都是常规的, 所以我们这里只给出一个简略的描述. 首先, 我们利用注 *4.15*去验证 G_K 在群乘法(4.9)下是封闭的, 这样 G_K 就形成一个 q^3/p 阶群. 那么我们就证明 $\mathfrak{g}_{0,0,t_C}^p \in G_K$ 和 $\mathfrak{g}_{0,0,t_C}^{-1} \circ \mathfrak{g}_{a,b,c} \circ \mathfrak{g}_{0,0,t_C} \in G_K$, 其中 $a, b \in \mathbb{F}_q, c \in K$, 因此 G 是 q^3 阶群, 并且 G_K 是其 *index* 为 p 的正规子群. 最后通过将群元素 $G = \cup_{i=0}^{p-1} G_K \circ \mathfrak{g}_{0,0,t_C}^i$ 作用到点 $\langle(0, 0, 0, 1)\rangle$ 上, 我们就能推出 G 在在 $\mathcal{Q}^P$ 的点上的作用是正则的. □

综上所述, 我们已经证明若 G 是 $\mathcal{Q}^P$ 的点正则群并且满足限制条件 $r_{A,B} = 0$ 和 $r_C = 1$, 那么它与构造 *4.37*中得到的群相共轭.

4.6.2 $r_{A,B} = 1$ 的情况下的分类结果

在这子节中, 我们将考虑 $r_{A,B} = 1$ 的情况. 这个证明将被分成两部分 *(Part* 1 和 *Part* 2*)*. 在 *Part* 1 中, 我们先通过探究 $G_{\mathcal{K}_0^*}$ 的群结构从而推出关于 σ_c 和 $S(c)$ 的一般性结果, 并且作为副产物, 我们完成 $r_C \leq 1$ 的情况的证明. 在 *Part* 2 中, 我们探究 $G_{\mathcal{K}_0^*}$ 是 G 中一个 *index* 为 p^s 的正规子群的事实, 这样我们就能完成 $r_C = 2$ 的情况的证明.

Part 1 : $G_{\mathcal{K}_0^*}$ 的群结构

引理 4.38. $\mathbb{F}_p$-线性子空间 $\mathcal{K}_0^*$ 是 g_1 不变的.

证明. 如果 $r_C \le r_{A,B}$, 那么 $\mathcal{K}_0^* = \mathbb{F}_q$, 此时结论平凡地成立. 如果 $r_C > r_{A,B}$, 那么我们根据假设 $r_{A,B} = 1$ 就有 $r_C = 2$, $s = 1$, 这里我们使用定理 *4.31*的 (2). 于是群元素 g_1 的阶为 p, 那么 g_C 的阶是 p^2. 根据定理 *4.31*可知 $\mathcal{K}_0^*$ 具有 g_C 不变性, 于是此时结论成立. □

引理 4.39. 令函数 $N_C : \langle g_1\rangle \to \mathbb{F}_q$ 是等式(4.38)中定义的. 我们定义 $B : \mathcal{K}_0^* \times \mathcal{K}_0^* \to \mathbb{F}_p$, 如下所示:

$$B(c,z) := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\mu_B c(N_C(\sigma_z) - S(z))\right), \tag{4.46}$$

并且设 $Q(x) := B(x,x)$. 那么 B 是 $\mathcal{K}_0^*$ 上对称的双线性型, 并且 $c \in \mathcal{K}_0^*$ 时有 $Q(g_1(c)) = Q(c)$. 此外, 存在 $\alpha \in \mathbb{F}_q$ 使得 $\alpha - g_1(\alpha) + \mu_B M(t_B) \in \mathbb{F}_p \cdot \mu_C$ 和

$$\sigma_z = g_1^{\frac{1}{2}Q(z)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha z)} \text{ for } z \in \mathcal{K}_0^*. \tag{4.47}$$

证明. 通过将等式(4.40)中的 c 替换成 $\theta_{0,b,0}^{-1}(c)$, 我们推出

$$\sigma_{\theta_{0,b,0}^{-1}(c)} = \sigma_c g_1^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c M(b))}, \quad b, c \in \mathbb{F}_q. \tag{4.48}$$

我们现在利用上式导出下面的等式:

$$\sigma_{c+z}(\sigma_c\sigma_z)^{-1} = g_1^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c(N_C(\sigma_z)-S(z)))}, \quad c \in \mathbb{F}_q,\ z \in \mathcal{K}_0^*. \tag{4.49}$$

固定一个元素 $z \in \mathcal{K}_0^*$, 并且取 $b \in \mathbb{F}_q$ 使得 $\theta_{0,b,0} = \sigma_z$. 通过将等式(4.44)中的 c 替换成 $\sigma_z^{-1}(c)$, 我们得到

$$\sigma_{\sigma_z^{-1}(c)} = \sigma_{c+z}\sigma_z^{-1} g_1^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c S(z))}. \tag{4.50}$$

因为 $\theta_{0,b,0} = \sigma_z$, 所以等式(4.48)和 (4.50)的右手边是相等的. 那么等式(4.49)现在就能从 $M(b) = N_C(\theta_{0,b,0}) = N_C(\sigma_z)$ 这事实中推出, 具体可参考 *(F5)*.

当 $c \in \mathcal{K}_0^*$ 时, 等式(4.49) 的左手边是关于 c, z 对称的, 于是右手边等于 $g_1^{B(z,c)}$. 显然从 $B(c,z)$ 的表达式可知 B 关于 c 是 $\mathbb{F}_p$ 线性的, 所以 B 是 $\mathcal{K}_0^*$ 上对称的双线性型. 于是就对 $c, z \in \mathcal{K}_0^*$ 有 $B(c,z) = \frac{1}{2}(Q(c+z) - Q(c) - Q(z))$, 其中 $Q(x) = B(x,x)$. 我们因此可以将等式(4.49) 改写下面的等式:

$$\sigma_{c+z} g_1^{-\frac{1}{2}Q(c+z)} = \left(\sigma_c g_1^{-\frac{1}{2}Q(c)}\right) \cdot \left(\sigma_z g_1^{-\frac{1}{2}Q(z)}\right), \quad c, z \in \mathcal{K}_0^*.$$

也就是说, $z \mapsto \sigma_z g_1^{-\frac{1}{2}Q(z)}$ 是从 $\mathcal{K}_0^*$ 到 $\langle g_1\rangle$ 的群同态. 因此存在一个元素 $\alpha \in \mathbb{F}_q$ 使得对 $z \in \mathcal{K}_0^*$ 有 $\sigma_z = g_1^{\frac{1}{2}Q(z)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha z)}$.

当 $c \in \mathcal{K}_0^*$ 和 $b \in \mathbb{F}_q$ 时, 我们由引理 *4.38*可知 $\theta_{0,b,0}^{-1}(c) \in \mathcal{K}_0^*$. 我们将 σ_c 和 $\sigma_{\theta_{0,b,0}^{-1}(c)}$ 的表达式代入等式(4.48) 并比较他们的幂指数从而得到

$$\frac{1}{2}Q(c^{\theta_{0,b,0}^{-1}}) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha^{\theta_{0,b,0}} c) = \frac{1}{2}Q(c) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha c) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c M(b)).$$

通过将 c 替换成 λc ($\lambda \in \mathbb{F}_p$) 以及比较 λ 和 λ^2 的系数, 我们可推出 $Q(c^{\theta_{0,b,0}^{-1}}) = Q(c)$ 以及 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left((\alpha^{\theta_{0,b,0}} - \alpha - \mu_B M(b)) \cdot c\right) = 0$. 取 $b = t_B$, 于是我们推出该引理的余下的结论. □

引理 4.40. *存在一个 $\mathbb{F}_q$ 上简化的线性化多项式 $S_1(X)$ 以及一个映射 $H : \mathcal{K}_0^* \to \mathbb{F}_p$ 使得*

$$S(z) = S_1(z) + N_C(\sigma_z) + \mu_B^{-1}\mu_C H(z), \quad z \in \mathcal{K}_0^*. \tag{4.51}$$

证明. 如果 $\mu_C \neq 0$, 则取 $e \in \mathbb{F}_q \setminus \mathcal{K}_0^*$, 并定义 $\tilde{B}(x + \lambda e, y + \lambda' e) := B(x, y)$, 其中 $x, y \in \mathcal{K}_0^*$ 和 $\lambda_1, \lambda_2 \in \mathbb{F}_p$. 然后从 B 在 $\mathcal{K}_0^*$ 上是双线性的这事实中可得 $\tilde{B}$ 是 $\mathbb{F}_q$ 上的一个双线性型. 因此无论 $\mu_C = 0$ 与否, 根据引理 *4.5*可知存在上一个在 $\mathbb{F}_q$ 简化的线性化多项式 $S_1(X)$ 使得对 $x, y \in \mathcal{K}_0^*$ 有 $B(x, y) = -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B x S_1(y))$. 联合等式(4.46), 我们就推出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B x(N_C(\sigma_y) - S(y) + S_1(y))) = 0$, 其中 $x, y \in \mathcal{K}_0^*$. 于是由引理 *4.3*可知对 $y \in \mathcal{K}_0^*$ 有 $N_C(\sigma_y) - S(y) + S_1(y) \in \mathbb{F}_p \cdot \mu_B^{-1}\mu_C$. 证毕. □

令 H 是在引理 *4.40*中引入的函数, 并且设

$$S_2(c) := S_1(c) + \mu_B^{-1}\mu_C H(c), \quad c \in \mathcal{K}_0^*. \tag{4.52}$$

根据等式(4.51)我们就有

$$S_2(c) = S(c) - N_C(\sigma_c), \quad c \in \mathcal{K}_0^*. \tag{4.53}$$

由等式(4.41)我们有

$$S_2(c^{g_1^i}) = S_2(c)^{g_1^i}, \quad \text{其中} c \in \mathcal{K}_0^*, i \geq 0. \tag{4.54}$$

我们从等式(4.46)中可知对 $c, z \in \mathcal{K}_0^*$ 有 $B(c, z) = -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c S_2(z))$, 故

$$Q(c) = -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c S_2(c)), \quad c \in \mathcal{K}_0^*. \tag{4.55}$$

当 $a, b \in \mathbb{F}_q$ 和 $c \in \mathcal{K}_0^*$ 时, 我们将 *(F4)* 和等式(4.47)中的 $\theta_{0,b,0}$ 和 σ_c 的表达式代入等式(4.42)和 (4.43)从而得到

$$\begin{aligned} \theta_{a,b,c} &= g_1^{\frac{1}{2}Q(c) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha c + \mu_B b)}, \\ T(a, b, c) &= S_2(c) + N_C(\theta_{a,b,c}), \end{aligned} \tag{4.56}$$

其中 N_C 是等式(4.38)中定义的函数. 这里我们在推导 $T(a, b, c)$ 的表达式过程中使用等式(4.42)和(4.39).

引理 4.41. 等式(4.52)中定义的映射 $x \mapsto S_2(x)$ 在 $\mathcal{K}_0^*$ 上是可加的.

证明. 由符号 *4.5.1*中 $\mathcal{K}_0^*$ 的定义, 我们有 $\sigma_z \in \langle g_1 \rangle$, 其中 $z \in \mathcal{K}_0^*$. 我们需要证明对 $c, z \in \mathcal{K}_0^*$ 有 $S_2(c)^{\sigma_z} + S_2(z) = S_2(c^{\sigma_z} + z)$, 于是引理的结论将跟随等式(4.54) 和引理 *4.38*而成立. 取固定的 $c, z \in \mathcal{K}_0^*$, 并且设 $v = \sigma_z(c)S(z)$, $w = \sigma_z(c) + z$. 由等式(4.44)可知我们有 $\sigma_c\sigma_z = \theta_{0,v,0}\sigma_w$. 因为 $M(v) = N_C(\theta_{0,v,0})$, 所以很容易地从等式(4.39)中看出 $N_C(\sigma_c)^{\sigma_z} + N_C(\sigma_z) = M(v)^{\sigma_w} + N_C(\sigma_w)$. 接着我们将 $S(z) = S_2(z) + N_C(\sigma_z)$ 代入等式(4.45), 这就得到所需的等式. 证毕. □

我们现在准备完成 $r_C \leq r_{A,B} = 1$ 的情况下的分类. 在这种情况下, 我们有 $s = 0$, $g = g_1$, $\mathcal{K}_0^* = \mathbb{F}_q$, $\mu_C = 0$ 以及 $S_2 = S_1$. 记 $S_2(X) = \sum_{i=0}^{pl-1} s_i X^{p^i}$. 然后从等式(4.54)中我们推出对每个 i 都有 $g_1(s_i) = s_i$, 即 $s_i \in \mathbb{F}_{p^l}$. 由取 $\mu = \mu_B$ 和 $\eta = 0$ 的引理 *4.8*可得函数 B 是 $\mathbb{F}_q$ 上对称的双线性型当且仅当对 $0 \leq i \leq pl-1$ 有 $\mu_B s_i - s_{m-i}^{p^i}\mu_B^{p^i} = 0$. T 和 θ 的表达式都是在等式(4.56)中定义的, 其中涉及的参数有 μ_B, α, S_2 和 $\nu_B := M(t_B)$. 特别地, 由引理 *4.38*可知 $\mu_B\nu_B := g_1(\alpha) - \alpha$, 遂 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu_B) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\mu_B^{-1}(g_1)(\alpha) - \alpha) = 0$. 事实证明, 我们目前推导出的对参数的限制也是充分的, 故我们得到下面的构造.

构造 4.42. 假定 $q = p^{pl}$, 其中 p 是奇素数以及 l 是正整数, 再令 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x) = x^{p^l}$.

(i) 取 $\mu_B \in \mathbb{F}_{p^l}^*$.

(ii) 取一个 pl 元组 $(s_0, s_1, \cdots, s_{pl-1})$, 并且其中每个数属于 $\mathbb{F}_{p^l}$ 使得对 $1 \leq i \leq pl-1$ 有 $\mu_B s_i - s_{pl-i}^{p^i}\mu_B^{p^i} = 0$.

(iii) 取 $\alpha \in \mathbb{F}_q$ 并设 $\nu_B := \mu_B^{-1}(g_1(\alpha) - \alpha)$.

设 $S_2(x) := \sum_{i=0}^{pl-1} s_i x^{p^i}$ 和 $Q(x) := -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B x S_2(x))$, 其中 $x \in \mathbb{F}_q$. 令 N_C 为等式(4.38)中用以上取定的 ν_B 所定义的函数. 令 θ 和 T 是等式(4.56)中定义的函数. 那么用规定形式的函数 T 和 θ 如定理 4.12所定义的集合 G 是 Payne 派生四边形 $\mathcal{Q}^P$ 的点正则群.

证明. 满足 *(ii)* 中条件的 pl 元组的数目等于 $p^{(pl+1)l/2}$, 这是通过与引理 *4.25*的证明类似的论证得到的.

我们简略地叙述一下如何去验证定理 *4.12*中的两个条件. 首先, 我们通过直接的检查去验证 $S_2(g_1(x)) = S_2(x)^{g_1}$, $Q(g_1(x)) = Q(x)$, 其中 $x \in \mathbb{F}_q$. 于是等式(4.10)经过

展开和简化后可得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((\alpha-\alpha^{\theta_2}+\mu_B N_C(\theta_2))c^{\theta_2})=0$, 其中 $c\in\mathbb{F}_q$ 和 $\theta_2=\theta_{x,y,z}$. 它进一步简化为 $g_1^i(\alpha)-\alpha=\mu_B N_C(g_1^i)$ *for* $1\le i\le p-1$, 这可以用归纳法从 $g_1(\alpha)-\alpha=\mu_B\nu_B$ 中得到. 接着从 $S_2(g_1(x))=S_2(x)^{g_1}$ 和等式(4.39)中, 我们能推出等式(4.11). 证毕. □

综上所述, 我们已经证明在 $r_C\le r_{A,B}=1$ 的情况下群 G 必然与来自构造 *4.42*的某个群相共轭.

Part 2: $G_{\mathcal{K}_0^*}$ 的正规性

从现在开始, 我们假设 $r_{A,B}=1$ 和 $r_C=2$, 即 $r=s=1$. 在这种情况下, g 的阶是 p^2, 而 $g_1=g^p$ 的阶是 p, 其中 $g(x)=x^{p^l}$. 在符号 *4.5.1*中, 我们指定 $g_B=g_1$, $g_C=g$, 遂由 *(F4)* 可得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B t_B)=1$, 且 $\sigma_{t_C}=g$. 记得我们对 $c\in\mathcal{K}_0^*$ 有 $S_2(c)=S(c)-N_C(\sigma_c)$, *cf.* 等式(4.53). 在后续的讨论中, 我们进一步引入一些符号:

$$\nu_B:=M(t_B),\quad \lambda_C:=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C t_C),\quad \nu_C:=S(t_C).$$

特别地, 我们有 $\mathfrak{g}_{0,0,t_C}=(\mathcal{M}_{0,0,t_C},g)$, 其中 $\mathcal{M}_{0,0,t_C}=E(0,0,t_C,\nu_C)$, 并且 E 是等式(4.8)中定义的矩阵. 因为 $t_C\notin\mathcal{K}_0^*$, 所以我们有 $\mu_C\neq 0$, $\lambda_C\neq 0$.

我们的策略是探究 $G_{\mathcal{K}_0^*}$ 是 G 中 *index* 为 p 的正规子群的条件, 参考推论 *4.32*. 这就被分成两个步骤 (1) : 我们检查 $G_{\mathcal{K}_0^*}$ 的正规性, 即 $\mathfrak{g}_{a,b,c}\in G_{\mathcal{K}_0^*}$ 时有 $\mathfrak{g}_{0,0,t_C}^{-1}\circ\mathfrak{g}_{a,b,c}\circ\mathfrak{g}_{0,0,t_C}\in G_{\mathcal{K}_0^*}$; (2) : 我们检查条件 $[G:G_{\mathcal{K}_0^*}]=p$, 即 $\mathfrak{g}_{0,0,t_C}^{p}\in G_{\mathcal{K}_0^*}$. 实际上 $\mathfrak{g}_{x,y,z}$ 的下标的第一个坐标是不相关的, 通过到注 *4.15*的计算结果发现此时的计算就能得到极大程度的简化.

我们从 $G_{\mathcal{K}_0^*}$ 的正规性开始. 具体而言, 我们考虑下面的特殊情况:$a,b\in\mathbb{F}_q$, $c\in\mathcal{K}_0^*$ 满足条件 $\theta_{a,b,c}=1$, 即

$$-\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B b)=\frac{1}{2}Q(c)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha c). \tag{4.57}$$

对于任意给定的 $c\in\mathcal{K}_0^*$, 我们由假设 $\mu_B\neq 0$（即 $r\neq 0$）可知存在 $b\in\mathbb{F}_q$ 使得等式(4.57) 成立. 根据注 *4.15*, 我们计算出

$$\mathfrak{g}_{0,0,t_C}^{-1}\circ\mathfrak{g}_{a,b,c}\circ\mathfrak{g}_{0,0,t_C}=\mathfrak{g}_{a',b',c'}. \tag{4.58}$$

其中 a' 是无关的, $b'=b^g-t_C S_2(c)^g+c^g\nu_C$ 和 $c'=c^g$. 我们有 $c'\in\mathcal{K}_0^*$, 这是因为 $\mathcal{K}_0^*$ 是 g 不变的. 通过比较等式(4.58)的两边中的 *Frobenius* 部分以及矩阵部分的第 $(3,2)$ 项, 我们可以推出 $\theta_{a',b',c'}=1$ 和 $T(a,b,c)^g=T(a',b',c')$. 因为 $\theta_{a,b,c}=\theta_{a',b',c'}=1$,

所以我们通过等式(4.56)有 $T(a,b,c)=S_2(c)$, $T(a',b',c')=S_2(c')$. 于是对 $c\in\mathcal{K}_0^*$ 有 $S_2(c)^g=S_2(c^g)$. 又因为 $\theta_{a',b',c'}=1$, 所以我们用等式(4.56) 中的 $\theta_{a',b',c'}$ 的表达式得到

$$-\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B b)=\frac{1}{2}Q(c^g)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha c^g-\mu_B t_C S_2(c)^g+\mu_B\nu_C c^g)).$$

再配合等式(4.57), 我们就能推出

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(\mu_B t_C S_2(c^g)\right)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left((-\alpha^g+\alpha+\mu_B\nu_C)c^g\right),\ c\in\mathcal{K}_0^*. \tag{4.59}$$

引理 4.43. $S_2(c)^g=S_2(c^g)$, $Q(c^g)=Q(c)$, 其中 $c\in\mathcal{K}_0^*$.

证明. 在前面的论证中, 我们已经建立了第一个等式；观察到它是比等式(4.41)更强的条件. 回想一下, 由定理 *4.33* 可知 $g(\mu_B)=\mu_B$, 并且根据推 *4.32*可知 $\mathcal{K}_0^*$ 是 g 不变的. 现在通过等式(4.55)中的 Q 的表达式可以验证 $Q(c^g)=Q(c)$, 其中 $c\in\mathcal{K}_0^*$. □

引理 4.44. 等式(4.52)中映射 $x\mapsto S_2(x)$ 可以扩展成 $\mathbb{F}_q$ 上的可加映射, 其中它对应的简化的线性化多项式中系数都属于 $\mathbb{F}_{p^l}$. 用 $S_2(X)$ 来表示这个多项式, 并且记 $S_2(X)=\sum_{i=0}^{p^2l-1}s_iX^{p^i}$ 其中每个系数 $s_i\in\mathbb{F}_{p^l}$. 记 $\lambda_C=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C t_C)$, $\nu_C=S(t_C)$.

(i) 存在 $u\in\mathbb{F}_q$ 使得 $u-g(u)\in\mathbb{F}_p\cdot\mu_C$, $(1-g)^2(u)=0$ 以及

$$-\mu_B s_i+s_{m-i}^{p^i}\mu_B^{p^i}=\mu_C u^{p^i}-u\mu_C^{p^i},\quad 0\le i\le p^2l-1. \tag{4.60}$$

(ii) 当 $x,\,y\in\mathbb{F}_q$ 时, 简写 $\mathrm{Tr}=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$, 下面等式成立:

$$\mathrm{Tr}\left(\mu_B x S_2(y)\right)=\mathrm{Tr}\left(\mu_B y S_2(x)\right)+\mathrm{Tr}(ux)\cdot\mathrm{Tr}(\mu_C y)-\mathrm{Tr}(\mu_C x)\cdot\mathrm{Tr}(uy). \tag{4.61}$$

(iii) 存在 $\lambda'\in\mathbb{F}_p$ 使得

$$\alpha^g-\alpha=\mu_B\nu_C-\mu_B S_2(t_C)+\lambda_C u+\lambda'\mu_C. \tag{4.62}$$

作为推论, 我们有 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu_C-S_2(t_C))=0$ 以及

$$\sum_{i=0}^{p-1}\alpha^{g^i}:=-\sum_{i=1}^{p-1}i\left(\mu_B\nu_C^{g^{i-1}}-\mu_B S_2(t_C)^{g^{i-1}}+\lambda_C u^{g^{i-1}}\right). \tag{4.63}$$

证明. 由引理 *4.43*, 我们对 $c\in\mathcal{K}_0^*$ 有 $S_2(c)^g=S_2(c^g)$. 再根据引理 *4.41*可知映射 $x\mapsto S_2(x)$ 在 $\mathcal{K}_0^*$ 上是可加的. 于是所需要的线性化多项式 $S_2(X)$ 的存在性就能从引理 *4.7*得到.

(i). 等式(4.60)可以通过取 $\mu = -\mu_B$, $\eta = \mu_C$ 和 $L = S_2$ 和使用引理 *4.8*后得到. 因为 μ_B 和每个系数 s_i 都是属于 $\mathbb{F}_{p^l}$, 所以等式(4.60)的左手边的取值就落在 $\mathbb{F}_{p^l}$. 于是就有

$$\mu_C u^{p^i} - u\mu_C^{p^i} = \mu_C g(u)^{p^i} - g(u)\mu_C^{p^i}, \textit{ i.e., } \mu_C(u - g(u))^{p^i} = (u - g(u))\mu_C^{p^i}.$$

当 $i = 1$ 时, 上式可得 $u - g(u) \in \mathbb{F}_p \cdot \mu_C$. 因为 $g(\mu_C) = \mu_C$, 所以我们推出所需的结果 $(1 - g)^2(u) = 0$.

(ii). 令 $\widetilde{S}_2$ 是 $S_2(X)$ 的迹对偶. 同样地取 $\mu = -\mu_B$, $\eta = \mu_C$ 和 $L = S_2$ 和使用引理 *4.8*, 我们就有

$$\widetilde{S}_2(\mu_B x) = \mu_B S_2(x) + \mu_C \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ux) - u\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C x),$$

其中 $x \in \mathbb{F}_q$. 对上式两边同时乘以 y, 接着取绝对迹函数 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$, 我们就通过观察 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B x S_2(y)) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\widetilde{S}_2(\mu_B x)y)$ 从而得到等式(4.61) .

(iii). 首先从等式(4.5)和 $(1 - g)^2(u) = 0$ 中观察到 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(u) = (1 - g)^{p^2-1}(u) = 0$. 取 $c \in \mathcal{K}_0^*$, 即 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C c) = 0$. 应用等式(4.61)到 $(x, y) = (t_C, c^g)$ 上, 我们就能推出等式(4.59)得左手边等于 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B c^g S_2(t_C) - \lambda_C u c^g)$. 通过多项式的化简, 它就简化为

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left((\alpha^g - \alpha - \mu_B\nu_C + \mu_B S_2(t_C) - \lambda_C u)c^g\right) = 0,\ c \in \mathcal{K}_0^*.$$

这是对所有 $c \in \mathcal{K}_0^*$ 都成立, 由引理 *4.3*可知存在 $\lambda' \in \mathbb{F}_p$ 使得等式(4.62)成立. 然后在等式(4.62)的两边取从 $\mathbb{F}_q$ 到 $\mathbb{F}_{p^l}$ 的相对迹函数, 我们就能推出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu_C - S_2(t_C)) = 0$. 根据二项式展开, 我们有

$$\binom{p-2}{i} = (-1)^i(i+1) \pmod p, \quad \binom{p-1}{i} = (-1)^i \pmod p,$$

因此有 $(1 - g)^{p-2} = \sum_{i=1}^{p-1} i g^{i-1}$, $(1 - g)^{p-1} = 1 + g + \cdots + g^{p-1}$. 通过把 $-(1 - g)^{p-2}$ 作用在等式(4.62)的两边上, 我们得到等式(4.63). □

最后, 我们探究一下条件 $\mathfrak{g}_{0,0,t_C}^p \in G_{\mathcal{K}_0^*}$. 当 $i \geq 0$, 设

$$\mathfrak{g}_{a_i,b_i,c_i} := \mathfrak{g}_{0,0,t_C}^i = (\mathcal{M}_{0,0,t_C}^{g^{i-1}} \cdot \cdots \cdot \mathcal{M}_{0,0,t_C},\ g^i).$$

特别注意的是, a_i 的值在我们讨论中是无关的, 而 $b_{i+1} = b_i^g + c_i^g\nu_C$, $c_{i+1} = c_i^g + t_C$. 从 $b_1 = 0$, $c_1 = t_C$ 中我们推出 $b_{i+1} = \sum_{j=1}^{i}\sum_{k=1}^{j} g^{i-j}(t_C^{g^k}\nu_C)$, $c_{i+1} = \sum_{j=0}^{i} t_C^{g^j}$. 特别地, 我们有 $\mathfrak{g}_{0,0,t_C}^p = \mathfrak{g}_{a'',b'',c''}$, 其中 a'' 是无关的, 并且

$$b'' = b_p = \sum_{i=1}^{p-1}\sum_{k=1}^{i} g^{p-1-i}(t_C^{g^k}\nu_C), \quad c'' = c_p = \sum_{i=0}^{p-1} t_C^{g^i}. \tag{4.64}$$

观察到 $c'' \in \mathcal{K}_0^*$, 这是因为从 $g(\mu_C) = \mu_C$ 中我们有

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C c'') = \sum_{i=0}^{p-1} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C^{g^{-i}} t_C) = 0.$$

引理 4.45. 使用在引理 4.44中定义的符号, 并记 $\nu_B = M(t_B)$. 那么 $p = 3$, $\lambda_C = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}((u-u^g)t_C)$, $\nu_B = \sum_{i=0}^{p-1}(\nu_C - S_2(t_C))^{g^i}$ 且 $\mu_C = u - u^g$.

证明. 我们继续引理之前的分析. 因为 $\sigma_{t_C}^p = g^p = g_1$, 所以 $\mathfrak{g}_{0,0,t_C}^p$ 的 *Frobenius* 部分是 g_1. 而 $\mathfrak{g}_{a'',b'',c''}$ 的 *Frobenius* 部分是 g_1^D, 其中由等式(4.56)可知 $D = \frac{1}{2}Q(c'') + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha c'' + \mu_B b'')$. 通过比较 $\mathfrak{g}_{0,0,t_C}^p = \mathfrak{g}_{a'',b'',c''}$ 的两边的 *Frobenius* 部分和矩阵部分的第 $(3,2)$ 项, 我们就有 $D = 1$, 以及

$$\nu_B = \nu_C + \nu_C^g + \cdots + \nu_C^{g^{p-1}} - S_2(c''). \tag{4.65}$$

为了便于表示, 我们在证明中记 $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. 我们现在可以显示地计算 D. 因为 S_2 的多项式系数都属于 $\mathbb{F}_{p^l}$, 所以我们对 $i \geq 0$ 有 $S_2(x^{g^i}) = S_2(x)^{g^i}$. 因为 $c'' = \sum_{i=0}^{p-1} t_C^{g^i}$ 且 $Q(c'') = -\mathrm{Tr}(\mu_B c'' S_2(c''))$, 所以我们能计算出

$$\begin{aligned}
Q(c'') &= -\textstyle\sum_{i,j=0}^{p-1} \mathrm{Tr}\left(\mu_B t_C^{g^i} S_2(t_C)^{g^j}\right) \\
&= -\textstyle\sum_{i<j} \mathrm{Tr}\left(\mu_B t_C^{g^i} S_2(t_C)^{g^j}\right) - \sum_{j<i} \mathrm{Tr}\left(\mu_B t_C^{g^i} S_2(t_C)^{g^j}\right) \\
&= -\textstyle\sum_{k=1}^{p-1}(p-k)\left(\mathrm{Tr}(\mu_B t_C S_2(t_C^{g^k})) + \mathrm{Tr}(\mu_B t_C^{g^k} S_2(t_C))\right) \\
&= \textstyle\sum_{k=1}^{p-1} k\left(2\mathrm{Tr}(\mu_B t_C^{g^k} S_2(t_C)) + \lambda_C \mathrm{Tr}(u t_C) - \lambda_C \mathrm{Tr}(u t_C^{g^k})\right) \\
&= \textstyle\sum_{k=1}^{p-1} k \cdot \mathrm{Tr}(2\mu_B t_C^{g^k} S_2(t_C) - \lambda_C u t_C^{g^k}).
\end{aligned}$$

这里, 在第二个等式中满足 $i = j$ 的 p 是相等的, 于是它们求和后为零, 在第四个等式中我们使用等式(4.61), 其中 $(x, y) = (t_C, t_C^{g^k})$, 而在第五个等式中我们使用 $\sum_{i=1}^{p-1} i \equiv 0 \pmod{p}$ 这事实. 相似地, 我们有

$$\begin{aligned}
\mathrm{Tr}(\alpha c'') &= \mathrm{Tr}(t_C^{g^{p-1}}(\alpha + \cdots + \alpha^{g^{p-1}})) \\
&= -\textstyle\sum_{i=1}^{p-1} \mathrm{Tr}\left(i t_C^{g^{p-1}}(\mu_B \nu_C^{g^{i-1}} - \mu_B S_2(t_C)^{g^{i-1}} + \lambda_C u^{g^{i-1}})\right) \\
&= \textstyle\sum_{i=1}^{p-1} i \cdot \mathrm{Tr}\left(-t_C^{g^{p-i}} \mu_B \nu_C + \mu_B t_C^{g^{p-i}} S_2(t_C) - \lambda_C t_C^{g^{p-i}} u\right) \\
&= \textstyle\sum_{k=1}^{p-1} k \cdot \mathrm{Tr}(\mu_B \nu_C t_C^{g^k} - \mu_B t_C^{g^k} S_2(t_C) + \lambda_C u t_C^{g^k}),
\end{aligned}$$

其中在第二个等式中我们使用等式(4.63), 并且在最后一个等式中我们做了变量替换 $p - i \mapsto k$. 易证

$$\mathrm{Tr}(\mu_B b'') = -\sum_{i=1}^{p-1} i \cdot \mathrm{Tr}(\mu_B t_C^{g^i} \nu_C).$$

最后把这些计算结果放在一起, 我们得到 $D = \frac{\lambda_C}{2} \cdot \sum_{i=1}^{p-1} i \cdot \mathrm{Tr}(ut_C^{g^i})$.

设 $v := u - u^g$, 根据引理 *4.44*可知该元素属于 $\mathbb{F}_p \cdot \mu_C$. 特别地, $v \in \mathbb{F}_{p^l}$. 从 $u^g = u - v$ 中我们通过归纳法可得对 $i \geq 0$ 有 $u^{g^i} = u - iv$. 记得 $\lambda_C = \mathrm{Tr}(\mu_C t_C) \neq 0$. 我们就计算出

$$\begin{aligned} 2\lambda_C^{-1} D &= \sum_{i=1}^{p-1} i \cdot \mathrm{Tr}(u^{g^{p-i-1}} t_C^{g^{p-1}}) = \sum_{i=1}^{p-1} i \cdot \mathrm{Tr}\left((u - (p-i-1)v) t_C^{g^{p-1}}\right) \\ &= \sum_{i=1}^{p-1} (i^2 + i) \cdot \mathrm{Tr}(v t_C^{g^{p-1}}) = \tfrac{p(p-1)(p+1)}{3} \cdot \mathrm{Tr}(v t_C). \end{aligned}$$

上式的值在 $p > 3$ 时为 0, 这意味着我们必须有 $p = 3$. 在这种情况下, $\frac{p(p-1)(p+1)}{3} = -1 \pmod 3$. 因为 $D = 1$ 和 $\lambda_C \in \{\pm 1\} = \mathbb{F}_3^*$, 所以从上式可以推出 $\lambda_C = \mathrm{Tr}(v t_C)$.

结合 $\lambda_C = \mathrm{Tr}(\mu_C t_C)$, $\lambda_C = \mathrm{Tr}(v t_C)$ 以及 $v \in \mathbb{F}_p \cdot \mu_C$ 这些事实, 我们能推出 $\mu_C = v$. 因为 $x \in \mathbb{F}_q$ 时 $S_2(x^g) = S_2(x)^g$, 所以 ν_B 的表达式就直接从等式(4.65)中得到. 证毕. □

结果是, 我们目前推导出的条件也是充分的. 这就引出了下面的构造.

构造 4.46. 假定 $q = 3^{3^2 l}$, 其中 l 是一个正整数. 再取 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得 $g(x) = x^{p^l}$. 设 $g_1 := g^3$.

(i) 取 $u \in \mathbb{F}_q$ 使得 $\mu_C := u - u^g \in \mathbb{F}_{3^l}^*$;

(ii) 取 $t_C \in \mathbb{F}_q^*$ 使得 $\lambda_C := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_C t_C) \neq 0$;

(iii) 取 $\mu_B \in \mathbb{F}_{3^l}^*$;

(iv) 取一个 $9l$ 元组 $(s_0, s_1, \cdots, s_{9l-1})$, $s_i \in \mathbb{F}_{3^l}$ 满足

$$-\mu_B s_i + s_{9l-i}^{3^i} \mu_B^{3^i} = \mu_C u^{3^i} - u \mu_C^{3^i},\ 1 \leq i \leq 9l-1;$$

设 $S_2(x) := \sum_{i=0}^{3^2 l - 1} s_i x^{3^i}$, $Q(x) := -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_B x S_2(x))$ 其中 $x \in \mathbb{F}_q$;

(v) 取 $\alpha \in \mathbb{F}_q, \lambda \in \mathbb{F}_3$ 并且令 $\nu_C := S_2(t_C) + \mu_B^{-1}(\alpha^g - \alpha - \lambda_C u - \lambda \mu_C)$;

令 $\nu_B := \sum_{i=0}^{2} g^i(\nu_C - S_2(t_C))$, 再令 N_C 是在等式(4.38)中用规定形式的 ν_B 定义的函数. 设 $K := \{z \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_C z) = 0\}$.

当 $a, b \in \mathbb{F}_q$ 和 $c \in K$, 令 $\theta_{a,b,c}$ 和 $T(a,b,c)$ 是在等式(4.56)中定义的函数, 并且设 $\mathcal{M}_{a,b,c} = E(a,b,c,T(a,b,c))$, 其中 E 是等式(4.8)中定义的矩阵. 那么 $G_K := \{\mathfrak{g}_{a,b,c} : a, b \in \mathbb{F}_q, c \in K\}$ 是一个 $q^3/3$ 阶子群, 其中 $\mathfrak{g}_{a,b,c} = (\mathcal{M}_{a,b,c}, \theta_{a,b,c})$. 取 $\mathfrak{g}_{0,0,t_C} = (\mathcal{M}_{0,0,t_C}, g)$ 且其中 $\mathcal{M}_{0,0,t_C} := E(0,0,t_C,\nu_C)$. 那么 $G := \langle G_K, \mathfrak{g}_{0,0,t_C} \rangle$ 是 Payne 派生四边形 $\mathcal{Q}^P$ 的一个点正则群.

证明. 通过类似于引理 *4.25*的证明可知满足 *(iv)* 中条件的 $9l$ 元组的数目恰好等于 $3^{(9l+1)l/2}$. 再用跟构造 *4.42*的证明一样的论证, 我们就能证明 G_K 是一个 $q^3/3$ 阶群. 令 G_1 是 G_K 中 *index* 为 *3* 的子群, 其中它里面的元素都是具有平凡的 *Frobenius* 部分. 那么我们讲这一子节上面的论证过程颠倒过来, 即可验证 $\mathfrak{g}_{0,0,t_C}$ 正规化 G_1 并且 $\mathfrak{g}^3_{0,0,t_C} \in G_K$. 因为 $\mathfrak{g}^3_{0,0,t_C}$ 的 *Frobenius* 部分是 $g_1 = g^3$, 所以我们能推出 $G_K = \langle G_1, \mathfrak{g}^3_{0,0,t_C}\rangle$. 于是 $\mathfrak{g}_{0,0,t_C}$ 属于 G_K 的正规化子. 我们因此得出结论 G 是一个 q^3 阶群. 于是 $\langle(0,0,0,1)\rangle$ 在 G_K 的作用下的轨道是 $X_1 = \{\langle(a,b,c,1) : a,b \in \mathbb{F}_q, c \in K\rangle\}$, 其大小为 $q^3/3$, 并且 $\langle(0,0,0,1)\rangle^{\mathfrak{g}_{0,0,t_C}} = \langle(0,0,t_C,1)\rangle$ 不属于 X_1. 因此 $\langle(0,0,0,1)\rangle$ 在 G 作用下的轨道大小比 $q^3/3$ 大. 因为它的长度也能被 $|G|$ 整除, 所以我们能得出它的大小恰好为 q^3, 即 G 是点正则的. □

综上所述, 我们已经证明了在 $r_{A,B} = 1$, $r_C = 2$ 情况下, 点正则群 G 必须是来自构造 *4.46*. 根据定理 *4.28*和定理 *4.31*, 我们就有 $r_{A,B} \leq 1, r_C \leq r_{A,B} + 1$. 因此, 结合第 *4.6.1*中在 $r_{A,B} = 0, r_C = 1$ 情况下的分类结果和本子节的 *Part* 1 中在 $r_{A,B} = 1, r_C = 1$ 情况下的分类结果, 我们就完成定理 *4.34*的证明.

4.7 奇特征情况下的同构问题

假定 q 是奇数. 记得当 a, b, c, t 属于 $\mathbb{F}_q$ 时, 我们已经定义了

$$E(a,b,c,t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -c & 1 & 0 & 0 \\ b-ct & t & 1 & 0 \\ a & b & c & 1 \end{pmatrix},$$

它不但能看作 $\mathrm{PSp}(4,q)_P$ 的元素, 而且保持派生四边形 $\mathcal{Q}^P$ 不变. 对 $\mathcal{Q}^P$ 中的点正则群 G, 我们用 $\mathfrak{g}_{a,b,c}$ 来表示 G 中把 $\langle(0,0,0,1)\rangle$ 映射到 $\langle(a,b,c,1)\rangle$. 的元素. 令 $\theta_{a,b,c}$ 是 $\mathfrak{g}_{a,b,c}$ 的 *Frobenius* 部分, 并且令 $T(a,b,c)$ 是它的矩阵部分的第 $(3,2)$ 项, 这些都是我们第 *4.2.2*子节中引入的符号.

4.7.1 $\mathrm{P\Gamma Sp}(4,q)_P$ 内的共轭类

在本子节中, 我们将会完成 q 是奇数时点正则群的分类结果的证明, 也就是定理 *4.20*的证明. 奇特征下的所有点正则群都是从定理 *4.22(*线性的情况*)* 和定理 *4.34(*非线性的情况*)* 中得到的, 同时这意味着构造 *4.37, 4.42*和 *4.46*产生的群分别在 $\mathrm{P\Gamma Sp}(4,q)$ 里面与构造 *4.17-4.19*中的群相共轭. 并且我们观察到构造 *4.17-4.19*分别是构造 *4.37, 4.42*和 *4.46*的特殊情形. 于是我们在接下来的讨论中对这三种情况的每一种情况下证明它们之间的共轭性, 从而完成定理 *4.20*的证明.

(A). 在构造 *4.37*中, 设 $\nu := \nu_C - S_1(t_C)$. 因为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu) = 0$, 所以 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(\nu) = 0$, 于是由引理 *4.1*可知存在 $u \in \mathbb{F}_q$ 使得 $u^g - u = \nu$. 取 $\mathfrak{g}_1 := (E(0,0,0,u), 1)$. 易知 $\tilde{G} := \mathfrak{g}_1^{-1} \circ G \circ \mathfrak{g}_1$ 也是 $\mathcal{Q}^P$ 的点正则群. 根据第 *4.2*节中的介绍, 群 $\tilde{G}$ 是由某两个函数 T' 以及 θ' 而生成的点正则群. 令 $\mathfrak{g}'_{a,b,c}$ 是 $\tilde{G}$ 中把 $\langle(0,0,0,1)\rangle$ 映射到 $\langle(a,b,c,1)\rangle$ 的元素, 设 $\sigma'_c := \theta'_{0,0,c}$, $M'(y) := T'(0,y,0)$ 和 $S'(z) := T'(0,0,z)$. 于是对 $M'(y) := T'(0,y,0)$ 和 $S'(z) := T'(0,0,z)$, 我们就能验证

$$\mathfrak{g}'_{a,b,c} = \mathfrak{g}_1^{-1} \circ \mathfrak{g}_{a,b-c\nu,c} \circ \mathfrak{g}_1 = (E(a,b,c,S_1(c)),\ 1).$$

于是在 $c \in K$ 就有 $T'(a,b,c) = S_1(c)$, $\theta'(a,b,c) = 1$. 特别地, $M' \equiv 0$, $\theta'_{0,y,0} \equiv 1$. 相似地, 我们有

$$\mathfrak{g}'_{0,ut_C,t_C} = \mathfrak{g}_1^{-1} \circ \mathfrak{g}_{0,0,t_C} \circ \mathfrak{g}_1 = (E(0,ut_C,t_C,S_1(t_C)),\ g).$$

也就是说, $T'(0,ut_C,t_C) = S_1(t_C)$, $\theta'_{0,ut_C,t_C} = g$. 根据等式(4.42)和(4.43), 我们有 $\sigma'_{t_C} = g$. 由此我们有 $\mathfrak{g}'_{0,0,t_C} = (E(0,0,t_C,S_1(t_C)),\ g)$.

设 $\tilde{G} := \mathfrak{g}_1^{-1} \circ G_K \circ \mathfrak{g}_1$, 注意到它恰好是群同态 $\mathfrak{g}'_{a,b,c} \mapsto \theta'_{a,b,c}$ 的核. 那么 $\tilde{G} = \langle \tilde{G}_K, \mathfrak{g}'_{0,0,t_C} \rangle$. 于是对每个三元组 (x,y,z) 存在 $a,b \in \mathbb{F}_q$, $c \in K$ 和 $i \geq 0$ 使得 $\mathfrak{g}'_{x,y,z} = \mathfrak{g}'_{a,b,c} \circ \mathfrak{g}'^i_{0,0,t_C}$. 根据群乘法(4.9), 我们就能直接地验证 $z = g^i(c) + \sum_{k=0}^{i-1} g^k(t_C)$, $T'(x,y,z) = S_1(z)$ 和 $\theta'_{x,y,z} = g^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu'_C z)}$, 其中 $\mu' = \mu_C \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_C t_C)^{-1}$. 因此 $\tilde{G}$ 是来自构造 *4.17*的. 而这证明 G 是来自构造 *4.37*的情况下的说法.

(B). 在构造 *4.42*中, 取 $u := \mu_B^{-1}\alpha$, 由 (iii) 可知 $\nu_B = u^g - u$. 我们就能从 $\nu_B = u^g - u$ 中推出 $N_C(\theta_{a,b,c}) = u^{\theta_{a,b,c}} - u$, 其中 N_C 是在等式(4.38)中定义的函数. 再用 $\mathfrak{g}_1 = (E(0,0,0,u),\ 1) \in \mathrm{P\Gamma Sp}(4,q)_P$ 对它共轭, 我们就计算出 $\mathfrak{g}'_{a,b,c} := \mathfrak{g}_1^{-1} \circ \mathfrak{g}_{a,b-uc,c} \circ \mathfrak{g}_1$ 等于 $(E(a,b,c,S_2(c)), g^{\frac{1}{2}Q(c) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha' c + \mu_B b)})$. 通过将符号 S_2 改成 S_1(为了保持跟前面的构造的符号的一致性), 我们就能看出 $\alpha'^g - \alpha' = 0$ 就采取构造 *4.18*的形式. 而这证明对构造 *4.42*的说法.

(C). 在构造 *4.46*中, 设 $\nu := \nu_C - S_2(t_C)$, 从 (v) 可知它等于 $\mu_B^{-1}(\alpha^g - \alpha - \lambda_C u - \lambda\mu_C)$. 我们就用 (i) 中 $(1-g)^u = 0$ 以及 $\mu_C \in \mathbb{F}_{3^l}$ 推出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{3^l}}(\nu) = 0$ 这些事实突出 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{3^l}}(\nu) = 0$. 于是根据引理 *4.1*可知存在 $u_0 \in \mathbb{F}_q$ 使得 $\nu = u_0^g - u_0$. 令 $\lambda := \lambda_C^{-1}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_B u_0 t_C)$ 和 $u_1 := u_0 - \lambda\mu_B^{-1}\mu_C$, 因此 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_B t_C u_1) = 0$. 因为 μ_B 和 μ_C 都属于 $\mathbb{F}^*_{3^l}$, 我们就能推出 $u_1^g - u_1 = \nu$. 于是就有 $\nu_B = \sum_{i=0}^{2} g^i(\nu) = g_1(u_1) - u_1$, 其中 $g_1 = g^3$. 以下是我们需要了解的一些事实:

(1) 设 $\alpha' := \alpha - u_1\mu_B$. 那么我们就能从 $u_1^g - u = \nu$ 和 $\nu = \mu_B^{-1}(\alpha^g - \alpha - \lambda_C u - \lambda\mu_C)$ 中推出 $g(\alpha') - \alpha' = \lambda_C u + \lambda\mu_C$. 因为 $u - u^g \in \mathbb{F}_{3^l}^*$ 和 $(g-1)^3 = g_1 - 1$, 所以我们能进一步地推出 $g_1(\alpha') - \alpha' = 0$, 即 $\alpha' \in \mathbb{F}_{3^{3l}}$.

(2) 因为 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(\mu_B t_C u_1) = 0$,, 所以根据等式(4.42) 我们有

$$\theta_{0,-t_Cu_1,t_C} = \theta_{0,-t_Cu_1,0} \cdot \sigma_{t_C} = g_1^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(-\mu_B t_C u_1)} \cdot g = g.$$

(3) 由等式(4.43)可知 $T(0, -t_C u_1, t_C) = M(b')^g + \nu_C$, 其中 $b' = -t_C u_1$. 于是我们有 $\theta_{0,b',0} = 1$, 所以从 *(F5)* 可得 $M(b') = N_C(1) = 0$. 由此就有 $T(0, -t_C u_1, t_C) = \nu_C$.

令 $\tilde{G} := \mathfrak{g}_1^{-1} \circ G \circ \mathfrak{g}_1$ 且 $\mathfrak{g}_1 = (E(0,0,0,u_1), 1) \in \mathrm{P\Gamma Sp}(4,q)_P$, 再令 $\mathfrak{g}'_{a,b,c}$ 是 $\tilde{G}$ 中把 $\langle(0,0,0,1)\rangle$ 映射到 $\langle(a,b,c,1)\rangle$ 的元素. 根据第 *4.2.2*节中的分析, 群 $\tilde{G}$ 是由某个函数 T' 和 θ' 而生成的点正则群. 通过与前面的例子完全相同的论证, 我们推断出子群 $\tilde{G}_K := \mathfrak{g}_1^{-1} \circ G_K \circ \mathfrak{g}_1$ 是由 $\mathfrak{g}'_{a,b,c} = (\mathcal{M}'_{a,b,c}, \theta'_{a,b,c})$, $a, b \in \mathbb{F}_q$, $c \in K$ 组成, 其中 $\theta'_{a,b,c} = g_1^{\frac{1}{2}Q(c) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha' c + \mu_B b)}$ 和 $\mathcal{M}'(a,b,c) = E(a,b,c,S_2(c))$. 相似地, $\mathfrak{g}'_{0,0,t_C} = \mathfrak{g}_1^{-1} \circ \mathfrak{g}_{0,-t_Cu_1,t_C} \circ \mathfrak{g}_1$, 并且由上面的 *(2)* 可知它的 *Frobenius* 部分是 g. 我们比较他们的矩阵部分, 于是就有 $T'(0,0,t_C) = \nu_C - g(u_1) + u_1 = S_2(t_C)$, 其中我们在推导过程中用了上面的 *(3)*. 通过将符号 S_2 改成 S_1*(*为了跟之前的构造中符号保持一致*)*, 我们就能看出 $\tilde{G} = \mathfrak{g}_1^{-1} \circ G \circ \mathfrak{g}_1$ 取构造 *4.19*给出的形式. 这证明对构造 *4.46*的说法, 因此就完成定理 *4.20*的证明.

4.7.2 点正则群的群不变量

本节的第一个目标是证明这四种构造在一般情况下产生不同构的点正则群. 我们从 G 的一些性质开始.

引理 4.47. *在构造 4.16-4.19产生的点正则群中, 我们都有 $T(x,y,z) = S_1(z)$.*

证明. 这对于前三个构造来说是显而易见的. 因此, 我们下面只考虑构造 *4.19*的情况. 因为多项式系数 $s_i (0 \le i \le 9l-1)$ 都属于 $\mathbb{F}_{3^l}$, 所以我们对 $x \in \mathbb{F}_q$ 有 $S_1(g(x)) = g(S_1(x))$, 即 S_1 和 g 是相互交换的. 因为对每个三元组 (x, y, z) 都有 $G = \langle G_K, \mathfrak{g}_{0,0,t_C}\rangle$, 所以存在 $a, b \in \mathbb{F}_q$, $c \in K$ 和 $i \ge 0$ 使得 $\mathfrak{g}_{x,y,z} = \mathfrak{g}_{a,b,c} \circ \mathfrak{g}_{0,0,t_C}^i$. 通过使用注 *4.15*中的计算以及 S_1 和 g 交换的事实进行直接地展开, 我们从这个等式中得到 $z = g^i(c) + \sum_{k=0} i - 1 g^k(t_C)$ 和 $T(x,y,z) = S_1(z)$. 证毕. □

引理 4.48. 令 G 为来自以上的四个构造其中之一的群. 令 G_F 是下面定义的 G 的子群

$$G_F := \{\mathfrak{g}_{a,b,c} : \theta_{a,b,c} = 1\}, \tag{4.66}$$

以及设 $U := \{c \in \mathbb{F}_q : \mathfrak{g}_{a,b,c} \in G_F \text{ 对某些} a, b \in \mathbb{F}_q\}$.

(P1) 对构造 4.16和 4.18有 $U = \mathbb{F}_q$, 而对构造 4.17和 4.19则有 U 是一个余维数为 1 的 $\mathbb{F}_p$-线性子空间.

(P2) 当 $\mathfrak{g}_{a,b,c} \in G_F$ 时, 它的阶是 p 或 p^2; 特别地, 后一种情况发生当且仅当 $p = 3$ 和 $S_1(c) \neq 0$.

证明. 结论 $(P1)$ 是通过一种一种情况地检查得到的, 这里我们省略了这些细节. 设 $T_1 := T(a, b, c)$ 和 $\mathfrak{g}_{a_i,b_i,c_i} := \mathfrak{g}^i_{a,b,c}$. 根据注 *4.15*, 我们能推出对每个 $i \geq 0$ 都有 $c_{i+1} = c_i + c$, $b_{i+1} = b_i + c_i T_1$ 和 $a_{i+1} = a_i - b_i c + c_i b - c_i c T_1$. 因为 $a_0 = b_0 = c_0 = 0$, 所以很容易地推出 $c_i = ic$, $b_i = ib + \frac{(i-1)i}{2} cT_1$ 以及 $a_i = ia - \frac{(i^2-1)i}{6} c^2 T_1$. 特别地, $\mathfrak{g}^p_{a,b,c} = \mathfrak{g}_{x,0,0}$, 其中 $x = -\frac{(p^2-1)p}{6} c^2 S_1(c)$, 还有 $\mathfrak{g}^{p^2}_{a,b,c} = 1$. 因为 p 是奇数, 所以 $\frac{(p^2-1)p}{6} \neq 0$ 当且仅当 $p = 3$. 此外, 因为 S_1 是可加的, 所以 $cS_1(c) \neq 0$ 当且仅当 $S_1(c) \neq 0$. 因此, $\mathfrak{g}_{a,b,c}$ 的阶是 p^2 当且仅当 $p = 3$ 和 $S_1(c) \neq 0$. 这就完成说法 $(P2)$ 的证明. □

定理 4.49. 令 G 为来自构造 4.16-4.19中的某个构造产生的群.

(1) 若 G 是来自构造 4.16的, 则 $\exp(G) = p$ 或 p^2, 其中后者发生当且仅当 $p = 3$ 和 S_1 不是零映射.

(2) 若 G 是来自构造 4.17或 4.18的, 则 $\exp(G) = p^2$ 或 p^3, 其中后者发生当且仅当 $p = 3$ 以及 S_1 限制到 $\mathbb{F}_{3^l}$ 时不是零映射.

(3) 若 G 是来自构造 4.19的, 则 $\exp(G) = 3^3$ 或 3^4, 其中后者发生当且仅当 $p = 3$ 以及 S_1 限制到 $\mathbb{F}_{3^l}$ 时不是零映射.

证明. 每个构造的分析都是相似的, 于是我们只对构造 *4.19*的情况给出详细的解释. 令 G_F 是在等式(4.66)中定义的集合, 并且定义群同态 $\psi : G \to \mathrm{Aut}(\mathbb{F}_q)$, $\mathfrak{g}_{a,b,c} \mapsto \theta_{a,b,c}$. 那么 $G_F = \ker(\psi)$. 我们首先做一些观察.

(i) $\mathbb{F}_q = \langle K, t_C \rangle_{\mathbb{F}_3}$, 这是因为 $t_C \notin K$ 和 K 是 $\mathbb{F}_q$ 中一个超平面. 此外, 根据线性代数可知 $\mathbb{F}_q = \langle t_C + K \rangle_{\mathbb{F}_3}$.

(ii) 因为 $[G:G_K]=3$ 且 $G_K=\{\mathfrak{g}_{a,b,c}:a,b\in\mathbb{F}_q,\,c\in K\}$, 所以我们有 $G_K\circ\mathfrak{g}_{0,0,t_C}=\{\mathfrak{g}_{a,b,t_C+g(c)}:a,b\in\mathbb{F}_q,\,c\in K\}$.

(iii) 因为 $\mathrm{Im}(\psi)=\langle g\rangle$ 的阶是 9, 所以此我们对任意 $\mathfrak{g}\in G$ 都有 $\mathfrak{g}^9\in G_F$.

我们这里声称如果 $S_1|_{\mathbb{F}_{3^l}}\neq 0$, 那么存在 $c\in K$ 使得 $S_1(w)\neq 0$, 其中 $w=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{3^l}}(t_C+c)$; 否则 t_C+K 落在 $\mathbb{F}_3$ 线性映射 $x\mapsto S_1(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{3^l}}(x))$ 的核里面, 于是 $\langle t_C+K\rangle_{\mathbb{F}_3}=\mathbb{F}_q$ 也落在这个核里面. 因为迹映射是满射的, 所以我们就推出一个矛盾：$\ker(S_1)=\mathbb{F}_{3^l}$. 这就证明我们的声称.

取一个三元组 (x,y,z), 并且记 $g^i=\theta_{x,y,z}$, $\mathfrak{g}_{u,v,w}=\mathfrak{g}^9_{x,y,z}$, 易从 *(iii)* 中可知它属于 G_F. 我们也根据乘法规则(4.9)计算出 $w=\sum_{k=0}^{8}g^{ik}(z)$. 如果进一步有某个 $c\in K$ 使得 $z=t_C+g(c)$, 那么从 *(2)* 可得 $\mathfrak{g}_{x,y,z}\in G_K\circ\mathfrak{g}_{0,0,t_C}$, 因此, 对某个 j 有 $\theta_{x,y,z}=g^{1+3j}$; 对应地, 根据 $\sum_{k=0}^{8}g^k(z)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{3^l}}(z)$ 这事实有 $w=\sum_{k=0}^{8}\theta^k_{x,y,z}(z)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{3^l}}(t_C+c)$.

接着我们声称 $3^3\leq\exp(G)\leq 3^4$. 因为 $\mathfrak{g}_{u,v,w}\in G_F$, 由引理 *4.48*可知它的阶至多是 3^2, 故 $\exp(G)\leq 3^4$. 另一方面, 根据 *(i)* 可知存在 $c\in K$ 使得 $\lambda:=\mathrm{Tr}_{q/3^l}(t_C+c)\neq 0$. 那么对某个 u,v 有 $\mathfrak{g}^9_{0,0,t_C+c}=\mathfrak{g}_{u,v,\lambda}$, 于是 $\mathfrak{g}_{0,0,t_C+c}$ 的阶至少是 3^3. 这就证明我们的声称.

剩下只需要确定何时存在这样的三元组 (x,y,z) 使得 $\mathfrak{g}:=\mathfrak{g}_{x,y,z}$ 的阶是 3^4. 由 *(iii)* 可知当且仅当 $\theta_{x,y,z}$ 的阶是 9 以及 $\mathfrak{g}_{u,v,w}=\mathfrak{g}^9$ 的阶也是 9 时, 才出现这种情况. 假设这两个条件都成立. 因为 $[G:G_K]=3$, 如果有需要把 $\mathfrak{g}$ 替换成 $\mathfrak{g}^{-1}$, 我们可以假设 $\mathfrak{g}\in G_K\circ\mathfrak{g}_{0,0,t_C}$. 因此, 由 *(ii)* 可知对某个 $c\in K$ 有 $z=t_C+g(c)$, 并且对应地, $w=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{3^l}}(t_C+c)\in\mathbb{F}_{3^l}$. 根据引理 *4.48*的 $(P2)$, 群元素 $\mathfrak{g}_{u,v,w}$ 的阶是 9 当且仅当 $S_1(w)\neq 0$. 因此, 当 $S_1|_{\mathbb{F}_{3^l}}\equiv 0$ 时不可能存在这样元素. 如果 S_1 在 $\mathbb{F}_{3^l}$ 不常为零, 那么我们早已经证明存在 $c\in K$ 使得 $c\in K$, 于是就有 $\mathfrak{g}^9_{0,0,t_C+g(c)}$ 的阶 9. 这就证明我们的说法. 证毕. □

定理 *4.49*对区分构造 *4.17*和构造 *4.18*没有帮助. 于是我们计算他们的 *Thompson* 子群, 这将能在一般情况下说明这两个构造是不同的. 取 $\mathfrak{g}_{a,b,c}\in G$, 并记 $\theta_1=\theta_{a,b,c}$. 当 $\mathfrak{g}_{x,y,z}\in C_G(\mathfrak{g}_{a,b,c})$ 时, 根据定理 *4.12*, 我们从 $\mathfrak{g}_{a,b,c}\circ\mathfrak{g}_{x,y,z}=\mathfrak{g}_{x,y,z}\circ\mathfrak{g}_{a,b,c}$ 中推出

$$\begin{aligned}
a^{\theta_2}+x-b^{\theta_2}z+c^{\theta_2}y-c^{\theta_2}zS_1(z)&=x^{\theta_1}+a-cy^{\theta_1}+bz^{\theta_1}-cz^{\theta_1}S_1(c);\\
b^{\theta_2}+y+c^{\theta_2}S_1(z)&=b+y^{\theta_1}+z^{\theta_1}S_1(c),\\
c^{\theta_2}+z&=c+z^{\theta_1},\\
S_1(c)^{\theta_2}+S_1(z)&=S_1(z)^{\theta_1}+S_1(c),
\end{aligned}\tag{4.67}$$

其中 $\theta_2=\theta_{x,y,z}$. 这是我们利用引理 *4.47*的结果 $T(x,y,z)=S_1(z)$.

定理 4.50. 令 G 是来自构造 4.17或构造 4.18的群, 并且假设 $1 < \deg(S_1) < q/p$. 那么 G 的 Thompson 子群是 $J(G) = \{\mathfrak{g}_{a,b,0} : a, b \in \mathbb{F}_q, \theta_{a,b,0} = 1\}$. 当 G 来自构造 4.17时, $|J(G)| = q^2$, 而当它来自构造 4.18时, $|J(G)| = q^2/p$.

证明. 我们这里只处理构造 *4.18*的情况, 另外一种情况是类似的. 令 d 为 G 中阿贝尔群的最大阶. 易知 $G_{ab} := \{\mathfrak{g}_{a,b,0} : a, b \in \mathbb{F}_q, \theta_{a,b,0} = 1\}$ 是阶为 q^2/p 的阿贝尔群, 所以 $d \geq q^2/p$.

我们首先证明 $J(G) \leq G_F$, 其中 G_F 是 G 中所有带有平凡的 *Frobenius* 部分的元素的集合. 这是通过证明任何 d 阶的阿贝尔子群都是 G_F 的子集来实现. 现在我们开始用反证法. 假设 H 是 d 阶阿贝尔子群并且包含一个元素 $\mathfrak{g}_{a,b,c} \in G$ 使得 $\theta_{a,b,c} = g^i \neq 1$. 因为子群 $C_G(\mathfrak{g}_{a,b,c})$ 不仅包含 H, 也至少有大小 $d \geq q^2/p$. 我们现在用另外一种方法估计 $C_G(\mathfrak{g}_{a,b,c})$ 的大小. 固定一个整数 j 使得 $0 \leq j \leq p-1$. 假定 $\mathfrak{g}_{x,y,z} \in C_G(\mathfrak{g}_{a,b,c})$, 且它的 *Frobenius* 部分为 $\theta_{x,y,z} = g^j$. 根据等式(4.67)中的第三个方程, 我们有 $z^{g^i} - z = -c^{g^j} + c$. 因为 $o(g^i) = p$ 和 $q = p^{pl}$, 所以这个方程关于 z 最多有 p^l 个解. 于是对于给定的 z, 相同的理由说明了等式(4.67)中的第二个方程关于变量 y 最多有 p^l 个解. 相似地, 对给定一对 (y, z), 等式(4.67)中的第一个方程关于变量 x 最多有 p^l 个解. 概括而言, 我们可以得到 $|C_G(\mathfrak{g}_{a,b,c})| \leq p^{3l+1}$. 易从 $(2p-3)l \geq 3$ 可知这个数小于 $q^2/p = p^{2pl-1}$. 这就证明我们需要的结论.

我们接着证明 $J(G) \leq G_{ab}$. 同上一段一样, 这只需要证明对 G_F 中任意元素 $\mathfrak{g}_{a,b,c}$ 且 $c \neq 0$ 都使它在 G_F 的中心化子（不是 G 中的中心化子）的大小比 q^2/p 小. 当 $\mathfrak{g}_{x,y,z} \in C_{G_F}(\mathfrak{g}_{a,b,c})$ 时, 它的 *Frobenius* 部分是平凡的（即 $\theta_{x,y,z} = 1$）, 于是等式(4.67)中的方程可以简化为 $cS_1(z) - zS_1(c) = 0$ 和 $2y = 2bc^{-1}z + zS_1(z) - zS_1(c)$. 记得我们有 S_1 是 $\mathbb{F}_p$-*l* 性的. 注意到 $\deg(S_1)$ 的限制, 我们可以看出最多存在 q/p^2 这样的 (y, z) 对. 因此 $C_{G_F}(\mathfrak{g}_{a,b,c})$ 的大小最多是 q^2/p^2.

因为 G_{ab} 是阿贝尔的, 所以我们断定 $J(G) = G_{ab}$, 并且它是唯一的最大阿贝尔子群, 而它的阶为 q^2/p. 证毕. □

我们下一个目标是确定 G 的幂零类的上下界. 我们先由 G 的中心开始. 记得 $G_A = \{\mathfrak{g}_{a,0,0,} : a \in \mathbb{F}_q\}$, 参考符号 *4.2.1*.

引理 4.51. 令 G 是由构造 4.16-4.19其中之一产生的群. 那么它的中心是 $Z(G) = \{\mathfrak{g}_{a,0,0} : a \in \mathbb{F}_{p^l}\}$.

证明. 取 $Z(G)$ 中一个元素 $\mathfrak{g}_{a,b,c}$. 首先我们证明 $\theta_1 = \theta_{a,b,c} = 1$. 假设 $\theta_1 \neq 1$. 如果三元组 (x, y, z) 满足 $\theta_2 = \theta_{x,y,z} = 1$, 那么等式(4.67)中的第三个方程可简化为 $z = z^{\theta_1}$,

即 z 属于 $\mathbb{F}_q$ 的真子域. 特别地, 至多存在 $\sqrt{q}$ 个 z's 使得存在一个三元组 (x, y, z) 满足 $\theta_{x,y,z} = 1$. 另一方面, 根据引理 *4.48*的性质 $(P1)$ 可知满足这样条件的三元组的数至少为 q/p: 矛盾. 这就证明 $\theta_1 = \theta_{a,b,c} = 1$.

接着, 我们证明 $c = 0$. 取 $(x, y, z) = (0, y_0, 0)$, 其中 y_0 是 $\mathbb{F}_q$ 中的某个元素以致 $\theta_{0,y_0,0} = 1$. 等式(4.67)中的第一个方程简化为 $2cy_0 = 0$, 于是就有 $c = 0$.

根据 $\theta_1 = 1$ 和 $c = 0$ 可将等式(4.67)中的方程简化为 $a^{\theta_2} - b^{\theta_2}z = a + bz$ 和 $b^{\theta_2} = b$, 其中 $\theta_2 = \theta_{x,y,z}$. 对满足 $z \neq 0$ 和 $\theta_{x,y,z} = 1$ 的三元组, 我们从第一个方程中推出 $2bz = 0$, 这意味着 $b = 0$. 并且等式(4.67)的方程可进一步简化为 $a^{\theta_{x,y,z}} = a$, 其中 x, y, $z \in \mathbb{F}_q$. 也就是说, $a^g = a$. 证毕. □

令 $g \in \mathrm{Aut}(\mathbb{F}_q)$ 使得对 $x \in \mathbb{F}_q$ 有 $g(x) = x^{p^l}$. 我们将 $\mathbb{F}_q$ 看作一个 $\mathbb{F}_{3^l}[\langle g\rangle]$ 模. 设 $R_0 := \mathbb{F}_q$, 并定义 $R_i := (1-g)^i(\mathbb{F}_q)$, 即 $R_i = \{(1-g)^i(x) : x \in \mathbb{F}_q\}$, 其中 $1 \leq i \leq p^e$, . 根据引理 *4.1*和 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^l}}(x) = (1-g)^{p^e-1}(x)$, 我们有 $R_{p^e-1} = \mathbb{F}_{p^l}$. 那么对每个 $0 \leq i \leq p^e - 1$ 有一个短正合列

$$0 \longrightarrow \mathbb{F}_{p^l} \xrightarrow{1} R_i \xrightarrow{1-g} R_{i+1} \longrightarrow 0.$$

由此断定 $\dim_{\mathbb{F}_p} R_i = (p^e - i)l$; 特别地, $R_{p^e} = 0$. 后面若有 $x - y \in R_i$, 我们记 $x \equiv y \pmod{R_i}$.

引理 4.52. 令 G 为来自构造 4.16-4.19其中一个中产生的群, 再令 p^e 为域自同构 g 的阶. 对于后面的三个构造, 我们进一步假设 $l > 1$. 对 $1 \leq i \leq p^e$, 我们有 $Z_i(G) := \{\mathfrak{g}_{a,0,0} : a \in (1-g)^{p^e-i}(\mathbb{F}_q)\}$. 特别地, $Z_{p^e}(G) = G_A$.

证明. 在 $i = 1$ 的情况下, 由引理 *4.51*和 $R_{p^e-1} = \mathbb{F}_{p^l}$ 即可推出结论. 于是我们不妨假设引理对 $1 \leq i \leq p^e - 1$ 成立, 接着我们打算证明结论 $i+1$ 时成立. 通过与前面的定理 *4.50*相似的论证, 我们能断定 $\mathfrak{g}_{a,b,c} \in Z_{i+1}(G)$ 当且仅当

$$\begin{aligned} a^{\theta_2} + x - b^{\theta_2}z + c^{\theta_2}y - c^{\theta_2}zS_1(z) \\ \equiv x^{\theta_1} + a - cy^{\theta_1} + bz^{\theta_1} - cz^{\theta_1}S_1(c) \pmod{R_{p^e-i}} \end{aligned} \tag{4.68}$$

以及等式(4.67)中的最后三个方程对所有 x, y, $z \in \mathbb{F}_q$ 都成立, 其中 $\theta_1 = \theta_{a,b,c}$, $\theta_2 = \theta_{x,y,z}$.

假定 $\mathfrak{g}_{a,b,c} \in Z_{i+1}(G)$. 通过与引理 *4.51*中一样的证明, 我们推出 $\theta_1 = 1$. 现在我们需要证明 $c = 0$. 在前面两个构造中, 对所有 $y_0 \in \mathbb{F}_q$ 有 $\theta_{0,y_0,0} = 1$; 在后面两个构造中, $\mathbb{F}_q$ 中有 q/p 个 y_0's 使得 $\theta_{0,y_0,0} = 1$. 于是对 $\mathbb{F}_q$ 中这样元素 y_0 取三元组 $(x, y, z) = (0, y_0, 0)$, 等式(4.68)就简化为 $2cy_0 \in R_{p^e-i}$, 其中 $1 \leq i \leq p^e - 1$. 如果

$c \neq 0$, 那么通过比较大小就得到一个矛盾. 这里我们在推导过程中对后面两个构造使用假设 $l > 1$. 因此我们推出当 $\mathfrak{g}(a,b,c) \in Z_{i+1}(G)$ 时就有 $c = 0$.

通过条件 $\theta_1 = 1$ 和 $c = 0$, $\mathfrak{g}_{a,b,c} \in Z_{i+1}(G)$ 的等价条件现在转化为 $b^{\theta_{x,y,z}} = b$ 和 $2bz \equiv a^{\theta_{x,y,z}} - a \pmod{R_{p^e-i}}$. 记得有 $U = \{c \in \mathbb{F}_q : \mathfrak{g}_{a,b,c} \in G_F\}$. 接着我们根据 $i = p^e - 1$ 与否将证明分成两种情况.

(1) 首先考虑情况 $i < p^e - 1$. 对每个 $z \in U$, 我们取一个三元组 (x,y,z) 使得 $\theta_{x,y,z} = 1$, 于是等式(4.68) 就简化为 $2bz \in R_{p^e-i}$. 由性质 $(P1)$, 我们通过在 $b \neq 0$ 比较大小推出一个矛盾, 这就意味着 $b = 0$. 于是等价条件就进一步简化为对所有 x, y, $z \in \mathbb{F}_q$ 有 $a^{\theta_{x,y,z}} - a \in R_{p^e-i}$, 或等价地, $a^g - a \in R_{p^e-i}$. 上式成立当且仅当 $a \in R_{p^e-i-1}$.

(2) 接着考虑情况 $i = p^e - 1$. 在这种情况中, $a^{g^k} - a = (g^k - 1)(a)$ 在 $k \geq 0$ 时总属于 $R_1 = R_{p^e-i}$, 于是等价条件就简化为对所有 x, y, $z \in \mathbb{F}_q$ 有 $b^{\theta_{x,y,z}} = b$ 和 $2bz \in R_1$. 我们因此通过比较大小断定 $b = 0$. 这时对 a 没有任何限制.

证毕. □

使用如引理 *4.52*中一样的符号和假设. 根据文献[73] 中的 *(9.7)* 可知 H 的幂零类等于 1 加上任何幂零群 H 的 $H/Z(H)$. 归纳起来, H 的幂零类等于 i 加上 $H/Z_i(H)$ 的幂零类. 由引理 *4.52*可知 G 的幂零类等于 p^e 加上 G/G_A 的幂零类, 其中 $p^e = o(g)$. 我们现在考虑 $\bar{G} := G/G_A = \{\bar{\mathfrak{g}}_{a,b,c} : b, c \in \mathbb{F}_q\}$ 的幂零类. 我们观察到 $\bar{\mathfrak{g}}_{a,b,c}$ 包含于 $Z(\bar{G})$ 当且仅当等式(4.67)中的最后三个方程对所有 y, $z \in \mathbb{F}_q$ 成立.

定理 4.53. *如果 G 是来自构造 4.16的群, 那么它幂零类是 2 或 3, 后者发生当且仅当* $\deg(S_1) > 1$.

证明. 在这种情况中下, 我们有 $p^e = 1$, 即 G 是线性的. 简记 $\bar{\mathfrak{g}}_{b,c} := \bar{\mathfrak{g}}_{a,b,c}$. 假定 $\bar{\mathfrak{g}}_{b,c} \in Z(\bar{G})$. 因为 $\theta_{x,y,z} \equiv 1$, 所以等式(4.67)中的最后三个方程简化后就等价于对所有 $z \in \mathbb{F}_q$ 有 $cS_1(z) = zS_1(c)$. 如果 $c \neq 0$, 那么 $S_1(z) = c^{-1}S_1(c)z$, 故 $\deg(S_1) \leq 1$. 因此当 $\deg(S_1) > 1$ 就有 $Z(\bar{G}) = \{\bar{\mathfrak{g}}_{b,0} : b \in \mathbb{F}_q\}$; 而且此时 $\bar{G}/Z(\bar{G})$ 是阿贝尔的, 即 $Z_2(\bar{G}) = \bar{G}$. 如果 $\deg(S_1) \leq 1$, 那么对所有 c, $z \in \mathbb{F}_q$ 有 $cS_1(z) = zS_1(c)$, 因此 $Z(\bar{G}) = \bar{G}$. 证毕. □

对于后面的三种构造, 群 G 的幂零类能在一个很大的范围内取值, 详见表 *4.1*. 在一般情况下, 给出幂零类的显式表达式是不可行的, 故作为替代品, 我们给出一个

合理且相对紧的上下界并且在假设 $l>1$ 下给出一些例子. 在接下来的叙述中, 我们改变我们的策略, 考虑 $\bar{G}=G/G_A$ 的下中心序列. 这里我们引入 $\bar{G}$ 的子群链如下:

$$\bar{G}_i:=\{\bar{\mathfrak{g}}_{a,b,c}:\, a,\, b\in\mathbb{F}_q,\, c\in R_i\},\quad 1\le i\le p^e, \tag{4.69}$$

其中 $R_i=(1-g)^i(\mathbb{F}_q)$. 特别地, 我们有 $\bar{G}_{p^e}=\bar{G}_B$, 其中 $\bar{G}_B:=\{\bar{\mathfrak{g}}_{b,0}:\, b\in\mathbb{F}_q\}$. 它们将有助于区别下中心链的子群 $\gamma_i(\bar{G})$'s.

取 $\bar{\mathfrak{g}}_{a,b,c}\in\bar{G}$. 当 $y,\, z\in\mathbb{F}_q$ 时, 我们设 $\bar{\mathfrak{g}}_{u,v,w}:=\bar{\mathfrak{g}}_{a,b,c}^{-1}\circ\bar{\mathfrak{g}}_{x,y,z}^{-1}\circ\bar{\mathfrak{g}}_{a,b,c}\circ\bar{\mathfrak{g}}_{x,y,z}$. 这里我们只需要关心下标 w, 其具体表达式是

$$w=(\theta_{0,y,z}-1)(c)-(\theta_{0,b,c}-1)(z). \tag{4.70}$$

定理 4.54. *令 G 为来自构造 4.17-4.19其中之一的群, 令 p^e 为域自同构 g 的阶, 再假设 $l>1$. 那么 G 的幂零类落在范围 $[2p^e,3p^e]$ 中.*

证明. 根据引理 *4.52*可知我们只需要证明 $\bar{G}=G/G_A$ 的幂零类落在范围 $[p^e,2p^e]$ 内. 记得 $U=\{c\in\mathbb{F}_q:\,\theta_{a,b,c}=1\}$, 简记 $\bar{\mathfrak{g}}_{b,c}=\overline{\mathfrak{g}_{a,b,c}}$, 再令 $\bar{G}_i$ 是在等式(4.69)中定义的子群. 对于这三种构造中每一种, 我们都有 $e\ge 1$.

我们断定对 $2\le i\le p^e$ 有 $\gamma_i(\bar{G})$ 包含于 $\bar{G}_{i-1}$ 但不包含于 $\bar{G}_i$, 并且 $\gamma_{p^e+1}(\bar{G})$ 是 $\bar{G}_{p^e}=\bar{G}_B$ 的子集, 其中 $\gamma_i(\bar{G})$ 是 $\bar{G}$ 的下中心链的第 i 项. 现在我们使用归纳法证明.

(1) 首先考虑情况 $i=2$. 根据性质 $(P1)$ 和假设 $l>1$ 可通过比较大小知道存在 $c\in U\setminus R_1$. 因为从等式(4.42)可知 $\theta_{a,b,c}$ 与 a 无关, 所以存在 $b\in\mathbb{F}_q$ 使得对这样的 c 有 $\theta_{a,b,c}=\theta_{0,b,c}=1$. 对选定一对 $(b,\,c)$ 和另外一对 $(y,\,z)=(0,\,t_C)$, 我们有 $w=c^g-c$, 其中 w 是如等式(4.70)中所示的. 于是 w 属于 $R_1\setminus R_2$, 即 $[\bar{\mathfrak{g}}_{b,c},\,\bar{\mathfrak{g}}_{0,t_C}]\in\bar{G}_1\setminus\bar{G}_2$. 另一方面, 对任意 $(b,\,c)$ 和 $(y,\,z)$, 其对应的元素 w 总是属于 R_1. 这就完成情况 $i=2$ 的证明.

(2) 假设已经证明了结论在 $2\le i\le p^e-1$ 时成立. 取 $\bar{\mathfrak{g}}_{b,c}\in\gamma_i(\bar{G})$. 我们有 $\theta_{0,b,c}=1$, 这是因为 $\gamma_i(\bar{G})$ 包含于 $\bar{G}'$. 于是等式(4.70) 可简化为 $w=(\theta_{0,y,z}-1)(c)$, 利用归纳法可知它总属于 R_i. 同样地, 通过归纳法可知存在 $\bar{\mathfrak{g}}_{b,c}\in\gamma_i(\bar{G})$, 其中 $c\in R_{i-1}\setminus R_i$. 取 $(y,\,z)=(0,\,t_C)$, 以及对应地有 $w=(g-1)(c)$. 元素 w 属于 $R_i\setminus R_{i+1}$. 这完成情况 $i+1$ 的证明.

对于 $\gamma_{p^e+1}(\bar{G})$ 的结论可以用跟 *(2)* 一样的方法证明. 当 $\gamma_{p^e+1}(\bar{G})$ 时, 易得 $c\in R_{p^e-1}/R_{p^e}=\mathbb{F}_{p^l}$, 因此从等式(4.70)中可得 $w=(g-1)(c)=0$. 这就证明我们的说法. 特别地, $\gamma_{p^e+1}(\bar{G})$ 包含于 $\bar{G}_B$ 但不包含于 $\gamma_{p^e}(\bar{G})$. 这给出 $\bar{G}$ 的幂零类的下界.

因为 $\gamma_{p^e+1}(\bar{G})$ 具有平凡的 *Frobenius* 部分, 所以它包含于 $\bar{G}_B$ 的子群 $H := \{\bar{\mathfrak{g}}_{b,0} : \theta_{0,b,0} = 1\}$. 在构造 *4.17*中, 我们有 $K_B = \mathbb{F}_q$; 而在构造 *4.18*和 *4.19*中, 我们有 $K_B = \{b : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mu_B b) = 0\}$. 于是我们现在定义 $e_0(H) := H$, 并且归纳地对 $i \geq 1$ 定义 $e_{i+1}(H) := [e_i(H), \bar{G}]$. 那么通过归纳法我们推出对 $i \geq 1$ 有 $\gamma_{p^e+i}(\bar{G}) \leq e_{i-1}(H)$. 于是用常规方法可以验证 $\bar{\mathfrak{g}}_{b,0}^{-1} \circ \bar{\mathfrak{g}}_{y,z}^{-1} \circ \bar{\mathfrak{g}}_{b,0} \circ \bar{\mathfrak{g}}_{y,z} = \bar{\mathfrak{g}}_{-b+b^{\theta_{0,y,z}},0}$. 这样就很容易地用归纳法得到 $e_i(H) = \{\bar{\mathfrak{g}}_{b,0} : b \in (1-g)^i(K_B)\}$, 其中 $1 \leq i \leq p^e$. 特别地, $e_{p^e}(H) = \{1\}$, 故 $\gamma_{2p^e+1}(\bar{G}) = 1$. 于是这就确定了 $\bar{G}$ 的幂零类的上界. □

在表 *4.1*中, 我们已经列出构造 *4.17*和 *4.18*中在有些特殊情况产生的点正则群的幂零类的显式值. 我们用下面的例子演示一下我们的计算过程, 实际的计算过程会比想象中的复杂, 于是我们省略表中某些情况下的细节.

例子 4.55. 在这个例子中, 我们将给出来自构造 4.17 的群 G 在表 4.1所列出的特殊情况下的上中心序列. 特别地, 上中心序列的前面 p 项 $Z_i(G), 1 \leq i \leq p$ 都已经在引理 4.52中确定, 故我们在这里不再重复地给出. 记得此时有 $q = p^{pl}$, $g(x) = x^{p^l}$, 并且我们设 $\mu_C = 1$, $K = \{x \in \mathbb{F}_q : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = 0\}$. 于是进一步地假设 $l > 1$. 像平常一样, 令 $R_0 := \mathbb{F}_q$ 和 $R_i := (1-g)^i(\mathbb{F}_q)$ 其中 $1 \leq i \leq p$.

(1) 如果 $S_1(z) \equiv 0$, 那么

$$Z_{p+i}(G) = \{\mathfrak{g}_{a,b,c} : a \in \mathbb{F}_q, b, c \in (1-g)^{p-i}(\mathbb{F}_q)\}, \quad 0 \leq i \leq p.$$

(2) 如果 $S_1(z) = z^{p^k}$ 且 $l \nmid k$, 那么

$$Z_{p+i}(G) = \{\mathfrak{g}_{a,b,0} : a \in \mathbb{F}_q, b \in R_{p-i}\}, \quad 0 \leq i \leq p,$$
$$Z_{2p+i}(G) = \{\mathfrak{g}_{a,b,c} : a, b \in \mathbb{F}_q, c \in R_{p-i}\}, \quad 0 \leq i \leq p.$$

(3) 如果 $S_1(z) = (1-g)^k(z)$ 其中 $1 \leq k \leq p-1$, 那么 $Z_{p+i}(G), 1 \leq i \leq p-k$ 的表达式就跟情况 (2) 中一样, 并且

$$Z_{2p-k+j}(G) = \{\mathfrak{g}_{a,b,c} : a \in \mathbb{F}_q, b \in R_{k-j}, c \in R_{p-j}\}, \quad 1 \leq j \leq k,$$
$$Z_{2p+j}(G) = \{\mathfrak{g}_{a,b,c} : a, b \in \mathbb{F}_q, c \in R_{p-k-j}\}, \quad 1 \leq j \leq p-k.$$

在表 4.1中 G 在其他情况时上中心序列可以用类似的方式推导得出, 这里我们省略这些细节.

4.8 小结

在本节中, 我们已经确定了经典辛对称四边形 $\mathcal{Q} = W(q)$ 在 q 是奇数时的 *Payne* 派生四边形 $\mathcal{Q}^P$ 的所有点正则群. 通过计算不同构造的点正则群的某些群不变量, 如 *exponents* 和 *Thompson* 子群等, 我们就解决了这些构造产生群的同构性问题. 我们还得到了构造出来的群的幂零类的严格上下界. 作为一个推论, 我们能看出正则地作用在一个有限广义四边形的点集上的有限群可以有无穷大的幂零类. 在我们的工作之前, 唯一已知的这样的群的幂零类最多为 *3*, 除了用计算机搜索得到小参数的例子的幂零类大小.

在第 *4.5*节中, 我们也已经确定了偶特征情况下 $\mathrm{PGL}(4, q)$ 中 $\mathcal{Q}^P$ 的所有点正则群. 事实上, q 是偶数时也存在一些平行于构造 *4.37*, 构造 *4.42* 以及构造 *4.46*的结果, 但是我们在这里就不进行叙述, 这是因为考虑到文章的篇幅, 不过这些构造的核心想法跟奇数的情况是一样的. 进一步而言, 计算机的数据结果说明了当 $q = 2^4$ 时具有满足 $r_{A,B} = 2$ 条件的例子, 这意味着可能存在更多不同于奇特征情况的构造. 如何对偶数特征情形进行完全的分类仍然是一个具有挑战性的问题.

5 有限 *Hermitian* 极空间中的传递 *ovoids*

5.1 介绍

一个秩为 $r > 2$ 的有限极空间 $\mathcal{P}$ 中的一个 *ovoid* 是 $\mathcal{P}$ 中的射影点集使得它与每个极大完全奇异或迷向子空间都恰好有一个公共点. 如果存在一个 *ovoid,* 那么它的大小被称作 *ovoid* 数 *(ovoid number),* 记作 $\theta(\mathcal{P})$. 或者说, $\mathcal{P}$ 中的一个 *ovoid* 是 $\mathcal{P}$ 中包含 $\theta(\mathcal{P})$ 个点的集合以致里面任意两点都是不正交的. 由于 *ovoids* 与各种几何对象以及组合学的其它分支有着密切的联系, 因此 *ovoids* 的相关相究得到广泛的关注, 详见文献[38,39]. 在过去 *40* 年中, 关于 *ovoids* 的概念有两个主要的推广, 即 *m-systems* 和 *intriguing sets*. 请参考文献[4] 中的第七章和文献[80] 及其里面的参考文献去获得更多信息.

令 V 是一个 $(n+1)$ 维 $\mathbb{F}_{q^2}$-线性空间, 并且赋予一个非退化 *Hermitian* 型 $h : V \times V \to \mathbb{F}_{q^2}$. 令 $\mathrm{PG}(V)$ 是 V 所对应的射影空间, 用 $\langle v \rangle$ 表示射影点, 即由非零向量 v 张成的一维向量空间. (V, h) 对应的 *Hermitian* 极空间 $H(n, q^2)$ 是由 V 中关于 h 的完全迷向子空间构成的, 以包含为其关联关系. $H(n, q^2)$ 中最大完全迷向子空间的维数是 $r = \lfloor (n+1)/2 \rfloor$, 于是 $H(n, q^2)$ 的秩是 r. 在 $n > 2$ 是偶数的情况下, $H(n, q^2)$ 不存在 *ovoids,* 详情可参考文献[38]. 在 $n \geq 3$ 是奇数的情况下, $H(3, q^2)$ 有很多 *ovoids,* 但是除了文献[40–42] 中的不存在性的结果, 人们对 $n > 3$ 时的 *ovoids* 了解甚少. 令 n 是奇数并且 O 是 $H(n, q^2)$ 中的一个 *ovoid.* 那么 O 的 *ovoid* 数是 $q^n + 1$. 对于 $H(n, q^2)$ 中的射影点 P, 我们有以下结果

$$|P^{\perp} \cap O| = \begin{cases} 1, & \text{if } \ P \in O \\ q^{n-2} + 1, & \text{if } \ P \notin O \end{cases}, \tag{5.1}$$

具体可参考文献[80]. 这里 $\perp$ 是与 $H(n, q^2)$ 关联的极性 *(polarity).* 显而易见, 对于每个 $g \in \mathrm{P\Gamma U}(n+1, q^2)$, $g(O)$ 也是一个 *ovoid*; 于是我们说 $g(O)$ 与 O 是射影等价的. 秩为 *r* 的 *Hermitian* 极空间中所有已知 *ovoids* 都是属于 $H(3, q^2)$. 特别地, $H(3, q^2)$ 的一个非退化的平面截面是经典 *ovoid,* 并且 $H(3, q^2)$ 中所有经典的 *ovoids* 都是射影等价的. 值得一提的是, 这里有一个强大的方法能从 $H(3, q^2)$ 的一个旧的 *ovoid* 中获得新的 *ovoids,* 这种方法被称为派生法 *(derivation),* 是由 *Payne* 和 *Thas* 最先提出的[81]. 具体而言, 取定 $H(3, q^2)$ 中一个 *ovoid* O, 再取 $\mathrm{PG}(3, q^2)$ 中一条交 O 于 $q+1$ 个点的线 ℓ. 令 O' 是通过去掉 O 在 ℓ 上所有的点以及加上 $\ell^{\perp}$ 上的迷向点而得到与 O 的大小一样的集合. 这样得到的 O' 也是 $H(3, q^2)$ 中的 *ovoid.* 当 q 是偶数时, 还有一类我们后面会提到的 *ovoids* 叫 *Singer-type ovoids,* 它们是由经典 *ovoids* 通过多重派生法

(multiple derivations) 得到的.

对于 $H(n,q^2)$ 中的一个 *ovoid,* 如果存在 $\mathrm{P\Gamma U}(n+1,q^2)$ 中的一个子群 H 固定 O 的点集并且它在 O 上的作用是传递的, 那么我们称它是传递的 *(transitive).* 如果 H 是 $\mathrm{PGU}(n+1,q^2)$ 的子群, 那么这个 *ovoid* 就被称为线性传递的 *(linearly transitive).* 在 $H(3,q^2)$ 中, 经典 *ovoids* 都是线性传递 *ovoids,* 而且它们的全稳定子群都有非阿贝尔因子 $\mathrm{PSU}(3,q^2)$. 当 $q>2$ 是偶数时, *Cossidente* 和 *Korchmáros*[1] 在 $H(2,q^2)$ 的循环 *spreads*[43] 的基础上构造出 $H(3,q^2)$ 中的新一类传递 *ovoids,* 并将其命名为 *Singer-type ovoids.* 这类 *ovoids* 的全自同构群是 $\mathrm{P\Gamma U}(4,q^2)$ 中的可解群. 在同一篇文献中, 他们将 q 为偶数时 $H(3,q^2)$ 中所有线性传递 *ovoids* 进行了分类, 并说明了这样的 *ovoids* 只能是经典的 *ovoids* 和 *Singer-type ovoids.* 这里要注意的是最小的情况 $q=2$ 是应归功于 *Brouwer* 和 *Wilbrink*[82], 他们完成这种情况下所有 *ovoids* 的分类. *2009* 年 *Bamberg* 和 *Penttila*[2] 对有限极空间中具有不可解传递自同构群的 *ovoids* 进行分类, 主要是利用文献[83] 中深刻的结果. 在 $H(n,q^2)$ 和 $n>3$ 中不存在这样的传递 *ovoids.* 在奇特征情况下, 除了经典 *ovoids* 以外, 只有在 $q=5$ 时 $H(3,q^2)$ 中才存在这样的稀疏的例子. 如果读者有兴趣的话, 可以去查阅文献[2] 去了解其他经典极空间中传递 *ovoids* 的分类结果.

在这章中, 我们对 $H(3,q^2)$ 的传递 *ovoids* 进行了完整的分类, 并且说明对于给定奇整数 $n\geq 5$, $H(n,q^2)$ 不存在传递 *ovoid.* 精确来说, 我们证明以下定理.

定理 5.1. 令 q 是素数幂和 $n\geq 3$ 是正整数. 假定 O 是 $H(n,q^2)$ 中的一个传递 ovoid. 那么 $n=3$, 并且 O 射影等价于下面其中一类 ovoids:

(1) 经典的 ovoid $H(2,q^2)$, 其中它的全稳定子群是 $\Gamma\mathrm{U}(3,q^2)$;

(2) 偶特征下 Singer-type ovoid, 其中它的全稳定子群同构于 $\mathbb{Z}_2\times(\mathbb{Z}_3\times\mathrm{PSL}(2,7)):2$;

(3) $H(3,5^2)$ 中例外的 ovoid, 其中全稳定子群同构于 $\mathbb{Z}_2\times(\mathbb{Z}_3\times\mathrm{PSL}(2,7)):2$;

(4) $H(3,8^2)$ 中某个 ovoid, 其中它的全稳定子群同构于 $\mathbb{Z}_{57}:9$;

(5) $H(3,8^2)$ 中某个 ovoid, 其中它的全稳定子群同构于 $\mathbb{Z}_{57}:18$.

注 5.2. 请查阅文献[2] 去了解 $H(3,5^2)$ 中这个特殊的 ovoid 的描述, 其构造是基于文献[84] 中发现的 $H(2,5^2)$ 中的一个 unital spread 而获得的. 对于 Singer-type ovoids 和 $H(3,8^2)$ 中两个稀疏的例子的描述, 请分别参考例子 5.9和例子 5.10.

本章结构安排如下所示. 在第 *5.2*节中, 我们首先展示一些初步结果和准备工作. 在第 *5.3*节中, 我们介绍将在本章中使用的 $H(n,q^2)$ 的模型, 其中 n 是奇数. 我们研究特定的 q^n+1 阶 *Singer* 群的轨道以及确定它们在什么情况下组成 $H(n,q^2)$ 的 *ovoids*. 特别地, 在 $n=3$ 和 q 是偶数时我们给出 *Singer-type ovoids* 的代数描述. 在第 *5.4*节中, 我们先推导出具有 $\mathrm{P\Gamma U}(n+1,q^2)$ 中的可解稳定子群的 *transitive ovoids* 的参数限制, 之后给出主要定理 *(*定理 *5.1)* 的证明.

5.2 准备工作

在这篇文章中, 让 p 是素数, d 是正整数以及 n 是大于等于 3 的奇整数. 设 $q=p^d$, 取 ω_0 是 $\mathbb{F}_{q^{2n}}$ 中的 $(q^n+1)(q-1)$ 阶固定元素, 以及记 $\omega=\omega_0^{q-1}$. 如果 E 是有限域 F 的有限次域扩张, 我们使用符号 $\mathrm{Tr}_{E/F}$ 去表示从 E 到 F 的相应迹函数.

5.2.1 技术引理

在这子节中, 我们将介绍一些后面需要的引理.

引理 5.3. 令 ω_0 分别是 $\mathbb{F}_{q^{2n}}$ 中的 $(q^n+1)(q-1)$ 阶元并且 $\omega=\omega_0^{q-1}$, 再设 $W:=\mathbb{F}_{q^n}^*\cdot\langle\omega\rangle$. 那么在 q 是偶数时 $\mathbb{F}_{q^{2n}}^*=W$, 而在 q 是奇数时 $\mathbb{F}_{q^{2n}}^*=W\cup W\omega_0$.

证明. 当 q 是奇数时, 因为 $\gcd(q^n+1,q^n-1)=2$, 所以 W 是 $\mathbb{F}_{q^{2n}}^*$ 中 *index* 为 *2* 的乘法群; 而且 $\frac{q^{2n}-1}{(q^n+1)(q-1)}=q^{n-1}+q^{n-2}+\cdots+1$ 是奇数, 故 ω_0 是 $\mathbb{F}_{q^{2n}}^*$ 中的非平方元. 这样就很容易推出奇数时的结论. 在 q 是偶数时, 我们可以直接根据事实 $\gcd(q^n+1,q^n-1)=1$ 即可推出结论. □

引理 5.4. 使用引理 5.3中定义的符号, 且假设 $n=3$. 令 x 是 $\langle\omega\rangle\setminus\mathbb{F}_{q^2}$ 中的元素. 那么 $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x)\neq 1$.

证明. 我们现在使用反证法证明. 假设 x 是 $\langle\omega\rangle\setminus\mathbb{F}_{q^2}$ 中的元素且满足 $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x)=1$. 记 $s:=x^{1+q^2+q^4}$, 它属于 $\mathbb{F}_{q^2}^*$. 接着我们计算

$$\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x^{q^2+q^4})=s\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x^{-1})=s\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x^{q^3})=s.$$

因为 $x\notin\mathbb{F}_{q^2}$, 所以 x 在 $\mathbb{F}_{q^2}$ 上的极小多项式是

$$\begin{aligned}(X-x)(X-x^{q^2})(X-x^{q^4})&=X^3-\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x)X^2+\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(x^{q^2+q^4})X-s\\&=X^3-X^2+sX-s.\end{aligned}$$

然而, 因式分解这个多项式后可得 $(X-1)(X^2+s)$：这与假设 $x \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ 相矛盾. 证毕. □

引理 5.5. 假定 $\gcd(n,e)=1$. 那么对于所有 $x \in \mathbb{F}_{q^n}$ 有 $\mathrm{Tr}_{\mathbb{F}_{q^{ne}}/\mathbb{F}_{q^e}}(x) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$, 并且 $\mathbb{F}_{q^e}$ 的一组 $\mathbb{F}_q$-线性基也是 $\mathbb{F}_{q^{ne}}$ 的一组 $\mathbb{F}_{q^n}$-线性基.

证明. 取 $x \in \mathbb{F}_{q^n}$ 使得 $x^{q^n} = x$. 因为 $\gcd(n,e)=1$, 我们有 $\{ie \pmod n : 0 \le i \le n-1\} = \{0, \cdots, n-1\}$, 所以

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{q^{ne}}/\mathbb{F}_{q^e}}(x) &= x + x^{q^e} + \cdots + x^{q^{e(n-1)}} \\ &= x + x^q + \cdots + x^{q^{n-1}} = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x).\end{aligned}$$

令 $\zeta_1, \cdots, \zeta_e$ 是 $\mathbb{F}_{q^e}$ 的一组 $\mathbb{F}_q$-线性基. 假定对某个 $c_i \in \mathbb{F}_{q^n}$ 有 $\sum_{i=1}^{e} c_i\zeta_i = 0$. 则对于任意 $x \in \mathbb{F}_{q^n}$, 我们根据之前的结果就有

$$0 = \mathrm{Tr}_{\mathbb{F}_{q^{ne}}/\mathbb{F}_{q^e}}(x \cdot \sum_{i=1}^{e} c_i\zeta_i) = \sum_{i=1}^{e} \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c_i x)\zeta_i$$

因为 ζ_i's 这些元素构成一组 $\mathbb{F}_q$-线性基, 所以对每个 i 和 $x \in \mathbb{F}_{q^n}$ 都有 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c_i x) = 0$, 也就是说, 对每个 i 有 $c_i = 0$. 证毕. □

5.2.2 Blokhuis 和 *Moorhouse* 的界

对于正整数 n 和素数 p, 定义下面的函数：

$$F(n,p) := \frac{1}{p^n}\binom{n+p-1}{n}^2 - \frac{1}{p^n}\binom{n+p-2}{n}^2. \tag{5.2}$$

定理 5.6. (推论 1.3, Moorhouse[42]) 令 $q = p^d$ 为素数幂, 其中 p 是素数和 n 是奇整数. 如果 $H(n,q^2)$ 包含一个 ovoid, 那么 $F(n,p) \ge 1$.

因为 $\binom{n+p-1}{n} = \frac{n+p-1}{n}\binom{n+p-2}{n-1}$ 和 $\binom{n+p-2}{n} = \frac{p-1}{n}\binom{n+p-2}{n-1}$, 所以我们有

$$F(n,p) = \binom{n+p-2}{n-1}^2 \frac{n+2p-2}{np^n}.$$

同时, 我们有 *Stirling* 估计*[85]*, 如下所示：

$$n! = (ne^{-1})^n\sqrt{2\pi n}e^{\alpha_n}, \quad \frac{1}{12n+1} < \alpha_n < \frac{1}{12n}. \tag{5.3}$$

引理 5.7. 令 n 是正整数和 p 是素数. 令 $F(n,p)$ 为如等式(5.2)所示的函数.

(1) 如果 $p > 3, n \ge (p+1)/2$ 或 $p \le 3, n \ge p+1$, 那么 $F(n+1,p) < F(n,p)$;

(2) 对于素数 $p > 45$, 我们有 $F((p+1)/2, p) < 1$.

证明. 因为 $\binom{n+p-1}{n} = \frac{n+p-1}{n}\binom{n+p-2}{n-1}$, 所以我们有

$$\begin{aligned} & \frac{n^2(n+1)p^{n+1}}{\binom{n+p-2}{n-1}^2} \cdot (F(n,p) - F(n+1,p)) \\ = \ & pn(n+1) \cdot (n+2p-2) - n^2 \cdot \tfrac{(n+p-1)^2}{n^2} \cdot (n+2p-1) \\ = \ & (p-1) \cdot (n^3 + (2p-3)n^2 - 3(p-1)n - 2p^2 + 3p - 1). \end{aligned}$$

记 $f(n,p) := n^3 + (2p-3)n^2 - 3(p-1)n - 2p^2 + 3p - 1$. 因此 $F(n,p) - F(n+1,p) > 0$ 当且仅当 $f(n,p) > 0$. 令 p 是固定的素数. 因为

$$f'(n,p) = 3n^2 + (4p-6)n - 3(p-1) = n^2 + 2n(n-1) + (p-1)(4n-3) > 0,$$

所以函数 $f(n,p)$ 在 $n \geq 1$ 时是关于 n 单调递增的. 于是我们可以直接计算

$$f\left(\frac{p+1}{2}, p\right) = \frac{1}{8}(p-1)(5p^2 - 18p + 1),$$

它的值在 $p > 3$ 时是正的. 而在 $p = 2, 3$ 时, 我们有 $f(p+1,p) = p(3p^2 - p + 2) > 0$. 这就证明第一个结果.

我们有 $\frac{p+1}{2} + p - 2 = \frac{3}{2}(p-1)$, 由等式(5.3)即可推出

$$\binom{3(p-1)/2}{(p-1)/2} = \frac{\left(\frac{3}{2}(p-1)\right)!}{\left(\frac{p-1}{2}\right)! \cdot (p-1)!} = \frac{3^{(3p-2)/2}}{2^{p-1}\sqrt{2\pi(p-1)}} e^{\beta}$$

其中 $\beta = \alpha_{3(p-1)/2} - \alpha_{(p-1)/2} - \alpha_{(p-1)}$. 因为 $\frac{1}{12n+1} < \alpha_n < \frac{1}{12n}$, 所以我们有

$$\beta < \frac{1}{18(p-1)} - \frac{1}{12(p-1)+1} - \frac{1}{6(p-1)+1} < 0.$$

接着我们计算

$$\begin{aligned} F((p+1)/2, p) &= \frac{3^{3p-2}}{4^{p-1} \cdot 2\pi(p-1)} \cdot \frac{5p-3}{p^{(p+1)/2}(p+1)} e^{2\beta} \\ &= \left(\frac{6.75^2}{p}\right)^{(p-1)/2} \frac{3(5p-3)}{2\pi p(p^2-1)} e^{2\beta}. \end{aligned}$$

因为 $6.75^2 = 45.5625$, $3(5p-3) < 15p < 2\pi p(p^2-1)$ 以及 $\beta < 0$, 所以我们推出所需的结论：在 $p > 45$ 时 $F((p+1)/2, p) < 1$. 证毕. □

因此, 对于固定的素数 p, $F(X,p)$ 在 X 大于某一个特定数时是单调递减的, 同时易验证存在正整数 x_0 使得 $F(x_0,p) < 1$, 这就意味着只要 n 足够大就有 $F(n,p) < 1$.

5.2.3 本原素因子

对于整数 x 和 k 且 $x, k \geq 2$, $x^k - 1$ 的本原素因子 *(primitive prime divisor)* 是 $x^k - 1$ 的素因子 r 且对所有 $1 \leq k' < k$ 都不整除 $x^{k'} - 1$. 换句话说, $x \mod r$ 的阶是 k. 作为一个推论, 我们有 $r \equiv 1 \pmod{k}$. 根据 *Zsigmondy* 定理[86] 可知 $x^k - 1$ 至少有一个本原素因子除非 $(x, k) = (2, 6)$ 或 $k = 2$ 和 $x + 1$ 是 2 的幂. 我们记这样的素数为 x_k. 注意, 如果 $(x, k) \neq (2, 3)$, 那么 $x^k + 1$ 能被 $x^{2k} - 1$ 的本原素因子 x_{2k} 整除.

本原素因子在研究具有特定传递条件的几何对象中起着重要的作用, 详情可参考文献[2,87]. 在本章研究的问题中, 我们具有比本原素因子的存在性更强的条件. $x^k - 1$ 因子 r 与每个 $x^i - 1$ 都是互素的, 其中 $1 \leq i \leq k$, 那么我们称它是 $x^k - 1$ 的本原因子 *(primitive divisor)*, 同时我们称 $x^k - 1$ 中最大本原因子 $\Phi_k^*(x)$ 为本原部分 *(primitive part)*. 易知 $\Phi_k^*(x)$ 的每个素因子都是 $x^k - 1$ 的本原素因子, 故倘若有 $\Phi_k^*(x) > 1$, 则 $\Phi_k^*(x) \equiv 1 \pmod{k}$; 相反地, $x^k - 1$ 每个本原素因子整除 $\Phi_k^*(x)$.

令 n 是一个奇整数并且 $n \geq 3$, 再设 $q = p^d$, 其中 p 是素数. 在环绕空间 V 中赋予 *Hermitian* 型来构造出一个 *Hermitian* 极空间, 假设 O 是 *Hermitian* 极空间中的传递 *ovoid*, 再令 H 是 $\mathrm{P\Gamma U}(n+1, q^2)$ 中这个 *ovoid* 的稳定子群. 当 $(q, n) = (2, 3)$ 时, 根据文献[82] 可知 O 要么是经典 *ovoid* 或者 *Singer-type ovoid*. 故**我们在本章之后讨论里假设** $(q, n) \neq (2, 3)$. 特别地, 我们总有 $\Phi_{2nd}^*(p) > 1$. 因为 $\Phi_{2nd}^*(p)$ 模 $2nd$ 同余于 1, 所以我们有 $\gcd(2nd, \Phi_{2nd}^*(p)) = 1$. 于是子群 $H \cap \mathrm{PGU}(n+1, q^2)$ 的阶能被 $\Phi_{2nd}^*(p)$ 整除. 因为 H 是不可解的情况已经在文献[2] 的定理 *4.3* 中解决, 所以我们只需要考虑 H 是可解的情况. 我们将需要使用文献[88] 中主要定理的可解部分, 具体如下所示, 其中它的证明依赖于文献[83] 的结果.

定理 5.8 ((Bamberg 和 Penttila[88], **定理** 4.2)). 令 p 是素数, $q = p^d$ 且 n 是奇整数使得 $n \geq 3$, $(p, nd) \neq (2, 3)$. 令 V 是一个 $n+1$ 维 $\mathbb{F}_{q^2}$-线性空间, 再令 h 是 V 上一个非退化的 Hermitian 型, 其中具有线性等距群 $\mathrm{GU}(n+1, q^2)$. 如果 $\mathrm{GU}(n+1, q^2)$ 中的可解群 G 的阶能被本原因子 $\Phi_{2nd}^*(p)$ 整除, 那么 G 固定一个 n 维子空间或商空间以及 $G^U \leq \Gamma\mathrm{U}(1, q^{2n})$, 其中 G^U 是从 G 对 U 的诱导作用中获得的. 此外, G^U 的阶能被 $\Phi_{2nd}^*(p)$ 整除.

根据之前的备注可知定理 *5.8*适用于 $H \cap \mathrm{PGU}(n+1, q^2)$ 在 $\mathrm{GU}(n+1, q^2)$ 中的完全原像. 因此, 存在被 H 固定的非迷向 1 维子空间 $P = \mathbb{F}_{q^2} \cdot v$ 使得 $U = P^\perp$ 或 $U = V/P$, 参考文献[89] 的命题 *4.1.4, 4.1.18* 或文献[79] 的表格 *2.3*. 因为 $\mathrm{P\Gamma U}(n+1, q^2)$ 传递地作用在所有非迷向点, 如果有必要将 O 替换成某个 $g(O)$ 其中 $g \in \mathrm{P\Gamma U}(n+1, q^2)$, 我们就选取 P 为特定的非迷向 1 维子空间. 此外, 根据文献[88] 的定理 *3.1*, 定理 *5.8*的群 G

模数乘对角矩阵后, 它的商像恰好是扩域形式的子群 *(Extension field case Example),* 并且由[89] 的命题 *4.3.6* 可得这样的群在 $\mathrm{P\Gamma U}(n, q^2)$ 里只有唯一一个共轭类.

5.3 $H(n, q^2)$ 的模型和 *Singer* 轨道

令 $n \geq 3$ 是奇整数. 设 $V := \mathbb{F}_{q^2} \times \mathbb{F}_{q^{2n}}$, 而且将其看做成 $(n+1)$ 维 $\mathbb{F}_{q^2}$-线性向量空间. 我们赋予它一个 *Hermitian* 型, 具体如下所示:

$$h((a, x)) = a^{q+1} - \mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}}(x^{q^n+1}), \quad \text{for } (a, x) \in V.$$

令 $H(n, q^2)$ 是用上述的 *Hermitian* 型定义的 *Hermitian* 极空间. 于是我们可定义

$$\begin{aligned} \psi: &\ (a, x) \mapsto (a, \omega x), \\ \phi: &\ (a, x) \mapsto (a^p, x^p), \end{aligned} \tag{5.4}$$

其中 ω 是之前定义的 $q^n + 1$ 阶元. 以上定义的两个映射都可看做成 $\mathrm{P\Gamma U}(n+1, q)$ 中元素且固定射影点 $P = \langle (1, 0) \rangle$. 令 G 是由 ψ 和 ϕ 生成的子群, 其群阶为 $2nd(q^n + 1)$. 设 $U := P^\perp$ 为 P 关于 *Hermitian* 型定义的对偶线性空间. 那么 G 也保持 U 不变. 我们用 $\langle S \rangle_{\mathbb{F}_{q^2}}$ 来表示由 S 张成的 $\mathbb{F}_{q^2}$-线性子空间.

例子 5.9. 取 $n = 3$, 并假设 q 是偶数. 射影点 $\langle (1, 1) \rangle_{\mathbb{F}_{q^2}}$ 在群 $G = \langle \psi, \phi \rangle$ 作用下的轨道 O 是 $H(3, q^2)$ 中的 ovoid, 并且当 $q > 2$ 时它恰好以 G 为全稳定子群. 在 $q = 2$ 的情况下, O 的全稳定子群的阶为 324. $H(3, q^2)$ 中任何与 O 射影等价的 ovoid 都是 *Singer-type* ovoid. 这个例子是在文献[1] 中发现的, 同时它的全稳定子群也在该文献中确定. 我们将会在后面的引理 5.13中证明 Singer-type ovoid 具有上述的代数描述.

例子 5.10. 取 $q = 8$ 和 $n = 3$, 再令 γ 是 $\mathbb{F}_{2^9}$ 的一个本原元且它在 $\mathbb{F}_2$ 上的极小多项式是 $X^9 + X^4 + 1$. 通过 Magma[69] 进行穷尽的计算机搜索, 我们发现在射影等价意义下还存在两个以 $\mathrm{P\Gamma U}(4, 8^2)$ 中可解群为自同构群的传递 ovoids, 具体如下所示:

(1) $\langle (1, \gamma^{39}) \rangle$ 在子群 $H_1 = \langle \psi^9, \psi^3\phi^2 \rangle$ 作用下得到的轨道 O_1 是传递 ovoid.

(2) $\langle (1, \gamma^{109}) \rangle$ 在子群 $H_2 = \langle \psi^9, \phi \rangle$ 作用下得到的轨道 O_2 是传递 ovoid.

在这两种情况下, H_i 是 O_i 在 $\mathrm{P\Gamma U}(4, 8^2)$ 中的全稳定子群, 其中 $i = 1, 2$.

我们定义以下的群同态:

$$\eta: G \to \mathrm{Aut}(\mathbb{F}_{q^{2n}}),\ \psi^j\phi^i \mapsto \phi^i. \tag{5.5}$$

那么 $\ker(\eta) = \langle \psi \rangle$, 而且 η 是满射的. 特别地, G 的群结构是 $\mathbb{Z}_{q^n+1} : 2nd$. 于是我们在下面的引理中总结一些 G 的基本性质.

引理 5.11. 令 G 是上面定义的群. 那么下面的结论成立.

(1) $\phi\psi\phi^{-1}=\psi^{p}$, 并且对于非负整数 l,k,i 都使下面等式成立:

$$(\psi^{l}\phi^{k})^{i}=\psi^{(p^{ki}-1)l/(p^{k}-1)}\phi^{ki}.$$

(2) 如果 $g\in G\setminus\langle\psi\rangle$ 是 2 阶元, 那么对某个整数 j 有 $g=\psi^{j}\phi^{nd}$.

证明. 我们省略结论 (1) 的证明, 这是因为证明是通过常规的计算去直接验证. 于是我们开始 (2) 的证明, 假定 $g=\psi^{l}\phi^{k}$ 是 2 阶元, 其中 $1\leq k\leq 2nd-1$. 那么根据 (1) 我们有 $2nd|2k$ 和 $q^{n}+1|(1+p^{k})l$, 于是从这些论据中我们推出 $k=nd$. 这就完成了 (2) 的证明. □

对 *Hermitian* 极空间 $H(n,q^{2})$ 的射影点 $\langle(1,y)\rangle$, 该点 $\langle(1,y)\rangle$ 对应的 *Singer* 轨道是该点在 $\langle\psi\rangle$ 作用下的像, 即

$$S_{y}:=\{\langle(1,\omega^{i}y)\rangle:0\leq i\leq q^{n}\}. \tag{5.6}$$

令 ω_{0} 是 $(q^{n}+1)(q-1)$ 阶元以及 $\omega=\omega_{0}^{q-1}$. 由引理 *5.3*可知, *Singer* 轨道 S_{y} 包含点 $\langle(1,x)\rangle_{\mathbb{F}_{q^{2}}}$ 或点 $\langle(1,x\omega_{0})\rangle_{\mathbb{F}_{q^{2}}}$, 其中 x 是 $\mathbb{F}_{q^{n}}^{*}$ 中的某个元素. 对满足 $0\leq i\leq\frac{q^{n}+1}{q+1}-1$ 的整数 i, 我们定义

$$L_{i,y}:=\{\langle(1,\omega^{i+j\frac{q^{n}+1}{q+1}}y)\rangle_{\mathbb{F}_{q^{2}}}:0\leq j\leq q\}. \tag{5.7}$$

每个子集 $L_{i,y}$ 的大小为 $q+1$, 并且他们恰好分割 *Singer* 轨道 S_{y}. 这里下标 i 都是取模 $\frac{q^{n}+1}{q+1}$, 故对每个整数 i 都可定义以上子集 $L_{i,y}$.

引理 5.12. 令 q 是偶数和 n 是奇整数, 其中 $n\geq 5$. 那么存在一个元素 $z\in\mathbb{F}_{q^{2n}}$ 使得

$$z^{q^{n}+1}=1,\ \mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^{2}}}(z)=1\ \text{and}\ z\neq 1.$$

证明. 取 $\mathbb{F}_{q^{2}}$ 中的一个元素 δ 使得 $\delta+\delta^{q}=1$, 接着设 $v:=\delta^{q+1}\in\mathbb{F}_{q}^{*}$. 那么 $1,\delta$ 构成 $\mathbb{F}_{q^{2}}$ 的一组 $\mathbb{F}_{q}$-线性基. 因为 n 是奇数, 所以根据引理 *5.5*可知它们同时也是 $\mathbb{F}_{q^{2n}}$ 的一组 $\mathbb{F}_{q^{n}}$-线性基.

令 N 是 $\mathbb{F}_{q^{2n}}$ 中满足以下方程的元素 z 的个数:

$$\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^{2}}}(z)=1,\ z^{q^{n}+1}=1.$$

这样就存在 $x,y\in\mathbb{F}_{q^{n}}$ 使得 $z=1+x+y\delta$. 接着通过直接展开方程, 第一个方程就简化为 $\mathrm{Tr}_{\mathbb{F}_{q^{n}}/\mathbb{F}_{q}}(x)=0$, $\mathrm{Tr}_{\mathbb{F}_{q^{n}}/\mathbb{F}_{q}}(y)=1$, 而第二个方程就简化为 $x^{2}+y^{2}v+xy+y=0$.

令 ψ 是 $\mathbb{F}_{q^n}$ 的正则加法特征, 即 $\psi(x)=(-1)^{\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(x)}$, 其中 $x\in\mathbb{F}_{q^n}$. 特别是对每个 $x\in\mathbb{F}_{q^n}$ 都有 $\psi(x^2)=\psi(x)$. 对 n 的每个因子 d, 易知当 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a)=0$ 时我们有 $\sum_{x\in\mathbb{F}_{q^d}}\psi(ax)=q^d$, 否则 $\sum_{x\in\mathbb{F}_{q^d}}\psi(ax)=0$, 具体可参考文献[76]. 我们因此推得 $q^{n+2}N$ 等于

$$\begin{aligned}
&\textstyle\sum_{x,y\in\mathbb{F}_{q^n}}\sum_{a,b\in\mathbb{F}_q}\sum_{z\in\mathbb{F}_{q^n}}\psi(ax+by+z(x^2+y^2v+xy+y))\\
=\;& q^{2n}+\textstyle\sum_{a,b\in\mathbb{F}_q}\sum_{x,y\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}^*}\psi(ax+by+z(x^2+y^2v+xy+y))\\
=\;& q^{2n}+\textstyle\sum_{a,b\in\mathbb{F}_q}\sum_{x,y\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}^*}\psi(ax+by+xz^{1/2}+y(zv)^{1/2}+zxy+zy))\\
=\;& q^{2n}+\textstyle\sum_{a,b\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}^*}\psi(by+y(zv)^{\frac{1}{2}}+yz)\cdot\sum_{x\in\mathbb{F}_{q^n}}\psi(x(a+z^{1/2}+yz)).
\end{aligned}$$

上式中最后一个求和项是非零就意味着 $a+z^{1/2}+yz=0$, 即 $y=az^{-1}+z^{-1/2}$. 于是我们就有

$$\begin{aligned}
q^{n+2}N=\;& q^{2n}+q^n\textstyle\sum_{a,b\in\mathbb{F}_q}\sum_{z\in\mathbb{F}_{q^n}^*}\psi(baz^{-1}+bz^{-1/2}+az^{-1/2}v^{1/2}+v^{1/2}+a+z^{1/2})\\
=\;& q^{2n}+q^n\textstyle\sum_{a,b\in\mathbb{F}_q}\psi(v+a)K(\psi;1,b^2+ba+a^2v).
\end{aligned}$$

其中 $K(\psi;1,u)=\sum_{z\in\mathbb{F}_{q^n}^*}\psi(z+u/z)$, 当 $u\neq0$ 是它是 *Kloosterman* 和, 而在 $u=0$ 时 $K(\psi;1,u)=-1$. 在这两种情况下, 我们根据文献[76] 定理 *5.45* 可知 $|K(\psi;1,u)|\leq 2q^{n/2}$. 于是我们就能推出

$$q^{n+2}N\geq q^{2n}+q^n\psi(v)-(q^2-1)\cdot 2q^{3n/2}\geq q^{2n}-q^n-(q^2-1)\cdot 2q^{3n/2}.$$

也就是说, $N\geq q^{n-2}-q^{-2}-2(q^2-1)q^{n/2-2}$. 这样我们就有 $N>1$ 除非 $(q,n)=(2,5)$, 后面一种情况是通过计算机去直接验证. 证毕. □

引理 5.13. 假定 q 是偶数以及 n 是奇整数, 其中 $n\geq3$. 那么 Singer 轨道 S_1 是 $H(n,q^2)$ 的一个 ovoid 当且仅当 $n=3$.

证明. 根据 *ovoid* 的定义, 集合 S_1 是一个 *ovoid* 当且仅当 S_1 中任意两个点都不正交. 换言之, $1+\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}}(\omega^k)\neq0$, 其中 $1\leq k\leq q^n$ 且 $o(\omega)=q^n+1$. 在 $\omega^k\in\mathbb{F}_{q^2}$ 的情况下, 结论显然成立. 因此我们只需要考虑 $\omega^k\notin\mathbb{F}_{q^2}$ 这种情况. 现在引理的结论在 $n=3$ 时可以从引理 *5.4*中获得, 而在 $n\geq5$ 从引理 *5.12*中获得. □

为了更好地理解 *Singer* 轨道的结构, 我们需要考虑它们与以下 $H(n,q^2)$ 的子集之间的相互作用.

$$T:=\{\langle(0,t)\rangle:t\in\mathbb{F}_{q^n}^*\text{ 且 }\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(t^2)=0\},\tag{5.8}$$

其中这子集恰好包含 $H(n,q^2)$ 中 $\frac{q^{n-1}-1}{q-1}$ 个不同的射影点. 令 $\Pi:=\{\langle(0,x)\rangle:x\in\mathbb{F}_{q^n}^*\}$ 为超平面 $P^\perp$ 的 *Baer* 子几何, 其中 $P=\langle(1,0)\rangle$. 在 q 是偶数的情况下, 这些

$\mathbb{F}_q$-射影点恰好构成 Π 的超平面. 而在 q 是奇数的情况下, 它们就构成 Π 的抛物型二次曲面 *(parabolic quadric)*.

引理 5.14. 使用以上定义的符号. 选取 $R_t = \langle (0,t) \rangle_{\mathbb{F}_{q^2}} \in T$ 和 $x \in \mathbb{F}_{q^n}^*$, 并且设 $y = x$ 或 $y = x\omega_0$, 其中 $o(\omega_0) = (q^n+1)(q-1)$. 如果 $U := R_t^\perp \cap S_y$, 那么对某个整数 k 有 $|U| = k(q+1)$. 此外, 如果 k 是奇数, 那么在两种情况 $y = x$ 和 $y = x\omega_0$ 下都有 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xt) = 0$.

证明. 易知射影点 $\langle (1, \omega^i y) \rangle$ 属于 $R_t^\perp$ 当且仅当

$$\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}}(w^i y t) = 0. \tag{5.9}$$

以下是两个简单的结果.

(*a*) 因为 ω 是 q^n+1 阶元, 所以 $\omega^{(q^n+1)/(q+1)} \in \mathbb{F}_{q^2}$. 因此从射影点 $\langle (1, \omega^i y) \rangle \in R_t^\perp$ 中推出 $L_{i,y} \subseteq R_t^\perp$. 也就是说, U 是某些子集 $L_{i,y}$'s 的并集. 作为推论, 对某个整数 k 有 $|U| = k(q+1)$.

(*b*) 因为 $y = x$ 或 $y = x\omega_0$, 所以存在唯一整数 a 使得 $0 \le a \le q^n$ 和 $\omega^a = y^{q^n-1}$, 也就是说, $a = 0$ 或 $a = (q^n-1)/(q-1)$. 通过将等式(5.9)两边提到 q^n 次方, 我们就得到 $\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}}(\omega^{a-i} y t) = 0$. 换言之, $L_{i,y} \subseteq U$ 当且仅当 $L_{a-i,y} \subseteq U$.

记 $M := \frac{q^n+1}{q+1}$, 这是奇整数. 两个子集 $L_{i,y}$ 和 $L_{a-i,y}$ 是相等的当且仅当 $i \equiv a-i \pmod M$, 即 $2i \equiv a \pmod M$. 因为 M 是奇数, 所以恰好存在一个整数 i_0 使得 $0 \le i_0 \le M-1$ 和 $L_{i_0,y} = L_{a-i_0,y}$. 具体而言, 若 $y = x$, 则 $a = 0$ 和 $i_0 = 0$; 此外如果 $y = x\omega_0$, 则 $a = \frac{q^n-1}{q-1}$ 和 $i_0 \equiv \frac{q^n-1}{q-1} t \pmod M$, 其中 t 是模 M 下 2 的逆元. 在后面的情况中, 我们有 $(q-1)i_0 + 1 = (q^n-1)t + 2t \equiv 0 \pmod M$, 即 $\omega^{i_0}\omega_0 \in \mathbb{F}_{q^2}^*$.

如果 k 是奇数, 那么我们必然从结果 *(b)* 中推出 $L_{i_0,y} \subseteq U$. 也就是说, 等式 (5.9)成立其中 $i = i_0$. 在两种情况下, 我们都将 i_0 和 y 的表达式代入等式, 接着简化后可推出 $\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}}(xt) = 0$. 因为 $xt \in \mathbb{F}_{q^n}$, 所以我们完成第二个结果的证明. □

定理 5.15. 令 $n \ge 3$ 是奇整数. 对 $H(n,q^2)$ 中的射影点 $\langle (1,y) \rangle$, 令子集 S_y 是如等式(5.6)中所示的. 于是 S_y 不是 $H(n,q^2)$ 中一个 ovoid 除非 q 是偶数且 S_y 是 $H(3,q^2)$ 中的 Singer-type ovoid S_1.

证明. 根据引理 *5.3*可知 S_y 包含射影点 $\langle (1,x) \rangle$ 或 $\langle (1, x\omega_0) \rangle$, 其中 $x \in \mathbb{F}_{q^n}^*$ 且 $o(\omega_0) = (q^n+1)(q-1)$. 故我们不失一般性地假设对某个 $x \in \mathbb{F}_{q^n}^*$ 有 $y = x$ 或 $y = x\omega_0$. 此外, 如果 q 是偶数则我们只需要考虑一种情况 $y = x \in \mathbb{F}_{q^n}^*$, 详见引理 *5.4*.

现在使用反证法证明结果. 假设 S_y 是 $H(n,q^2)$ 中的一个 *ovoid*. 令 T 是如等式(5.8)所示的. 利用等式(5.1), 我们能推出 $|R_t^{\perp} \cap S_y| = q^{n-2}+1$, 其中 t 是 $\mathbb{F}_{q^n}$ 中某个元素使得 $R_t = \langle (0,t) \rangle \in T$. 因为 n 是奇数, 所以 $\frac{q^{n-2}+1}{q+1}$ 也是奇数. 由引理 *5.14*我们有 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xt) = 0$. 这是对所有满足 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xt) = 0$ 的 $t \in \mathbb{F}_{q^n}^*$ 都成立.

(1) 在 q 是偶数的情况下, 根据假设可知 $y = x \in \mathbb{F}_q^*$. 因为 $\langle (1,y) \rangle \in H(n,q^2)$, 所以我们从 $1+y^2 = 0$ 中推出 $y = 1$. 于是由引理 *5.13*即可得结论.

(2) 在 q 是奇数的情况下, 这意味着 T 中 $\mathbb{F}_q$-射影点都存在于 $\mathrm{PG}(\{0\} \times \mathbb{F}_{q^{2n}})$ 的 *Baer* 子几何 $\Pi = \mathrm{PG}(\{0\} \times \mathbb{F}_{q^n})$ 的超平面 $\{\langle (0,t) \rangle : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xt) = 0\}$ 中. 这显然与事实 T 是 Π 上一个非退化抛物型二次曲面相矛盾, 故这种情况是不可能的.

证毕. □

5.4 $H(n,q^2)$ 中的传递 *ovoids* 的分类结果

在这节中, 我们主要给出定理 *5.1*的证明. 由文献[38] 可知当 n 是偶数时 $H(n,q^2)$ 不存在 *ovoid*, 所以我们假设 n 是大于等于 3 的奇数. 令 $q = p^d$, 其中 p 是素数. 假定 O 是 $H(n,q^2)$ 中的一个传递 *ovoid*, 其中它在 $\mathrm{P\Gamma U}(n+1,q^2)$ 中的稳定子群是 H. 因为 H 是不可解的情况已经在文献[2] 中解决, 所以我们只需要考虑 H 是可解的情况. 借助第 *5.2.3*小节中叙述, 我们可以取第 *5.3*节中 $H(n,q^2)$ 的模型, 并且不失一般性地假设 H 是 $G = \langle \psi, \phi \rangle$ 的子群, 其中 ψ, ϕ 是如等式(5.4)定义的映射.

令 ω_0 是 $\mathbb{F}_{q^{2n}}$ 中固定的 $(q^n+1)(q-1)$ 阶元, 并且记 $\omega = \omega_0^{q-1}$. 我们继续使用第 *5.3*节中介绍的 $H(n,q^2)$ 的模型和符号. 令 S_y 和 T 分别是如等式(5.6)和(5.8)所定义的子集. 由引理 *5.3*可知 G 存在某个元素 g 使得 $g(O)$ 具有下列其中一种形式的射影点.

(1) $\langle (1, x) \rangle$ 其中 $x \in \mathbb{F}_{q^n}^*$;

(2) $\langle (1, x\omega_0) \rangle$ 其中 $x \in \mathbb{F}_{q^n}^*$, 并且此时 q 是奇数.

如果 q 是偶数, 只有第一种情况出现. 因此我们不失一般性地假设 O 包含以上两种指定形式之一的点 $\langle (1,y) \rangle$.

5.4.1 参数限制

因为 H 在 O 上作用是传递的, 所以存在正整数 m 使得 $|H| = m(q^n+1)$. 记 $H \cap \langle \psi \rangle = \langle \psi^s \rangle$, 其中 $s | q^n+1$. 在 $s = 1$ 的情况下, 对某个 $y \in \mathbb{F}_{q^{2n}}^*$ 有 $O = S_y$, 而这

种情况已经在定理 *5.15*中得到解决, 故我们下面假设 $s>1$. 通过考虑限制到 H 上的群同态 $\eta: G\to \mathrm{Aut}(\mathbb{F}_{q^{2n}})$, 我们可以看出对某些整数 k,j 有

$$H=\langle \psi^s,\, \psi^j\phi^k\rangle$$

使得 $0\le j\le s-1$, $k|2nd$ 和 $\frac{q^n+1}{s}\cdot\frac{2nd}{k}=|H|$. 最后的等式等价于 $2nd=mks$.

引理 5.16. 我们有 $mks=2nd$, $s|(q^n+1)$, 和 $\frac{p^{2nd}-1}{p^k-1}\cdot j\equiv 0 \pmod{s}$.

证明. 利用引理 *5.11*中 (1) 可得 $(\psi^j\phi^k)^{2nd/k}=\psi^{j(p^{2nd}-1)/(p^k-1)}$, 故它属于集合 $H\cap\langle\psi\rangle=\langle\psi^s\rangle$. 由此得到引理中最后的同余式. □

推论 5.17. 当 q 是偶数时, 则 s 就是奇数; 而当 q 是奇数时, 则 s 不可能是 4 的倍数.

证明. q 是偶数这种情况是显然, 因为 q^n+1 是奇数且 s 整除 q^n+1. 于是只需要考虑 q 是奇数的情况. 假设 s 是 *4* 的倍数. 由于 $2nd=mks$, 所以我们推出 $2|d$. 于是就有 $q^n+1=p^{nd}+1\equiv 2 \pmod 4$, 这意味着 q^n+1 不能被 4 整除. 这就与 s 整除 q^n+1 相矛盾. 证毕. □

引理 5.18. 假定 $q=p^d$ 是奇数和 s 是偶数, 再令 $\langle(1,y)\rangle_{\mathbb{F}_{q^2}}$ 是 O 中的射影点.

(1) 如果 m 是偶数且 $y\in\mathbb{F}_{q^n}^*$, 那么 $y\in\mathbb{F}_{p^{ks}}^*$.

(2) 如果对某个 $x\in\mathbb{F}_{q^n}^*$ 有 $y=x\omega_0$, 那么 m 是奇数和 $y^{(p^{ks/2}-1)(q^n+1)}=1$.

证明. 回忆一下, H 是 O 在群 G 中的稳定子群, 同时 ω_0 是 $(q^n+1)(q-1)$ 阶元并且 $\omega=\omega_0^{q-1}$. 因为 H 的阶为 $m(q^n+1)$ 并且 H 作用在 O 是传递的, 所以 $\langle(1,y)\rangle$ 在 H 中稳定子群的阶是 m. 很明显, $A\cap\langle\psi\rangle=1$, 故 $\eta(A)$ 的阶是 m, 其中 η 是如等式 (5.5)中所示的群同态. 利用引理 *5.16*结果 $2nd=mks$, 我们就有 $A=\langle\psi^l\phi^{ks}\rangle$, 其中 l 是某个非负整数. 因为

$$\psi^l\phi^{ks}(\langle(1,y)\rangle)=\langle(1,y^{p^{ks}}\omega^l)\rangle=\langle(1,y)\rangle,$$

所以我们有

$$y^{p^{ks}-1}=\omega^{-l}. \tag{5.10}$$

因为 $H=\langle\psi^s,\psi^j\phi^k\rangle$ 和 $\eta(\psi^l\phi^{ks})=\eta(\psi^j\phi^k)^s$, 所以存在整数 a 使得

$$\psi^{sa}(\psi^j\phi^k)^s=\psi^{sa+j(p^{ks}-1)/(p^k-1)}\phi^{ks}=\psi^l\phi^{ks}\in A.$$

这里我们在第一等式使用引理 *5.11*中 (1). 于是就有

$$l \equiv sa + j\frac{p^{ks}-1}{p^k-1} \pmod{q^n+1}. \tag{5.11}$$

因为 q 是奇数和 s 是偶数, 所以我们能推出 $\frac{p^{ks}-1}{p^k-1} = \frac{p^{ks}-1}{p^{2k}-1}\cdot(p^k+1)$ 是偶数. 这就意味着 l 是偶数. 我们现在就准备证明引理中两个命题.

(1). 假设 m 是偶数以及 $y \in \mathbb{F}_{q^n}^*$. 在这种情况下, $\omega^l = y^{1-p^{ks}}$ 既属于 $\mathbb{F}_{q^n}^*$ 也属于 ω 生成的 $\langle w\rangle$, 于是它的阶整除 $\gcd(q^n+1, q^n-1) = 2$. 另一方面, 因为 $2nd = mks$ 和 m, s 都是偶数, 所以 d 是偶数. 由此断定 $q^n+1 = p^{nd}+1 \equiv 2 \pmod 4$. 因为 l 是偶数, 所以 ω^l 的阶是奇数. 我们就得出 $\omega^l = 1$ 的结果, 因此就有 $y^{p^{ks}-1} = 1$. 这就证明第一个命题.

(2). 假设对某个 $x \in \mathbb{F}_{q^n}^*$ 有 $y = x\omega_0$. 回想一下, 我们定义 $\omega = \omega_0^{q-1}$. 由于

$$\psi^{-\frac{q^n-1}{q-1}}\phi^{nd}(\langle(1,\, x\omega_0)\rangle) = \langle(1,\, x\omega_0^{q^n}w^{-\frac{q^n-1}{q-1}})\rangle = \langle(1,\, x\omega_0)\rangle,$$

所以群元素 $\psi^{-(q^n-1)/(q-1)}\phi^{nd}$ 保持 $\langle(1,\, x\omega_0)\rangle$ 不变.

我们先证明 m 是奇数. 这里我们使用反证法, 假设 m 是偶数, 则我们从 $mks = 2nd$ 中得到 $ks|nd$, 故 A 里面存在一个元素 $\psi^v\varphi^{nd}$. 由此即可推出 $\psi^{v+(q^n-1)/(q-1)} = (\psi^v\varphi^{nd})(\psi^{-(q^n-1)/(q-1)}\phi^{nd})^{-1} \in A$, 这意味着 $v = -(q^n-1)/(q-1)$. 因此, 存在整数 i, b 使得

$$\psi^{si}(\psi^l\phi^{ks})^b = \psi^{si+\frac{p^{ksb}-1}{p^{ks}-1}l}\phi^{ksb} = \psi^{-\frac{q^n-1}{q-1}}\phi^{nd}. \tag{5.12}$$

这里我们在第一个等式里使用引理 *5.11*的 *(1)*. 我们就推出

$$si + \frac{p^{ksb}-1}{p^{ks}-1}l \equiv -\frac{q^n-1}{q-1} \pmod{q^n+1}.$$

注意到 l 和 s 都是偶数, 因此上式的左手边是偶数. 这导致 $(q^n-1)/(q-1)$ 是偶数, 但这与 n 是奇数的条件相矛盾. 故我们得到结论：m 是奇数.

记 $y = \gamma^h$, 其中 γ 是 $\mathbb{F}_{q^{2n}}$ 中的本原元. 因为 l 是偶数, 所以我们将等式 *5.10*的两边提至 $\frac{q^n+1}{2}$ 次方就能推出

$$h(p^{ks}-1)\cdot\frac{(q^n+1)}{2} \equiv 0 \pmod{q^{2n}-1}, \text{ 即 } h(p^{ks}-1)/2 \equiv 0 \pmod{q^n-1}.$$

因为 m 是奇数且 $ks = \frac{2nd}{m}$, 所以我们有 $\gcd(ks, nd) = \frac{nd}{m}\cdot\gcd(2, m) = \frac{nd}{m}$. 由此就有

$$\gcd(p^{ks}-1, q^n-1) = p^{\gcd(ks,nd)}-1 = p^{nd/m}-1.$$

因为 $\frac{p^{ks}-1}{p^{nd/m}-1} = p^{nd/m}+1$ 是偶数, 所以我们从中推出 $p^{nd/m}-1$ 也能整除 $\frac{p^{ks}-1}{2}$. 因此 $p^{nd/m}-1$ 整除 $\gcd\left(\frac{p^{ks}-1}{2}, q^n-1\right)$, 显然它也整除 $\gcd(p^{ks}-1, q^n-1)$. 我们就有

$\gcd\left(\frac{p^{ks}-1}{2}, q^n-1\right) = p^{nd/m}-1$. 由此推出 h 是 $\frac{q^n-1}{p^{nd/m}-1}$ 的倍数, 这就得所需的结果: $y^{(p^{nd/m}-1)(q^n+1)} = 1$. 证毕. □

对整数 i 而言, $\psi^i(O)$ 也是 $H(n,q^2)$ 中的一个 *ovoid*. 设

$$\mathfrak{O} := \cup_{i=0}^{s-1}\psi^i(O), \tag{5.13}$$

这是一个多重集. 回忆一下, *Singer* 轨道 S_y 是如等式(5.6)中定义的. 下面的引理将在我们的论证中起到重要的作用.

引理 5.19. 使用以上定义的符号, 再令 $\langle(1,y)\rangle$ 是 O 中的射影点.

(i) 我们有 $\mathfrak{O} = \cup_{i=0}^{s-1}\phi^{ik}(S_y)$, 且对 T 中任何射影点 $R_t = \langle(0,t)\rangle$ 都有 $\sum_{i=0}^{s-1}|R_t^{\perp}\cap\phi^{ik}(S_y)| = s(q^{n-2}+1)$, 其中 T 是如等式(5.8)中定义的集合;

(ii) 我们有 $S_y = \phi^{ks}(S_y)$ 和 $y^{(p^{ks}-1)(q^n+1)} = 1$.

证明. 令 C_y 是 $\langle(1,y)\rangle$ 在 $\langle\psi^s\rangle$ 作用下的像集; 特别地, $\psi^s(C_y) = C_y$. 那么 $S_y = \cup_{i=0}^{s-1}\psi^i(C_y)$, 以及 $O = \cup_{a=0}^{s-1}(\psi^j\phi^k)^a(C_y)$. 故我们有

$$\begin{aligned}\mathfrak{O} &= \cup_{i,a=0}^{s-1}\psi^i(\psi^j\phi^k)^a(C_y) = \cup_{i,a=0}^{s-1}\psi^{i+j(p^{ka}-1)/(p^k-1)}\phi^{ka}(C_y)\\ &= \cup_{i,a=0}^{s-1}\phi^{ka}\psi^{(i+j(p^{ka}-1)/(p^k-1))p^{2nd-ka}}(C_y) = \cup_{i=0}^{s-1}\phi^{ik}(S_y).\end{aligned}$$

在以上最后一个等式中, 我们使用了

$$\left\{\left(i+j\frac{p^{ka}-1}{p^k-1}\right)p^{2nd-ka} \pmod s : 0\le i\le s-1\right\} = \{0,1,\cdots,s-1\}$$

其中 a 是给定的整数. 这里 j,k 是满足 $H = \langle\psi^s, \psi^j\phi^k\rangle$ 条件的常数. 这就证明 (i) 中第一个等式. 对于射影点 $R_t = \langle(0,t)\rangle \in T$, 它第一个坐标为零, 故它不属于任何一个子集 $\psi^i(O)$'s, 因此根据等式(5.1)可知对每个 i 都有 $|R_t^{\perp}\cap\psi^i(O)| = q^{n-2}+1$. 现在就可以从 $\mathfrak{O} = \cup_{i=0}^{s-1}\phi^{ik}(S_y)$ 中推出 (i) 中第二个等式.

我们现在从这里开始证明结论 (ii). 我们通过归纳法从引理 *5.11*的 (ii) 中得到 $\phi^b\psi^a = \psi^{ap^b}\phi^b$, 其中 a,b 都是非负整数. 将 ϕ^k 作用到 $\mathfrak{O}$, 我们有

$$\phi^k(\mathfrak{O}) = \cup_{i=0}^{s-1}\phi^k\psi^i(O) = \cup_{i=0}^{s-1}\psi^{ip^k-j}(\psi^j\phi^k(O)) = \cup_{i=0}^{s-1}\psi^{ip^k-j}(O).$$

这里我们主要使用 $\psi^j\phi^k$ 保持 O 不变的结果. 集合 $\{ip^k-j \pmod s : 0\le i\le s-1\}$ 和 $\{0,1,\cdots,s-1\}$ 是相等, 并且 ψ^s 保持 O 不变. 由此断定 $\phi^{ks}(S_y) = S_y$. 因此, 存在一个整数 i 使得

$$\phi^{ks}(\langle(1,y)\rangle) = \langle(1,\, y^{p^{ks}})\rangle = \langle(1,\,\omega^i y)\rangle \in S_y,\ \text{i.e., } y^{p^{ks}} = \omega^i y.$$

于是就有 $y^{(p^{ks}-1)(q^n+1)}=1$. 证毕. □

引理 5.20. 如果 $q=2^d$ 和 $2^d \geq nd$, 那么 $s \geq q+1$ 除非 $n=3$ 和 O 是一个 Singer-type ovoid.

证明. 通过本节开始的论证, 我们可以不失一般性地假设 O 包含射影点 $\langle(1,y)\rangle$ 其中 $y \in \mathbb{F}_{q^n}^*$. 记 $X := \{y^{p^{ki}} : 0 \leq i \leq s-1\}$.

我们声称对某个整数 $0 \leq i \leq s-1$ 有 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y^{p^{ki}}t)=0$, 其中 t 是 $\mathbb{F}_{q^n}^*$ 中某个元素使得 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(t)=0$. 令 t 为以上定义的元素, 再设 $R_t := \langle(0,t)\rangle$, 这也是 T 中的射影点. 通过引理 *5.19*中的 (i), 我们有 $\sum_{i=0}^{s-1}|R_t^{\perp} \cap \phi^{ki}(S_y)| = s(q^{n-2}+1)$. 根据引理 *5.14*可知求和前每一项都是 $(q+1)$ 的倍数. 通过推论 *5.17*可知 s 是奇数; 此外, 我们也很容易看出 $\frac{q^{n-2}+1}{q+1}$ 也是奇数. 由此断定至少存在一个整数 i 使得对某个整数 u 有 $|R_t^{\perp} \cap \phi^{ki}(S_y)| = u(q+1)$. 因为 $\phi^{ki}(S_y) = S_{y^{p^{ki}}}$, 所以我们的声称现在就直接从引理 *5.14*中推出.

在 $y \in \mathbb{F}_q^*$ 的情况下, 我们根据事实 $\langle(1,y)\rangle$ 是 $H(n,q^2)$ 中的迷向点中推出 $y=1$. 于是对每个 i 都有 $\phi^{ki}(S_1)=S_1$, 因此 $\mathfrak{O}=s\cdot S_1$, 这就意味着 $O=S_1$. 通过引理 *5.13*可知 S_1 是 $H(n,q^2)$ 中的一个 *ovoid* 当且仅当 $n=3$.

剩下只需要处理 $y \notin \mathbb{F}_q^*$ 这种情况. 我们使用反证法, 假设 $s \leq q$. 于是有 $\lceil \frac{q^{n-1}-1}{s} \rceil \geq \lceil q^{n-2}-q^{-1} \rceil = q^{n-2}$. 根据鸽笼原理 *(*抽屉原理*)*, 存在某个 i 使得对至少 $q-2$ 个非零元 $t \in \mathbb{F}_{q^n}$ 有 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y^{p^{ki}}t)=0$ 和 $t \in \mathbb{F}_{q^n}$. 我们就推出 $y^{p^{ki}} \in \mathbb{F}_q^*$, 即 $y \in \mathbb{F}_q^*$: 矛盾. 因此 $y \notin \mathbb{F}_q^*$ 不可能发生. 证毕. □

我们现在考虑奇特征的情况. 证明的主要思路与引理 *5.20*相同. 我们需要下面的引理.

引理 5.21. 假定 $q=p^d$ 是奇数并且 $\langle(1,y)\rangle$ 是 O 中的射影点, 其中 $x := y \in \mathbb{F}_{q^n}^*$ 或 $x := y\omega_0^{-1} \in \mathbb{F}_{q^n}^*$. 设 $X := \{x^{p^{ka}} : 0 \leq a \leq s-1\}$; 特别地, 当 s 是偶数时, 设 $X_h := \{x^{p^{ka}} : 0 \leq a \leq s/2-1\}$. 令 $R_t = \langle(0,t)\rangle$ 是 T 中的射影点, 其中 T 是如等式(5.8)中所定义的集合.

(i) 如果 m 或 s 是奇数, 那么存在 X 中的元素 x 使得 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xt)=0$;

(ii) 如果 m 和 s 都是偶数和 $t \in \mathbb{F}_{p^{nd/e}}$, 那么存在 X_h 中的元素 x 使得 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xt)=0$, 其中 e 是整除 d 的 2 的最高次幂.

证明. 在 s 是奇数的情况下, 这个论证恰好与引理 *5.20*的证明完全相同, 故我们下面

假设 s 是偶数. 根据推论 *5.17*, 存在奇整数 s_0 使得 $s = 2s_0$. 通过引理 *5.16*, 我们有 $2nd = mks$. 由此断定 $nd = mks_0$. 此外, 我们通过引理 *5.19*的 (ii) 得到 $S_y = \phi^{ks}(S_y)$ 和 $y^{(p^{ks}-1)(q^n+1)} = 1$.

首先考虑 m 是奇数的情况. 我们声称 $S_y = \phi^{ks_0}(S_y)$. 为了证明这个结论, 我们下面分别考虑两种不同的情况.

(1) 如果 $y \in \mathbb{F}_{q^n}^*$, 那么 y 的阶整除 $D := \gcd(q^n - 1, (q^n + 1)(p^{ks} - 1))$. 于是我们有

$$\begin{aligned} D &= \gcd(q^n - 1, 2(p^{ks} - 1)) = (p^{ks_0} - 1) \cdot \gcd\left(\frac{q^n - 1}{p^{ks_0} - 1}, 2(p^{ks_0} + 1)\right) \\ &= (p^{ks_0} - 1) \cdot \gcd\left(\frac{q^n - 1}{p^{ks_0} - 1}, p^{ks_0} + 1\right) = \gcd(q^n - 1, p^{2ks_0} - 1) \\ &= p^{\gcd(mks_0, 2ks_0)} - 1 = p^{ks_0} - 1. \end{aligned}$$

这里我们在第三个等式里使用 $\frac{q^n-1}{p^{ks_0}-1} = 1 + p^{ks_0} + \cdots + p^{(m-1)ks_0}$ 是奇数这个事实. 由此断定 $y \in \mathbb{F}_{p^{ks_0}}^*$, 于是就有 $S_y = \phi^{ks_0}(S_y)$.

(2) 如果对某个 $x \in \mathbb{F}_{q^n}^*$ 有 $y = x\omega_0$, 那么通过引理 *5.18*我们就有 $y^{(p^{ks_0}-1)(q^n+1)} = 1$, 即 $y^{p^{ks_0}} \in y\langle\omega\rangle$. 在这种情况下, 我们有 $\phi^{ks_0}(S_y) = S_y$.

在这两种情况下, 对每个整数 i 都有 $\phi^{ki}(S_y) = \phi^{k(s_0+i)}(S_y)$. 因此我们通过引理 *5.19*的 (i) 有 $\sum_{i=0}^{s_0-1} |R_t^\perp \cap \phi^{ki}(S_y)| = s_0(q+1)$. 这样结论 (i) 现在就从关于奇偶性的论证以及像引理 *5.20*的证明一样调用引理 *5.14*来获得.

接着我们考虑 m 是偶数的情况. 令 e 是整除 m 的 *2* 的最高次幂. 从 $nd = mks_0$ 和 n 是奇数的事实中推得 e 整除 d. 设 $q_1 := p^{d/e}$, 再定义下面一个子集 T_1:

$$T_1 := \{\langle(0, t)\rangle : t \in \mathbb{F}_{q_1^n}^* \ |\mathrm{Tr}_{\mathbb{F}_{q_1^n}/\mathbb{F}_{q_1}}(t^2) = 0\}|. \tag{5.14}$$

因为 $\gcd(d, nd/e) = \frac{d}{e} \cdot \gcd(e, n) = d/e$, 所以我们有 $\mathbb{F}_q \cap \mathbb{F}_{q_1^n} = \mathbb{F}_{q_1}$. 于是就对 $t \in \mathbb{F}_{q_1^n}$ 有 $\mathrm{Tr}_{\mathbb{F}_{q_1^n}/\mathbb{F}_{q_1}}(t^2) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(t^2)$. 因此 T_1 是 T 中大小为 $\frac{q_1^{n-1}-1}{q_1-1}$ 的子集.

根据引理 *5.18*中 (2) 可知 $y\omega_0^{-1} \in \mathbb{F}_{q^n}^*$ 这种情况不可能发生, 在通过同一引理中的 (1) 我们必然有 $y \in \mathbb{F}_{p^{ks}}^*$. 对 T_1 中的射影点 $R_t = \langle(0, t)\rangle$, $\langle(1, \omega^a y^{p^{ki}}\rangle$ 属于 $R_t^\perp \cap \phi^{ki}(S_y)$ 当且仅当

$$\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}}(\omega^a y^{p^{ki}} t) = 0. \tag{5.15}$$

注意到 $q_1^n = p^{mks_0/e}$ 且 m/e 是奇数. 将等式(5.15)的两边同时提到 $p^{mks_0/e}$ 次方, 我们推断出条件(5.15)等价于 $\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}}(\omega^{ap^{mks_0/e}} y^{p^{ks_0+ki}} t) = 0$. 于是就有 $\langle(1, \omega^a y^{p^{k(s_0+i)}})\rangle$ 属于 $R_t^\perp \cap \phi^{k(s_0+i)}(S_y)$. 这就得到了 $R_t^\perp \cap \phi^{ki}(S_y)$ 和 $R_t^\perp \cap \phi^{k(s_0+i)}(S_y)$ 之间的一个双

射, 即

$$\langle(1,\omega^a y^{p^{ki}})\rangle \mapsto \langle(1,\omega^{ap^{mks_0/e}} y^{p^{k(s_0+i)}})\rangle.$$

我们因此从引理 *5.19*的 (i) 中得到 $\sum_{i=0}^{s_0-1}|R_t^\perp \cap \phi^{ki}(S_y)| = s_0(q^{n-2}+1)$. 于是结论就通过类似于 m 是奇数时的论证得到. □

引理 5.22. 假定 $q=p^d$ 是奇数. 那么我们就有:

(i) 如果 m,s 中的一个数是奇数, 那么当 $n=3$ 时 $s \geq \frac{q+1}{2}$, 而当 $n \geq 5$ 时就有 $s \geq q$;

(ii) 如果 m 和 s 都是偶数, 那么当 $n=3$ 时 $s \geq p^{d/e}+1$, 而当 $n \geq 5$ 时 $s \geq 2p^{d/e}$, 其中 e 是整除 m 的 2 的最高次幂.

证明. 通过本节开始的论证, 我们不失一般性地假设 O 包含射影点 $\langle(1,y)\rangle$, 其中 $x := y \in \mathbb{F}_{q^n}^*$ 或 $x := y\omega_0^{-1} \in \mathbb{F}_{q^n}^*$. 令 X 和 X_h 是在引理 *5.21*中定义的两个集合, 再记 $x_i := x^{p^{ki}}$.

首先, 考虑 m 或 s 是奇数的情况. 令 Π 是环绕 $\mathbb{F}_q$-线性向量空间 $\mathbb{F}_{q^m}$ 的射影几何, 再令 $\mathcal{Q}$ 为抛物型二次曲线 $Q(t)=\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(t^2)$. 由于 $\langle(1,y)\rangle \in H(n,q^2)$, 我们根据 $y=x$ 或 $y=x\omega_0$ 推出 $Q(x)=1$ 或 $Q(x)=\omega_0^{-(q^n+1)}$; 回忆一下, $o(\omega_0)=(q^n+1)(q-1)$. 令 π_i 是 Π 中超平面, 其方程为 $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x_i t)=0$, $0 \leq i \leq s-1$. 通过引理 *5.21*的 (i) 可得 $\mathcal{Q}$ 中每个顶点都会属于某个超平面 π_i 里. 因为 $Q(x_i)=Q(x)^{p^{ki}} \neq 0$, 所以我们看出每个超平面 π_i 交 $\mathcal{Q}$ 于一个非退化的二次曲面, 即 $Q^+(n-2,q)$ 或 $Q^-(n-2,q)$. 因此我们有 $|\mathcal{Q}| \leq |X| \cdot |Q^+(n-2,q)|$, 即

$$\begin{aligned}|X| &\geq \left\lceil \frac{q^{n-1}-1}{(q^{(n-1)/2}-1)(q^{(n-1)/2-1}+1)} \right\rceil = \left\lceil \frac{q^{(n-1)/2}+1}{q^{(n-1)/2-1}+1} \right\rceil \\ &= q - \left\lfloor \frac{q-1}{q^{(n-1)/2-1}+1} \right\rfloor.\end{aligned}$$

当 $n=3$ 时, 我们得到 $|X| \geq \frac{q+1}{2}$; 而当 $n \geq 5$ 时, 则我们有 $|X| \geq q$. 因为 $|X| \leq s$, 所以我们在这种情况下推出想要的结论.

接着, 我们考虑 m 和 s 都是偶数的情况. 根据引理 *5.18*, 我们有 $x=y \in \mathbb{F}_{p^{ks}}^*$. 令 e 是整除 m 的 *2* 的最高次幂, 再设 $q_1 := p^{d/e}$. 于是我们有 $q=q_1^e$ 和 $\gcd(e,n)=1$. 选取 $\mathbb{F}_{q_1}$ 上 $\mathbb{F}_q$ 的一组基 $\zeta_1,\cdots,\zeta_e$; 由引理 *5.5*可知它们也构成 $\mathbb{F}_{q_1^n}$ 上 $\mathbb{F}_{q^m}$ 的一组基. 对于每个 i, 我们记 $x_i=\sum_{j=0}^{e-1} x_{ij}\zeta_j$ 其中 $x_{ij} \in \mathbb{F}_{q_1^n}$, 再设 z_i 为所有非零的 x_{ij}'s 中的某个数. 令 Π 是环绕 $\mathbb{F}_{q_1}$-线性向量空间 $\mathbb{F}_{q_1^m}$ 的射影几何, 再令 $\mathcal{Q}$ 为抛物型二次曲线 $Q(t)=\mathrm{Tr}_{\mathbb{F}_{q_1^n}/\mathbb{F}_{q_1}}(t^2)$. 我们在从 $\langle(1,x)\rangle \in H(n,q^2)$ 的事实中推出 $Q_1(x)=1$. 再令 π_i

为 Π 中的超平面, 其方程为 $\mathrm{Tr}_{\mathbb{F}_{q_1^n}/\mathbb{F}_{q_1}}(z_i t)=0, 0\le i\le s/2-1$. 根据引理 *5.21*可知对 $\mathcal{Q}_1$ 中每个射影点都存在 i 使得

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xt)=0, \textit{ i.e.}, \sum_{j=1}^{e}\mathrm{Tr}_{\mathbb{F}_{q_1^n}/\mathbb{F}_{q_1}}(x_{ij}t)\zeta_j=0.$$

于是就有 $\langle t\rangle_{\mathbb{F}_{q_1}}$ 属于这个超平面 π_i. 像之前的情况一样, π_i 交二次曲面于 $Q^-(n-2,q_1)$ 或 $Q^+(n-2,q_1)$. 于是就有 $|\mathcal{Q}_1|\le|Q^+(n-2,q_1)|\cdot s/2$. 同样地, 我们用类似的方法推出当 $n=3$ 时则 $\frac{s}{2}\ge\frac{q_1+1}{2}$, 而当 $n\ge5$ 时则 $\frac{s}{2}\ge q_1$. 证毕. □

5.4.2 定理 *5.1*的证明

我们继续使用这节开始时已经介绍的符号. 特别地, $q=p^d$ 其中 p 是素数, 假定 O 是 $H(n,q^2)$ 中包含射影点 $\langle(1,y)\rangle$ 的传递 *ovoid*, 其中 $x:=y\in\mathbb{F}_{q^n}^*$ 或 $x:=y\omega_0^{-1}\in\mathbb{F}_{q^n}^*$, 同时令 $H=\langle\psi^s,\phi^j\psi^k\rangle$ 是 O 在 $\mathrm{P\Gamma U}(n+1,q^2)$ 中的稳定子群, 其中 ψ 和 ϕ 是在等式(5.4)中定义的群同态. 我们记 $|H|=m(q^n+1)$. 根据引理 *5.16*, 我们有 $mks=2nd$, $s|q^n+1$.

引理 5.23. 令 p 为素数, d 是正整数, 再记 $q=p^d$. 假定 s 是 $\gcd(6d,\,q^3+1)$ 的因子.

(1) 如果 $p=2$ 和 $d\ge4$, 那么 $s<q+1$.

(2) 如果 p 是奇数, 那么 $2s<q+1$ 除非 $(p,d)\in\{(3,1),\,(5,1),\,(11,1)\}$.

证明. 在 $p=2$ 这种情况下, 我们有 $\gcd(6d,\,q^3+1)=\gcd(3d,q^3+1)\le3d$, 所以在 $d\ge4$ 时 $s\le3d<2^d+1$. 在 p 是奇数的情况下, 我们考虑下面的两种情况.

(i) 如果 $p\equiv0,1\pmod3$, 那么 q^3+1 不能被 3 整除, 则有 $\gcd(6d,q^3+1)=\gcd(2d,q^3+1)$. 由此推出 $2s\le4d<p^d+1$ 除非 $(p,d)=(3,1)$.

(ii) 如果 $p\equiv2\pmod3$, 那么在 $d\ge3$ 时 $2s\le12d<5^d+1\le p^d+1$. 剩下只需要考虑 $d=1$ 这种情况. 在此情况下, 易知 $p>11$ 时有 $2s\le12<p+1$.

证毕. □

我们首先重新叙述并证明 $n=3$ 时群是可解的情况下的定理 *5.1*.

定理 5.24 **(定理** 5.1, $n=3$ **时群是可解的情况)**. 令 p 是素数再令 $q=p^d$. 假定 O 是 $H(3,q^2)$ 的传递 ovoid, 其中它在 $\mathrm{P\Gamma U}(4,q^2)$ 中的稳定子群是可解的. 那么 q 是偶数, 并且 O 射影等价于一个 Singer-type ovoid 或者在例子 5.10中所描述的两个 $H(3,8^2)$ 的 ovoids 的其中之一.

证明. 首先考虑 q 是偶数的情况. 当 $d \leq 3$ 时, 通过使用 *Magma*[69] 进行穷尽的搜索表明在射影等价意义下, 除了经典的 *ovoids* 和 *Singer-type ovoids* 以外, 恰好还有两个不同构的传递 *ovoids*, 也就是例子 *5.10*中列出的例子. 而当 $d \geq 4$ 时, 我们从引理 *5.23*可得 $s < q + 1$. 因为在这种情况下有 $2^d \geq 3d$, 所以我们从引理 *5.20*中看出 O 必然射影等价于一个 *Singer-type ovoid*.

接着我们考虑 $q = p^d$ 是奇数的情况. 在 $q \in \{3, 5, 11\}$ 时, 同样通过 *Magma*[69] 得到的一个穷尽的计算机搜索表明不存在具有这种规定形式的传递 *ovoid* O. 所以我们下面假设 $q \notin \{3, 5, 11\}$. 根据引理 *5.23*, 我们有 $2s < q + 1$. 如果 m, s 其中之一是奇数, 这就与定理 *5.22*的 (i) 矛盾. 如果 m 和 s 都是偶数, 根据定理 *5.22*的 (ii), 我们有 $s \geq p^{d/e} + 1$, 其中 e 是整除 m 的 2 的最高次幂. 另一方面, 由于 d 是偶数则有 $\gcd(3, q^3 + 1) = 1$, 所以 $\gcd(3, s) = 1$. 由此从 $mks = 6d$ 中推断 s 整除 $2d/e$. 于是我们就推出 $2d/e \geq p^{d/e} + 1$, 这是不可能的. 证毕. □

我们接着考虑定理 *5.1*中 $n \geq 5$ 和群是可解的情况.

定理 5.25 (定理 5.1, $n \geq 5$ 和群是可解的情况). 令 n 是奇整数且 $n \geq 5$, 再令 q 是素数幂. 那么在 $H(n, q^2)$ 中不存在传递 ovoid 使得它在 $\mathrm{P\Gamma U}(n + 1, q^2)$ 中的稳定子群是可解的.

证明. 我们首先考虑 $p > 45$ 的情况. 如果 $n \geq \frac{p+1}{2}$, 那么根据引理 *5.7*和定理 *5.6*可知 $H(n, q^2)$ 中不存在 *ovoid*. 如果 $n \leq \frac{p-1}{2}$ 时, 那么我们继续使用反证法. 假设存在某一个传递 *ovoid*. 接着考虑下面的两种情况:

(1) 如果 m, s 中的一个数是奇数, 那么我们从引理 *5.22*的 (i) 得到 $s \geq q = p^d$. 另一方面, 因为 $s | 2nd$, 所以 $s \leq (p - 1)d < pd < p^d$: 这是一个矛盾.

(2) 如果 m 和 s 都是偶数, 那么由 *5.22*中 (ii) 可知 $s \geq 2p^{d/e}$, 其中 e 是整除 m 的 2 的最高次幂. 另一方面, 从 $mks = 2nd$ 中我们推断 s 整除 $2nd/e$, 故 $s \leq (p - 1)d/e < pd/e < 2p^{d/e}$: 这是一个矛盾.

综上所述, 在 $n \leq \frac{p-1}{2}$ 时, 我们都得到矛盾, 因此当 $p > 45$ 时 $H(n, q^2)$ 中不存在传递 *ovoids*.

剩下只需要考虑 $p < 45$ 的情况. 由引理 *5.7*的 (1) 可知对给定的素数 p 当 $n \geq p + 1$ 时 $F(n, p)$ 是关于 n 的递减函数, 其中 F 是在等式(5.2)中定义的函数. 在表 *5.4.2*中, 我们列出最大奇整数 n_p 使得对每个素数 $p < 45$ 有 $F(n_p, p) \geq 1$, 具体如下所示. 于是在 $n \leq n_p$ 时 $H(n, p^{2d})$ 中的传递 *ovoids* 的存在性不能被定理 *5.6*排除. 对

表 5.1　在 $p < 45$ 时不被定理 5.6排除的最大维数 n_p

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
n_p	5	5	7	7	9	9	11	11	13	15	15	17	17	17

于这样一对 (p,n) 且 $5 \le n \le n_p$, 我们搜索所有 *4* 元组使得 $2nd = mks$, $s|p^{nd}+1$, 并且满足引理 *5.20*和引理 *5.22*的界. 于是在表 *5.4.2*中我们列出所有不被排除的情况, 其中参数 $k = \frac{2nd}{ms}$ 被省略. 在 $H(n,q^2) = H(5,2^4)$ 或 $H(5,3^4)$ 时, 同样使用 *Magma*[69]

表 5.2　所有满足参数限制的四元组 (n,p^d,s,n) 的情况

(n,p^d)	$(5,2^2)$	$(5,3^2)$	$(9,11)$	$(7,13)$	$(9,17)$	$(15,29)$
s	5	10	18	14	18	30
m	$1,2,4$	$1,2$	1	1	1	1

得到的计算机搜索表明不可能存在具有这种规定形式的传递 *ovoid*. 而在剩下的情况下, 我们有 $s = 2n$, $m = 1$, $k = 1$ 以及 $d = 1$. 在引理 *5.22*的证明中, 我们已经说明了 $|X| \ge q$ *(*$m = 1$ 是奇数*)*, 其中对 $\mathbb{F}_{q^n}^*$ 中某个 x 有 $X = \{(x^{p^{ka}}) : 0 \le a \le s-1\}$. 因为 q 在这些情况下都是素数, 所有我们可以看出 $|X| \le n$. 由此我们推断出 $n \ge p$, 显然在这每一种情况下都是不正确的. 这就排除了表 *5.4.2*中列出的所有情况. 证毕. □

综上所述, 结合文献[2,38] 的结果以及定理 *5.24*, 定理 *5.25*, 我们完成了定理 *5.1*的证明.

6 讨论与展望

本章主要简略叙述一下作者在攻读博士学位期间其他工作, 并且列出与上述介绍的工作的一些展望和进一步可行的问题. 更多与有限几何相关的问题可以查阅下面的文献[14,21,28,63,90].

Unitals

在第 3章中, 我们针对目前已知一类能嵌入到 *Desarguesian* 射影平面 $\mathrm{PG}(2,q^2)$ 的 *unitals(Buekenhout unitals)* 进行研究, 说明这类 *unitals* 中所有非经典的例子都存在 *O'Nan* 构型, 这也部分验证了 *Piper* 的猜想. 但是 $\mathrm{PG}(2,q^2)$ 是否存在与 *Buekenhout unital* 不同构的 *unitals* 仍然是这方向热点的研究问题。此外, 存在能嵌入到 *non-Desargusian* 射影平面的 *unitals* 的例子[18,20], 这意味着解决 *Piper* 猜想仍然需要一些新的想法和工具。而且作为设计而言, *unitals* 中存在参数为非素数幂的例子[52], 因此能构造新非素数幂参数的 *unital* 也是非常有意思的题目.

$W(q)$ 的 *Payne* 派生四边形的点正则群

在第 4章中, 我们已经对奇特征下 $W(q)$ 的 *Payne* 派生四边形的点正则群进行了完整的分类, 但是偶特征时仍然存在未知的点正则群. 同样的方法也能诱导出很多满足 $\max(r_{A,B}, r_C) \leq 2$ 的点正则群的构造, 然而我们的方法也不能完全给出所有满足 $\max(r_{A,B}, r_C) \leq 2$ 的构造, 借助计算机软件 *Manga*[69] 能发现在 $q = 16$ 时存在不少新的点正则群难以用我们第 4章的方法进行刻画, 因此偶特征下的点正则群的完全刻画仍然是值得挑战的问题. 值得一提的是我们第 4章中给出的方法需要进行大量矩阵或线性化多项式的计算, 若果存在更好的数学工具对我们的证明进行优化, 或许能找到研究偶特征下的点正则群的新方法.

此外, *Kantor*[26] 在 *1982* 年用群论的语言对广义四边形描述成一类特殊的子群结构, 名为 4-*gonal family,* 这种群论语言只适用于具有经典参数的广义四边形. 随后, *Ghinelli* 构造类似于 4-*gonal family* 的 *AS*-构型去对非经典参数 $(q-1, q+1)$ 的广义四边形进行描述. 值得注意的是目前已知存在 *AS*-构型的群都是初等阿贝尔群, 因此寻找具有 *AS*-构型的非阿贝尔群或者从一些 q^3 阶群中用类似 *Kantor* 的想法构造出一个陪集几何 *(coset geometry)* 使其恰好是 $(q-1, q+1)$ 阶广义四边形也将是相当有意思的研究.

Intriguing Sets

有限极空间的 *intriguing sets* 是近 *20* 年来有限几何中重点的研究对象, 它恰好对应于具有特定的参数的强正则图. 在文献[80] 中, *Bamberg* 等人将广义四边形的

intriguing set[91] 延伸到秩大于 2 的有限极空间. 对于极空间 $\mathcal{S}$ 中的点集 $\mathcal{I}$, 如果存在两个常数 h_1 和 h_2 使得

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

那么我们称这个点集合是 *intriguing*, 其中 $P^{\perp}$ 是 $\mathcal{S}$ 中所有与 P 关联的点组成的集合. 精确而言, *intriguing sets* 可以分为两类：*i-tight sets* 和 *m-ovoids*. 这两类集合对应 h_1 和 h_2 都是确定的, 详情参考文献[80] 的引理 1. 目前很多以有趣的群为自同构群的 *intriguing sets* 以代数或者几何等方式构造出来, 详情查阅文献[92–97] 以及里面引用的文献, 寻找新参数的 *intriguing set* 一直以来是这个方向的研究热点.

在第 *5*章中, 我们已经确定了 *Hermitian* 极空间中所有传递 *ovoids* 的分类, 自然的想法是完成有限极空间中所有传递 *ovoids* 的分类, 因为 *ovoids* 本身就是 *intriguing set* 的特殊例子, 所以同样的想法也将适用于其他参数的 *intriguing sets*. 因此, 我们借助于文献[83,88] 中深刻的结果以及典型群的子群结构[79,89], 考虑一些具有特殊性质的自同构群的 *intriguing sets*. 具体就是让它们的自同构群的阶能被某个本原素因子整除, 这样我们的问题也能利用文献[83,88] 中深刻的结果把自同构群限制到特定的极大子群中, 其中文献[94,98] 给出的 *intriguing sets* 的例子也是具有这种性质. 特别值得一提的, *Singer* 群是一类具有这种性质的群, 能否把有限极空间中所有以 *Singer* 群为自同构群的 *intriguing sets* 给出一个刻画或分类也是值得挑战和研究的问题.

极小线性码

参数为 $[n,k]_q$ 的线性码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的 k 维 $\mathbb{F}_q$-线性子空间, 其中该子空间中的向量 $c = (c_1, c_2, \cdots, c_n)$ 是 $\mathcal{C}$ 的码字. 对于 $\mathcal{C}$ 中的码字 c, 只有码字 $\lambda \cdot c, \lambda \in \mathbb{F}_q^*$ 才有 $supp(\lambda \cdot c) \subseteq supp(c)$, 那么我们称该码字 c 是极小的 *(minimal)*, 其中 $supp(c) = \{i \in \{1, 2, \cdots, n\} : c_i \neq 0\}$. 特别地, 线性码 $\mathcal{C}$ 是极小的当且仅当所有码字都是极小的. 近年来, 极小线性码越来越受到学者们的关注, 不仅因为它在共享方案以及安全双方计算的应用[99–101], 而且它与射影空间 $\mathrm{PG}(n-1,q)$ 中的 *cutting blocking set* 有着密切的联系[102]. 有一种有效和方便的方法去判断线性码是否极小的, 这种方法叫做 *Ashikhmin-Barg* 条件[103]. 然而这个条件仅仅是充分的并不是必要的, 目前已经很多线性码的例子是不满足 *Ashikhmin-Barg* 条件. 我们借助一些有限域和指数和等工具给出一种从部分差集 *(partial difference sets)* 中得到极小线性码的方法, 并且说明几乎所有部分差集都能产生极小线性码. 这工作已经投稿至《*IEEE Transaction on Information Theory*》.

此外, 其他在研工作目前仍处于初步阶段, 我们这里就不做介绍.

参考文献

[1] *Cossidente A, Korchmáros G. Transitive ovoids of the Hermitian surface of* $\mathrm{PG}(3,q^2)$*, q even[J]. J. Combin. Theory Ser. A. 2003, 101(1):117–130. DOI: 10.1016/S0097-3165(02)00021-3.*

[2] *Bamberg J, Penttila T. A classification of transitive ovoids, spreads, and m-systems of polar spaces[J]. Forum Math. 2009, 21(2):181–216. DOI: 10.1515/FORUM.2009.010.*

[3] *Budaghyan L, Helleseth T. New commutative semifields defined by new PN multinomials[J]. Cryptogr. Commun. 2011, 3(1):1–16. DOI: 10.1007/s12095-010-0022-2.*

[4] *Hirschfeld J W P, Thas J A. Springer Monographs in Mathematics General Galois geometries[M]. [S.l.]: Springer, London, 2016: xvi+409. DOI: 10.1007/978-1-4471-6790-7.*

[5] *Dickson L E. Linear algebras in which division is always uniquely possible[J]. Trans. Amer. Math. Soc. 1906, 7(3):370–390. DOI: 10.2307/1986324.*

[6] *Knuth D E. Finite semifields and projective planes[J]. J. Algebra. 1965, 2:182–217. DOI: 10.1016/0021-8693(65)90018-9.*

[7] *Zhou Y. A note on commutative semifield planes[J]. Adv. Geom. 2018, 18(1):115–118. DOI: 10.1515/advgeom-2017-0017.*

[8] *Kantor W M. Finite semifields[M]. [S.l.]: Walter de Gruyter, Berlin, 2006: 103–114.*

[9] *Lavrauw M, Polverino O. Finite Semifields[M]. [S.l.]: NOVA Academic Publishers New York, 2011: 131–160.*

[10] *Sheekey J. New semifields and new mrd codes from skew polynomial rings[J]. J. London Math. Soc. 2020, 101(1):432–456. DOI: 10.1112/jlms.12281.*

[11] *Budaghyan L, Helleseth T. New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p[M]. Sequences and their applications—SETA 2008: volume 5203. [S.l.]: Springer, Berlin, 2008: 403–414. DOI: 10.1007/978-3-540-85912-3_35.*

[12] *Buekenhout F. Existence of unitals in finite translation planes of order q^2 with a kernel of order q[J]. Geometriae Dedicata. 1976, 5(2):189–194. DOI: 10.1007/BF00145956.*

[13] Metz R. On a class of unitals[J]. Geom. Dedicata. 1979, 8(1):125–126. DOI: 10.1007/BF00147935.

[14] Barwick S, Ebert G. Springer Monographs in Mathematics Unitals in projective planes[M]. [S.l.]: Springer, New York, 2008: xii+193.

[15] O'Nan M E. Automorphisms of unitary block designs[J]. J. Algebra. 1972, 20: 495–511. DOI: 10.1016/0021-8693(72)90070-1.

[16] Piper F. Unitary block designs[J]. Graph theory and combintorics. 1979, 34: 98–105.

[17] Wilbrink H. Lecture Notes in Pure and Appl. Math.: volume 82 A characterization of the classical unitals[M]. [S.l.]: Dekker, New York, 1983: 445–454.

[18] Hui A M, Law H, Tai Y, et al. Non-classical polar unitals in finite Dickson semifield planes[J]. J. Geom. 2013, 104(3):469–493. DOI: 10.1007/s00022-013-0174-2.

[19] Hui A M, Wong P P. On embedding a unitary block design as a polar unital and an intrinsic characterization of the classical unital[J]. J. Combin. Theory Ser. A. 2014, 122:39–52. DOI: 10.1016/j.jcta.2013.09.007.

[20] Tai Y, Wong P P. On the structure of the Figueroa unital and the existence of O'Nan configurations[J]. Discrete Math. 2014, 330:41–50. DOI: 10.1016/j.disc.2014.04.012.

[21] Hirschfeld J W, Thas J A. Open problems in finite projective spaces[J]. Finite Fields and Their Applications. 2015, 32:44–81.

[22] Tits J. Sur la trialité et certains groupes qui s'en déduisent[J]. Inst. Hautes Études Sci. Publ. Math. 1959, (2):13–60.

[23] Payne S E. The equivalence of certain generalized quadrangles[J]. J. Combinatorial Theory Ser. A. 1971, 10:284–289. DOI: 10.1016/0097-3165(71)90033-1.

[24] Payne S E. Nonisomorphic generalized quadrangles[J]. J. Algebra. 1971, 18: 201–212. DOI: 10.1016/0021-8693(71)90053-6.

[25] Payne S E. Quadrangles of order $(s-1,\ s+1)$[J]. J. Algebra. 1972, 22:97–119. DOI: 10.1016/0021-8693(72)90107-X.

[26] Kantor W M. Generalized quadrangles associated with $G_2(q)$[J]. J. Combin. Theory Ser. A. 1980, 29(2):212–219. DOI: 10.1016/0097-3165(80)90010-2.

[27] Ghinelli D. Characterization of some 4-gonal configurations of Ahrens-Szekeres type[J]. European J. Combin. 2012, 33(7):1557–1573. DOI: 10.1016/j.ejc.2012.03.018.

[28] Payne S E, Thas J A. EMS Series of Lectures in Mathematics Finite generalized quadrangles[M]. Second. [S.l.]: European Mathematical Society (EMS), Zürich, 2009: xii+287. DOI: 10.4171/066.

[29] Singer J. A theorem in finite projective geometry and some applications to number theory[J]. Transactions of the American Mathematical Society. 1938, 43(3):377–385.

[30] Ghinelli D. Regular groups on generalized quadrangles and nonabelian difference sets with multiplier -1[J]. Geom. Dedicata. 1992, 41(2):165–174. DOI: 10.1007/BF00182417.

[31] De Winter S, Thas K. Generalized quadrangles with an abelian Singer group[J]. Des. Codes Cryptogr. 2006, 39(1):81–87. DOI: 10.1007/s10623-005-2747-z.

[32] De Winter S, Thas K. The automorphism group of Payne derived generalized quadrangles[J]. Adv. Math. 2007, 214(1):146–156. DOI: 10.1016/j.aim.2007.01.020.

[33] De Winter S, Thas K. Generalized quadrangles admitting a sharply transitive Heisenberg group[J]. Des. Codes Cryptogr. 2008, 47(1-3):237–242. DOI: 10.1007/s10623-007-9146-6.

[34] De Winter S, Thas K, Shult E E. Singer Quadrangles[M]. [S.l.]: Oberwolfach Preprint OWP, 2009-07.

[35] Yoshiara S. A generalized quadrangle with an automorphism group acting regularly on the points[J]. European J. Combin. 2007, 28(2):653–664. DOI: 10.1016/j.ejc.2004.11.004.

[36] Bamberg J, Giudici M. Point regular groups of automorphisms of generalised quadrangles[J]. J. Combin. Theory Ser. A. 2011, 118(3):1114–1128. DOI: 10.1016/j.jcta.2010.11.004.

[37] Grundhöfer T, Joswig M, Stroppel M. Slanted symplectic quadrangles[J]. Geom. Dedicata. 1994, 49(2):143–154. DOI: 10.1007/BF01610617.

[38] Thas J A. Ovoids and spreads of finite classical polar spaces[J]. Geom. Dedicata. 1981, 10(1-4):135–143. DOI: 10.1007/BF01447417.

[39] Thas J A. London Math. Soc. Lecture Note Ser.: volume 288 Ovoids, spreads and m-systems of finite classical polar spaces[M]. [S.l.]: Cambridge Univ. Press, Cambridge, 2001: 241–267.

[40] Blokhuis A, Moorhouse G E. Some p-ranks related to orthogonal spaces[J]. J. Algebraic Combin. 1995, 4(4):295–316. DOI: 10.1023/A:1022477715988.

[41] De Beule J, Metsch K. The Hermitian variety $H(5,4)$ has no ovoid[J]. Bull. Belg. Math. Soc. Simon Stevin. 2005, 12(5):727–733.

[42] Moorhouse G E. Some p-ranks related to Hermitian varieties: volume 56[M]. [S.l.]: [s.n.], 1996: 229–241. DOI: 10.1016/S0378-3758(96)00020-1.

[43] Baker R D, Ebert G L, Korchmáros G, et al. London Math. Soc. Lecture Note Ser.: volume 191 Orthogonally divergent spreads of Hermitian curves[M]. [S.l.]: Cambridge Univ. Press, Cambridge, 1993: 17–30. DOI: 10.1017/CBO9780511526336.004.

[44] Maclagan-Wedderburn J H. A theorem on finite algebras[J]. Trans. Amer. Math. Soc. 1905, 6(3):349–352. DOI: 10.2307/1986226.

[45] Bierbrauer J. Commutative semifields from projection mappings[J]. Des. Codes Cryptogr. 2011, 61(2):187–196. DOI: 10.1007/s10623-010-9447-z.

[46] Zha Z, Wang X. New families of perfect nonlinear polynomial functions[J]. J. Algebra. 2009, 322(11):3912–3918. DOI: 10.1016/j.jalgebra.2009.04.042.

[47] Lunardon G, Marino G, Polverino O, et al. Symplectic semifield spreads of $\mathrm{PG}(5,q)$ and the Veronese surface[J]. Ric. Mat. 2011, 60(1):125–142. DOI: 10.1007/s11587-010-0098-1.

[48] Marino G, Polverino O. On the nuclei of a finite semifield[M]. Theory and applications of finite fields: volume 579. [S.l.]: Amer. Math. Soc., Providence, RI, 2012: 123–141. DOI: 10.1090/conm/579/11525.

[49] Marino G, Polverino O. On isotopisms and strong isotopisms of commutative presemifields[J]. J. Algebraic Combin. 2012, 36(2):247–261. DOI: 10.1007/s10801-011-0334-0.

[50] Blokhuis A, Lavrauw M, Ball S. On the classification of semifield flocks[J]. Adv. Math. 2003, 180(1):104–111. DOI: 10.1016/S0001-8708(02)00084-1.

[51] Coulter R S, Henderson M. Commutative presemifields and semifields[J]. Adv. Math. 2008, 217(1):282–304. DOI: 10.1016/j.aim.2007.07.007.

[52] Bagchi S, Bagchi B. Designs from pairs of finite fields. I. A cyclic unital $U(6)$ and other regular Steiner 2-designs[J]. J. Combin. Theory Ser. A. 1989, 52(1):51–61. DOI: 10.1016/0097-3165(89)90061-7.

[53] Mathon R. Constructions for cyclic Steiner 2-designs[M]. Combinatorial design theory: volume 149. [S.l.]: North-Holland, Amsterdam, 1987: 353–362. DOI: 10.1016/S0304-0208(08)72901-3.

[54] Grundhöfer T, Stroppel M, Van Maldeghem H. Unitals admitting all translations[J]. J. Combin. Des. 2013, 21(10):419–431. DOI: 10.1002/jcd.21329.

[55] Bruck R H, Bose R C. The construction of translation planes from projective spaces[J]. J. Algebra. 1964, 1:85–102. DOI: 10.1016/0021-8693(64)90010-9.

[56] Bruck R H, Bose R C. Linear representations of projective planes in projective spaces[J]. J. Algebra. 1966, 4:117–172. DOI: 10.1016/0021-8693(66)90054-8.

[57] Barwick S G. A characterization of the classical unital[J]. Geom. Dedicata. 1994, 52(2):175–180. DOI: 10.1007/BF01263605.

[58] Baker R D, Ebert G L. On Buekenhout-Metz unitals of odd order[J]. J. Combin. Theory Ser. A. 1992, 60(1):67–84. DOI: 10.1016/0097-3165(92)90038-V.

[59] Ebert G L. On Buekenhout-Metz unitals of even order[J]. European J. Combin. 1992, 13(2):109–117. DOI: 10.1016/0195-6698(92)90042-X.

[60] Ebert G L. Buekenhout-Tits unitals[J]. J. Algebraic Combin. 1997, 6(2):133–140. DOI: 10.1023/A:1008691020874.

[61] Payne S E. Topics in Finite Geometry:Ovals,Ovoids,and Generalized Quadrangles[M]. [S.l.]: [s.n.], 2007.

[62] Korchmáros G, Siciliano A, Szőnyi T. Embedding of classical polar unitals in $\mathrm{PG}(2,q^2)$[J]. J. Combin. Theory Ser. A. 2018, 153:67–75. DOI: 10.1016/j.jcta.2017.08.002.

[63] Thas J A, Thas K, Van Maldeghem H. Series in Pure Mathematics: volume 26 Translation generalized quadrangles[M]. [S.l.]: World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2006: xxx+345. DOI: 10.1142/9789812772916.

[64] Thas K. Frontiers in Mathematics Symmetry in finite generalized quadrangles[M]. [S.l.]: Birkhäuser Verlag, Basel, 2004: xxii+214.

[65] Ahrens R W, Szekeres G. On a combinatorial generalization of 27 lines associated with a cubic surface[J]. J. Austral. Math. Soc. 1969, 10:485–492.

[66] Hall Jr. M. Affine generalized quadrilaterals[M]. [S.l.]: Academic Press, London, 1971: 113–116.

[67] Swartz E. On generalized quadrangles with a point regular group of automorphisms[J]. European J. Combin. 2019, 79:60–74. DOI: 10.1016/j.ejc.2018.12.006.

[68] Bamberg J, Glasby S P, Swartz E. AS-configurations and skew-translation generalised quadrangles[J]. J. Algebra. 2015, 421:311–330. DOI: 10.1016/j.jalgebra.2014.08.031.

[69] Bosma W, Cannon J, Fieker C, et al. Handbook of magma functions[J]. Handbook of Magma Functions. 2013.

[70] Chen Y. Private communication[M]. [S.l.]: [s.n.], 2013.

[71] De Winter S, Thas K. A criterion concerning singer groups of generalized quadrangles, and construction of uniform lattices in $\widetilde{\mathbf{c}}_2$-buildings[J]. arXiv 1407.0616. 2014.

[72] Essert J. A geometric construction of panel-regular lattices for buildings of types $\widetilde{A_2}$ and $\widetilde{C_2}$[J]. Algebr. Geom. Topol. 2013, 13(3):1531–1578. DOI: 10.2140/agt.2013.13.1531.

[73] Aschbacher M. Cambridge Studies in Advanced Mathematics: volume 10 Finite group theory[M]. Second. [S.l.]: Cambridge University Press, Cambridge, 2000: xii+304. DOI: 10.1017/CBO9781139175319.

[74] Rose J S. A course on group theory[M]. [S.l.]: Cambridge University Press, Cambridge-New York-Melbourne, 1978: ix+310.

[75] Suzuki M. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]: volume 248 Group theory. II[M]. [S.l.]: Springer-Verlag, New York, 1986: x+621. DOI: 10.1007/978-3-642-86885-6.

[76] Lidl R, Niederreiter H. Encyclopedia of Mathematics and its Applications: volume 20 Finite fields[M]. Second. [S.l.]: Cambridge University Press, Cambridge, 1997: xiv+755.

[77] Milies C P, Sehgal S K. Algebra and Applications: volume 1 An introduction to group rings[M]. [S.l.]: Kluwer Academic Publishers, Dordrecht, 2002: xii+371. DOI: 10.1007/978-94-010-0405-3.

[78] Passman D S. Pure and Applied Mathematics The algebraic structure of group rings[M]. [S.l.]: Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977: xiv+720.

[79] Bray J N, Holt D F, Roney-Dougal C M. London Mathematical Society Lecture Note Series: volume 407 The maximal subgroups of the low-dimensional finite classical groups[M]. [S.l.]: Cambridge University Press, Cambridge, 2013: xiv+438. DOI: 10.1017/CBO9781139192576.

[80] Bamberg J, Kelly S, Law M, et al. Tight sets and m-ovoids of finite polar spaces[J]. J. Combin. Theory Ser. A. 2007, 114(7):1293–1314. DOI: 10.1016/j.jcta.2007.01.009.

[81] Thas J A, Payne S E. Spreads and ovoids in finite generalized quadrangles[J]. Geom. Dedicata. 1994, 52(3):227–253. DOI: 10.1007/BF01278475.

[82] Brouwer A E, Wilbrink H A. Ovoids and fans in the generalized quadrangle $Q(4,2)$[J]. Geom. Dedicata. 1990, 36(1):121–124. DOI: 10.1007/BF00181468.

[83] Guralnick R, Penttila T, Praeger C E, et al. Linear groups with orders having certain large prime divisors[J]. Proc. London Math. Soc. (3). 1999, 78(1):167–214. DOI: 10.1112/S0024611599001616.

[84] Cossidente A, Penttila T. Hemisystems on the Hermitian surface[J]. J. London Math. Soc. (2). 2005, 72(3):731–741. DOI: 10.1112/S0024610705006964.

[85] Robbins H. A remark on Stirling's formula[J]. Amer. Math. Monthly. 1955, 62: 26–29. DOI: 10.2307/2308012.

[86] Zsigmondy K. Zur Theorie der Potenzreste[J]. Monatsh. Math. Phys. 1892, 3(1): 265–284. DOI: 10.1007/BF01692444.

[87] Bamberg J, Penttila T. Transitive eggs[J]. Innov. Incidence Geom. 2006, 4:1–12.

[88] Bamberg J, Penttila T. Overgroups of cyclic Sylow subgroups of linear groups[J]. Comm. Algebra. 2008, 36(7):2503–2543. DOI: 10.1080/00927870802070108.

[89] Kleidman P, Liebeck M. London Mathematical Society Lecture Note Series: volume 129 The subgroup structure of the finite classical groups[M]. [S.l.]: Cambridge University Press, Cambridge, 1990: x+303. DOI: 10.1017/CBO9780511629235.

[90] Payne S E. Happy 70th, Jef[J]. Innov. Incidence Geom. 2017, 15:287–297. DOI: 10.2140/iig.2017.15.287.

[91] Bamberg J, Law M, Penttila T. Tight sets and m-ovoids of generalised quadrangles[J]. Combinatorica. 2009, 29(1):1–17. DOI: 10.1007/s00493-009-2179-x.

[92] Cossidente A, Pavese F. Intriguing sets of $W(5,q)$, q even[J]. J. Combin. Theory Ser. A. 2014, 127:303–313. DOI: 10.1016/j.jcta.2014.07.006.

[93] Feng T, Momihara K, Xiang Q. A family of m-ovoids of parabolic quadrics[J]. J. Combin. Theory Ser. A. 2016, 140:97–111. DOI: 10.1016/j.jcta.2016.01.002.

[94] Bamberg J, Lee M, Momihara K, et al. A new infinite family of hemisystems of the Hermitian surface[J]. Combinatorica. 2018, 38(1):43–66. DOI: 10.1007/s00493-016-3525-4.

[95] Cossidente A, Pavese F. New Cameron-Liebler line classes with parameter $\frac{q^2+1}{2}$[J]. J. Algebraic Combin. 2019, 49(2):193–208. DOI: 10.1007/s10801-018-0826-2.

[96] Cossidente A, Pavese F. Cameron-Liebler line classes of $\mathrm{PG}(3,q)$ admitting $\mathrm{PGL}(2,q)$[J]. J. Combin. Theory Ser. A. 2019, 167:104–120. DOI: 10.1016/j.jcta.2019.04.004.

[97] Feng T, Tao R. An infinite family of m-ovoids of $Q(4,q)$[J]. Finite Fields Appl. 2020, 63:101644, 16. DOI: 10.1016/j.ffa.2020.101644.

[98] Cossidente A, Culbert C, Ebert G L, et al. On m-ovoids of $W_3(q)$[J]. Finite Fields Appl. 2008, 14(1):76–84. DOI: 10.1016/j.ffa.2006.04.001.

[99] Ding C, Yuan J. Lecture Notes in Comput. Sci.: volume 2731 Covering and secret sharing with linear codes[M]. [S.l.]: Springer, Berlin, 2003: 11–25. DOI: 10.1007/3-540-45066-1_2.

[100] Yuan J, Ding C. Secret sharing schemes from three classes of linear codes[J]. IEEE Trans. Inform. Theory. 2006, 52(1):206–212. DOI: 10.1109/TIT.2005.860412.

[101] Chabanne H, Cohen G, Patey A. Lecture Notes in Comput. Sci.: volume 8565 Towards secure two-party computation from the wire-tap channel[M]. [S.l.]: Springer, Cham, 2014: 34–46. DOI: 10.1007/978-3-319-12160-4_3.

[102] Bonini M, Borello M. Minimal linear codes arising from blocking sets[J]. J.Algebr. Combin. 2020, 1–15. DOI: 10.1007/s10801-019-00930-6.

[103] Ashikhmin A, Barg A. Minimal vectors in linear codes[J]. IEEE Trans. Inform. Theory. 1998, 44(5):2010–2017. DOI: 10.1109/18.705584.

作者简历

李伟聪，男，*1992* 年，汉族，广东东莞人。

2011 年考入浙江大学数学科学学院 *(*信息与计算科学专业*)*，*2015* 年本科毕业，获得理学学士学位。*2015* 年 *9* 月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：*conglw@zju.edu.cn*

3. 研究兴趣：有限几何，代数编码，代数组合学，组合设计。

4. 攻读博士学位期间主要的研究成果

- *Tao Feng, Weicong Li. On the isotopism classes of the Budaghyan-Helleseth commutative semifields, Finite Fields and Their Application; 53:175-188, 2018*
- *Tao Feng, Weicong Li. On the existence of O'Nan configuration in ovoidal Buekenhout-Metz unitals in* $\mathrm{PG}(2, q^2)$*, Discrete Mathematics; 342(8):2324-2332, 2019.*
- *Tao Feng, Weicong Li. The point regular automorphism groups of the Payne derived quadrangle of* $W(q)$*, Submitted to Journal Combinatorial Theory Series A.*
- *Tao Feng, Weicong Li. On transitive ovoids of finite Hermitian polar spaces, Submitted to Combinatorica.*
- *Ran Tao, Tao Feng, Weicong Li. A construction of minimal linear codes from partial difference sets. Submitted to IEEE Transaction on Information Theory.*