分类号：O175.2　　单位代码：10335
密　级：　　学　　号：11635024

浙江大学

博士学位论文

中文论文题目：强正则图及相关线性码的研究

英文论文题目：**On strongly regular graphs and related linear codes**

申请人姓名：何智文
指导教师：冯涛
专业名称：应用数学
研究方向：组合设计与编码
所在学院：数学科学学院

论文提交日期：二〇二一年四月

强正则图及相关线性码的研究

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：王军 教授 上海师范大学

委员 1：王军 教授 上海师范大学

委员 2：李吉有 教授 上海交通大学

委员 3：李松 教授 浙江大学

委员 4：蔺宏伟 教授 浙江大学

委员 5：谈之奕 教授 浙江大学

答辩日期：二〇二一年五月

On strongly regular graphs and related linear codes

Author's signature: _____

Supervisor's signature: _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committe Chairperson:

Jun Wang Prof. Shanghai Normal University

Examining Committe Members:

Jun Wang Prof. Shanghai Normal University

Jiyou Li Prof. Shanghai Jiao Tong University

Song Li Prof. Zhejiang University

Hongwei Lin Prof. Zhejiang University

Zhiyi Tan Prof. Zhejiang University

Date of oral defence: May 2021

浙江大学研究生学位论文独创性声明

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

学位论文作者签名：　　签字日期：　　年　　月　　日

学位论文版权使用授权书

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

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：　　导师签名：

签字日期：　　年　　月　　日　　签字日期：　　年　　月　　日

致 谢

光阴荏苒, 日月如梭, 转眼间已经到了五年直博毕业之际. 回望在浙大的这段博士生涯, 磨难的痛苦和成长的喜悦互相参杂, 我对这一切满怀感激. 在此, 我也想对那些帮助我, 支持我的老师, 朋友, 家人表示衷心的感谢.

首先要感谢我的导师冯涛老师. 冯老师要求严格, 总是耐心解答和指导我们在科研中遇到的疑问. 虽然大家做的问题涉及面广泛, 各不相同, 但冯老师依然能提取到关键信息和思想本质. 冯老师组织了好几次国际会议, 同时鼓励我们参加其他学校组织的学术会议, 与领域内的专家教授当面交流, 学习新思想, 接触有意思的问题. 很感谢冯老师这五年来对我的指导和帮助.

我也要感谢周悦老师, 丁存生老师, 文洁晶老师, 方伟军老师, 向青老师, 他们对我在学术上的指导与建议让我受益颇丰. 衷心感谢方爱敏老师, 陈志国老师, 李萌老师, 他们在生活上给予了我许多关心和建议, 让我勇敢地跨过了很多坎坷.

感谢我的同门: 李伟聪师兄, 张一炜师兄, 张韬师兄, 汪馨师兄, Jerod Michel 师兄, 丁报昆师兄, 马景学师兄, 钱昺辰师兄, 林灯师兄, 戚立波师兄, 陶然, 王野, 奚元霄, 徐子翔, 韩雪姣, 兰昭君, 陈婷婷, 周靖坤, 孙秀芳, 狄文帝, 陆建兵, 林培贤等. 这是一个十分温暖的集体, 大家经常在一起探讨问题, 一起学习新知识, 互相鼓励, 共同进步.

感谢我的朋友: 李书杨, 张晶晶, 白一格, 许佳攀, 刘中东, 巩亮琴等. 他们一直站在我的身旁陪伴我成长, 用美好充实了我的博士生涯.

感谢我的父母, 他们一直站在我身后, 默默付出, 成为我最坚强的后盾. 他们始终鼓励我追求梦想, 为社会作贡献. 感谢我的妹妹何颖琦, 她对我的关心和鼓励让我勇敢向前, 不惧艰难险阻.

感谢所有帮助过我的人.

最后我要感谢浙江大学, 浙大为我们提供了很好的科研平台, 让我们能接触到很多国际前沿的领域, 学习到很多新的思想和工具. 学校不仅用很浓厚的人文情怀感染我们, 还教我们脚踏实地做一个求是人, 为国家建设贡献一份力量.

摘 要

强正则图和有向强正则图是组合图论中十分重要的两类图, 它们与不同领域中的许多有意思的结构有着密切的联系, 如有限几何、编码理论以及组合设计理论等等. 研究者们通常借助凯莱图对这两类图进行研究和构造, 得到了许多不同类型的强正则图和有向强正则图. 组合理论中的结合方案和 t-设计是近几十年来被大量研究的两种组合结构, 它们在图论、编码理论、密码学、通信和统计学领域有着广泛的应用. 特别地, 强正则图和无定形对称结合方案有着很强的联系, 另外 t-设计和线性码之间的相互作用的研究也一直是大家感兴趣的课题. 本文将通过代数方法构造非交换 2-群上的强正则凯莱图和无定形凯莱结合方案, 并利用部分和族构造新的有向强正则凯莱图. 本文亦致力于研究由一类三元线性码对应的支撑 2-设计所生成的线性码.

在第一章中, 我们简要介绍了本文的研究背景、文献综述以及主要内容.

在第二章中, 我们首先考虑了 RT2 图, Davis-Xiang 图和它们对应的无定形交换凯莱结合方案的正则自同构群. 接着得到了通过交换正则自同构群构造非交换的正则自同构群的一般性结论, 并将它们应用到这两类图以及对应的无定形交换凯莱结合方案中, 从而得到了无定形非交换凯莱结合方案.

在第三章中, 我们利用了局部环对上的部分和族构造了具有新参数的有向强正则图. 得到了 16 个新的有向强正则图无穷类, 并给出了一类新的一致部分和族.

在第四章中, 我们讨论了由 Hermitian 函数定义的仿射不变三元码. 首先计算了这些三元码的最小重量码字所对应的支撑 2-设计的关联矩阵. 然后证明了由这些关联矩阵的行所生成的线性码是四阶广义 Reed-Muller 码的子码, 并且它们可以得到 2-设计. 最后, 确定了所得的三元线性码的维数, 并给出了该码的最小距离的下界.

在第五章中, 我们总结了本文所涉及的主要工作, 并简略叙述了接下来工作的展望.

关键词: 凯莱图; 无定形凯莱方案; 正则自同构群; 强正则图; 有向强正则图; 部分和族; 局部环; 三元码; 2-设计; 广义 Reed-Muller 码.

Abstract

Strongly regular graphs and directed strongly regular graphs are two important kinds of graphs in combinatorial graph theory. They are closely related to many interesting structures in different fields, such as finite geometry, coding theory, combinatorial design theory and so on. By means of Cayley graph, many different types of strongly regular graphs and directed strongly regular graphs have been obtained. The association scheme and the t-design in combinatorial theory are two kinds of combinatorial structures which have been studied extensively in recent decades. They are widely used in graph theory, coding theory, cryptography, communication and statistics. In particular, strong regular graphs have a strong connection with the amorphic Cayley schemes, and the interaction between t-designs and linear codes has been a topic of interest. In this paper, we will construct strongly regular Cayley graph and amorphic Cayley schemes on non-abelian 2-groups by algebraic method, and construct new directed strongly regular Cayley graph by using partial sum families. This paper is also devoted to the study of linear codes generated by supporting 2-designs corresponding to a class of ternary linear codes.

In Chapter 1, we will briefly introduce the research background, literature review and the main content of this paper.

In Chapter 2, we consider regular automorphism groups of graphs in the RT2 family and the Davis-Xiang family and amorphic abelian Cayley schemes from these graphs. We derive general results on the existence of non-abelian regular automorphism groups from abelian regular automorphism groups and apply them to the RT2 family and Davis-Xiang family and their amorphic abelian Cayley schemes to produce amorphic non-abelian Cayley schemes.

In Chapter 3, we construct directed strongly regular graphs with new parameters by using partial sum families with local rings. 16 families of new directed strongly regular graphs are obtained and the uniform partial sum families are given.

In Chapter 4, we study the affine-invariant ternary codes defined by Hermitian functions. We first compute the incidence matrices of the 2-designs supported by the minimum weight codewords of these ternary codes. Then we show that the linear codes spanned by the rows of these incidence matrices are subcodes of the 4-th order generalized Reed-Muller codes and also hold 2-designs. Finally, we determine the dimension and develop a lower bound on the minimum distance of our ternary linear

codes.

In chapter 5, we summarize the main work of this paper and briefly describe the future work.

Keywords: Cayley graph; amorphic Cayley scheme; regular automorphism group; strongly regular graph; directed strongly regular graph; partial sum family; local ring; ternary code; 2-design; generalized Reed-Muller code.

目 次

1 引言

1.1 选题背景与意义

强正则图是近几十年来十分热门的研究课题. Bose[51] 于 1963 年首次通过偏几何和对称几何方案研究了强正则图的结构. 在这之后, 陆陆续续涌现了很多关于强正则图的一般性质和结构的研究. 对于一个图 Γ, 若其存在一个自同构群 G 对其点集的作用是正则的, 则图 Γ 可等价转化为凯莱图. 于是我们可以通过在不同的群 G 上寻找合适的子集 D 来得到强正则凯莱图 $\mathrm{Cay}(G, D)$, 这里的子集 D 被称为偏差集. Ma[56] 就 1994 年以前偏差集的相关研究做了详细且全面的总结, 并定义了好几种类型的偏差集. 其中的拉丁方型偏差集和负拉丁方型偏差集受到了广泛的关注. 本文将关注 RT 图和 Davis-Xiang 图这两类图, 它们对应于拉丁方型或负拉丁方型的偏差集. 相关文献表明, 关于负拉丁方型的偏差集的构造比起拉丁方型的偏差集的构造相对欠缺.

研究者们利用有限域和有限局部环构造了大量的有限交换 p-群上的偏差集. 然而非交换 p-群上的偏差集的研究相对较少, 目前已知的只有 Ghineli[18]、Swartz[20] 和 Smith[42] 构造的非交换 p-群上的偏差集. 构造偏差集的方法有很多，其中包括：二次型、bent 函数、二次曲面以及群直积等. 本文通过研究已知图的正则自同构群的方法来得到新的非交换 2-群上的偏差集. 强正则图和无定形对称结合方案有着密切的联系, Ivanov[11] 和 Ito 等人[58] 的结果表明一个参数 $n > 2$ 的对称结合方案 $\mathcal{S}$ 是无定形的当且仅当其子图均为拉丁方型或者均为负拉丁方型的强正则图. 另外, van Dam[19] 证明了如果一个点集 X 上的完全图能被划分为拉丁方型或者负拉丁方型的强正则图, 那么由点集和这些图的关系就能得到一个对称结合方案. 文献[19] 表明若把 $G \setminus \{1\}$ 做任意的划分使得 $D_1, D_2, \cdots, D_n$ 均为拉丁方型的偏差集或者均为负拉丁方型的偏差集, 我们将得到一个凯莱结合方案 $\mathcal{S} = (G; D_1, D_2, \cdots, D_n)$. 显然这也是一个无定形凯莱结合方案. 对于给定的参数集, 如何确定包含拥有这些参数的偏差集的群是现今偏差集研究领域中的一个核心问题. 于是本文尝试构造已知的两类图以及其对应的无定形结合方案的正则自同构群来试图给这个问题一个解决方案.

1988 年 Duval[4] 首次提出了有向强正则图的概念. Duval 对于有向强正则图的参数和结构的研究工作推动了这个新领域的发展, 同时吸引了大量研究者的关注. 众所周知, 无向图在代数图论中起到了核心作用. 有向图是强正则图关于有向性的一种推广, 其由于有趣的结构性质被与各种组合结构相联系. 研究者们使用了许多不同的工具去构造有向强正则图, 其中包括: 二次剩余类、克罗内克积、组合块设计、分块矩阵、凝聚代数、凯莱有向图、广义凯莱有向图、半直积、

有限关联结构、设计以及部分和族等. Hobart 和 Shaw[53] 关于无法通过交换群上的凯莱图得到有向强正则图的结论给大家提供了构造有向强正则图的两个清晰的方向: 考虑交换群上的 m-凯莱图, $m \geq 2$, 或者通过非交换群上的凯莱图构造有向强正则图. Martínez 和 Araluze[44] 考虑群上的集族, 通过集族构造 m-凯莱图, 并给出 m-凯莱图成为有向强正则图时集族所需要满足的条件, 由此引入了部分和族的概念. 部分和族概念的引入为构造有向强正则图提供了新的方向, 加上其清晰的代数结构性质, 使得我们很容易借助代数方法去进行构造. 在文献[44] 的最后, 他们提出了三个未解决的问题, 其中的第二个是对任意的 $m \geq 2$, 有向强正则 m-凯莱图的存在性问题. 本文试图去解决这个问题并构造具有新参数的有向强正则图. 很自然地, 我们能借助强正则图为研究有向强正则图寻找新的思路. 受到 Polhill 在文献[32] 中使用 Galois 环构造强正则图的启发, 本文尝试使用局部环以及他们所用到的 "spread" 来构造得到有向强正则图. 得益于群环互反公式, 我们亦使用群环语言和特征理论来处理部分和族的证明部分, 由此我们的运算得到了大量的简化. 虽然目前已经有许多论文讨论不同参数值的有向强正则图的存在性和唯一性问题, 但至今仍有大量的有向强正则图的存在性尚未确定. 因此我们认为有向强正则图领域还有许多问题值得研究和推广.

组合 t-设计是近几十年来组合数学中一个十分有意思的课题, 其在编码理论、密码学、通信和统计学等领域有着广泛的应用. 尤其关于 t-设计理论和编码理论之间的相互作用一直是组合学家和编码理论家非常感兴趣的话题, 这在许多文献中得到了印证. Ding 在其最近发表的著作[12] 中详细总结了 t-设计和线性码之间的联系并且研究了这两者所需要的基本知识和性质. 从线性码得到 t-设计有两种经典的方法: 第一种是利用 Assmus-Mattson 定理[35], 第二种是研究线性码的自同构群, 如果自同构群的置换部分在码上是 t-传递的, 则可通过线性码得到 t-设计, 详见[34]. 关于这两种方法的使用都有大量的参考文献. 例如, 最近 Ding 和 Tang[14] 借助 Assmus-Mattson 定理得到了包含 2-设计和 3-设计的接近最大距离可分码无穷类, 解决了一个 70 年来的公开问题. 这表明线性码和 t-设计之间还有很多问题有待深入挖掘. 当线性码是仿射不变时, 那么就存在一个置换子群作用在该码上是 2-传递的, 这意味着我们可以通过该码得到 2-设计. 研究者们常常借助一个判定条件, 即线性码是否为仿射不变的来判断该码是否能得到 2-设计. Ding 等人[13] 考虑利用由线性码得到的 t-设计再次生成线性码, 并对所得到的线性码进行研究. 他们所使用的三元码是由函数 $\mathrm{Tr}_{2m}(at^2+bt)+h$ 定义得到的, 于是我们很自然地想到去考虑由 Hermitian 函数 $\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h$ 定义的三元码. 类似地去研究该三元码得到的支撑设计对应的线性码所具有的性质以及这些码的参数.

1.2 文献综述

Bose[51](1963) 首次通过偏几何和对称几何方案研究了强正则图的结构. 1975 到 1991 年之间, Hubant[68](1975)、Cameron[49](1978)、Seidel[36](1979)、Brouwer 和 van Lint[6](1984) 以及 Cameron 和 van Lint[50](1991) 等人进行了很多关于强正则图的一般性质理论和结构的研究. 之后 Brouwer 和 Haemers 在文献[5](2012) 中总结了有关图谱、研究图的线性代数工具、图的特征值和特征向量、结合方案以及强正则图的基本性质和背景等内容. 大量的文献表明, 凯莱图是用于研究强正则图十分常见且有用的工具. 通过寻找群 G 中合适的子集 D 来得到强正则凯莱图 $\mathrm{Cay}(G, D)$, 这样的子集 D 被称为偏差集. 偏差集与组合学的其他分支、编码理论以及有限几何有着密切的联系. Calderbank 和 Kantor[10](1986) 利用射影 2-重码和射影 2-交集构造了大量的偏差集. Leung 和 Ma 在文献[39](1990) 中使用有限局部环构造了 p-群上的偏差集和相关差集, 之后又在文献[37](1994) 中得到了 Paley 偏差集. Ma[56](1994) 就 1994 年以前偏差集的研究构造进行了详尽而全面的总结.

在这之后, 有许多新的构造方法和技巧被挖掘, 改进和完善. 其中有大量的工作是利用有限域和有限局部环构造有限交换 p-群上的偏差集. Hou 等人在文献[61](2000)、文献[64](2001)、文献[62](2002)、文献[63](2003) 和文献[65](2007) 分别使用了有限拟 Frobenius 局部环、Galois 环、有限 Frobenius 局部环以及有限链环构造了一系列新的偏差集. Hamilton[47](2002) 利用投射空间中的嵌套 “放大” 二次型构造了新的强正则图. Davis 和 Xiang[27](2004) 利用二次曲面构造了指数为 4 的非初等交换 2-群上的负拉丁方型偏差集. Polhill 在文献[28](2008) 中通过将有限域上分圆类进行推广, 从而得到了非初等交换 p-群上新的负拉丁方型偏差集. 之后 Polhill 等人在文献[31] 中使用了直积构造方法. Tan 等人[72](2010) 通过有限域上的几种已知的 bent 函数得到了基本交换 p-群上的新强正则图. 之后 Chee 等人[69](2011) 将 Tan 等人所用的 3 元 bent 函数推广至 p 元 bent 函数, 并用 p 元 bent 函数构造了新的强正则图. Chen 和 Polhill[70](2012) 构造了一种伪二次 bent 函数, 并用这些函数代替二次型构造了交换 p-群上的偏差集. Feng 等人[57](2013) 使用二次型和 p 元弱正则 bent 函数构造了交换 p-群上新的负拉丁方型的偏差集. Bouyukliev 等人[24](2006) 和 Kohnert[8](2007) 利用所得到的新二重码等价得到了交换 p-群上的新偏差集. 然而对于有限非交换群 p-群上的偏差集的研究相对较少, 目前 Smith[42](1995)、Ghineli[18](2012) 和 Swartz[20](2015) 分别构造了非交换 p-群上的偏差集.

Ivanov[11](1985) 和 Ito 等人[58](1991) 研究了无定形对称结合方案 S 与拉丁方型以及负拉丁方型的强正则图之间的关系. van Dam 在文献[19](2003) 中给出了由点集上的完全图得到无定形对称结合方案的等价条件.

关于有向强正则图, Duval[4](1988) 首次提出有向强正则图的概念, 并给出了有向强正则图的参数所要满足的几个必要条件. 除了一些非存在性的证明, Duval 亦通过块构造和克罗内克积

构造给出了有向强正则图的一些存在性的结果. Jørgensen[43](2001) 为 Duval 关于顶点数 $v \leq 20$ 的有向强正则图的存在性问题提供了完整的答案. Fiedler 等人[22](2002) 在计算机的帮助下确定了所有点数 $v \leq 20$ 的具有顶点传递自同构群的有向强正则图, 同时他们还通过凝聚代数 (coherent algebras) 研究有向强正则图. 除此之外, 用凝聚代数研究有向强正则图的还有 Fiedler 等人[23](1999) 和 Klin 等人[46](2004). 我们还可以通过许多组合结构得到有向强正则图, 例如 Olmez、Song[48](2012) 和 Brouwer 等人[3](2012) 利用了有限关联结构, Gyürki[55](2016) 借助了平衡分割以及 Adams 等人[21](2018) 使用了块矩阵等等.

类似于强正则图, 有向强正则图的研究和有向凯莱图以及有向 m-凯莱图有着密切的联系. Hobart 和 Shaw[53](1999) 给出了有限群的子集成为一个有向强正则图的连通集的充要条件并得到了有向强正则图的无穷类. 他们还证明了一个非平凡的有向强正则图无法通过交换群上的凯莱有向图得到. Duval 和 Iourinski[9](2003) 在非交换的半直积群上构造了有向强正则凯莱图. 大量的文献表明, m-凯莱图是研究强正则图非常有用的工具, 例如 Resmini 和 Jungnickel[45](1992) 以及 Leung 和 Ma[40](1993) 借助了半凯莱图以及 Kutnar 等人[41](2009) 使用了 3-凯莱图等等. Martínez 和 Araluze[44](2010) 基于 Duval 和 Iourinski[9](2003) 早期的工作, 提出了部分和族的概念, 并用部分和族构造了 m-有向凯莱图. Araluze 等人[1](2011) 借助部分和族得到了有向强正则图的一些构造, 并给出了一致部分和族的定义, 证明了部分和族的实用性. Araluze 等人[2](2012) 通过部分和四元组 (即 $m = 2$ 时的部分和族) 研究了循环群的 2-凯莱有向强正则图的结构并得到了一些无穷类.

众所周知 t-设计和线性码是密切相关的, Assumus 和 Mattson[35](1969) 给出了通过线性码的码字所定义的点和块成为一个 t-设计所需要满足的条件, 由此得到了 Assmus-Mattson 定理. 该定理对于用线性码构造 t-设计来说是一个十分有用的工具. 例如, Ding 和 Li[16](2017) 以及 Ding[15](2017) 通过该定理在线性码中找到了大量的 2-设计和 3-设计无穷类. 另外，Dodunekov 和 Landgev[54](1995) 给出了一个接近最大距离可分码中存在 t-设计的充分条件. 基于他们的结论, Ding 和 Tang[14](2020) 得到了包含 2-设计和 3-设计的接近最大距离可分码无穷类, 从而解决了 70 年来一直未得到解决的问题: 是否存在包含 t-设计无穷类的接近最大距离可分码.

为了通过线性码得到 t-设计, 除了使用 Assmus-Mattson 定理外, 我们还可以通过 Assmus 和 Key 在文献[34](1992) 中所得到的结论: 如果码的自同构群的置换部分在码上是 t-传递的, 则该码可以得到 t-设计. Ding[12](2018) 详细总结了这两者之间的关系以及所需要的基本知识和性质. 另外, Ding 提到当线性码是仿射不变时, 其置换子群在码上的作用是 2-传递的. Du 等人[66](2019) 和 Du 等人[67](2019) 通过证明所用的码是仿射不变的, 从而得到这些码是可以得到 2-设计的. 建立在线性码和 t-设计可以相互转化的基础上, Ding 等人[13](2020) 使用文献[16] 中的一类三元线性码的最小重量码, 得到了这些码字对应的支撑 2-设计的关联矩阵, 并计算了关联矩阵的行所生

成的线性码的参数.

1.3 文章主要内容与创新点

本文的主要内容集中在第二、三、四章节中, 分别对非交换 2-群上的偏差集和无定形凯莱结合方案的构造问题, 局部环上有向强正则图的构造问题以及由 Hermitian 函数定义的仿射不变三元码进行了研究. 下面简单介绍每一章节的主要内容和创新点.

- 第二章: 我们主要尝试构造非交换 2-群上的拉丁方型和负拉丁方型的偏差集以及对应的无定形凯莱结合方案. 如果需要得到这类偏差集, 最经典的方法之一是利用非退化二次型的零点进行构造, 我们称由这类方法得到的强正则图为 RT2 图. 另一种方法是由 Davis 和 Xiang 提出的, 即将上述偏差集通过变形得到的非初等交换 2-群上的偏差集, 我们称这类偏差集所对应的图为 Davis-Xiang 图. 本章研究了这两类图的正则自同构群, 并从交换的正则自同构群出发, 得到了这两类图的非交换正则自同构群. 在此基础上, 这两类图以及对应的无定形凯莱结合方案在非交换 2 群上的存在性得以证明. 目前几乎所有已知的包含拉丁方型或负拉丁方型偏差集的群都是交换 p-群, 然而关于非交换 p-群上的拉丁方型和负拉丁方型的偏差集的研究和构造非常少. 通过本章的构造可以得到许多非交换的正则自同构群, 它们分别具有幂零类数 $2, 3, 4$ 或 6 以及指数 $4, 8$ 或 16. 由此表明, 非交换群上的偏差集的构造是一个值得继续研究的问题. 如文献[27] 所述, 现今研究偏差集的一个核心问题是, 对于给定的参数集, 如何确定包含拥有这些参数的偏差集的群. 我们的研究表明, 通过已知的强正则图和无定形结合方案的正则自同构群构造非交换正则自同构群是解决这个问题的一个比较可取的办法. 这部分的内容已发表在 “Journal of Combinatorial Designs” 杂志上.

- 第三章: 我们借助部分和族在由局部环 $\mathcal{R}$ 得到的群 $G = (\mathcal{R} \times \mathcal{R}, +)$ 上构造了一类新的有向强正则图. 我们考虑群 G 上定义的部分和族. 因为由部分和族定义的 m-凯莱图是一个有向强正则图, 所以我们试图通过构造部分和族来获得有向强正则图. 借助群环语言和特征理论, 我们简化了集族成为部分和族的条件, 从而找到了构造部分和族的新方法. 对比 Brouwer 的主页[7] 上列出的参数, 可以发现该构造在 $v < 110$ 的情况下有 16 个新的 5 元组的参数:

  $$(50, 18, 7, 6, 12),\quad (75, 28, 11, 10, 16),\quad (75, 32, 13, 14, 20),\quad (98, 26, 9, 6, 16),$$
  $$(98, 32, 11, 10, 22),\quad (98, 39, 16, 15, 27),\quad (100, 38, 15, 14, 20),\quad (100, 42, 17, 18, 24),$$

  以及这些参数的补参数

  $$(50, 31, 18, 21, 25),\quad (75, 46, 27, 30, 34),\quad (75, 42, 23, 24, 30),\quad (98, 71, 50, 55, 61),$$
  $$(98, 65, 42, 45, 55),\quad (98, 58, 33, 36, 46),\quad (100, 61, 36, 39, 43),\quad (100, 57, 32, 33, 39).$$

由此证明了部分和族是一种构造有向强正则图的强有力的工具. 在一些情况下, 还可以通过此构造方法得到 $\mathcal{R}$ 为有限域的情况下的一致部分和族, 解决了文献[1] 中关于一致部分和族的存在性的疑虑. 这部分的内容已发表在 “Designs, Codes and Cryptography” 杂志上.

- 第四章: 我们研究了由 Hermitian 函数定义的仿射不变三元码. 首先利用三元码的最小重量码字得到了 2-设计, 然后计算这些 2-设计对应的关联矩阵. 在此基础上, 我们将关联矩阵的行生成的向量空间定义为 2-设计对应的线性码. 然后证明了所得到的这些线性码是四阶广义 Reed-Muller 码的子码, 并且能通过其子码再次得到 2-设计. 另外, 本章所得到的线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 包含了最开始所使用的三元线性码 $\mathcal{C}(2m,3)$. 这意味着, 线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的结构比原来的线性码 $\mathcal{C}(2m,3)$ 的结构更加丰富. 最后我们确定了这些三元线性码的维数, 并给出了其最小距离的下界. 本章的研究展现了 t-设计和线性码之间很强的关联性, 同时也意味着不仅可以通过线性码来获得 t-设计, 还可以从 t-设计所对应的关联矩阵获得具有良好性质的线性码. 这部分的内容已经发表在 “Cryptography and Communications” 杂志上.

在本文的写作过程中, 得到了国家自然科学基金 (No.11771392) 的支持.

由于作者自身的学术水平有限, 加上时间和篇幅的限制, 本文的研究难免有谬误和不详之处, 恳请各位专家和读者不吝批评和指正.

2 非交换 2-群上的偏差集和无定形凯莱结合方案

本章研究了 RT2 图和 Davis-Xiang 图的正则自同构群, 以及这些图对应的无定形交换凯莱结合方案. 我们从无定形凯莱结合方案的交换正则自同构群出发, 得到了非交换的正则自同构群的存在性的一般结果, 并将这些结果应用到 RT2 图和 Davis-Xiang 图及其无定形交换凯莱结合方案中, 得到了无定形非交换凯莱结合方案. 我们所构造的是幂零类数为 $2, 3, 4$ 或 6 以及指数为 $4, 8$ 或 16 的正则自同构群.

本章的主要内容组织如下. 在第一节中, 我们引入强正则图、凯莱图以及对称结合方案的基本知识. 在第二节中, 介绍了一个研究 RT2 图和 Davis-Xiang 图以及对应的无定形对称结合方案的一般框架, 并描述了研究它们的正则自同构群的策略. 在第三节中, 首先得到了由二次型构造的偏差集的正则自同构群的一般性结论, 然后将这些结论运用到 RT2 图, Davis-Xiang 图以及无定形结合方案中. 我们通过计算群的不变量来区分所得到的正则自同构群.

2.1 基本知识

一个图 $\Gamma = (V, E)$ 是由点集 V 和边集 E 组成的, 其中对任意两个顶点 $x, y \in V$, x 和 y 之间有边当且仅当 $(x, y) \in E$. 若对任意的顶点 $x \in V$ 均有 k 条边与之相关联, 则称 Γ 是 k 正则图. 若 Γ 的任意两个顶点间均有边, 则称 Γ 是一个完全图.

定义 2.1 一个参数为 (v, k, λ, μ) 的**强正则图 (strongly regular graph)**$\Gamma = (V, E)$ 是一个有 v 个顶点的非完全并且非空的 k 正则图, 其中对任意两个不同的顶点 $x, y \in V$:

(1) 如果 $(x, y) \in E$, 则恰好有 λ 个 $z \in V$ 使得 (x, z) 和 $(z, y) \in E$;

(2) 如果 $(x, y) \notin E$, 则恰好有 μ 个 $z \in V$ 使得 (x, z) 和 $(z, y) \in E$.

对于一个图 $\Gamma = (V, E)$, 若存在 Γ 的一个自同构群 G 作用于顶点集 V 上是正则的, 即 G 作用在顶点集上是传递的且任意非单位元不固定任何点, 则我们在顶点集中任意选取一个点 a 并定义 G 中的一个子集 $D = \{g \in G : (a, a^g) \in E\}$. 易知 Γ 的点集 $V = \{a^g : g \in G\}$, 边集 E 和群 G, 子集 D 分别建立了一一对应关系.

定义 2.2 对于群 G 和其子集 D, **凯莱图 (Cayley graph)Cay**(G, D) 的定义如下:

(1) 其顶点是 G 中的元素;

(2) 对于任意的两个顶点 g_1 和 $g_2 \in G$, g_1 和 g_2 在凯莱图 Cay(G, D) 中相邻当且仅当 $g_2 g_1^{-1} \in D$.

易证图 Γ 同构于凯莱图 Cay(G, D). 此时我们可以通过凯莱图 Cay(G, D) 描述图 Γ 的性质:

(1) 图 Γ 无圈当且仅当 $1 \notin D$,

(2) 图 Γ 无向当且仅当 $D = D^{(-1)}$,

(3) 图 Γ 是强正则的当且仅当 (i) 若 $g \in D$, 则 $|D \cap gD| = \lambda$; (ii) 若 $g \in G \setminus D$, 则 $|D \cap gD| = \mu$.

定义 2.3 对任意的 v 阶群 G 和 G 的一个大小为 k 的子集 D, 我们将满足以上三个条件的集合 D, 称为群 G 中的 (v, k, λ, μ)-**偏差集 (partial difference set)**.

定义 2.4 假设 D 为具有参数 $(n^2, r(n-\epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$ 的偏差集, 其中 n 和 r 均为正整数, $\epsilon = \pm 1$. 当 $\epsilon = 1$ 时, D 被称为**拉丁方型 (Latin square type) 的偏差集**; 当 $\epsilon = -1$ 时, D 被称为**负拉丁方型 (negative Latin square type) 的偏差集**.

在本次课题中, 我们主要尝试构造非交换 p-群上的拉丁方型偏差集以及负拉丁方型偏差集.

定义 2.5 记 $\Gamma(X)$ 为点集 X 上的完全图. 有限集 X 上的**对称结合方案 (symmetric association scheme)** 是 $\Gamma(X)$ 的一个划分 $\Gamma_1, \Gamma_2, \cdots, \Gamma_n$ 使得这些子图的邻接矩阵 $A_1, A_2, \cdots, A_n$ 满足: 对任意正整数 $1 \leqslant i, j \leqslant n$, 存在非负整数 $p_{i,j}^0, p_{i,j}^1, \cdots, p_{i,j}^n$ 使得 $A_i A_j = p_{i,j}^0 I_X + p_{i,j}^1 A_1 + p_{i,j}^2 A_2 + \cdots + p_{i,j}^n A_n$, 其中 I_X 是阶为 $|X|$ 的单位矩阵. 假设子图 $\Gamma_1', \Gamma_2', \cdots, \Gamma_m'$ 是完全图 $\Gamma(X)$ 的一个划分且满足: 对任意 $1 \leqslant i \leqslant n$, 存在 $1 \leqslant j \leqslant m$ 使得 $\Gamma_i \subseteq \Gamma_j'$. 若所有这样的划分所对应的组合结构 $\mathcal{S}' = (X; \Gamma_1', \Gamma_2', \cdots, \Gamma_m')$ 仍旧是一个对称结合方案, 则称对称结合方案 $\mathcal{S} = (X; \Gamma_1, \Gamma_2, \cdots, \Gamma_n)$ 是**无定形 (amorphic) 的**.

根据 Ivanov[11] 和 Ito[58] 等人的结果, 我们知道一个参数为 $n > 2$ 的对称结合方案 S 是无定形的当且仅当子图 $\Gamma_1, \Gamma_2, \cdots, \Gamma_n$ 均为拉丁方型或者均为负拉丁方型的强正则图. 另外, van Dam[19] 证明了如果能将点集 X 上的完全图划分成全都是拉丁方型或者全都是负拉丁方型的强正则图 $\Gamma_1, \Gamma_2, \cdots, \Gamma_n$, 那么所得到的 $\mathcal{S} = (X; \Gamma_1, \Gamma_2, \cdots, \Gamma_n)$ 就是一个无定形对称结合方案.

对于点集 X 的一个置换, 若其是所有子图 $\Gamma_1, \Gamma_2, \cdots, \Gamma_n$ 的自同构, 则称该置换为 $\mathcal{S}$ 的一个自同构. 包含结合方案 $\mathcal{S}$ 的所有自同构的集合是置换群的一个子群, 我们称之为 $\mathcal{S}$ 的完全自同构群, 并记为 Aut$(\mathcal{S})$. 完全自同构群 Aut$(\mathcal{S})$ 的任意子群 G 被称为 $\mathcal{S}$ 的自同构群.

定义 2.6 如果有一个自同构群 G 在 $\mathcal{S}$ 上的作用是正则的, 那么群 G 和点集 X 就可等价对应起

来, 并且可以得到 $G\setminus\{1\}$ 的一个划分 $D_1, D_2, \cdots, D_n$ 使得对任意的 $1 \leqslant i \leqslant n$, $D_i = D_i^{(-1)}$ 以及 $\Gamma_i \cong \mathrm{Cay}(G, D_i)$. 我们称这样的 $\mathcal{S}$ 为**凯莱结合方案 (Cayley association scheme)**, 并将其记为 $\mathcal{S} = (G; D_1, D_2, \cdots, D_n)$.

一个凯莱结合方案 $\mathcal{S}$ 是无定形的当且仅当 $D_1, D_2, \cdots, D_n$ 均为拉丁方型或者均为负拉丁方型的偏差集. 利用 van Dam 在文献[19] 中的一个定理, 若把 $G\setminus\{1\}$ 做任意的划分使得 $D_1, D_2, \cdots, D_n$ 均为拉丁方型的偏差集或者均为负拉丁方型的偏差集, 我们将得到一个凯莱结合方案 $\mathcal{S} = (G; D_1, D_2, \cdots, D_n)$. 显然这也是一个无定形凯莱结合方案.

2.2 RT2 图、Davis-Xiang 图及其无定形结合方案

设 q 是一个素数幂, $\mathbb{F}_q$ 是有 q 个元素的有限域. 我们定义 V 为 $\mathbb{F}_q$ 上的 n 维向量空间. 若函数 $Q: V \to \mathbb{F}_q$ 满足如下条件, 则被称为 $\mathbb{F}_q$ 上的二次型:

(1) 对所有的 $s \in \mathbb{F}_q$ 以及 $v \in V$, $Q(sv) = s^2 Q(v)$;

(2) 函数 $B(v_1, v_2) := Q(v_1 + v_2) - Q(v_1) - Q(v_2)$ 是 $\mathbb{F}_q$ 上的双线性型.

二次型 Q 的根式定义为

$$\mathrm{Rad}(Q) := \{v \in V : Q(v) = 0 \text{ 且 } \forall x \in V, B(v, x) = 0\}.$$

若 $\mathrm{Rad}(Q) = \{0\}$, 则二次型 Q 被称为非退化二次型. 当二次型 Q 是非退化时, 我们能找到 V 中的一组基 $e_1, \cdots, e_n$ 使得以下之一成立:

(1) 当 n 是偶数时, $Q(x) = x_1x_2 + \cdots + x_{n-1}x_n$(此时称 Q 是双曲线二次型);

(2) 当 n 是偶数时, $Q(x) = x_1x_2 + \cdots + x_{n-3}x_{n-2} + x_{n-1}^2 + ax_{n-1}x_n + bx_n^2$, 其中 a 和 b 是 $\mathbb{F}_q$ 中的元素且满足式子 $X^2 + aX + b$ 在 $\mathbb{F}_q$ 上不可约 (此时称 Q 是椭圆二次型);

(3) 当 n 是奇数时, $Q(x) = x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n^2$(此时称 Q 是抛物线二次型);

当 n 为偶数且 Q 非退化时, 若 Q 是双曲线二次型, 则定义 $s(Q) = 1$; 若 Q 是椭圆二次型, 则定义 $s(Q) = -1$. 如果 V_1 和 V_2 是两个偶数维向量空间, $Q_1 \colon V_1 \to \mathbb{F}_q$ 和 $Q_2 \colon V_2 \to \mathbb{F}_q$ 是两个非退化二次型, 我们定义 $V_1 \oplus V_2$ 上的二次型 $Q_1 \oplus Q_2$ 如下,

$$\begin{aligned} Q_1 \oplus Q_2 \colon V_1 \oplus V_2 &\to \mathbb{F}_q \\ (v_1, v_2) &\mapsto Q_1(v_1) + Q_2(v_2), \end{aligned}$$

易证该二次型亦是非退化的. 对于 V 上的线性变换 g, 若 g 是一个双射并且对于任意 $x \in V$, 均满足 $Q(g(x)) = Q(x)$, 则称 g 为 V 上关于 Q 的一个等距变换. 如果存在伽罗瓦群 $\mathrm{Gal}(\mathbb{F}_q)$ 中的一个元素 σ 使得对任意 $x \in V$, 均有 $Q(g(x)) = Q(x)^\sigma$, 就称 g 是关于 Q 的广义等距变换.

以下是构造强正则图的一个经典方法, 该方法利用非退化二次型的零点构造偏差集从而得到强正则图. 我们将这类图称为 RT2 图, 详细见文献[10].

定理 2.1 *假设 V 是 $\mathbb{F}_q$ 上的一个 $2l$ 维向量空间, Q 是 V 上的一个非退化二次型. 集合 $Q^{-1}(0) \setminus \{0\} = \{x \in V : x \neq 0 \text{ 且 } Q(x) = 0\}$ 是一个偏差集, 其参数为*

$$(q^{2l}, (q^{l-1} + s(Q))(q^l - s(Q)), q^{2l-2} + s(Q)q^{l-1}(q-1) - 2, q^{2l-2} + s(Q)q^{l-1}).$$

当 Q 是椭圆二次型时, 偏差集 $Q^{-1}(0) \setminus \{0\}$ 是负拉丁方型的. 当 Q 是双曲线二次型时, 偏差集 $Q^{-1}(0) \setminus \{0\}$ 是拉丁方型的.

在文献[27] 中, Davis 和 Xiang 发现了一种非常有趣的构造偏差集的方法, 该方法通过将上述定理中的偏差集做一些变形，从而得到了非初等交换 2 群上的偏差集无穷类. 我们将这类强正则图称为 Davis-Xiang 图. 本文描述了 RT2 图和 Davis-Xiang 图的统一构造, 以及它们在一些 2-群上的无定形凯莱结合方案.

设 $\mathbb{F}_4 = \{0, 1, w, w+1\}$ 为一个阶为 4 的有限域, 其中 w 是 $\mathbb{F}_4$ 中的本原元. 对于 $\mathbb{F}_4$ 中任意两个元素 α 和 β, 定义 $\mathbb{F}_4$ 上的二维二次型 $Q_{\alpha,\beta}(x, y) = \alpha x^2 + xy + \beta y^2$. 于是 $Q_{\alpha,\beta}$ 满足性质:

(1) 若 $s(Q_{\alpha,\beta}) = 1$, 则对 $\mathbb{F}_4$ 中的任意非零元 x, $Q^{-1}_{\alpha,\beta}(x)$ 均是参数为 $(16, 3, 2, 0)$-偏差集;

(2) 若 $s(Q_{\alpha,\beta}) = -1$, 则对 $\mathbb{F}_4$ 中的任意非零元 x, $Q^{-1}_{\alpha,\beta}(x)$ 均是参数为 $(16, 5, 0, 2)$-偏差集.

设 ϵ 是 $\mathbb{F}_2$ 中的一个元素. 定义交换群 $G_\epsilon = (\mathbb{F}_4 \times \mathbb{F}_4, +)$, 其中的加法运算为: 对任意 (x, y), $(x', y') \in \mathbb{F}_4 \times \mathbb{F}_4$, $(x, y) + (x', y') = (x + x', y + y' + \epsilon(xx')^2)$. 注意到, 当 $\epsilon = 0$ 时, 群 $G_\epsilon \cong \mathbb{Z}_2^4$; 当 $\epsilon = 1$ 时, 群 $G_\epsilon \cong \mathbb{Z}_4^2$. 设 α 为 $\mathbb{F}_4$ 中的一个元素. 定义 $\mathbb{F}_4$ 上的一个二维二次型 $Q_\alpha(x, y) = \alpha x^2 + xy + y^2$. 易知, $s(Q_\alpha) = (-1)^{\mathrm{Tr}(\alpha)}$, 其中 $\mathrm{Tr}(\alpha) = \alpha + \alpha^2$ 是 α 的迹. 我们可以将二次型 Q_α 视为从群 G_ϵ 到 $\mathbb{F}_4$ 上的函数, 其中 $\epsilon = 0$ 或 1. 容易验证:

(1) 对任意的非零元 $x \in \mathbb{F}_4$, $Q_\alpha^{-1}(x)$ 是群 G_ϵ 上参数为 $(16, 4 - s(Q_\alpha), 1 + s(Q_\alpha), 1 - s(Q_\alpha))$ 的偏差集, 其中 $\epsilon = 0$ 或 1;

(2) 当 $s(Q_\alpha) = 1$ 时, $Q_\alpha^{-1}(0) \setminus \{0\}$ 是群 G_ϵ 上参数为 $(16, 6, 2, 2)$ 的偏差集, 亦是一个参数为 $(16, 6, 2)$ 的 Hadamard 差集. 当 $s(Q_\alpha) = -1$ 时, $Q_\alpha^{-1}(0) \setminus \{0\}$ 在 G_ϵ 中是一个空集, 其中 $\epsilon = 0$ 或 1.

下面的定理是文献[70] 中性质 3.6 和定理 3.7 的推论.

定理 2.2 设 $n \geqslant 2$ 为一个整数. 对于给定的 $\mathbb{F}_2^n$ 中的向量 $\mathbf{e} = (\epsilon_1, \epsilon_2, \cdots, \epsilon_n)$ 和 $\mathbb{F}_4^n$ 中的向量 $\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, 定义一个交换群 $G_{\mathbf{e}} = G_{\epsilon_1} \oplus G_{\epsilon_2} \oplus \cdots \oplus G_{\epsilon_n}$ 和一个二次型 $Q_{\mathbf{a}} = Q_{\alpha_1} \oplus Q_{\alpha_2} \oplus \cdots \oplus Q_{\alpha_n}$: $G_{\mathbf{e}} \to \mathbb{F}_4$. 对任意的 $\mathbf{a} \in \mathbb{F}_4^n$ 和 $\mathbf{e} \in \mathbb{F}_2^n$, 子集 $Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}$ 是 $G_{\mathbf{e}}$ 中的一个偏差集, 其参数为

$$(4^{2n}, (4^{n-1} + s(Q_{\mathbf{a}}))(4^n - s(Q_{\mathbf{a}})), 4^{2n-2} + 3 \cdot 4^{n-1} s(Q_{\mathbf{a}}) - 2, 4^{2n-2} + 4^{n-1} s(Q_{\mathbf{a}})).$$

对任意的 $\mathbf{a} \in \mathbb{F}_4^n$, $\mathbf{e} \in \mathbb{F}_2^n$ 和任意的 $\mathbb{F}_4$ 中的非零元 x, 子集 $Q_{\mathbf{a}}^{-1}(x)$ 是 $G_{\mathbf{e}}$ 中的一个偏差集, 其参数为

$$(4^{2n}, 4^{n-1}(4^n - s(Q_{\mathbf{a}})), 4^{2n-2} + 4^{n-1} s(Q_{\mathbf{a}}), 4^{2n-2} - 4^{n-1} s(Q_{\mathbf{a}})).$$

另外, 当 $s(Q_{\mathbf{a}}) = -1$ 时, 偏差集 $Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}$, $Q_{\mathbf{a}}^{-1}(1)$, $Q_{\mathbf{a}}^{-1}(\omega)$ 和 $Q_{\mathbf{a}}^{-1}(\omega + 1)$ 均为负拉丁方型的. 当 $s(Q_{\mathbf{a}}) = 1$ 时, 偏差集 $Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}$, $Q_{\mathbf{a}}^{-1}(1)$, $Q_{\mathbf{a}}^{-1}(\omega)$ 和 $Q_{\mathbf{a}}^{-1}(\omega + 1)$ 均为拉丁方型的. 因此,

$$\mathcal{S}_{\mathbf{e},\mathbf{a}}^{(4)} = (G_{\mathbf{e}}; Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}, Q_{\mathbf{a}}^{-1}(1), Q_{\mathbf{a}}^{-1}(\omega), Q_{\mathbf{a}}^{-1}(\omega + 1))$$

和

$$\mathcal{S}_{\mathbf{e},\mathbf{a}}^{(3)} = (G_{\mathbf{e}}; Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}, Q_{\mathbf{a}}^{-1}(1), Q_{\mathbf{a}}^{-1}(\omega) \cup Q_{\mathbf{a}}^{-1}(\omega + 1))$$

均为无定形交换凯莱结合方案.

注 2.1 当向量 $\mathbf{e} = \mathbf{0}$ 时, $G_{\mathbf{e}}$ 中的偏差集 $Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}$ 对应的强正则图是 RT2 图; 当 $\mathbf{e} \neq \mathbf{0}$ 时, $G_{\mathbf{e}}$ 中的偏差集 $Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}$ 对应的强正则图是 Davis-Xiang 图.

注 2.2 在文献[27] 中, Davis 和 Xiang 证明了 $Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}$ 是 $G_{\mathbf{e}}$ 中的偏差集. Polhill 在文献[30] 中用乘积构造的方法证明了, 对 $\mathbb{F}_4$ 中任意非零元 x, $Q_{\mathbf{a}}^{-1}(x)$ 是 $G_{\mathbf{e}}$ 中的偏差集.

注 2.3 我们亦可以证明 $Q_{\mathbf{a}}^{-1}(0) \cup Q_{\mathbf{a}}^{-1}(1)$ 和 $Q_{\mathbf{a}}^{-1}(\omega) \cup Q_{\mathbf{a}}^{-1}(\omega + 1)$ 均为 $G_{\mathbf{e}}$ 中的 Hadamard 差集.

文献[27] 中提出: "... 研究偏差集的中心问题之一是对于给定的参数集, 哪些适当阶的群包含拥有该参数的偏差集". 我们的研究给这个问题提供了一些答案.

2.3 强正则图的正则自同构群和无定形结合方案

在这一节中, 我们简要地描述了获得定理 2.2中所提到的凯莱结合方案 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 和 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 的正则自同构群的方法. 对任意的 $g \in G_{\mathbf{e}}$, 映射

$$R(g)\colon G_{\mathbf{e}} \to G_{\mathbf{e}}$$
$$x \mapsto x + g, \forall x \in G_{\mathbf{e}}$$

保持了 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 和 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 中所有强正则图的关联关系. 显然, 对任意的 $g_1, g_2 \in G_{\mathbf{e}}$, $R(g_1)R(g_2) = R(g_1+g_2)$. 对 $G_{\mathbf{e}}$ 的一个子群 K, 记 $R(K) = \{R(g) : g \in K\}$. 容易验证, $R(K)$ 是 $R(G_{\mathbf{e}})$ 的一个子群, 并且 $R(K) \cong K$.

引理 2.1 假设 $\tau \in \mathrm{Aut}(G_{\mathbf{e}})$ 是 $G_{\mathbf{e}}$ 的一个自同构.

(1) 若 τ 是 $Q_{\mathbf{a}}$ 的一个等距变换, 也就是说, 对任意的 $g \in G_{\mathbf{e}}$, $Q_{\mathbf{a}}(\tau(g)) = Q_{\mathbf{a}}(g)$, 则有 $\tau \in \mathrm{Aut}(\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}})$.

(2) 若 τ 是 $Q_{\mathbf{a}}$ 的一个广义等距变换, 也就是说, 对任意的 $g \in G_{\mathbf{e}}$, $Q_{\mathbf{a}}(\tau(g)) = Q_{\mathbf{a}}(g)^2$, 则有 $\tau \in \mathrm{Aut}(\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}})$.

证明 给定一个自同构 $\tau \in \mathrm{Aut}(G_{\mathbf{e}})$. 自同构 $\tau \in \mathrm{Aut}(\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}})$(或者 $\tau \in \mathrm{Aut}(\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}})$) 当且仅当对无定形凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$(或者 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$) 中任意的偏差集 D, 均有 $\tau(D) = D$. 因此, 如果对所有的 $g \in G_{\mathbf{e}}$ 都有 $Q_{\mathbf{a}}(\tau(g)) = Q_{\mathbf{a}}(g)$ 成立, 那么就有 $\tau \in \mathrm{Aut}(\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}})$; 如果对所有的 $g \in G_{\mathbf{e}}$ 都有 $Q_{\mathbf{a}}(\tau(g)) = Q_{\mathbf{a}}(g)^2$ 成立, 那么就有 $\tau \in \mathrm{Aut}(\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}})$.

引理 2.1保证了当 τ 是 $Q_{\mathbf{a}}$ 的广义等距变换或等距变换时, $\langle R(G_{\mathbf{e}}), \tau\rangle \cong G_{\mathbf{e}} \rtimes \langle\tau\rangle$ 是 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的一个自同构群. 我们将借助自同构 τ 和 $G_{\mathbf{e}}$ 的一个子群来构造 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 和 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的非交换正则自同构群. 由此将无定形交换凯莱结合方案转换成无定形非交换凯莱结合方案.

定理 2.3 如果如下条件被满足:

(1) $\mathrm{Aut}(G_{\mathbf{e}})$ 中存在 $Q_{\mathbf{a}}$ 的一个阶为 $e > 1$ 的等距变换 τ,

(2) $G_{\mathbf{e}}$ 中存在一个指数为 e 的 τ-不变子群 K,

(3) $G_{\mathbf{e}}$ 中有一个元素 h 使得 $h_e \in K$ 和 $h_1, \cdots, h_{e-1} \notin K$, 其中 $h_1 = h$,

$$h_i := h + \tau(h) + \cdots + \tau^{i-1}(h), \quad 2 \leqslant i \leqslant e,$$

于是群

$$G_{K,\tau,h} := \langle R(K),\, R(h)\tau \rangle \tag{2.1}$$

是无定形交换凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的正则自同构群. 另外, 对任意的 $k \geqslant 1$, 记 $G^{(0)} := G_{K,\tau,h}$ 和 $G^{(k)} := [G^{(k-1)} : G^{(0)}]$, $Z(G^{(0)})$ 为 $G^{(0)}$ 的中心, $\Phi(G^{(0)})$ 为 $G^{(0)}$ 的 Frattini 子群, 那么

$$\begin{aligned} G^{(1)} &= \langle R(x-\tau(x)) :\, x \in K \rangle, \\ G^{(k)} &= \langle R(x-\tau(x)) :\, x \in G^{(k-1)} \rangle \text{ 对所有 } k \geqslant 2, \end{aligned} \tag{2.2}$$

并且 $G^{(0)}$ 是非交换的当且仅当 τ 不固定 K 中的所有元素, 也就是说, $t = o(\tau|_K) > 1$. 假设 m 为 $R(h_t)\tau^t$ 的阶. 于是中心

$$Z(G^{(0)}) \cong \begin{cases} [\langle R(x) :\, x \in K \text{ 且 } \tau(x) = x \rangle \,/\, \langle R(h_e) \rangle] \times \mathbb{Z}_m & \text{如果 } t < e, \\ \langle R(x) :\, x \in K \text{ 且 } \tau(x) = x \rangle & \text{如果 } t = e, \end{cases} \tag{2.3}$$

以及 Frattini 子群

$$\Phi(G^{(0)}) = \left\langle R(2x), R(x+\tau(x)), R(h_2)\tau^2 :\, x \in K \right\rangle. \tag{2.4}$$

证明 容易验证 $(R(h)\tau)^{-1} = R(\tau^{-1}(h))\tau^{-1}$ 以及对任意的 $x \in K$,

$$R(h)\tau R(x) \left(R(h)\tau\right)^{-1} = R(\tau(x)).$$

由此可得 $R(K)$ 是 $G_{K,\tau,h}$ 的一个正规子群. 另外, 对任意的 $1 \leqslant i \leqslant e$, $(R(h)\tau)^i = R(h_i)\tau^i$, 其中 h_i 如条件 (3) 中所定义. 因为 $h_e \in K$ 并且对所有的 $1 \leq i \leq e$, $R(K+h_i)\tau^i$ 两两不同, 所以

$$G_{K,\tau,h} = \cup_{i=1}^{e} R(K+h_i)\tau^i. \tag{2.5}$$

特别地, 群 $G_{K,\tau,h}$ 的大小为 $|G_{\mathbf{e}}|$.

对任意的 $1 \leqslant i < j \leqslant e$, 我们有 $h_j - h_i = \tau^i(h_{j-i})$. 因为 K 是 τ 不变的, 并且由条件 (3) 可知 $h_{j-i} \notin K$, 所以 $h_j - h_i \notin K$. 另外, 可由 $h_e \in K$ 得到 $\cup_{i=1}^{e}(K+h_i) = G_{\mathbf{e}}$. 为了证明 $G_{K,\tau,h}$ 是一个正则子群, 我们只需要证明 $0 \in G_{\mathbf{e}}$ 在群 $G_{K,\tau,h}$ 作用下的轨道是 $G_{\mathbf{e}}$. 因为 $R(k)R(h_i)\tau^i(0) = h_i + k$, 于是等价地, 只需要证明 $\cup_{i=1}^{e}(K+h_i) = G_{\mathbf{e}}$. 这部分刚刚已经被证明了, 所以我们完成了第一部分的证明.

可以直接计算

$$\begin{aligned} G^{(1)} &= \langle R(x)R(h_t)\tau^t R(x)^{-1}(R(h_t)\tau^t)^{-1} :\, x \in K,\, 1 \leqslant t \leqslant e-1 \rangle \\ &= \langle R(x-\tau^t(x)) :\, x \in K,\, 1 \leqslant t \leqslant e-1 \rangle. \end{aligned}$$

因为

$$x-\tau^t(x)=(x-\tau(x))+(\tau(x)-\tau(\tau(x)))+(\tau^2(x)-\tau(\tau^2(x)))+\cdots+(\tau^{t-1}(x)-\tau(\tau^{t-1}(x)))$$

以及 K 是 τ-不变的, 我们得到

$$G^{(1)}=\langle R(x-\tau^t(x)):\, x\in K,\, 1\leqslant t\leqslant e-1\rangle=\langle R(x-\tau(x)):\, x\in K\rangle.$$

同样地, 对任意的 $k\geqslant 2$, $G^{(k)}=\langle R(x-\tau(x)):\, x\in G^{(k-1)}\rangle$. 显然中心

$$\begin{aligned} Z(G_{K,\tau,h}) &= \left\langle R(x),\, R(h_t)\tau^t:\, x\in K \text{ 且 } \tau(x)=x,\, t=o(\tau|_K)\right\rangle \\ &\cong \begin{cases} [\langle R(x):\, x\in K \text{ 且 } \tau(x)=x\rangle \,/\, \langle R(h_e)\rangle]\times\mathbb{Z}_m & \text{如果 } t<e, \\ \langle R(x):\, x\in K \text{ 且 } \tau(x)=x\rangle & \text{如果 } t=e, \end{cases} \end{aligned}$$

这是由于 $\langle R(x):x\in K \text{ 且} \tau(x)=x\rangle\cap\langle R(h_t)\tau^t\rangle=\langle R(h_e)\rangle$, 阶 $o(R(h_t)\tau^t)=m$, 以及 $\tau(h_e)=h_e$. 因为 $G_{\mathbf{e}}$ 是一个 2-群, $G_{K,\tau,h}$ 的 Frattini 子群 $\Phi(G_{K,\tau,h})$ 是由 g^2 生成的, 其中 $g\in G_{K,\tau,t}$. 因为

$$R(x+h_i)\tau^iR(x+h_i)\tau^i=R(x+h_i+\tau^i(x+h_i))\tau^{2i}=R(x+\tau^i(x)+h_{2i})\tau^{2i},$$

所以有

$$\begin{aligned} \Phi(G_{K,\tau,h}) &= \left\langle R(x+\tau^i(x)+h_{2i})\tau^{2i}:\, x\in K,\, i\geqslant 1\right\rangle \\ &= \left\langle R(x+\tau^i(x)),\, R(h_{2i})\tau^{2i}:\, x\in K,\, i\geqslant 1\right\rangle \\ &= \left\langle R(2x),\, R(x+\tau^i(x)),\, R(h_{2i})\tau^{2i}:\, x\in K,\, 1\leqslant i\leqslant e-1\right\rangle \\ &= \left\langle R(2x),\, R(x-\tau^i(x)),\, R((h_2)\tau^2)^i:\, x\in K,\, 1\leqslant i\leqslant e-1\right\rangle \\ &= \left\langle R(2x),\, R(x-\tau(x)),\, R(h_2)\tau^2:\, x\in K\right\rangle \\ &= \left\langle R(2x),\, R(x+\tau(x)),\, R(h_2)\tau^2:\, x\in K\right\rangle. \end{aligned}$$

我们将使用(2.2), (2.3)和(2.4)作为不变量来区分这些正则子群 $G_{K,\tau,h}$ 的同构类.

2.4 RT2 图和 Davis-Xiang 图的正则子群及其无定形交换凯莱结合方案

给定一个交换群 G, 记 End(G) 为包含 G 的所有自同态的集合. 对 End(G) 中的每一个自同态 f, 记 $\mathrm{Im}_G(f):=\{f(g):g\in G\}$ 为 G 在 f 下的像, 并记 $\mathrm{Ker}_G(f):=\{g\in G:f(g)=0\}$ 为 f 在 G 中的核, 即单位元的原像. 对整数 n, 记 $\mathrm{Im}_G(n):=\{ng:g\in G\}$ 和 $\mathrm{Ker}_G(n):=\{g\in G:ng=0\}$. 例如, $G_{\mathbf{e}}$ 的 Frattini 子群是 $\Phi(G_{\mathbf{e}})=\mathrm{Im}_{G_{\mathbf{e}}}(2)$ 以及 $\mathrm{Fix}(\tau)=\mathrm{Ker}_{G_{\mathbf{e}}}(\tau-1)$. 在本节中, 我

们假设 $G_{\mathbf{e}}$ 是定理 2.2中定义的交换 2-群, $\tau \in \mathrm{Aut}(G_{\mathbf{e}})$ 是关于 $Q_{\mathbf{a}}$ 的 $e=2$ 阶等距变换或 $e=4$ 阶广义等距变换, 其中 $Q_{\mathbf{a}}$ 是定理 2.2中定义的二次型.

本节的主要目标是找到 $G_{\mathbf{e}}$ 中满足定理 2.3中条件的子空间 K 和元素 h. 下面这个简单的观察是非常有用的.

引理 2.2 若 $[G_{\mathbf{e}} : \mathrm{Fix}(\tau)] > e$, 则定理 2.3中定义的正则子群 $G_{K,\tau,h}$ 是非交换的.

证明 通过定理 2.3的第二部分, 可以知道群 $G_{K,\tau,h}$ 交换当且仅当 τ 固定 K 中的所有元素, 也就是说, $K \leqslant \mathrm{Fix}(\tau)$. 通过比较他们的大小, 我们可以知道这是不可能的.

2.4.1 一般性的结论

假设 G 是一个交换群, ϕ 是群 G 的一个自同构. 我们首先证明了一些关于 G 的 ϕ-不变子群的一般性结论.

引理 2.3 假设 K 是 G 的一个指数为 2 的子群, 即 $K \leqslant G$ 且 $[G:K]=2$. 子群 K 是 ϕ-不变的当且仅当 $\mathrm{Im}_G(1+\phi) \leqslant K$.

证明 如果 K 是 ϕ-不变的, 那么 $x \in K$ 当且仅当 $\phi(x) \in K$. 显然, 对任意的 $x \in K$, $(1+\phi)(x) = x+\phi(x) \in K$. 由于 $[G:K]=2$, 对任意的 $x \notin K$, $(1+\phi)(x) = x+\phi(x) \in K$. 因此, $\mathrm{Im}_G(1+\phi) \leqslant K$. 反之, 如果 $\mathrm{Im}_G(1+\phi) \leqslant K$, 就有对任意的 $x \in K$, $(1+\phi)(x) = x+\phi(x) \in K$. 由此得到 $\phi(x) \in K$ 以及 K 是 ϕ-不变的.

引理 2.4 假设 K 是 G 中的一个指数为 4 的子群. 若 ϕ 的阶不被 3 整除, 并且 K 是 ϕ-不变的, 则 G 包含一个指数为 2 的子群 H, 其中 H 是 ϕ-不变的, 并且 $K \leqslant H$. 另外, 我们有 $\mathrm{Im}_G(1+\phi+\phi^2+\phi^3) \leqslant K$.

证明 由于 K 是 G 的 ϕ-不变子群, 则可由 ϕ 得到商群 $\bar{G} := G/K$ 的一个自然的自同构 $\bar{\phi}$. 假设 $\pi : G \to \bar{G}$ 是一个自然投射同态. 因为 $|\bar{G}|=4$, 所以 $\bar{G} \cong C_4$ 或 $C_2 \times C_2$. 当 $\bar{G} \cong C_4$ 时, $\bar{G}$ 中的二阶元被 $\bar{\phi}$ 固定. 当 $\bar{G} \cong C_2 \times C_2$ 时, 由于 ϕ 的阶不被 3 整除, 可以知道 $\bar{G}$ 中一定存在一个阶为 2 的元素 x 使得 $\bar{\phi}(x) = x$. 定义 $H = \pi^{-1}(\{0, x\})$. 易知 H 是 ϕ-不变的, $[G:H]=2$ 以及 $K \leqslant H$. 由引理 2.3, 可得 $\mathrm{Im}_G(1+\phi) \leqslant H$. 又因为 K 也是 ϕ^2-不变的, 可以根据引理 2.3得到 $\mathrm{Im}_H(1+\phi^2) \leqslant K$. 因此, $\mathrm{Im}_G(1+\phi+\phi^2+\phi^3) = \mathrm{Im}_G((1+\phi^2)(1+\phi)) \leqslant K$.

我们在下面的定理中完全解决了当 $o(\tau)=2$ 时, 子群 K 和元素 h 的存在性问题.

定理 2.4 假设 $\tau \in \mathrm{Aut}(G_{\mathbf{e}})$ 为 $Q_{\mathbf{a}}$ 的一个阶为 2 的广义等距变换或等距变换. 存在 $G_{\mathbf{e}}$ 的一个阶为 2 的 τ-不变子群 K 使得 $G_{K,\tau,h}$ 是式子 (2.1)中定义的无定形交换凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的一个正则子群. 若 $\tau|_K = 1_K$, 则 $G_{K,\tau,h}$ 的幂零类数为 1. 若 $\tau|_K \neq 1_K$ 且 $\tau|_{\Phi(K)} = 1_{\Phi(K)}$, 则 $G_{K,\tau,h}$ 的幂零类数为 2. 若 $\tau|_{\Phi(K)} \neq 1_{\Phi(K)}$, 则 $G_{K,\tau,h}$ 的幂零类数是 3.

证明 因为 τ 的阶是 2, 所以 $|G_{\mathbf{e}}| \geqslant 4$. 易知, 群 $G_{\mathbf{e}}$ 的极大子群的个数是 $|G_{\mathbf{e}}/\Phi(G_{\mathbf{e}})| - 1$, 其中 $|G_{\mathbf{e}}/\Phi(G_{\mathbf{e}})| - 1$ 是奇数. 因此, 一定存在 $G_{\mathbf{e}}$ 的一个 τ-不变极大子群 K. 根据引理 2.2和定理 2.3, 对任意的 $h \in G_{\mathbf{e}} \setminus K$, 式子(2.1)中定义的群 $G_{K,\tau,h}$ 是无定形交换凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的正则自同构群. 如果 c 是使得式子 $(1-\tau)^c|_K = 0_K$ 成立的最小的正整数, 就可以通过定理 2.3得到正则子群 $G_{K,\tau,h}$ 的幂零类是 c 个. 因为 $(1-\tau)^2 = 2(1-\tau)$ 且 $(1-\tau)^3 = 0$，当 $\tau|_K = 1_K$，群 $G_{K,\tau,h}$ 的幂零类数为 1. 当 $\tau|_K \neq 1_K$ 且 $\tau|_{\Phi(K)} = 1_{\Phi(K)}$ 时, 群 $G_{K,\tau,h}$ 的幂零类数为 2. 当 $\tau|_{\Phi(K)} \neq 1_{\Phi(K)}$ 时, 群 $G_{K,\tau,h}$ 的幂零类数为 3.

例 2.1 任取 $\mathbb{F}_2^2$ 中的一个向量 $\mathbf{e} = (\epsilon_1, \epsilon_2)$ 以及 $\mathbb{F}_4^2$ 中的一个向量 $\mathbf{a} = (\alpha_1, \alpha_2)$. 设 $G_{\mathbf{e}}$ 和 $Q_{\mathbf{a}}$ 分别为定理 2.2中定义的交换群和二次型. 如下定义一个阶为 2 的等距变换 $\tau \in \mathrm{Aut}(G_{\mathbf{e}})$:

$$\begin{aligned}&\tau\colon G_{\mathbf{e}} \longrightarrow G_{\mathbf{e}}\\ &\tau(((x_1,y_1),(x_2,y_2))) = ((x_1, y_1+x_1),(x_2,y_2+x_2)).\end{aligned}$$

易知群

$$K := \{\{((x_1,y_1),(x_2,y_2)) \in G_{\mathbf{e}} : \mathrm{Tr}(wx_1) = 0\}$$

是群 $G_{\mathbf{e}}$ 的指数为 2 的 τ-不变子群. 定义 $h = ((w,0),(0,0)) \in G_{\mathbf{e}} \setminus K$, 其中 $w \in \mathbb{F}_4$ 使得 $\mathrm{Tr}(w) = 1$. 由此可得式子(2.1)定义的群 $G_{K,\tau,h}$ 是无定形交换凯莱结合方案 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的正则自同构群. 因为 $\Phi(K) = \{((0,\epsilon_1 x_1),(0,\epsilon_2 x_2)) \in G_{\mathbf{e}} : \mathrm{Tr}(wx_1) = 0\}$, 可得 $\tau|_K \neq 1_K$ 和 $\tau|_{\Phi(K)} = 1_{\Phi(K)}$. 于是群 $G_{K,\tau,h}$ 的幂零类是 2.

我们接下来考虑 $o(\tau) = 4$ 时, 子群 K 和元素 h 的存在性问题.

定理 2.5 假设 $\tau \in \mathrm{Aut}(G_{\mathbf{e}})$ 是二次型 $Q_{\mathbf{a}}$ 的 4 阶广义等距变换或等距变换. 存在 $G_{\mathbf{e}}$ 中的一个指数为 4 的 τ-不变子群 K 以及元素 h 使得由式子(2.1)定义的群 $G_{K,\tau,h}$ 是无定形交换凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的正则自同构群当且仅当存在 $G_{\mathbf{e}}$ 的一个指数为 2 的子群 H 使得

$$\begin{aligned}&\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) + \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \leqslant H,\\ &\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \not\leqslant \Phi(H) + \mathrm{Im}_H(1+\tau).\end{aligned}$$

如果这样的一个正则子群 $G_{K,\tau,h}$ 存在, 则该群的幂零类数不大于 6.

证明 假设定理中提到的 K 和 h 是存在的. 由引理 2.4可知, 存在 $G_{\mathbf{e}}$ 的一个指数为 2 的 τ-不变子群 H 使得 $K \leqslant H$. 根据引理 2.3, $\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \leqslant H$, $\mathrm{Im}_H(1+\tau) \leqslant K$ 以及 $\Phi(H) \leqslant K$. 这是由于 $[G_{\mathbf{e}} : H] = [H : K] = 2$. 进一步可得

$$\Phi(H) + \mathrm{Im}_H(1+\tau) \leqslant K.$$

我们可以由定理 2.3中的 (c) 得到 $(1+\tau)(h) \notin K$ 和 $(1+\tau)(h) \in H$, 于是就有

$$\mathrm{Im}_H(1+\tau) < \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)$$

和

$$\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \not\leqslant \Phi(H) + \mathrm{Im}_H(1+\tau) \leqslant K.$$

我们接下来利用反证法证明 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) \leqslant H$. 假设 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) \not\leqslant H$. 由 $[G_{\mathbf{e}} : H] = 2$, 可得 $\mathrm{Ker}_H(1+\tau) = \mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) \cap H$ 是 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau)$ 的一个指数为 2 的子群. 从式子 $G_{\mathbf{e}}/\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) \cong \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)$ 和 $H/\mathrm{Ker}_H(1+\tau) \cong \mathrm{Im}_H(1+\tau)$ 可以看出 $|\mathrm{Im}_H(1+\tau)| = |\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)|$. 由此可知 $\mathrm{Im}_H(1+\tau) = \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)$. 显然这与 $\mathrm{Im}_H(1+\tau) < \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)$ 是矛盾的. 因此, $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) + \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \leqslant H$.

反之, 假设 H 是 $G_{\mathbf{e}}$ 中的一个指数为 2 的子群, 其满足条件 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) + \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \leqslant H$ 以及 $\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \not\leqslant \Phi(H) + \mathrm{Im}_H(1+\tau)$. 通过引理 2.3, 子群 H 是 τ-不变的并且存在一个 $G_{\mathbf{e}} \setminus H$ 中的元素 h 满足 $h + \tau(h) = (1+\tau)(h) \notin \Phi(H) + \mathrm{Im}_H(1+\tau)$. 因此, H 有一个指数为 2 的子群 K 使得 $h + \tau(h) \notin K$ 和 $\mathrm{Im}_H(1+\tau) \leqslant K$, 并且通过引理 2.3, K 在 H 中是 τ-不变的. 因为 H 在 $G_{\mathbf{e}}$ 中是 τ-不变的, 所以 K 在 $G_{\mathbf{e}}$ 中亦是 τ-不变的, 并且 $[G_{\mathbf{e}} : K] = 4$. 通过引理 2.4, $h + \tau(h) + \tau^2(h) + \tau^3(h) = (1+\tau+\tau^2+\tau^3)(h) \in \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau+\tau^2+\tau^3) \leqslant K$. 又由 $h \notin H$ 和 $h + \tau(h) \in H$ 以及 H 是 $G_{\mathbf{e}}$ 中 τ-不变的, 可得元素 $h + \tau(h) + \tau^2(h) \notin H$. 因此, K 和 h 满足定理 2.3中的条件 (a), (b) 和 (c).

因为 $\tau^4 = 1$ 以及 $4x = 0$ 对所有的 $x \in G_{\mathbf{e}}$ 都成立, 所以有 $(1-\tau)^6 = 0$. 又根据定理 2.3, 易知 $G_{K,\tau,h}$ 的幂零类数小于等于 6.

推论 2.1 假设 $\tau \in \mathrm{Aut}(G_{\mathbf{e}})$ 是 $Q_{\mathbf{a}}$ 的一个 4 阶广义等距变换或等距变换使得 $\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \cap \Phi(G_{\mathbf{e}}) = \{0\}$. 存在 $G_{\mathbf{e}}$ 的一个 4 阶 τ-不变子群 K 以及 $G_{\mathbf{e}}$ 中的一个元素 h 使得由式子(2.1)定义的群 $G_{K,\tau,h}$ 是无定形交换凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的正则自同构群当且仅当

$$\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) \cap \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau) \neq \{0\},$$

或者等价地说,

$$\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau) < \mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau)^2.$$

其中, 群 $G_{K,\tau,h}$ 的幂零类数不大于 6.

证明 若 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau)\cap\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\neq\{0\}$ 成立, 则 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau)+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\neq G_{\mathbf{e}}$, 并且存在 $G_{\mathbf{e}}$ 中的一个指数为 2 的子群 H 使得 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau)+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\leqslant H$. 由于 $\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\cap\Phi(G_{\mathbf{e}})=\{0\}$ 以及 $\Phi(H)=\mathrm{Im}_H(2)\subseteq\Phi(G_{\mathbf{e}})=\mathrm{Im}_{G_{\mathbf{e}}}(2)$, 对于任何这样的 $G_{\mathbf{e}}$ 的指数为 2 的子群 H, 都有 $\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\not\leqslant\Phi(H)+\mathrm{Im}_H(1+\tau)$. 根据定理 2.5, 存在 $G_{\mathbf{e}}$ 的一个指数为 4 的 τ-不变子群 K 和元素 h 使得式子(2.1)中定义的 $G_{K,\tau,h}$ 是 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的一个正则子群.

反之, 若这样的指数为 4 的 τ-不变子群 K 和元素 $h\in G_{\mathbf{e}}$ 存在, 则由定理 2.5可知, 存在 $G_{\mathbf{e}}$ 的指数为 2 的子群 H 使得 $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau)+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\leqslant H$. 因此, $\mathrm{Ker}_{G_{\mathbf{e}}}(1+\tau)\cap\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\neq\{0\}$.

接下来我们证明定理 2.4中关于群 $G_{\mathbf{e}}$ 的指数为 4 的 τ-不变子群 K 和元素 h 的存在性的另一个结果.

定理 2.6 假设 $\tau\in\mathrm{Aut}(G_{\mathbf{e}})$ 是 $Q_{\mathbf{a}}$ 的 4 阶广义等距变换或等距变换. 若 τ 在 $G_{\mathbf{e}}/(\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2))$ 上的诱导作用是非平凡的, 则存在 $G_{\mathbf{e}}$ 中指数为 4 的子群 K 和元素 h 使得其所对应的群 $G_{K,\tau,h}$ 是无定形交换凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的正则自同构群, 并且满足定理 2.3. 其中, 群 $G_{K,\tau,h}$ 的幂零类数不超过 6.

证明 根据引理 2.3, 可以知道 $G_{\mathbf{e}}$ 中所有指数为 2 的 τ^2-不变子群的交为 $\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2)$ 以及 $G_{\mathbf{e}}$ 中所有指数为 2 的 τ-不变子群的交为 $\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)$. 因此, $\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2)\leqslant\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)$, 这是由于 τ-不变子群亦为 τ^2-不变子群. 因为 τ 在商群 $G_{\mathbf{e}}/(\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2))$ 上的诱导作用是非平凡的, 所以子群 $\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)\not\leqslant\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2)$, 并且存在一个元素 $h\in G_{\mathbf{e}}$ 使得 $h+\tau(h)\in\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau)$ 有一个非零的像在商群 $G_{\mathbf{e}}/(\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2))$ 中. 另外, $h+\tau(h)\notin\Phi(G_{\mathbf{e}})$, 这意味着 $G_{\mathbf{e}}$ 中存在一个指数为 2 的子群 H 满足 $\Phi(G_{\mathbf{e}})+\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2)\subseteq H$ 并且 $h+\tau(h)\notin H$. 由引理 2.3, $\tau(H)\neq H$ 并且 $\tau^2(H)=H$. 假设 $K=H\cap\tau(H)$. 易知, K 是 $G_{\mathbf{e}}$ 的一个指数为 4 的 τ-不变子群. 根据 $h+\tau(h)\notin H$, 可得 $h+\tau(h)\notin K$, 并且由 K 是 τ-不变的得到 $h\notin K$. 因为 $h\notin K$ 以及 K 是 τ-不变的, 由引理 2.4, 可得 $h+\tau(h)+\tau^2(h)+\tau^3(h)\in K$ 和 $h+\tau(h)+\tau^2(h)\notin K$.

例 2.2 任取 $\mathbb{F}_2^2$ 中的一个向量 $\mathbf{e}=(\epsilon_1,\epsilon_2)$ 和 $\mathbb{F}_4^2\setminus\mathbb{F}_2^2$ 中的一个向量 $\mathbf{a}=(\alpha_1,\alpha_2)$. 假设 $G_{\mathbf{e}}$ 和 $Q_{\mathbf{a}}$ 分别为定理 2.2中定义的交换群和二次型. 如下定义一个 4 阶的广义等距变换 $\tau\in\mathrm{Aut}(G_{\mathbf{e}})$: 对任意的 $((x_1,y_2),(x_2,y_2))\in G_{\mathbf{e}}$,

$$\tau(((x_1,y_1),(x_2,y_2)))=((x_1^2,y_1^2+\alpha_1x_1^2),(x_2^2,y_2^2+\alpha_2x_2^2)).$$

通过计算可得

$$\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2)=\{((0,(\mathrm{Tr}(\alpha_1)+\epsilon_1)x_1),(0,(\mathrm{Tr}(\alpha_2)+\epsilon_2)x_2)):x_1,x_2\in\mathbb{F}_4\}$$

和

$$\Phi(G_{\mathbf{e}}) = \{((0, \epsilon_1 x_1), (0, \epsilon_2 x_2)) : x_1, x_2 \in \mathbb{F}_4\}.$$

易知, τ 在群 $G_{\mathbf{e}}/(\Phi(G_{\mathbf{e}}) + \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2))$ 上的诱导作用是非平凡的. 取元素 $h = ((w, 0), (0, 0)) \in G_{\mathbf{e}}$. 可以验证得到 $h + \tau(h) = ((1, \alpha_1 w^2 + \epsilon_1), (0, 0))$ 在 $G_{\mathbf{e}}/(\Phi(G_{\mathbf{e}}) + \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau^2))$ 中有非零的像. 子群

$$H := \{((x_1, y_1), (x_2, y_2)) \in G_{\mathbf{e}} : \mathrm{Tr}(wx_1) = 0\}$$

是 $G_{\mathbf{e}}$ 指数为 2 的子群且满足 $h + \tau(h) \notin H$. 假设 $K = H \cap \tau(H)$. 于是得到一个 τ-不变子群

$$K = \{((x_1, y_1), (x_2, y_2)) \in G_{\mathbf{e}} : x_1 = 0\},$$

其为群 $G_{\mathbf{e}}$ 指数为 4 的子群, 且满足定理 2.3中的条件 (c). 于是由式子(2.1)定义的群 $G_{K,\tau,h}$ 是无定形交换凯莱结合方案 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 的一个正则自同构群. 可以直接计算得到 $(1-\tau)^4|_K = 0$ 以及

$$(1-\tau)^3(K) = \{((0, 0), (0, \mathrm{Tr}(\alpha_2)x) \in G_{\mathbf{e}} : x \in \mathbb{F}_2\}.$$

由式子(2.2), 当 $\mathrm{Tr}(\alpha_2) = 0$, 群 $G_{K,\tau,h}$ 的幂零类数为 3. 当 $\mathrm{Tr}(\alpha_2) \neq 0$, 群 $G_{K,\tau,h}$ 的幂零类数为 4.

接下来我们具体给出定理 2.3中所提到的 RT2 图和 Davis-Xiang 图以及与这些图有关的无定形交换凯莱结合方案的非交换正则自同构群. 我们将使用阶为 2 或 4 的广义等距变换或等距变换, 因此我们可以借助以上所得到的结论.

2.5 无定形交换凯莱结合方案的非交换正则自同构群

对于任意两个向量 $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ 和 $\mathbf{v} = (v_1, v_2, \cdots, v_n)$, 定义

$$\mathbf{u} * \mathbf{v} := (u_1 v_1, u_2 v_2, \cdots, u_n v_n)$$

和

$$\mathrm{Tr}(\mathbf{u}) = (\mathrm{Tr}(u_1), \mathrm{Tr}(u_2), \cdots, \mathrm{Tr}(u_n)).$$

记 $\mathbf{1} := (1, 1, \cdots, 1)$ 和 $\mathbf{0} := (0, 0, \cdots, 0)$. 另外, 我们用符号 $w(\mathbf{u})$ 表示向量 $\mathbf{u}$ 的汉明重量.

在这里我们使用在定理 2.2之前定义的符号 G_ϵ 和 Q_α, 其中 $\epsilon \in \mathbb{F}_2, \alpha \in \mathbb{F}_4$. 对任意的 $\nu \in \mathbb{F}_4$, 如下定义两个自同构 $\rho_\nu \in \mathrm{Aut}(G_\epsilon)$ 和 $\tau_\nu \in \mathrm{Aut}(G_\epsilon)$: 对任意的 $(x, y) \in G_\epsilon$,

$$\begin{aligned} \rho_\nu(x, y) &= (x^2, y^2 + \nu x^2), \\ \tau_\nu(x, y) &= (x, y + \nu x). \end{aligned} \tag{2.6}$$

自同构 τ_ν 是 Q_α 的一个等距变换, 并且当 $\nu=0$ 时, 其阶为 1; 当 $\nu=1$ 时, 其阶为 2. 容易验证 $\rho_\nu^2=\tau_{\mathrm{Tr}(\nu)}$, 并且 $Q_\alpha(\rho_\alpha(x,y))=Q_\alpha(x,y)^2$. 于是自同构 ρ_α 是 Q_α 的一个广义等距变换, 并且当 $\mathrm{Tr}(\alpha)=0$ 时, 其阶为 2; 当 $\mathrm{Tr}(\alpha)=1$ 时, 其阶为 4.

可以通过计算得到, 对任意的 $\nu\in\mathbb{F}_2$,

$$\begin{aligned}
&\mathrm{Im}_{G_\epsilon}(1+\tau_\nu)=\{(0,(\nu+\epsilon)x):x\in\mathbb{F}_4\},\\
&\mathrm{Ker}_{G_\epsilon}(1+\tau_\nu)=\{((\nu+\epsilon+1)x,y)\in G_\epsilon:x,y\in\mathbb{F}_4\},\\
&\mathrm{Im}_{G_\epsilon}(1-\tau_\nu)=\{(0,\nu x):x\in\mathbb{F}_4\},\\
&\mathrm{Ker}_{G_\epsilon}(1-\tau_\nu)=\{((\nu+1)x,y)\in G_\epsilon:x,y\in\mathbb{F}_4\}.
\end{aligned}\tag{2.7}$$

对任意的 $\alpha\in\mathbb{F}_4$,

$$\begin{aligned}
\mathrm{Im}_{G_\epsilon}(1+\rho_\alpha)&=\{(x,y)+\rho_\alpha(x,y):(x,y)\in G_\epsilon\}\\
&=\{(x+x^2,y+y^2+\alpha x^2+\epsilon x^3):x,y\in\mathbb{F}_4\}\\
&=\begin{cases}
\{(0,0),(0,1),(1,0),(1,1)\} & \text{如果 } \alpha=0,\\
\{(0,0),(0,1),(1,\omega),(1,\omega+1)\} & \text{如果 } \alpha=1,\\
\{(0,y),(1,y):y\in\mathbb{F}_4\} & \text{如果 } \alpha=\omega \text{ 或 } \omega+1,
\end{cases}
\end{aligned}\tag{2.8}$$

$$\begin{aligned}
\mathrm{Ker}_{G_\epsilon}(1+\rho_\alpha)&=\{(x,y)\in G_\epsilon:x,y\in\mathbb{F}_4 \text{ 且} x+x^2=0,y+y^2+\alpha x^2+\epsilon x^3=0\}\\
&=\begin{cases}
\{(0,0),(0,1),(1,0),(1,1)\} & \text{如果 } \alpha+\epsilon=0,\\
\{(0,0),(0,1),(1,\omega),(1,\omega+1)\} & \text{如果 } \alpha+\epsilon=1,\\
\{(0,0),(0,1)\} & \text{如果 } \alpha=\omega \text{ 或 } \omega+1,
\end{cases}
\end{aligned}\tag{2.9}$$

$$\begin{aligned}
\mathrm{Im}_{G_\epsilon}(1-\rho_\alpha)&=\{(x,y)-\rho_\alpha(x,y):(x,y)\in G_\epsilon\}\\
&=\{(x+x^2,y+y^2+(\alpha+\epsilon)x^2+\epsilon x^3):x,y\in\mathbb{F}_4\}\\
&=\begin{cases}
\{(0,0),(0,1),(1,0),(1,1)\} & \text{如果 } \alpha+\epsilon=0,\\
\{(0,0),(0,1),(1,\omega),(1,\omega+1)\} & \text{如果 } \alpha+\epsilon=1,\\
\{(0,y),(1,y):y\in\mathbb{F}_4\} & \text{如果 } \alpha=\omega \text{ 或 } \omega+1,
\end{cases}
\end{aligned}\tag{2.10}$$

$$\mathrm{Ker}_{G_\epsilon}(1-\rho_\alpha)=\{(x,y)\in G_\epsilon : x,y\in\mathbb{F}_4 \text{ 且} x+x^2=0, y+y^2+\alpha x^2=0\} \tag{2.11}$$
$$=\begin{cases}\{(0,0),(0,1),(1,0),(1,1)\} & \text{若 } \alpha=0,\\ \{(0,0),(0,1),(1,\omega),(1,\omega+1)\} & \text{若 } \alpha=1,\\ \{(0,0),(0,1)\} & \text{若 } \alpha=\omega \text{ 或 } \omega+1.\end{cases}$$

我们现在准备给出四个无定形非交换凯莱结合方案, 它们同构于 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 或 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$, 分别对应于非交换的拉丁方型和负拉丁方型的偏差集.

定理 2.7 假设 n 是一个大于等于 2 的整数, $\mathbf{e}=(\epsilon_1,\epsilon_2,\cdots,\epsilon_n)$ 是向量空间 $\mathbb{F}_2^n$ 中的向量, 以及 $\mathbf{a}=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是向量空间 $\mathbb{F}_4^n$ 中的向量. 假设 $G_\mathbf{e}$, $Q_\mathbf{a}$ 和 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 分别为定理 2.2中定义的交换群、二次型和无定形交换凯莱结合方案. 对任意满足 $0\leqslant l\leqslant w(\mathbf{e})$ 和 $1\leqslant n-l\leqslant k\leqslant n$ 的整数 k 和 l, 存在 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的一个正则自同构群 G, 其中 G 的幂零类数是 2, 指数是 4, 并且满足

$$[G,G]\cong\mathbb{Z}_2^{2k} \text{ 或 } \mathbb{Z}_2^{2k-1}, \tag{2.12}$$
$$Z(G)\cong\mathbb{Z}_2^{4n-2k-4l}\oplus\mathbb{Z}_4^{2l} \text{ 或 } \mathbb{Z}_2^{4n-2k-4l+1}\oplus\mathbb{Z}_4^{2l-1} \text{ 或 } \mathbb{Z}_2^{4n-2k-4l-1}\oplus\mathbb{Z}_4^{2l}, \tag{2.13}$$
$$\Phi(G)\cong\mathbb{Z}_2^{2l+2w(\mathbf{e})-1} \text{ 或 } \mathbb{Z}_2^{2l+2w(\mathbf{e})}. \tag{2.14}$$

证明 假设 $\mathbf{v}=(\nu_1,\nu_2,\cdots,\nu_n)$ 为 $\mathbb{F}_2^n$ 中的一个向量, 使得 $w(\mathbf{v}*\mathbf{e}+\mathbf{e})=l$ 且 $w(\mathbf{v})=k$. 定义群 $G_\mathbf{e}$ 的一个自同构 $\tau_\mathbf{v}=(\tau_{\nu_1},\tau_{\nu_2},\cdots,\tau_{\nu_n})\in\mathrm{Aut}(G_\mathbf{e})$. 易知, $\tau_\mathbf{v}$ 亦是 $Q_\mathbf{a}$ 的一个 2 阶等距变换. 由

$$\mathrm{Im}_{G_\mathbf{e}}(1+\tau_\mathbf{v})=\mathrm{Im}_{G_{\epsilon_1}}(1+\tau_{\nu_1})\oplus\mathrm{Im}_{G_{\epsilon_2}}(1+\tau_{\nu_2})\oplus\cdots\oplus\mathrm{Im}_{G_{\epsilon_n}}(1+\tau_{\nu_n}),$$

以及引理 2.3和式子 (2.7), 可得对于 $\mathbb{F}_4^n$ 中的一个给定的非零向量 $(b_1,b_2,\cdots,b_n)$, 子群

$$K:=\{((x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n))\in G_\mathbf{e} : \mathrm{Tr}(b_1x_1+b_2x_2+\cdots+b_nx_n)=0\}$$

是 $G_\mathbf{e}$ 的一个指数为 2 的 $\tau_\mathbf{v}$-不变子群. 记 $h=((u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n))$ 为 $G_\mathbf{e}$ 的一个元素, 其满足 $\mathrm{Tr}(b_1u_1+b_2u_2+\cdots+b_nu_n)\neq 0$ 且 $(\mathbf{v}+\mathbf{e})*(u_1,u_2,\cdots,u_n)\neq\mathbf{0}$. 根据定理 2.4, 定理 2.3中定义的群 $G:=G_{K,\tau_\mathbf{v},h}$ 是无定形交换凯莱结合方案 $\mathcal{S}^{(4)}_{\mathbf{e},\mathbf{a}}$ 的一个正则自同构群. 通过定理 2.3和式子 (2.7), 交换子群

$$\begin{aligned}[G,G]&\cong\mathrm{Im}_K(1-\tau_\mathbf{v})\\ &=\{((0,\nu_1x_1),(0,\nu_2x_2),\cdots,(0,\nu_nx_n))\in G_\mathbf{e} : \mathrm{Tr}(b_1x_1+b_2x_2+\cdots+b_nx_n)=0\}\\ &\cong\begin{cases}\mathbb{Z}_2^{2w(\mathbf{v})-1} & \text{如果 } \mathbf{b}*(\mathbf{v}+\mathbf{1})=\mathbf{0},\\ \mathbb{Z}_2^{2w(\mathbf{v})} & \text{如果 } \mathbf{b}*(\mathbf{v}+\mathbf{1})\neq\mathbf{0}.\end{cases}\end{aligned}$$

由式子 (2.3), 中心

$$
\begin{aligned}
Z(G) &\cong \mathrm{Ker}_K(1-\tau_{\mathbf{v}}) \\
&= \{(((\nu_1+1)x_1, y_1), ((\nu_2+1)x_2, y_2), \cdots, ((\nu_n+1)x_n, y_n)) \in G_{\mathbf{e}} : \mathrm{Tr}(b_1(\nu_1+1)x_1 \\
&\qquad + b_2(\nu_2+1)x_2 + \cdots + b_n(\nu_n+1)x_n) = 0\} \\
&\cong \begin{cases}
\mathbb{Z}_2^{4n-2w(\mathbf{v})-4w(\mathbf{v}*\mathbf{e}+\mathbf{e})} \oplus \mathbb{Z}_4^{2w(\mathbf{v}*\mathbf{e}+\mathbf{e})} & \text{如果 } \mathbf{b}*(\mathbf{v}+\mathbf{1}) = \mathbf{0}, \\
\mathbb{Z}_2^{4n-2w(\mathbf{v})-4w(\mathbf{v}*\mathbf{e}+\mathbf{e})+1} \oplus \mathbb{Z}_4^{2w(\mathbf{v}*\mathbf{e}+\mathbf{e})-1} & \text{如果 } \mathbf{b}*(\mathbf{v}+\mathbf{1}) \neq \mathbf{0}, \mathbf{b}*(\mathbf{v}+\mathbf{1})*(\mathbf{e}+\mathbf{1}) = \mathbf{0}, \\
\mathbb{Z}_2^{4n-2w(\mathbf{v})-4w(\mathbf{v}*\mathbf{e}+\mathbf{e})-1} \oplus \mathbb{Z}_4^{2w(\mathbf{v}*\mathbf{e}+\mathbf{e})} & \text{如果 } \mathbf{b}*(\mathbf{v}+\mathbf{1})*(\mathbf{e}+\mathbf{1}) \neq \mathbf{0}.
\end{cases}
\end{aligned}
$$

由式子 (2.4), Frattini 子群

$$
\begin{aligned}
\Phi(G) &\cong \Phi(K) + \mathrm{Im}_K(1+\tau_{\mathbf{v}}) + \langle h_2 \rangle = \Phi(K) + \mathrm{Im}_K(1+\tau_{\mathbf{v}}) + \langle h + \tau_{\mathbf{v}}(h) \rangle \\
&= \Phi(K) + \mathrm{Im}_{G_{\mathbf{e}}}(1+\tau_{\mathbf{v}}) \\
&= \{((0, (\nu_1+\epsilon_1)x_1 + \epsilon_1 x_1'), (0, (\nu_2+\epsilon_2)x_2 + \epsilon_2 x_2'), \cdots, (0, (\nu_n+\epsilon_n)x_n + \epsilon_n x_n')) \\
&\qquad \in G_{\mathbf{e}} : \mathrm{Tr}(b_1 x_1' + b_2 x_2' + \cdots + b_n x_n') = 0\} \\
&\cong \begin{cases}
\mathbb{Z}_2^{2w(\mathbf{v}*\mathbf{e}+\mathbf{v})+2w(\mathbf{e})-1} & \text{如果 } \mathbf{b}*(\mathbf{v}*\mathbf{e}+\mathbf{1}) = \mathbf{0}, \\
\mathbb{Z}_2^{2w(\mathbf{v}*\mathbf{e}+\mathbf{v})+2w(\mathbf{e})} & \text{如果 } \mathbf{b}*(\mathbf{v}*\mathbf{e}+\mathbf{1}) \neq \mathbf{0}.
\end{cases}
\end{aligned}
$$

因为 $\mathrm{Im}_K(1-\tau_{\mathbf{v}}) \neq \{0\}$ 以及 $\mathrm{Im}_{\Phi(K)}(1-\tau_{\mathbf{v}}) = \{0\}$, 根据定理 2.4, 群 G 的幂零类数是 2. 根据假设可知 $x_i (1 \leqslant i \leqslant n)$ 不全为零. 对任意的 $x \in K$ 和 $R(h_t)\tau^t$, 我们有 $(R(h_t+x)\tau^t)^4 = R(0)$. 另外, $(R(h)\tau)^2 = R(((0, (\nu_1+\epsilon_1)u_1), \cdots, (0, (\nu_n+\epsilon_n)u_n)))$. 根据假设可知 $(\mathbf{v}+\mathbf{e})*(u_1, \cdots, u_n) \neq \mathbf{0}$, 于是 G 的指数是 4.

定理 2.8 假设 n 为一个大于等于 2 的整数, $\mathbf{e} = (\epsilon_1, \epsilon_2, \cdots, \epsilon_n)$ 和 $\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ 均为 $\mathbb{F}_2^n$ 中的向量. 假设 $G_{\mathbf{e}}, Q_{\mathbf{a}}$ 和 $\mathcal{S}_{\mathbf{e},\mathbf{a}}^{(3)}$ 分别是定理 2.2中定义的交换群、二次型和无定形交换凯莱结合方案. $\mathcal{S}_{\mathbf{e},\mathbf{a}}^{(3)}$ 有一个正则自同构群 G, 其中 G 的幂零类数是 2 或 3, 指数是 4 或 8, 并且有

$$
\begin{aligned}
[G, G] &\cong \mathbb{Z}_2^{2(n-w(\mathbf{e}))+1} \oplus \mathbb{Z}_4^{w(\mathbf{e})-1} \text{ 或 } \mathbb{Z}_2^{2(n-w(\mathbf{e}))-1} \oplus \mathbb{Z}_4^{w(\mathbf{e})}, \\
Z(G) &\cong \mathbb{Z}_2^{2(n-w(\mathbf{e}))} \oplus \mathbb{Z}_4^{w(\mathbf{e})}, \\
\Phi(G) &\cong \mathbb{Z}_2^{2n-w(\mathbf{e})-1} \oplus \mathbb{Z}_4^{w(\mathbf{e})} \text{ 或 } \mathbb{Z}_2^{2n-w(\mathbf{e})} \oplus \mathbb{Z}_4^{w(\mathbf{e})}.
\end{aligned}
$$

证明 定义交换群 $G_{\mathbf{e}}$ 的一个自同构 $\rho_{\mathbf{a}} = (\rho_{\alpha_1}, \rho_{\alpha_2}, \cdots, \rho_{\alpha_n})$, 其中 $\rho_{\alpha_i} (1 \leqslant i \leqslant n)$ 是 G_{ϵ_i} 的同构. 易知, $\rho_{\mathbf{a}}$ 是 $Q_{\mathbf{a}}$ 的一个阶为 2 的广义等距变换. 给定一个非零向量 $\mathbf{b} = (b_1, b_2, \cdots, b_n) \in \mathbb{F}_2^n$. 通过引理 2.3, 由

$$
\mathrm{Im}_{G_{\mathbf{e}}}(1+\rho_{\mathbf{a}}) = \mathrm{Im}_{G_{\epsilon_1}}(1+\rho_{\alpha_1}) \oplus \mathrm{Im}_{G_{\epsilon_2}}(1+\rho_{\alpha_2}) \oplus \cdots \oplus \mathrm{Im}_{G_{\epsilon_n}}(1+\rho_{\alpha_n})
$$

和式子 (2.8), 可得子群

$$K := \{((x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)) \in G_{\mathbf{e}} : \mathrm{Tr}(b_1x_1 + b_2x_2 + \cdots + b_nx_n) = 0\}$$

是群 $G_{\mathbf{e}}$ 的一个指数为 2 的 $\rho_{\mathbf{a}}$-不变子群. 令 $h = ((u_1, v_1), (u_2, v_2), \cdots, (u_n, v_n))$ 是 $G_{\mathbf{e}} \setminus H$ 中的任意一个元素. 定理 2.3中所定义的群 $G := G_{K,\rho_{\mathbf{a}},h}$ 是 $\mathcal{S}^{(3)}_{\mathbf{e},\mathbf{a}}$ 的一个正则自同构群. 由定理 2.3和式子 (2.10), 交换子群

$$\begin{aligned}
[G, G] &\cong \mathrm{Im}_K(1 - \rho_{\mathbf{a}}) \\
&= \{((x_1 + x_1^2, y_1 + y_1^2 + (\alpha_1 + \epsilon_1)x_1^2 + \epsilon_1x_1^3), (x_2 + x_2^2, y_2 + y_2^2 + (\alpha_2 + \epsilon_2)x_2^2 + \epsilon_2x_2^3), \\
&\cdots, (x_n + x_n^2, y_n + y_n^2 + (\alpha_n + \epsilon_n)x_n^2 + \epsilon_nx_n^3)) \in G_{\mathbf{e}} : \mathrm{Tr}(b_1x_1 + b_2x_2 + \cdots + b_nx_n) = 0\} \\
&\cong \begin{cases} \mathbb{Z}_2^{2(n-w(\mathbf{e}))+1} \oplus \mathbb{Z}_4^{w(\mathbf{e})-1} & \text{如果 } \mathbf{b} * \mathbf{e} = \mathbf{b}, \\ \mathbb{Z}_2^{2(n-w(\mathbf{e}))-1} \oplus \mathbb{Z}_4^{w(\mathbf{e})} & \text{如果 } \mathbf{b} * \mathbf{e} \neq \mathbf{b}. \end{cases}
\end{aligned}$$

由式子 (2.10), 中心

$$\begin{aligned}
Z(G) &\cong \mathrm{Ker}_K(1 - \rho_{\mathbf{a}}) \\
&= \{((x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)) \in G_{\mathbf{e}} : \mathrm{Tr}(b_1x_1 + b_2x_2 + \cdots + b_nx_n) = 0, \\
&\qquad\qquad x_i + x_i^2 = 0 \text{ 和 } y_i + y_i^2 = \alpha_ix_i^2 \text{ 其中 } i = 1, 2, \cdots, n\} \\
&\cong \mathbb{Z}_2^{2(n-w(\mathbf{e}))} \oplus \mathbb{Z}_4^{w(\mathbf{e})}.
\end{aligned}$$

由式子 (2.4), Frattini 子群

$$\begin{aligned}
\Phi(G) &\cong \Phi(K) + \mathrm{Im}_K(1 + \rho_{\mathbf{a}}) + \langle h_2 \rangle = \Phi(K) + \mathrm{Im}_K(1 + \rho_{\mathbf{a}}) + \langle h + \rho_{\mathbf{a}}(h) \rangle \\
&= \Phi(K) + \mathrm{Im}_{G_{\mathbf{e}}}(1 + \rho_{\mathbf{a}}) \\
&= \{((x_1 + x_1^2, y_1 + y_1^2 + \alpha_1x_1^2 + \epsilon_1x_1^3 + \epsilon_1x_1'), (x_2 + x_2^2, y_2 + y_2^2 + \alpha_2x_2^2 + \epsilon_2x_2^3 + \epsilon_2x_2'), \\
&\cdots, (x_n + x_n^2, y_n + y_n^2 + \alpha_nx_n^2 + \epsilon_nx_n^3 + \epsilon_nx_n')) \in G_{\mathbf{e}} : \mathrm{Tr}(b_1x_1' + b_2x_2' + \cdots + b_nx_n') = 0\} \\
&\cong \begin{cases} \mathbb{Z}_2^{2n-w(\mathbf{e})-1} \oplus \mathbb{Z}_4^{w(\mathbf{e})} & \text{如果} \mathbf{b} * \mathbf{e} = \mathbf{b}, \\ \mathbb{Z}_2^{2n-w(\mathbf{e})} \oplus \mathbb{Z}_4^{w(\mathbf{e})} & \text{如果} \mathbf{b} * \mathbf{e} \neq \mathbf{b}. \end{cases}
\end{aligned}$$

通过计算 $[G, G]$, 可知 G 是非交换的. 当 $\mathbf{e} = \mathbf{0}$ 或 $w(\mathbf{e}) = w(\mathbf{b}) = w(\mathbf{e} * \mathbf{b}) = 1$ 时, $\mathrm{Im}_K((1-\rho_{\mathbf{a}})^2) = 0$, 否则 $\mathrm{Im}_K((1 - \rho_{\mathbf{a}})^2) \neq 0$ 且 $\mathrm{Im}_K((1 - \rho_{\mathbf{a}})^3) = 0$. 于是根据引理 2.3, 当 $\mathbf{e} = \mathbf{0}$ 或 $w(\mathbf{e}) = w(\mathbf{b}) = w(\mathbf{e} * \mathbf{b}) = 1$ 时, G 的幂零类数是 2, 否则 G 的幂零类数是 3. 对任意的 $x \in K$ 和 $R(h_t)\rho_{\mathbf{a}}^t$, 我们有 $(R(h_t + x)\rho_{\mathbf{a}}^t)^8 = R(0)$. 另外, $(R(h)\rho_{\mathbf{a}})^4 = R(((0, \epsilon_1(u_1 + u_1^2)), \cdots, (0, \epsilon_n(u_n + u_n^2)))$. 如果 $\mathbf{e} * (\mathrm{Tr}(u_1), \cdots, \mathrm{Tr}(u_n)) = \mathbf{0}$, G 的指数是 4, 否则 G 的指数是 8.

定理 2.9 假设 $n \geqslant 2$ 是一个整数, $\mathbf{e} = (\epsilon_1, \epsilon_2, \cdots, \epsilon_n)$ 是 $\mathbb{F}_2^n$ 中的向量, 以及 $\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是 $\mathbb{F}_4^n \setminus \mathbb{F}_2^n$ 中的一个向量. 假设 $G_{\mathbf{e}}, Q_{\mathbf{a}}$ 和 $\mathcal{S}_{\mathbf{e},\mathbf{a}}^{(3)}$ 分别是定理 2.2中定义的交换群、二次型和无定形交换凯莱结合方案. $\mathcal{S}_{\mathbf{e},\mathbf{a}}^{(3)}$ 有一个非交换正则自同构群 G, 其中 G 的幂零类是 2 或 4, 指数是 4 或 8, 并且

$$\begin{aligned}
|[G,G]| &= 2^{2(n-1)+w(\mathrm{Tr}(\mathbf{a}))} \text{ 或 } 2^{2n+w(\mathrm{Tr}(\mathbf{a}))-1},\\
|Z(G)| &= 2^{2n-w(\mathrm{Tr}(\mathbf{a}))} \text{ 或 } 2^{2n-w(\mathrm{Tr}(\mathbf{a}))-1},\\
|\Phi(G)| &= 2^{2n-1+w(\mathrm{Tr}(\mathbf{a}))+w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*\mathbf{e})}.
\end{aligned}$$

证明 定义交换群 $G_{\mathbf{e}}$ 的一个自同构 $\rho_{\mathbf{a}} = (\rho_{\alpha_1}, \rho_{\alpha_2}, \cdots, \rho_{\alpha_n})$, 其中 ρ_{α_i}, $1 \leqslant i \leqslant n$, 是定义在式子 (2.6) 中的 G_{ϵ_i} 的自同构. 易知, $\rho_{\mathbf{a}}$ 亦是 $Q_{\mathbf{a}}$ 的一个 4 阶等距变换. 给定一个非零向量 $\mathbf{b} = (b_1, b_2, \cdots, b_n) \in \mathbb{F}_2^n$. 根据引理 2.3, 由

$$\mathrm{Im}_{G_{\mathbf{e}}}(1+\rho_{\mathbf{a}}) = \mathrm{Im}_{G_{\epsilon_1}}(1+\rho_{\alpha_1}) \oplus \mathrm{Im}_{G_{\epsilon_2}}(1+\rho_{\alpha_2}) \oplus \cdots \oplus \mathrm{Im}_{G_{\epsilon_n}}(1+\rho_{\alpha_n})$$

和式子 (2.8), 群

$$H := \{((x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)) \in G_{\mathbf{e}} : \mathrm{Tr}(b_1x_1 + b_2x_2 + \cdots + b_nx_n) = 0\}$$

是 $G_{\mathbf{e}}$ 的一个指数为 2 的 $\rho_{\mathbf{a}}$-不变子群, 并且群

$$K := \{((x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)) \in G_{\mathbf{e}} : b_1x_1 + b_2x_2 + \cdots + b_nx_n = 0\}$$

是 H 的一个指数为 2 的 $\rho_{\mathbf{a}}$-不变子群. 令 $h = ((u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n))$ 是 $G_{\mathbf{e}} \setminus H$ 中的任意一个元素. 定理 2.3中定义的群 $G := G_{K,\rho_{\mathbf{a}},h}$ 是分别对应于偏差集 $Q_{\mathbf{a}}^{-1}(0) \setminus \{0\}$ 和 $Q_{\mathbf{a}}^{-1}(1)$ 的图 $\Gamma_{\mathbf{e},\mathbf{a}}^{(0)}$ 和图 $\Gamma_{\mathbf{e},\mathbf{a}}^{(1)}$ 的正则子群. 通过定理 2.3和式子 (2.10), 交换子群

$$\begin{aligned}
[G,G] &\cong \mathrm{Im}_K(1-\rho_{\mathbf{a}})\\
&= \{((x_1+x_1^2, y_1+y_1^2+(\alpha_1+\epsilon_1)x_1^2+\epsilon_1x_1^3), (x_2+x_2^2, y_2+y_2^2+(\alpha_2+\epsilon_2)x_2^2+\epsilon_2x_2^3),\\
&\cdots, (x_n+x_n^2, y_n+y_n^2+(\alpha_n+\epsilon_n)x_n^2+\epsilon_nx_n^3)) \in G_{\mathbf{e}} : b_1x_1+b_2x_2+\cdots+b_nx_n = 0\}\\
&\cong \begin{cases}
\mathbb{Z}_2^{2(n-w(\mathbf{e}))+w(\mathrm{Tr}(\mathbf{a}))} \oplus \mathbb{Z}_4^{w(\mathbf{e})-1} & \text{如果 } \mathbf{b}*\mathrm{Tr}(\mathbf{a}) = \mathbf{b} \text{ 且 } \mathbf{b}*\mathbf{e} = \mathbf{b},\\
\mathbb{Z}_2^{2(n-w(\mathbf{e})-1)+w(\mathrm{Tr}(\mathbf{a}))} \oplus \mathbb{Z}_4^{w(\mathbf{e})} & \text{如果 } \mathbf{b}*\mathrm{Tr}(\mathbf{a}) = \mathbf{b} \text{ 且 } \mathbf{b}*\mathbf{e} \neq \mathbf{b},\\
\mathbb{Z}_2^{2(n-w(\mathbf{e}))+w(\mathrm{Tr}(\mathbf{a}))+1} \oplus \mathbb{Z}_4^{w(\mathbf{e})-1} & \text{如果 } \mathbf{b}*\mathrm{Tr}(\mathbf{a}) \neq \mathbf{b} \text{ 且 } \mathbf{b}*\mathbf{e} = \mathbf{b},\\
\mathbb{Z}_2^{2(n-w(\mathbf{e}))+w(\mathrm{Tr}(\mathbf{a}))-1} \oplus \mathbb{Z}_4^{w(\mathbf{e})} & \text{如果 } \mathbf{b}*\mathrm{Tr}(\mathbf{a}) \neq \mathbf{b} \text{ 且 } \mathbf{b}*\mathbf{e} \neq \mathbf{b}.
\end{cases}
\end{aligned}$$

因此 $|[G,G]| = 2^{2(n-1)+w(\mathrm{Tr}(\mathbf{a}))}$ 或 $2^{2n+w(\mathrm{Tr}(\mathbf{a}))-1}$. 通过定理 2.3和式子 (2.11), 如果

$$w(\mathrm{Tr}(\mathbf{a})) = w(\mathbf{b}) = w(\mathrm{Tr}(\mathbf{a})*\mathbf{b}) = 1,$$

就有 $o(\rho_{\mathbf{a}}|_K)=2$, 并且当 $h_4\in\Phi(\mathrm{Ker}_K(1-\rho_{\mathbf{a}}))$, 中心 $Z(G)\cong\mathrm{Ker}_K(1-\rho_{\mathbf{a}})\times\mathbb{Z}_2$; 当 $h_4\notin\Phi(\mathrm{Ker}_K(1-\rho_{\mathbf{a}}))$, 中心 $Z(G)\cong[\mathrm{Ker}_K(1-\rho_{\mathbf{a}})/\langle h_4\rangle]\times\mathbb{Z}_4$. 否则, $o(\rho_{\mathbf{a}}|_K)=o(\rho_{\mathbf{a}})=4$, 并且中心 $Z(G)\cong\mathrm{Ker}_K(1-\rho_{\mathbf{a}})$, 其中

$$\begin{aligned}&\mathrm{Ker}_K(1-\rho_{\mathbf{a}})\\=&\{((x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n))\in G_{\mathbf{e}}:b_1x_1+b_2x_2+\cdots+b_nx_n=0,x_i+x_i^2=0\\&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\text{且 }y_i+y_i^2=\alpha_ix_i^2,i=1,2,\cdots,n\}\\\cong&\begin{cases}\mathbb{Z}_2^{w(\mathrm{Tr}(\mathbf{a}))+2w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*(\mathbf{e}+\mathbf{1}))}\oplus\mathbb{Z}_4^{w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*\mathbf{e})} & \text{如果 }\mathbf{b}*\mathrm{Tr}(\mathbf{a})=\mathbf{b},\\ \mathbb{Z}_2^{w(\mathrm{Tr}(\mathbf{a}))+2w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*(\mathbf{e}+\mathbf{1}))+1}\oplus\mathbb{Z}_4^{w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*\mathbf{e})-1} & \text{如果 }\mathbf{b}*\mathrm{Tr}(\mathbf{a})\neq\mathbf{b}\text{ 且 }\mathbf{b}*\mathbf{e}=\mathbf{b},\\ \mathbb{Z}_2^{w(\mathrm{Tr}(\mathbf{a}))+2w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*(\mathbf{e}+\mathbf{1}))-1}\oplus\mathbb{Z}_4^{w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*\mathbf{e})} & \text{如果 }\mathbf{b}*\mathrm{Tr}(\mathbf{a})\neq\mathbf{b}\text{ 且 }\mathbf{b}*\mathbf{e}\neq\mathbf{b}.\end{cases}\end{aligned}$$

因此 $|Z(G)|=2^{2n-w(\mathrm{Tr}(\mathbf{a}))}$ 或 $2^{2n-w(\mathrm{Tr}(\mathbf{a}))-1}$. 通过定理 2.3, 可得 Frattini 子群 $\Phi(G)\cong\langle\Phi(K)+\mathrm{Im}_K(1+\rho_{\mathbf{a}}),h_2\rho_{\mathbf{a}}^2\rangle$. 因为

$$\begin{aligned}&\Phi(K)+\mathrm{Im}_K(1+\rho_{\mathbf{a}})\\=&\{((x_1+x_1^2,y_1+y_1^2+\alpha_1x_1^2+\epsilon_1x_1^3+\epsilon_1x_1'),(x_2+x_2^2,y_2+y_2^2+\alpha_2x_2^2+\epsilon_2x_2^3+\epsilon_2x_2'),\\&\cdots,(x_n+x_n^2,y_n+y_n^2+\alpha_nx_n^2+\epsilon_nx_n^3+\epsilon_nx_n'))\in G_{\mathbf{e}}:b_1x_1+b_2x_2+\cdots+b_nx_n=0,\\&\qquad\qquad\qquad\qquad\qquad\qquad b_1x_1'+b_2x_2'+\cdots+b_nx_n'=0\}\\\cong&\begin{cases}\mathbb{Z}_2^{2(n-w(\mathbf{e}))+w(\mathrm{Tr}(\mathbf{a}))+w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*\mathbf{e})}\oplus\mathbb{Z}_4^{w(\mathbf{e})-1} & \text{如果 }\mathbf{b}*\mathbf{e}=\mathbf{b},\\ \mathbb{Z}_2^{2(n-w(\mathbf{e})-1)+w(\mathrm{Tr}(\mathbf{a}))+w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*\mathbf{e})}\oplus\mathbb{Z}_4^{w(\mathbf{e})} & \text{如果 }\mathbf{b}*\mathbf{e}\neq\mathbf{b},\end{cases}\end{aligned}$$

和 $(h_2\rho_{\mathbf{a}}^2)^2=h_4=(1+\rho_{\mathbf{a}}+\rho_{\mathbf{a}}^2+\rho_{\mathbf{a}}^3)(h)=(1+\rho_{\mathbf{a}})(1+\rho_{\mathbf{a}}^2)(h)\in\mathrm{Im}_K(1+\rho_{\mathbf{a}})$ 以及 $(1+\rho_{\mathbf{a}}^2)(h)\in K$, 所以阶 $|\Phi(G)|=2^{2n-1+w(\mathrm{Tr}(\mathbf{a}))+w((\mathrm{Tr}(\mathbf{a})+\mathbf{1})*\mathbf{e})}$. 由于 $|[G,G]|\neq0$, G 的幂零类数大于 1. 因为 $(1-\rho_{\mathbf{a}})^4=2(1+\rho_{\mathbf{a}}^2)=0\in\mathrm{End}(G_{\mathbf{e}})$, G 的幂零类数不大于 4. 同样地, 由

$$\begin{aligned}\mathrm{Im}_K(1-\rho_{\mathbf{a}})^2=\{&((0,(\alpha_1^2+\alpha_1)x_1+\epsilon_1(x_1+x_1^2)),(0,(\alpha_2^2+\alpha_2)x_2+\epsilon_2(x_2+x_2^2)),\\&\cdots,(0,(\alpha_n^2+\alpha_n)x_n+\epsilon_n(x_n+x_n^2)))\colon b_1x_1+b_2x_2+\cdots+b_nx_n=0\}\end{aligned}$$

和

$$\begin{aligned}\mathrm{Im}_K(1-\rho_{\mathbf{a}})^3=\{&((0,(\alpha_1^2+\alpha_1)(x_1+x_1^2)),(0,(\alpha_2^2+\alpha_2)(x_2+x_2^2)),\cdots,\\&(0,(\alpha_n^2+\alpha_n)(x_n+x_n^2)))\colon b_1x_1+b_2x_2+\cdots+b_nx_n=0\},\end{aligned}$$

可得 $(1-\rho_{\mathbf{a}})^3|_K=0$ 当且仅当 $w(\mathrm{Tr}(\mathbf{a}))=w(\mathbf{b})=w(\mathrm{Tr}(\mathbf{a})*\mathbf{b})=1$, 并且有 $(1-\rho_{\mathbf{a}})^2|_K\neq0$. 因此 G 的幂零类是 3 或 4. 对任意的 $x\in K$ 和 $R(h_t)\rho_{\mathbf{a}}^t$, 我们有 $(R(h_t+x)\rho_{\mathbf{a}}^t)^8=R(0)$. 另外,

$(R(h)\rho_{\mathbf{a}})^4 = R(((0,(\alpha_1+\alpha_1^2+\epsilon_1)(u_1+u_1^2)),\cdots,(0,(\alpha_n+\alpha_n^2\epsilon_n)(u_n+u_n^2)))$. 如果 $(\mathrm{Tr}(\mathbf{a})+\mathbf{e})*(\mathrm{Tr}(u_1),\cdots,\mathrm{Tr}(u_n))=\mathbf{0}$, 那么 G 的指数是 4, 否则 G 的指数是 8.

定理 2.10 假设 $n \geqslant 0$ 是一个整数, $\mathbf{e}=(\epsilon_1,\epsilon_2,\cdots,\epsilon_n)$ 是向量空间 $\mathbb{F}_2^n$ 中的向量以及 $\mathbf{a}=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是向量空间 $\mathbb{F}_4^n$ 中的向量. 对任意的元素 $\epsilon\in\mathbb{F}_2$, 定义 $\mathbf{e}'=(\epsilon,\epsilon,\epsilon,\epsilon)$. 对任意的元素 $\alpha\in\mathbb{F}_4$, 定义 $\mathbf{a}'=(\alpha,\alpha,\alpha,\alpha)$. 令 $G_{\mathbf{e}'}, G_{\mathbf{e}}$ 和 $Q_{\mathbf{a}'}, Q_{\mathbf{a}}$ 分别为定理 2.2中定义的交换群和二次型. 定义 $G_{\mathbf{e}'\oplus\mathbf{e}}=G_{\mathbf{e}'}\oplus G_{\mathbf{e}}$ 和 $Q_{\mathbf{a}'\oplus\mathbf{a}}=Q_{\mathbf{a}'}\oplus Q_{\mathbf{a}}$. 假设 $\mathcal{S}^{(4)}_{\mathbf{e}'\oplus\mathbf{e},\mathbf{a}'\oplus\mathbf{a}}$ 是定理 2.2中定义的无定形交换凯莱结合方案. 对任意的整数 $0\leqslant l\leqslant w(\mathbf{e})$ 和 $0\leqslant n-l\leqslant k\leqslant n$, $\mathcal{S}^{(4)}_{\mathbf{e}'\oplus\mathbf{e},\mathbf{a}'\oplus\mathbf{a}}$ 有一个正则自同构群 G, 其中 G 的幂零类数为 4 或 6, 指数为 8 或 16, 并且有 $|[G,G]|=4^{5+k}$, $|Z(G)|=4^{n+l+2}$ 和 $|\Phi(G)|=2^{2(5+k+l)+1}$ 或 $2^{2(6+k+l)+1}$.

证明 假设 $\mathbf{v}=(\nu_1,\nu_2,\cdots,\nu_n)$ 为 $\mathbb{F}_2^n$ 中的一个向量, $\tau_{\mathbf{v}}\colon G_{\mathbf{e}}\to G_{\mathbf{e}}$ 为定理 2.7证明中定义的 $Q_{\mathbf{a}}$ 的等距变换. 记 $w(\mathbf{v}*\mathbf{e}+\mathbf{e})=l$ 和 $w(\mathbf{v})=k$. 如下定义 $Q_{\mathbf{a}'}\oplus Q_{\mathbf{a}}$ 的一个 4 阶等距变换: 对任意的 $((x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4))\in G_{\mathbf{e}'}$ 和 $z\in G_{\mathbf{e}}$,

$$\pi\colon G_{\mathbf{e}'\oplus\mathbf{e}}\longrightarrow G_{\mathbf{e}'\oplus\mathbf{e}}$$
$$\pi(((x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4)),z)=(((x_4,y_4),(x_1,y_1),(x_2,y_2),(x_3,y_3)),\tau_{\mathbf{v}}(z)).$$

定义子群

$$K:=\{(((x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4)),z)\in G_{\mathbf{e}'\oplus\mathbf{e}'}\colon \mathrm{Tr}(x_1)=\mathrm{Tr}(x_3),\mathrm{Tr}(x_2)=\mathrm{Tr}(x_4)\}$$

和 $h=(((\omega,0),(0,0),(0,0),(0,0)),0)$. 容易验证 K 是 $G_{\mathbf{e}'\oplus\mathbf{e}}$ 的一个指数为 4 的 π-不变子群, 并且 K,π 和 h 满足定理 2.3中的条件. 因此 $G:=G_{K,\pi,h}$ 是 $\mathcal{S}^{(4)}_{\mathbf{e}'\oplus\mathbf{e}}$ 的一个正则自同构群. 通过定理 2.3, 交换子群

$$\begin{aligned}[G,G]\cong\mathrm{Im}_K(1-\pi)=\{(((&x_1+x_4,y_1+y_4+\epsilon x_4+\epsilon x_1^2x_4^2),(x_2+x_1,y_2+y_1+\epsilon x_1+\epsilon x_2^2x_1^2),\\&(x_3+x_2,y_3+y_2+\epsilon x_2+\epsilon x_3^2x_2^2),(x_4+x_3,y_4+y_3+\epsilon x_3+\epsilon x_4^2x_3^2)),z)\in G_{\mathbf{e}'\oplus\mathbf{e}}\colon\\&\mathrm{Tr}(x_1)=\mathrm{Tr}(x_3)\text{ 且 }\mathrm{Tr}(x_2)=\mathrm{Tr}(x_4)\text{ 且 }z\in\mathrm{Im}_{G_{\mathbf{e}}}(1-\tau_{\mathbf{v}})\}\end{aligned}$$
$$=\begin{cases}\mathbb{Z}_2^{2(5+w(\mathbf{v}))} & \text{如果 } \epsilon=0,\\ \mathbb{Z}_2^{2(1+w(\mathbf{v}))}\oplus\mathbb{Z}_4^4 & \text{如果 } \epsilon=1.\end{cases}$$

根据定理 2.3和 $o(\pi|_K)=4$，中心

$$\begin{aligned}Z(G) \cong & \mathrm{Ker}_K(1-\pi)\\ =&\{(((x,y),(x,y),(x,y),(x,y)),z)\in G_{\mathbf{e}'\oplus\mathbf{e}} : x,y\in\mathbb{F}_4, z\in \mathrm{Ker}_{G_{\mathbf{e}}}(1-\tau_{\mathbf{v}})\}\\ =&\begin{cases}\mathbb{Z}_2^{2(w(\mathbf{v})+2w((\mathbf{v}+\mathbf{1})*(\mathbf{e}+\mathbf{1}))+2)}\oplus\mathbb{Z}_4^{2w((\mathbf{v}+\mathbf{1})*\mathbf{e})} & \text{如果 } \epsilon=0,\\ \mathbb{Z}_2^{2(w(\mathbf{v})+2w((\mathbf{v}+\mathbf{1})*(\mathbf{e}+\mathbf{1})))}\oplus\mathbb{Z}_4^{2(1+w((\mathbf{v}+\mathbf{1})*\mathbf{e}))} & \text{如果 } \epsilon=1.\end{cases}\end{aligned}$$

根据定理 2.3, Frattini 子群 $\Phi(G)\cong\langle\Phi(K)+\mathrm{Im}_K(1+\pi),h_2\pi^2\rangle$, 其中

$$\begin{aligned}&\Phi(K)+\mathrm{Im}_K(1+\pi)\\ =&\{(((x_1+x_4,y_1+y_4+\epsilon x_1^2x_4^2+\epsilon x_1'),(x_2+x_1,y_2+y_1+\epsilon x_2^2x_1^2+\epsilon x_2'),\\ &(x_3+x_2,y_3+y_2+\epsilon x_3^2x_2^2+\epsilon x_3'),(x_4+x_3,y_4+y_3+\epsilon x_4^2x_3^2)+\epsilon x_4'),z)\in G_{\mathbf{e}'\oplus\mathbf{e}}:\\ &\mathrm{Tr}(x_1)=\mathrm{Tr}(x_3),\mathrm{Tr}(x_2)=\mathrm{Tr}(x_4),\mathrm{Tr}(x_1')=\mathrm{Tr}(x_3'),\mathrm{Tr}(x_2')=\mathrm{Tr}(x_4'),z\in\mathrm{Im}_{G_{\mathbf{e}}}(1+\tau_{\mathbf{v}})+\Phi(G_{\mathbf{e}})\}\\ =&\begin{cases}\mathbb{Z}_2^{2(n+5-w((\mathbf{v}+\mathbf{1})*(\mathbf{e}+\mathbf{1}))} & \text{如果 } \epsilon=0,\\ \mathbb{Z}_2^{2(n+2-w((\mathbf{v}+\mathbf{1})*(\mathbf{e}+\mathbf{1}))}\oplus\mathbb{Z}_4^4 & \text{如果 } \epsilon=1.\end{cases}\end{aligned}$$

由此可知 $|\Phi(G)|=2^{2(5+k+l)+1}$ 或 $2^{2(6+k+l)+1}$.

易知元素 $x=(((1,0),(0,0),(0,0),(0,0)),0)\in K$ 且

$$(1+\pi+\pi^2+\pi^3)(x)=(((1,0),(1,0),(1,0),(1,0)),0)\neq 0.$$

当 $\epsilon=0$ 时, $\mathrm{End}(G_{\mathbf{e}'\oplus\mathbf{e}})$ 中的自同态

$$\begin{aligned}(1-\pi)^3&=1+\pi+\pi^2+\pi^3,\\ (1-\pi)^4&=2(1+\pi^2)=0,\end{aligned}$$

并且阶 $o(R(h)\pi)=8$, 因此 G 的幂零类数是 4, 指数是 8. 当 $\epsilon=1$ 时,

$$\begin{aligned}(1-\pi)^5&=2(1+\pi+\pi^2+\pi^3),\\ (1-\pi)^5(x)&=(((0,1),(0,1),(0,1),(0,1)),0)\neq 0,\end{aligned}$$

并且阶 $o(R(h)\pi)=16$, 因此 G 的幂零类数是 6, 指数是 16.

2.6 本章小结

本章构造了许多 RT2 图和 Davis-Xiang 图的非交换正则自同构群, 它们分别具有幂零类数 $2,3,4$ 或 6 以及指数 $4,8$ 或 16. 由这些正则自同构群可以得到无定形非交换凯莱结合方案, 同时

这些群包含与 RT2 图和 Davis-Xiang 图具有相同参数的偏差集. 由于检验两个 2-群之间是否同构是一个困难的问题, 因此在所有正则子群中考虑同构群似乎是困难的. 于是我们通过计算一些群的同构不变量来作为区分这些正则子群的依据. 我们的结果表明, 考虑已知的强正则图和无定形结合方案的正则子群是构造包含非平凡的偏差集和无定形非交换凯莱结合方案的非交换群的一个可取的办法.

3 有向强正则图的构造

本章利用局部环对上的部分和族构造了具有新参数的有向强正则图并给出了一类一致部分和族.

本章的主要内容组织如下. 在第一节中, 我们给出了有向强正则图、局部环、m-凯莱有向图以及部分和族的定义和基本性质. 在第二节中, 我们利用局部环对得到了一个部分和族的无穷类, 其中一些部分和族生成了具有新参数的有向强正则图. 在同一框架下, 我们也得到了有限域情况下的一致部分和族.

3.1 基本知识

3.1.1 有向强正则图

有向强正则图是 1988 年由 Duval[4] 提出的.

定义 3.1 带有参数 (v,k,λ,μ,t) 的**有向强正则图 (directed strongly regular graph)**$\mathcal{G}=(V,E)$ 是一个没有圈的有向图且满足如下条件:

(1) 对任意顶点 $x\in V$, 有 k 个不同的顶点 $y\in V$ 和 k 个不同的顶点 $z\in V$ 使得 $(x,y),(z,x)\in E$;

(2) 对任意顶点 x, 恰有 t 个顶点 y 使得 $(x,y),(y,x)\in E$;

(3) 对任意两个不同的顶点 $x,y\in V$, 如果 $(x,y)\in E$, 则恰有 λ 个顶点 $z\in V$ 使得 $(x,z),(z,y)\in E$; 如果 $(x,y)\notin E$, 则恰有 μ 个顶点 $z\in V$ 使得 $(x,z),(z,y)\in E$.

若 (x,y) 和 (y,x) 均属于 E, 则 $\{(x,y),(y,x)\}$ 可被视为一个无向边. 显然, $\mathcal{G}$ 的每个顶点都在 t 条无向边和 $2k-2t$ 条有向边上. 如果 $t=k$, 则 $\mathcal{G}$ 是一个强正则图. 如果 $t=0$, 则 $\mathcal{G}$ 是一个双正则竞赛图. 这两种情况, 加上 $\mathcal{G}$ 是完全图的情况, 被统称为平凡的. 在这一章节中我们只考虑非平凡的有向强正则图.

定义 3.2 假设整数 $m\geq 1, n\geq 2$. 假设 $\mathcal{G}$ 是一个有 mn 个点的有向图. 如果图 $\mathcal{G}$ 有一个阶为 n 的自同构群 G 使得 $\mathcal{G}$ 的点集在 G 的作用下能被划分为 m 个大小为 n 的轨道, 并且其中每个轨道在 G 的作用下是正则的, 则称 $\mathcal{G}$ 是一个 m-**凯莱有向图 (m-Cayley digraph)**. 特别地, 当 $m=1$ 时, 称 $\mathcal{G}$ 为凯莱有向图; 当 $m=2$ 时, 称 $\mathcal{G}$ 为**半凯莱有向图 (semi-Cayley digraph)**.

凯莱有向图是一种构造强正则图和有向强正则图的重要工具. 假设 $\mathcal{G}=(V,E)$ 是一个有向图且有一个正则自同构群 G. 定义 $S=\{g\in G:(a,a^g)\in E\}\subseteq G$, 其中 $a\in V$ 是 $\mathcal{G}$ 中一个给定的点. 定义凯莱有向图 Cay(G,S), 其中凯莱图的点是 G 中的元素, (g_1,g_2) 是弧当且仅当 $g_2g_1^{-1}\in S$. 我们视 $\mathcal{G}$ 和 Cay(G,S) 等价, 并称 S 是 $\mathcal{G}$ 的连通集. 在文献[53] 中, 作者给了有限群的子集成为一个有向强正则图的连通集的充要条件并得到了有向强正则图的无穷类.

通过文献[53], 一个非平凡的有向强正则图无法通过交换群上的凯莱有向图得到. 由此, 构造非平凡有向强正则图常用的方法有两种, 一种是考虑通过非交换群的凯莱有向图构造, 另一种是借助 $m\geq 2$ 时的 m-凯莱图来构造. 本章借助第二种方法来构造有向强正则图. 我们利用群环和特征理论证明了 $m\geq 2$ 的部分和族的存在性, 于是得到了 m-凯莱图的无穷类. 由此为这个问题提供了一个答案.

有向图 $\mathcal{G}=(V,E)$ 的补图 $\overline{\mathcal{G}}=(V',E')$ 亦是一个有向图, 其中的点集 $V'=V$, 弧集 $E'=\{(x,y)\in V\times V:x\neq y,(x,y)\notin E\}$. Duval 在文献[4] 中提出, 带有参数 (v,k,λ,μ,t) 的有向强正则图的补图的参数为

$$(v',k',\lambda',\mu',t')=(v,v-k-1,v-2k+\mu-2,v-2k+\lambda,v-2k+t-1).$$

这两组参数是共同存在的. 所以我们只需考虑 $k\leq v/2$ 的有向强正则图.

3.1.2 群环与特征理论

假设 G 是一个有限群. 群环 $\mathbb{Z}[G]$ 被定义为 G 中元素的形式和的集合, 其中每个元素的系数均为整数. 群环 $\mathbb{Z}[G]$ 中的运算 "+" 和 "$\cdot$" 分别定义如下:

$$\sum_{g\in G}a_gg+\sum_{g\in G}b_gg=\sum_{g\in G}(a_g+b_g)g$$

以及

$$\left(\sum_{g\in G}a_gg\right)\cdot\left(\sum_{h\in G}b_hh\right)=\sum_{g,h\in G}a_gb_h(gh).$$

许多组合结构均是利用群环来研究的. 为了方便, 我们将不区分 G 中的子集 S 和 $\mathbb{Z}[G]$ 中的相应的元素 $\sum_{s\in S}s$. 特征论是另一个强有力的工具, 我们将在后文中主要用到特征论来证明一般性. 特征论的优势主要在于它可以在很大程度上简化运算. 有限交换群 G 上的一个特征是 G 到绝对值为 1 的复数构成的乘法子群上的一个同态. 群 G 的平凡特征是 χ_0, 其满足对任意的 $x\in G,\chi_0(x)=1$. 对 G 的任意子集 S, 定义 χ 在 S 上的作用为 $\chi(S)=\sum_{s\in S}\chi(s)$.

我们亦要用到如下引理中著名的群环互反公式.

引理 3.1 假设 G 是一个有限交换群, $A=\sum_{g\in G}a_gg$ 是群环 $\mathbb{Z}[G]$ 中的一个元素. 于是 A 的系数

a_g 能具体表示为

$$a_g = \frac{1}{|G|}\sum_{\chi\in\hat{G}}\chi(A)\chi(g^{-1}),$$

其中 $\hat{G}$ 为 G 的特征群. 特别地, 如果 $A, B \in \mathbb{Z}[G]$ 满足 $\chi(A) = \chi(B)$ 对所有的特征 $\chi \in \hat{G}$ 均成立, 那么就有 $A = B$.

3.1.3 局部环

受到文献[32] 使用 Galois 环构造偏差集的方法的启发, 我们尝试使用局部环构造部分和族. 局部环是具有唯一极大理想的环. 这里只考虑有限交换局部环, 其极大理想为主理想环. 这样的局部环有时被称为有限链环. 记 $\mathcal{R}$ 为一个有限链环 (finite chain ring), 其极大理想为 I. 易知 I 是由某个素元 π 生成的, 并且可以说 I 是由 $\mathcal{R}$ 中的所有零因子以及 0 组成的. 于是 $\mathcal{R}\setminus I$ 是 $\mathcal{R}$ 中所有单位的集合. Leung 和 Ma[39] 在 $\mathcal{R}\times\mathcal{R}$ 中构造了偏差集, 其中 $\mathcal{R}$ 是具有某些性质的有限链环. 很自然地, 可以想到在同样的群 $\mathcal{R}\times\mathcal{R}$ 上去构造部分和族从而得到有向强正则图. 下面我们先列出一些出现在文献[39] 中的性质, 这些性质将在第 3.2节中被使用.

引理 3.2 [文献[39], 性质 2.4] 对任意的素数 p 以及正整数 s, r, d, 其中 $r \le s$, 存在一个有限链环 $\mathcal{R}$ 以及 $\mathcal{R}$ 的极大理想 $I = (\pi)$, 其中 π 为素元, 使得 (1) $I^{s-1} \neq 0, I^s = 0$, (2) 元素 p 和元素 π^r 互相伴随, (3) $\mathcal{R}/I$ 是一个有 p^d 的元素的有限域.

事实上, 我们可以得到许多满足引理 3.2中条件的有限链环. 例如, 任意一个有限域或者 Galois 环均满足引理 3.2中的条件. 在文献[39] 中, 亦有一个相对复杂的示例: 假设 $\mathbb{Q}_p$ 为 $\mathbb{Q}$ 的 p 进完备化数域, $\mathbb{Z}_p$ 是所有 p 进整数的集合. 假设 K 是 $\mathbb{Q}_p$ 的有限扩张, R' 是 $\mathbb{Z}_p$ 在 K 中的整闭包. 那么 R' 是一个拥有极大理想 (π) 的局部环. 于是就可以得到有限链环 $R := R'/\pi^s R'$.

假设 R 是一个满足引理 3.2中条件的有限链环, H 是环 $\mathcal{R}$ 的加法群. 记 $\hat{H}$ 为 H 的加法特征群. 因为 $I^{s-1} \neq 0$, 所以存在一个特征 $\psi \in \hat{H}$ 使得 ψ 在 I^{s-1} 上作用是非平凡的. 对任意的 $a \in \mathcal{R}$, 定义映射 ψ_a: 对任意的 $x \in \mathcal{R}$, $\psi_a(x) = \psi(ax)$. 于是 $\{\psi_a : a \in \mathcal{R}\} \subseteq \hat{H}$. 显然有 $\psi_a \neq \psi_b$ 对任意的 $a \neq b$ 均成立, 这是因为 ψ 在 $I^{s-1} \subseteq (a-b)$ 上的作用是非平凡的. 由此, $\hat{H} = \{\psi_a : a \in \mathcal{R}\}$. 我们将以上讨论所得到的结论总结在下面的引理中.

引理 3.3 [文献[39]] 假设 $\mathcal{R}$ 是满足引理 3.2中条件的有限链环, H 是 $\mathcal{R}$ 的加法群, $\hat{H}$ 是 H 的加法特征群. 存在一个加法特征 $\psi \in \hat{H}$ 满足 ψ 在 I^{s-1} 上是非平凡的. 另外, $\hat{H} = \{\psi_a : a \in \mathcal{R}\}$, 其中对任意的 $x \in \mathcal{R}$, $\psi_a(x) = \psi(ax)$.

我们考虑群 $G = (H \times H, +)$. 关于群 G 的特征表示, 将用到下面的引理.

引理 3.4 [文献[39], 性质 3.2] 对任意的特征 $\chi \in \hat{G}$, 存在元素 $a,b \in H$ 以及特征 $\psi \in \hat{H}$ 使得 $\chi(x,y) = \psi(ax+by)$ 对任意 $x,y \in H$ 均成立.

在文献[32] 中所用到的群 $G = (H \times H, +)$, 其中 H 是一个 Galois 环. Polhill 通过群 G 上所定义的 "spread" 构造了偏差集. 本章用类似的思想尝试在群 G 中构造部分和族. 我们将他们文章中定义的 "spread" 由 Galois 环推广到有限链环 $\mathcal{R}$ 上:

$$L_a = \{(x, ax) : x \in \mathcal{R}\},$$

$$L_\infty = \{(0, x) : x \in \mathcal{R}\}.$$

固定理想 I 在有限链环 $\mathcal{R}$ 中的陪集代表元, 并将由这些陪集代表元所组成的集合记为 J. 假设 $J' = J \cup \{\infty\}$. 由于对任意的 $a \neq b \in J'$, $L_a \cap L_b = \{(0,0)\}$ 并且 $|L_a| = |L_b| = |H|$, 我们可以得到 $L_a L_b = \{x + y : x \in L_a, y \in L_b\} = G$.

3.1.4 m-凯莱有向图和部分和族

我们先简要介绍有向差图的一些符号, 并使用部分和族的概念来说明有向差图成为一个有向强正则图的条件. 假设 G 是一个阶为 n 的交换群, G 上的运算为加法运算. 假设 $\{S_{i,j}\}_{0 \leq i,j \leq m-1}$ 是 G 的 m^2 个子集. 我们利用 G 和这些子集 $\{S_{i,j}\}_{0 \leq i,j \leq m-1}$ 定义有向图 $\mathcal{G}$:

(1) 点集 V 是 m 个 G 的直积, 也就是说,

$$V = \bigcup_{0 \leq i \leq m-1} G_i,$$

其中每个 G_i 是 G 的一个复制. 对任意的 $a \in G$, 定义 G 的左作用 ρ_a 为 $\rho_a(x) = x + a$, $\forall x \in G$. 于是 ρ_a 作用在点集 V 上可使得每个 G_i 均是在 ρ_a 作用下的一个轨道.

(2) 弧集 E 是由子集 $\{S_{i,j}\}_{0 \leq i,j \leq m-1}$ 所定义的. 对任意两个不同的点 $x \in G_i$ 和 $y \in G_j$, $0 \leq i,j \leq m-1$, 设定 $(x,y) \in E$ 当且仅当 $x - y \in S_{i,j}$.

由此可知 G 是有向图 $\mathcal{G} = (V, E)$ 的自同构群, 并且作用在每个 G_i 上都是正则的. 有向图 $\mathcal{G}$ 被称为关于集族 $\{S_{i,j}\}_{0 \leq i,j \leq m-1}$ 的有向差图. 注意到, 如果一个有向图 $\mathcal{G}$ 是一个关于集族 $\{S_{i,j}\}_{0 \leq i,j \leq m-1}$ 的有向差图, 那么它的补图 $\overline{\mathcal{G}}$ 是关于集族 $\{S'_{i,j}\}_{0 \leq i,j \leq m-1}$ 的有向差图, 其中对任意的 $0 \leq i \neq j \leq m-1$,

$$S'_{i,i} = G^* \setminus S_{i,i}$$

以及

$$S'_{i,j} = G \setminus S_{i,j},$$

这里的 $G^* = G \setminus \{e\}$. 在文献[1] 中, Araluze 等人得到 $\mathcal{G}$ 是一个有向强正则图当且仅当集族 $\{S_{i,j}\}_{0 \leq i,j \leq m-1}$ 是一个如下定义的部分和族.

定义 3.3 有限交换群 G 中的一个子集族 $\{S_{i,j}\}_{0\le i,j\le m-1}$ 被称为一个 (m,n,k,λ,μ,t)-**部分和族 (partial sum family)**, 如果这个子集族满足如下条件:

(1) 对任意的 $0\le i\le m-1, e\notin S_{i,i}$, 其中 e 是 G 中的单位元;

(2) 对任意的 $0\le i\le m-1, \sum_{j=0}^{m-1}|S_{i,j}|=\sum_{j=0}^{m-1}|S_{j,i}|=k$;

(3) 对任意的 $0\le i,j\le m-1, \sum_{l=0}^{m-1}S_{l,j}S_{i,l}=\mu G+\beta S_{i,j}+\delta_{i,j}\gamma e$, 其中 $\beta=\lambda-\mu, \gamma=t-\mu$, 并且 $\delta_{i,j}$ 是克罗内克函数.

引理 3.5 [文献[1], 性质 1.2] 有限交换群 G 的一个子集族 $\{S_{i,j}\}_{0\le i,j\le m-1}$ 是一个 (m,n,k,λ,μ,t)-部分和族当且仅当由 $\{S_{i,j}\}_{0\le i,j\le m-1}$ 定义的有向差图是是一个 (mn,k,λ,μ,t)-有向强正则图.

在 $m=2$ 的情况下, 由 $\mathcal{G}$ 的正则性可得 $|S_{0,0}|=|S_{1,1}|$ 和 $|S_{0,1}|=|S_{1,0}|$. 但是对 $m>2$ 的情况我们无法通过 $\mathcal{G}$ 的正则性得到这样的性质. 类似于 $m=2$ 的情况下集族所拥有的性质, 文献[2] 中的作者提出了此类性质在 $m>2$ 的情况下的推广并且给出了一致部分和族的定义.

定义 3.4 [文献[2]] 有限交换群 G 上的一个部分和族 $\{S_{i,j}\}_{0\le i,j\le m-1}$ 被称为**一致的 (uniform)**, 如果该部分和族满足如下条件:

(1) $|S_{i,i}|$ 均相等;

(2) $|S_{i,j}|$ 对所有的 $i\ne j$ 均相等;

(3) $\{S_{i,i}:0\le i\le m-1\}$ 是 $G\setminus\{0\}$ 的一个划分.

3.2 基于部分和族的有向强正则图的构造

假设 $\mathcal{R}$ 是满足引理 3.2中条件的局部环, 其阶为 p^{sd}, I 是 $\mathcal{R}$ 中唯一的极大理想. 假设 H 是 $\mathcal{R}$ 的加法群, $G=H\times H$. 在这一节中我们先介绍利用第 3.1.3节中所定义的 "spread" 获得部分和族的方法. 然后通过引理 3.5以及这些部分和族得到了一类新的有向强正则图的无穷类. 当环 $\mathcal{R}$ 的极大理想 $I=0$ 时, 我们亦可获得一致部分和族. 这里我们使用第 3.1.3节中所定义的符号 J, J' 和 $L_a, a\in J'$, 并且简记 $(0,0)\in G$ 为 0_G.

我们首先陈述主要的结论.

定理 3.1 对任意的素数 p 和正整数 s,d,w,z_1, $1\le w\le p^d, 1\le z_1\le p^d-w+1$, 存在参数为 $(mn,k,\lambda,\mu,t)=((z_1+1)p^{2sd},(p^{sd}-1)w+z_1z_2p^{sd},p^{sd}+w^2-3w+z_1z_2^2,w^2-w+z_1z_2^2,p^{sd}w-w+z_1z_2^2)$ 的有向强正则图, 其中如果 $w=1, z_2=1$; 如果 $2\le w\le p^d, z_2=w-1$ 或 w.

假设 $J' = \{a_0 = \infty, a_1, \ldots, a_{p^d}\}$. 对任意满足 $0 \le i \le j \le p^d$ 的整数 i, j, 记 $D_{[i,j]} = \{a_i, a_{i+1}, \cdots, a_j\}$. 对任意的 $1 \le w \le p^d$, 定义 $\mathcal{D}_w = \{D_{[i,w+i-1]} : 0 \le i \le p^d - w + 1\}$. 任取 $\mathcal{D}_w$ 中 $z_1 + 1$ 个不同的元素 $A_0, \cdots, A_{z_1}$, 其中 $1 \le z_1 \le p^d - w + 1$, $A_i = D_{[k_i, w+k_i-1]}$. 不失一般性, 假设对任意的 $i < j$, $k_i < k_j$. 令

$$b_{i,j} = \begin{cases} a_{k_i} & \text{如果 } i < j, \\ a_{w+k_i-1} & \text{如果 } i > j, \end{cases} \tag{3.1}$$

以及 $T_{i,j} (0 \le i \ne j \le z_1)$ 为 G 关于 $L_{b_{i,j}}$ 的大小为 z_2 的陪集代表元集合. 注意到 $1 \le z_2 \le p^{sd}$. 接着我们如下定义 G 的一个子集族 $\mathcal{S} = \{S_{i,j}\}_{0 \le i,j \le z_1}$: 对任意的 $0 \le i \ne j \le z_1$,

$$\begin{aligned} S_{i,i} &= \bigcup_{a \in A_i} L_a \setminus \{0_G\}, \\ S_{i,j} &= \bigcup_{g \in T_{i,j}} (g + L_{b_{i,j}}). \end{aligned} \tag{3.2}$$

注 3.1 每个 $b_{i,j}$ 的选择均需要使得 $L_{b_{i,l}} L_{b_{l,j}} = G$ 对任意的 $l \ne i, j$ 成立. 注意到 $L_{b_{i,l}} L_{b_{l,j}} = G$ 当且仅当 $b_{i,l} \ne b_{l,j}$. 根据 $b_{i,j}$ 在式子 (3.1) 中的定义, 我们能验证对任意满足 $l \ne i, j$ 的整数 i, j, l, 均有 $b_{i,l} \ne b_{l,j}$.

引理 3.6 式子 (3.2) 中定义的集族是一个部分和族当且仅当 $z_2 = 1$ 对 $w = 1$ 成立, 或 $z_2 = w - 1$ 或 w 对 $2 \le w \le p^d$ 成立. 另外, 当 $\mathcal{S}$ 是一个部分和族时, 其参数为 $(m, n, k, \lambda, \mu, t) = (z_1 + 1, p^{2sd}, (p^{sd} - 1)w + z_1 z_2 p^{sd}, p^{sd} + w^2 - 3w + z_1 z_2^2, w^2 - w + z_1 z_2^2, p^{sd} w - w + z_1 z_2^2)$.

证明 根据 $S_{i,i}$ 的定义, 显然每个 $S_{i,i}$ 均不包含 0_G. 注意到, 对任意的整数 $0 \le i \le z_1$, $|S_{i,i}| = (p^{sd} - 1)w$. 对任意的整数 $0 \le i \ne j \le z_1$, $|S_{i,j}| = p^{sd} z_2$. 由此得到对任意的整数 $0 \le i \le z_1$, $\sum_{j=0}^{z_1} |S_{i,j}| = \sum_{j=0}^{z_1} |S_{j,i}| = (p^{sd} - 1)w + z_1 z_2 p^{sd}$ 是一个常数. 所以 $\mathcal{S} = \{S_{i,j}\}_{0 \le i,j \le z_1}$ 满足成为一个部分和族的条件 (1) 和 (2). 接下来我们需要验证集族 $\mathcal{S}$ 满足定义 3.3中的条件 (3) 当且仅当 $z_2 = w - 1$ 或 w.

我们重述定义 3.3中的条件 (3): 对任意的 $0 \le i \ne j \le z_1$,

$$S_{i,i}^2 + \sum_{l=0, l \ne i}^{z_1} S_{i,l} S_{l,i} = \mu G + \beta S_{i,i} + \gamma 0_G, \tag{3.3}$$

$$S_{i,j}(S_{i,i} + S_{j,j}) + \sum_{l=0, l \ne i,j}^{z_1} S_{i,l} S_{l,j} = \mu G + \beta S_{i,j}. \tag{3.4}$$

根据 $S_{i,j}$ 的定义, 对任意的整数 $l \ne i, j$,

$$S_{i,l} S_{l,j} = \sum_{g \in T_{i,l}} (g + L_{b_{i,l}}) \sum_{h \in T_{l,j}} (h + L_{b_{l,j}}) = \sum_{g \in T_{i,l}} \sum_{h \in T_{l,j}} (g + h + G) = |T_{i,l}||T_{l,j}| G = z_2^2 G,$$

这里是根据 $L_{b_{i,l}}L_{b_{l,j}} = G$. 因此

$$S_{i,l}S_{l,j} = z_2^2 G. \tag{3.5}$$

将式子 (3.5) 代入式子 (3.3) 和 (3.4), 可得

$$S_{i,i}^2 = (\mu - z_1 z_2^2)G + \beta S_{i,i} + \gamma 0_G \tag{3.6}$$

对任意的 $0 \le i \le z_1$ 成立, 并且

$$S_{i,j}(S_{i,i} + S_{j,j}) = (\mu - (z_1 - 1)z_2^2)G + \beta S_{i,j} \tag{3.7}$$

对任意的 $0 \le i \ne j \le z_1$ 成立. 我们只需要证明式子 (3.6) 和式子 (3.7) 成立当且仅当 $z_2 = w - 1$ 或 w 即可.

假设式子 (3.6) 和式子 (3.7) 成立. 利用特征作用在这两个式子上便得到 $z_2 = w - 1$ 或 w. 由引理 3.4, 群 G 的特征为

$$\chi_b : (x, y) \mapsto \chi_b(x, y) = \psi(b_1 x + b_2 y),$$

其中 $b = (b_1, b_2) \in G, \psi \in \hat{H}$. 通过用平凡特征 χ_0 作用在式子 (3.6) 上, 可得

$$|S_{i,i}|^2 = (\mu - z_1 z_2^2)|G| + \beta|S_{i,i}| + \gamma, \tag{3.8}$$

由此得到

$$(p^{sd} - 1)^2 w^2 = (\mu - z_1 z_2^2)p^{2sd} + \beta(p^{sd} - 1)w + \gamma. \tag{3.9}$$

用 χ_0 作用在式子 (3.7) 上得到

$$2p^{sd}(p^{sd} - 1)wz_2 = (\mu - (z_1 - 1)z_2^2)p^{2sd} + \beta p^{sd} z_2. \tag{3.10}$$

通过将非平凡的特征 χ_b 作用在 $L_a, a \in J'$, 上得到

$$\chi_b(L_a) = \begin{cases} p^{sd} & \text{如果 } \chi_b \text{ 作用在 } L_a \text{上是平凡的,} \\ 0 & \text{否则.} \end{cases}$$

如第 3.1.2节中所述, 如果一个特征 χ 作用在两个不相等的 spread L_{a_1} 和 L_{a_2} 上均是平凡的, 则 χ 在整个群 G 上是平凡的. 因此

$$\chi_b(S_{i,i}) = \begin{cases} p^{sd} - w & \text{如果 } \chi_b \text{ 作用在某个 } L_a \text{上是平凡的, } L_a \setminus \{0\} \subseteq S_{i,i}, \\ -w & \text{否则.} \end{cases}$$

将非平凡的特征 χ_b 作用在式子 (3.6) 上, 可得

$$\chi_b(S_{i,i})^2 = \beta\chi_b(S_{i,i}) + \gamma. \tag{3.11}$$

假设 b_1 是 R 上的单位元, 也就是说, $b_1 \in R \setminus I$. 特征 $\chi_{(0,b_1)}$ 和 $\chi_{(b_1,0)}$ 是非平凡的, 且分别作用在 L_0 和 L_∞ 上是平凡的. 对任意的 $a \in J \setminus \{0\}$, 非平凡特征 $\chi_{(b_1,-b_1a^{-1})}$ 作用在 L_a 上是平凡的. 因为 $z_1 \geq 1$, 我们能取 $a \in A_0 \setminus A_1$. 于是存在一个非平凡的特征 χ_b 作用在 L_a 上是平凡的. 在这种情况下, $\chi_b(S_{0,0}) = p^{sd} - w$ 以及 $\chi_b(S_{1,1}) = -w$, 并且 $\chi_b(S_{0,0})$ 和 $\chi_b(S_{1,1})$ 均满足式子 (3.11). 所以 $\chi_b(S_{0,0}) + \chi_b(S_{1,1}) = \beta$ 和 $\chi_b(S_{0,0})\chi_b(S_{1,1}) = -\gamma$. 这意味着,

$$\beta = p^{sd} - 2w, \gamma = p^{sd}w - w^2.$$

通过式子 (3.9), 可得

$$\mu = w^2 - w + z_1z_2^2,$$

并且根据式子 (3.10) 我们有

$$z_2^2 - (2w-1)z_2 + w^2 - w = 0,$$

由此可得

$$z_2 = w - 1 \text{ 或 } w.$$

注意到 $1 \leq w \leq p^d$ 以及 $1 \leq z_2 \leq p^{sd}$, 并且当 $w = 1$ 时, $z_2 = 1$.

反之, 假设当 $w = 1$ 时, $z_2 = 1$; 当 $2 \leq w \leq p^d$ 时, $z_2 = w - 1$ 或 w. 通过将非平凡特征 χ_b 作用到式子 (3.7) 上, 可得

$$\chi_b(S_{i,j})\chi_b(S_{i,i} + S_{j,j}) = \beta\chi_b(S_{i,j}). \tag{3.12}$$

根据引理 3.1, 只需要证明式子 (3.9), (3.10), (3.11) 和 (3.12) 在 G 的所有特征的作用下均成立. 假设 $\mu = w^2 - w + z_1z_2^2$, $\beta = p^{sd} - 2w$ 和 $\gamma = p^{sd}w - w^2$. 易知, 式子 (3.9) 和 (3.10) 均成立. 因为对任意的整数 $0 \leq i \leq z_1$ 和非平凡特征 χ_b, 均有 $\chi_b(S_{i,i}) \in \{p^{sd} - w, -w\}$ 成立, 所以式子 (3.11) 成立. 现在只需证明式子 (3.12) 成立. 由 $\beta = p^{sd} - 2w$ 以及对任意两个不同的子集 $S_{i,i}$ 和 $S_{j,j}$ 以及非平凡特征 χ_b, 均有

$$\chi_b(S_{i,i} + S_{j,j}) \in \{-2w, p^{sd} - 2w, 2p^{sd} - 2w\},$$

可得 $\chi_b(S_{i,j}) = 0$ 对任意的使得 $\chi_b(S_{i,i} + S_{j,j}) \neq \beta$ 的非平凡特征 χ_b 均成立. 令特征 χ_b 满足上述条件, 则有 $\chi_b(S_{i,i}) = \chi_b(S_{j,j}) = p^{sd} - w$ 或 $-w$. 在这两种情况下, 我们都能得到 χ_b 在 $L_{b_{i,j}}$ 上是非平凡的. 于是

$$\chi_b(S_{i,j}) = \chi_b(\bigcup_{g \in T_{ij}} (g + L_{b_{i,j}})) = \chi_b(L_{b_{i,j}}) \sum_{g \in T_{i,j}} \chi_b(g) = 0.$$

因此式子 (3.12) 成立.

我们现在可以证明定理 3.1.

证明 (定理 3.1) 通过引理 3.5和引理 3.6, 就能得到该定理的结论.

注 3.2 假设 $\mathcal{S}$ 是定义在式子 (3.2) 中的集族. 记 $\mathcal{G}$ 为由 $\mathcal{S}$ 得到的有向差图. 因为 $w \leq p^d$, 集合 $S_{i,i}(0 \leq i \leq z_1)$, 均不等于 $G \setminus \{0_G\}$, 这意味着 $\mathcal{G}$ 不是完全的. 我们需要排除 $t = k$ 和 $t = 0$ 这两种情况, 因为在这两种情况下的有向差图 $\mathcal{G}$ 均为平凡的. 容易知道 $t = p^{sd}w - w + z_1 z_2^2 > 0$. 当 $t = k$ 时, 我们得到 $w = z_2 = p^d$ 和 $s = 1$. 此时 $\mathcal{G}$ 为一个 (非完全的) 强正则图. 另外, 当 $s = 1$ 时, 局部环同构于一个有限域.

我们将上面的定理证明中用 w, z_1 和 z_2 来表示的参数 k, λ, μ, t 分别记为 $k(w, z_1, z_2), \lambda(w, z_1, z_2)$, $\mu(w, z_1, z_2), t(w, z_1, z_2)$.

注 3.3 列在第一章节中的 16 个新参数是两两互补的, 这些新参数均可以由我们的构造在 $s = 1$ 的情况下得到. 也就是说, 我们既可以得到一个参数为 $(z_1 + 1, p^{2d}, k(w, z_1, z_2), \lambda(w, z_1, z_2), \mu(w, z_1, z_2), t(w, z_1, z_2))$ 的部分和族, 也可以得到这个部分和族的补的参数 $(z_1 + 1, p^{2d}, k(p^d + 1 - w, z_1, p^d - z_2), \lambda(p^d + 1 - w, z_1, p^d - z_2), \mu(p^d + 1 - w, z_1, p^d - z_2), t(p^d + 1 - w, z_1, p^d - z_2))$ 所对应的部分和族.

假设 $\mathcal{S} = \{S_{i,j}\}_{0 \leq i,j \leq z_1}$ 是由式子 (3.2) 得到的集族, c 是满足 $0 \leq c \leq z_1$ 的一个固定的整数. 由 $\mathcal{S}$ 删减得到的集族 $\mathcal{S}' = \{S_{i,j}\}_{0 \leq i,j \leq z_1, i,j \neq c}$ 亦是一个部分和族, 并且具有参数 $(z_1, p^{2sd}, k(w, z_1 - 1, z_2), \lambda(w, z_1 - 1, z_2), \mu(w, z_1 - 1, z_2), t(w, z_1 - 1, z_2))$. 另外, 在 $s = 1$ 时, 我们可以适当选取子集 $A_0, A_1, \cdots, A_{z_1}$ 使得部分和族是一致的.

推论 3.1 对任意的素数 p 和正整数 d, w 使得 $w | p^d + 1$, 存在一个具有参数 $(z_1 + 1, p^{2d}, k(w, z_1, z_2), \lambda(w, z_1, z_2), \mu(w, z_1, z_2), t(w, z_1, z_2))$ 的一致部分和族 $\{S_{i,j}\}_{0 \leq i,j \leq z_1}$, 其中 $z_1 = \frac{p^d + 1}{w} - 1$ 以及 $z_2 = w - 1$ 或 w.

证明 设定 $z_1 = \frac{p^d + 1}{w} - 1$ 和 $A_i = D_{[wi, w(i+1)-1]}$, $0 \leq i \leq z_1$. 假设 $\{S_{i,j}\}_{0 \leq i,j \leq z_1}$ 是由 $\{A_0, \cdots, A_{z_1}\}$ 在式子 (3.2) 中定义的集族, 其中 $z_2 = w - 1$ 或 w. 如引理 3.6所述, 这个集族是一个具有参数 $(z_1 + 1, p^{2d}, k(w, z_1, z_2), \lambda(w, z_1, z_2), \mu(w, z_1, z_2), t(w, z_1, z_2))$ 的部分和族. 容易看出 $\{S_{i,i} : 0 \leq i \leq z_1\}$ 是 $G \setminus \{0\}$ 的一个划分. 由引理 3.6中的证明, $|S_{i,i}| = (p^d - 1)w$ 以及 $|S_{i,j}| = p^d z_2$ 对任意的 $i \neq j$ 均成立. 这样保证了定义 3.4中的条件 (1) 和 (2) 被满足. 因此这个部分和族是一致的.

3.3 本章小结

本章考虑了局部环 R 以及群 $G = (R \times R, +)$, 并定义了 G 上的 spread. 我们借助群环的语言和特征理论, 简化了一个集族成为 G 上的部分和族的条件, 从而找到了构造部分和族的新方法. 通过部分和族的构造得到了大量的新的有向强正则图. 在 R 为有限域的情况下, 我们的构造还可以得到一致部分和族, 从而解决了关于一致部分和族的存在性的疑虑.

4 广义 Reed-Muller 码的子码–2 设计的线性码

本章研究由 Hermitian 函数定义的仿射不变三元码. 我们首先通过三元码的最小码字得到了 2-设计, 然后计算这些 2-设计所对应的关联矩阵. 接着证明了这些关联矩阵行所生成的线性码是四阶广义 Reed-Muller 码的子码, 同时包含最初所使用的三元码. 最后确定了所得到的线性码的维数, 并给出了最小距离的下界.

本章的主要内容组织如下. 在第一节中, 我们介绍了线性码、t-设计、循环码、广义 Reed-Muller 码和线性码的自同构群的一些符号和基本结果. 在第二节中, 考虑了仿射不变三元码和由这些设计的关联矩阵的行张成的线性码. 接着定理 4.9和定理 4.10给出了线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的具体表达形式. 我们还在定理 4.11中确定了 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的维数和最小重量的一个下界. 在第四节中, 证明了在第二节中给出的主要结果.

4.1 基本知识

4.1.1 线性码和 t-设计

定义 4.1 带有参数 (n,k,λ) 的 **t-设计**是由点集 $\mathcal{P}$ 和块集 $\mathcal{B}$ 组成的组合结构 $\mathbb{D}=(\mathcal{P},\mathcal{B})$, 其中 $\mathcal{P}$ 的大小为 n, $\mathcal{B}$ 中的每个块是 $\mathcal{P}$ 的一个 k 元子集, 且满足点集 $\mathcal{P}$ 中任何 t 个点都恰好包含在块集 $\mathcal{B}$ 的 λ 块中.

我们只考虑简单设计, 即不包含重复块的设计, 并且参数 $n>k>\lambda$.

定义 4.2 假设 q 为素数幂, $\mathbb{F}_q$ 为含有 q 个元素的有限域. 一个在有限域 $\mathbb{F}_q$ 上参数为 $[n,k,d]$ 的 **线性码** $\mathcal{C}$ 是一个向量空间 $\mathbb{F}_q^n$ 的 k 维向量子空间, 且最小重量是 d. 对任意的 $0\le i\le n$, 我们记 A_i 为码 $\mathcal{C}$ 中重量为 i 的码字的个数. 序列 $(A_0,A_1,\cdots,A_n)$ 和 $\sum_{i=0}^{n}A_it^i$ 分别被称为 $\mathcal{C}$ 的**重量分布 (weight distribution)** 和**重量计数子 (weight enumerator)**.

t-设计理论和线性码理论关系十分密切. 假设 $\mathbb{D}=(\mathcal{P},\mathcal{B})$ 是一个 t-(n,k,λ) 设计, 并且设 b 是 $\mathcal{B}$ 中的块数. 设计 $\mathbb{D}$ 的关联矩阵 $M_{\mathbb{D}}=(m_{ij})$ 是一个 $b\times n$ 阶的矩阵, 其中如果点 p_j 在块 $B_i\in\mathcal{B}$ 中, 那么 $m_{ij}=1$; 如果点 p_j 不在块 $B_i\in\mathcal{B}$ 中, 那么 $m_{ij}=0$. 关联矩阵 $M_{\mathbb{D}}$ 的行可以作为 $\mathbb{F}_q^n$ 中的向量. 然后, 这 b 个向量所张成的子空间 $\mathcal{C}_q(\mathbb{D})$ 被称为设计 $\mathbb{D}$ 在 $\mathbb{F}_q$ 上的线性码. 设 $\mathcal{C}$ 是 $\mathbb{F}_q$ 上参数为 $[n,k,d]$ 的一个线性码, 码中的每个码字由有序元素 $\{p_0,p_1,\cdots,p_{n-1}\}$ 作为索引. 对于任意 $A_i\neq 0$, 我们将 $\mathcal{B}_i$ 表示为所有重量为 i 的码字的支撑 $\mathrm{Suppt}(c)=\{p_j:c_{p_j}\neq 0, 0\le j\le n-1\}$ 的集合, 其中 $c=(c_{p_0},c_{p_1},\cdots,c_{p_{n-1}})\in\mathcal{C}$ 以及 $0\le i\le n$. 令 $\mathcal{P}=\{p_0,p_1,\cdots,p_{n-1}\}$. 如果组合

结构 $(\mathcal{P}, \mathcal{B}_i)$ 是一个 t-(n, i, λ) 设计, 其中 λ 和 t 均为正整数, 那么我们称之为码 $\mathcal{C}$ 的支撑设计, 并用 $\mathbb{D}_i(\mathcal{C})$ 表示.

Ding, Tang 和 Tonchev 最近研究了一类仿射不变三元码中 2-设计的线性码, 详见文献[13]. 在他们的文献[13] 中所使用的三元码是由二次函数 $\mathrm{Tr}(ax^2 + bx + c)$ 所定义的. 本章考虑由 Hermintian 函数定义的仿射不变三元码, 该码用 $\mathcal{C}(2m, 3)$ 来表示. 用 d 表示码 $\mathcal{C}(2m, 3)$ 的最小重量, 并用 $\mathbb{D}_d(\mathcal{C}(2m, 3))$ 表示 $\mathcal{C}(2m, 3)$ 中拥有最小重量的码字的支撑所对应的设计. 我们的目的是研究线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 的性质. 在后续我们将了解到, 线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 是仿射不变的, 也就是说, 这种码的码字的支撑是存在 2-设计的. 另外线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 包含码 $\mathcal{C}(2m, 3)$, 并且拥有许多其他的仿射不变子码. 这意味着 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 的结构比之前的线性码 $\mathcal{C}(2m, 3)$ 更丰富. 最后, 我们发现线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 是 4 阶三元广义 Reed-Muller 码的子码.

4.1.2 循环码

对于 $\mathbb{F}_q$ 上的一个参数为 $[n, k, d]$ 的线性码 $\mathcal{C}$, 如果其中的任意码字 $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ 的平移 $(c_{n-1}, c_0, \cdots, c_{n-2})$ 也在 $\mathcal{C}$ 中, 那么该线性码被称为循环码. 我们定义一个剩余类环 $\mathcal{R}_n[x] = \mathbb{F}_q[x]/(x^n - 1)$ 和对应于循环码 $\mathcal{C}$ 的 $\mathcal{R}_n[x]$ 中的子集

$$\mathcal{C}(x) = \{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathcal{R}_n[x] : (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}\}.$$

易知, 循环码 $\mathcal{C}$ 与子集 $\mathcal{C}(x)$ 之间存在一一对应关系. 根据循环码的性质, 对任意的 $c(x) \in \mathcal{C}(x)$, 不难看出 $xc(x) \in \mathcal{C}(x)$. 因此 $\mathcal{C}(x)$ 是剩余类环 $\mathcal{R}_n[x]$ 中的一个理想. 由于 $\mathcal{R}_n[x]$ 是主理想整环, $\mathcal{C}(x)$ 是一个主理想, 并且存在一个在该理想中拥有最小次数的首一多项式 $g(x) \in \mathcal{R}_n[x]$ 使得 $\mathcal{C}(x) = \langle g(x) \rangle$. 我们称 $g(x)$ 为 $\mathcal{C}$ 的生成多项式, $h(x) = (x^n - 1)/g(x)$ 为 $\mathcal{C}$ 的奇偶校验多项式. 由文献[60] 中的定理 4.2.1 可知, 循环码 $\mathcal{C}$ 的维数是 $n - \deg(g(x))$.

设 n 是一个整数, 使得 $\gcd(n, q) = 1$. 对于给定的 $0 \le s < n$, 定义 s 模 n 的 q-分圆陪集 C_s 如下,

$$C_s = \{s, sq, \cdots, sq^{r-1}\} \pmod{n},$$

其中 r 是使得 $sq^r \equiv s \pmod{n}$ 成立的最小正整数. 集合 C_s 中最小的正整数被称为 C_s 的陪集首位. 注意, 这些不同的 q-分圆陪集 $C_s, 0 \le s < n$, 是集合 $\{0, 1, \cdots, n-1\}$ 的一个划分. 设 m 是 q 模 n 的阶, γ 是 $\mathbb{F}_{q^m}$ 的本原元, 即 $\mathbb{F}_{q^m}^* = \langle \gamma \rangle$. 令 $\beta = \gamma^{\frac{q^m-1}{n}}$, 易知 β 是 $\mathbb{F}_{q^m}$ 中的一个 n 次单位根. 对每一个 $s, 0 \le s < n$, β^s 在 $\mathbb{F}_q$ 上的极小多项式是 $M_{\beta^s}(x) = \Pi_{i \in C_s}(x - \beta^i)$. 于是循环码 $\mathcal{C}$ 的生成多项式可以被写成 $g(x) = \Pi_{s \in S} M_{\beta^s}(x)$, 其中 S 是一些分圆陪集的陪集首位的集合. 我们把这些分圆陪集的并称为 $\mathcal{C}$ 的定义集. 集合 $Z = \{\beta^i : i \in T\}$ 中的单位根称为循环码 $\mathcal{C}$ 的零元, 而集合 $\{\beta^i : i \notin T\}$ 中的元素称为非零元. 关于分圆陪集和极小多项式的更多细节, 请参阅文献[60].

线性码 $\mathcal{C}$ 的对偶码定义如下

$$\mathcal{C}^{\perp} := \{c' \in \mathbb{F}_q^n \ : \ c \cdot c' = 0, \text{ 对任意的} c \in \mathcal{C}\},$$

其中符号 $\cdot$ 表示内积. 如果 $\mathcal{C}$ 是具有奇偶校验多项式 $h(x)$ 的循环码, 那么 $\mathcal{C}^{\perp}$ 有生成多项式 $x^k h(x^{-1})/h(0)$, 其中 $k = \deg(h(x))$.

下面来自文献[60] 的定理表明, $\mathcal{C}^{\perp}$ 的零元是可以由 $\mathcal{C}$ 的非零元得到.

定理 4.1 [文献[60], 定理 4.4.9] 设 $\mathcal{C}$ 是域 $\mathbb{F}_q$ 上具有参数 $[n, k, d]$ 的循环码. 如果 $\gamma_1, \cdots, \gamma_k$ 是 $\mathcal{C}$ 的非零元, 那么 $\gamma_1^{-1}, \cdots, \gamma_k^{-1}$ 是 $\mathcal{C}^{\perp}$ 的零元.

命题 4.1 [文献[60], 章节 4.4] 设 $\mathcal{C}_i$ 是 $\mathbb{F}_q$ 上长度为 n 的循环码, 且有定义集 T_i, $1 \le i \le 2$. 于是线性码 $\mathcal{C}_1 + \mathcal{C}_2 = \{c_1 + c_2 \ : \ c_i \in \mathcal{C}_i, 1 \le i \le 2\}$ 的定义集为 $T_1 \cap T_2$.

线性码 $\mathcal{C}$ 的扩展码定义如下

$$\overline{\mathcal{C}} = \{(c_0, c_1, \cdots, c_n) \in \mathbb{F}_q^{n+1} \ : \ (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C} \text{ 使得} \sum_{i=0}^{n} c_i = 0\}.$$

如果 H 是码 $\mathcal{C}$ 的奇偶校验矩阵, 那么 $\overline{\mathcal{C}}$ 的奇偶校验矩阵是

$$\overline{H} = \begin{bmatrix} \mathbf{1} & 1 \\ H & \mathbf{0} \end{bmatrix},$$

其中 $\mathbf{1} = (1, 1, \cdots, 1)$ 且 $\mathbf{0} = (0, 0, \cdots, 0)^{\top}$.

定理 4.2 [文献[60], 定理 4.4.19] 设 n 是一个正整数, q 是一个素数幂. 设 $g(x)$ 是 $x^n - 1$ 在 $\mathbb{F}_q$ 上次数为 s 的不可约因式. 设 $\gamma \in \mathbb{F}_{q^s}$ 是 $g(x)$ 的一个根. 令 $\mathrm{Tr}_s : \mathbb{F}_{q^s} \to \mathbb{F}_q$ 为 $\mathbb{F}_{q^s}$ 到 $\mathbb{F}_q$ 的一个迹映射. 那么

$$\mathcal{C}_{\gamma} = \{\sum_{i=0}^{n-1} \mathrm{Tr}_s(a\gamma^i)x^i \ : \ a \in \mathbb{F}_{q^s}\}$$

是一个参数为 $[n, s]$ 的不可约循环码, 其非零元为 $\{\gamma^{-q^i} \ : \ 0 \le i < s\}$.

4.1.3 广义 Reed-Muller 码

设 q 是素数幂, l 和 m 是满足 $1 \le l < (q-1)m$ 的正整数. 有限域 $\mathbb{F}_q$ 上的 l 阶删余广义 Reed-Muller 码 $\mathcal{R}_q(l, m)^*$ 是一个长度为 $n = q^m - 1$ 的循环码, 其生成多项式为

$$g(x) = \prod_{\substack{1 \le i \le n-1 \\ w_q(i) < (q-1)m - l}} (x - \gamma^i),$$

其中 γ 是 $\mathbb{F}_{q^m}$ 的本原元, $i = \sum_{j=0}^{m-1} i_j q^j$, $0 \le i_j \le q-1$ 且 $w_q(i) = \sum_{i=0}^{m-1} i_j$.

Assmus 和 Key 在文献[33] 中提供了删余广义 Reed-Muller 码 $\mathcal{R}_q(l,m)^*$ 的参数, 我们将其复述在如下定理中.

定理 4.3 [文献[33], 章节 5] 删余广义 Reed-Muller 码 $\mathcal{R}_q(l,m)^*$ 的长度为 $n=q^m-1$, 维数为

$$k=\sum_{i=0}^{l}\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{i-jq+m-1}{i-jq}$$

以及最小重量为 $d=(q-l_0)q^{m-l_1-1}-1$, 其中 $l=l_1(q-1)+l_0, 0\le l_0<q-1$.

在文献[33] 和文献[34] 中, 作者得到了删余广义 Reed-Muller 码 $\mathcal{R}_q(l,m)^*$ 的对偶码 $(\mathcal{R}_q(l,m)^*)^\perp$ 以及对偶码的参数.

定理 4.4 [文献[33], 引理 5.21] 线性码 $(\mathcal{R}_q(l,m)^*)^\perp$ 是一个循环码, 其生成矩阵是

$$g^\perp(x)=\prod_{\substack{1\le i\le n-1\\ \omega_q(i)<l}}(x-\gamma^i).$$

定理 4.5 [文献[34], 章节 5.4] 线性码 $(\mathcal{R}_q(l,m)^*)^\perp$ 的长度为 $n=q^m-1$, 维数为

$$k^\perp=n-\sum_{i=0}^{l}\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{i-jq+m-1}{i-jq},$$

以及最小重量为

$$d^\perp\ge(q-l_0')q^{m-l_1'-1},$$

其中 $m(q-1)-1-l=l_1'(q-1)+l_0', 0\le l_0'<q-1$.

广义 Reed-Muller 码 $\mathcal{R}_q(l,m)$ 是删余广义 Reed-Muller 码 $\mathcal{R}_q(l,m)^*$ 的扩展码.

定理 4.6 [文献[33], 章节 5] 线性码 $\mathcal{R}_q(l,m)$ 的长度为 $n=q^m$, 维数为

$$k=\sum_{i=0}^{l}\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{i-jq+m-1}{i-jq},$$

最小重量为 $d=(q-l_0)q^{m-l_1-1}$, 其中 $l=l_1(q-1)+l_0, 0\le l_0<q-1$.

4.1.4 线性码的自同构群

设 $\mathcal{C}$ 是 $\mathbb{F}_q$ 上的一个参数为 $[n,k,d]$ 的线性码. 所有能将码 $\mathcal{C}$ 映射到自身的下标置换组成的集合关于置换的乘法成为对称群 Sym(n) 的一个子群. 我们称这个子群为码 $\mathcal{C}$ 的置换自同构群, 并用 PAut$(\mathcal{C})$ 表示. 有限域 $\mathbb{F}_q$ 上的一个单项矩阵是一个正方形矩阵, 使得每一行和每一列恰好有

一个 $\mathbb{F}_q$ 中的非零元素. 将 $\mathcal{C}$ 映射到自己的所有单项矩阵的集合构成一个群 MAut($\mathcal{C}$), 它被称为 $\mathcal{C}$ 的单项自同构群. 根据定义, 每个 MAut($\mathcal{C}$) 中的元素均可被表示为 DP 或 PD_1, 其中 D 和 D_1 均为对角矩阵, P 是一个置换矩阵. 所有形为 $DP\gamma$ 且固定 $\mathcal{C}$ 的矩阵形成一个群, 称为 $\mathcal{C}$ 的自同构群, 用 Aut($\mathcal{C}$) 表示, 其中 γ 是有限域 $\mathbb{F}_q$ 的一个自同构. 根据定义, 可知 PAut($\mathcal{C}$) $\subseteq$ MAut($\mathcal{C}$) $\subseteq$ Aut($\mathcal{C}$). 自同构群 Aut($\mathcal{C}$) 被称为是 t-传递的, 如果对码 $\mathcal{C}$ 中码字的任意两个大小为 t 的有序下标子集 A 和 B, 都存在一个矩阵 $DP\gamma \in$ Aut($\mathcal{C}$) 使得 P 将 A 映射到 B.

下面的定理是线性码 $\mathcal{C}$ 能得到 t-设计的充分条件.

定理 4.7 [文献[60], 定理 8.4.7] 设 $\mathcal{C}$ 是域 $\mathbb{F}_q$ 上一个长度为 n 的码. 如果 Aut($\mathcal{C}$) 是 t-传递的, 那么对任意的整数 $i, i \geq t$, 重量为 i 的码字都对应一个 t-设计.

一般仿射群 $\mathrm{GA}_1(\mathbb{F}_{q^m})$ 是 $\mathbb{F}_{q^m}$ 上的下列置换的集合:

$$\{\sigma_{s_1,s_2} : s_1 \in \mathbb{F}_{q^m}^*, s_2 \in \mathbb{F}_{q^m}\},$$

其中 $\sigma_{s_1,s_2}(x) = s_1x + s_2, \forall x \in \mathbb{F}_{q^m}$. 设 $\mathcal{C}$ 是域 $\mathbb{F}_q$ 上长度为 q^m 的线性码. 我们用 $\mathbb{F}_{q^m}$ 中的元素为码 $\mathcal{C}$ 中的码字建立索引. 如果码 $\mathcal{C}$ 在一般仿射群 $\mathrm{GA}_1(\mathbb{F}_{q^m})$ 的作用下是不变的, 则称线性码 $\mathcal{C}$ 是仿射不变的, 即 $\mathrm{GA}_1(\mathbb{F}_{q^m}) \leq$ PAut($\mathcal{C}$). 众所周知群 $\mathrm{GA}_1(\mathbb{F}_{q^m})$ 在 $\mathbb{F}_{q^m}$ 上是双传递的. 下面的定理是由定理 4.7得到的.

定理 4.8 [文献[12], 定理 6.6] 设 i 是一个整数, $0 \leq i \leq n$. 令 A_i 是重量为 i 的码字的个数. 如果线性码 $\mathcal{C}$ 是仿射不变的, 那么对任意的 i 使得 $A_i \neq 0$, 码 $\mathcal{C}$ 中重量为 i 的码字对应一个 2-设计.

4.1.5 一类仿射不变三元码对应设计的码

假设 $m \geq 2$ 是一个正整数, p 是一个奇素数. 定义 Tr_s 是一个从 $\mathbb{F}_{p^s}$ 到 $\mathbb{F}_p$ 的迹函数. 我们考虑线性码

$$\mathcal{C}(2m,p) = \{c(a,b,h) \ : \ a \in \mathbb{F}_{p^m}, b \in \mathbb{F}_{p^{2m}}, h \in \mathbb{F}_p\}, \tag{4.1}$$

其中

$$c(a,b,h) = (\mathrm{Tr}_{2m}(at^{p^m+1} + bt) + h)_{t \in \mathbb{F}_{p^{2m}}}.$$

如文献[67] 中所述, 码 $\mathcal{C}(2m,p)$ 是仿射不变的, 因此由该码可以得到 2-设计. 对 $\mathcal{C}(2m,p)$ 中的每个码字 $c(a,b,h)$, 汉明重量 $w_H(c(a,b,h)) = p^{2m} - T(a,b,h)$, 其中

$$T(a,b,h) = |\{t \in \mathbb{F}_{p^{2m}} \ : \ \mathrm{Tr}_{2m}(at^{p^m+1} + bt) + h = 0\}|. \tag{4.2}$$

引理 4.1 [文献[67]] 对任意的 $a \in \mathbb{F}_{p^m}, b \in \mathbb{F}_{p^{2m}}$ 和 $h \in \mathbb{F}_p$, 假设 $T(a,b,h)$ 是如式子 (4.2) 中所定义的函数.

(1) 当 $a=b=h=0$ 时, $T(a,b,h)=p^{2m}$.

(2) 当 $a=b=0$ 和 $h\neq 0$ 时, $T(a,b,h)=0$.

(3) 当 $a=0$ 和 $b\neq 0$ 时, $T(a,b,h)=p^{2m-1}$.

(4) 当 $a\neq 0$ 时,

$$T(a,b,h)=\begin{cases} p^{2m-1}-p^{m-1}(p-1) & \text{如果 } h=\mathrm{Tr}_{2m}(as_{at,bt}^{p^m+1}),\\ p^{2m-1}+p^{m-1} & \text{如果 } h\neq \mathrm{Tr}_{2m}(as_{at,bt}^{p^m+1}),\end{cases}$$

其中 $t\in\mathbb{F}_p^*$, $s_{at,bt}^{p^m+1}$ 是 $((at)^{p^m}+at)s=2ats=-(bt)^{p^m}$ 的一个解, 也就是说, $s_{at,bt}^{p^m+1}=-2^{-1}a^{-1}b^{p^m}t^{p^m-1}=-2^{-1}a^{-1}b^{p^m}$.

根据上述引理可知, 一个码字 $c(a,b,h)$ 有最小重量 $d=p^{2m-1}(p-1)-p^{m-1}$ 仅当 $a\in\mathbb{F}_{p^m}^*$, $b\in\mathbb{F}_{p^{2m}}$ 以及 $h\in\mathbb{F}_p\setminus\{\mathrm{Tr}_{2m}(-2^{-1}b)\}$. 由文献[67] 的定理 3 可知, 线性码 $\mathcal{C}(2m,p)$ 有参数 $[p^{2m},3m+1,p^{2m-1}(p-1)-p^{m-1}]$ 和表 4.1中所列的重量分布。我们之前所提到的码中支撑设计的块是由 $\mathcal{C}(2m,p)$ 中具有最小重量 d 的码字的支撑组成的. 假设 $\mathbb{D}_d(\mathcal{C}(2m,p))$ 是码 $\mathcal{C}(2m,p)$ 的支撑设计. 根据文献[67], 可知 $\mathbb{D}_d(\mathcal{C}(2m,p))$ 是一个 2-设计. 令 $M_{\mathbb{D}_d}$ 是设计 $\mathbb{D}_d(\mathcal{C}(2m,p))$ 的关联矩阵, $\mathcal{C}_p(\mathbb{D}_d(\mathcal{C}(2m,p)))$ 是由关联矩阵 $M_{\mathbb{D}_d}$ 的行在域 $\mathbb{F}_p$ 上所生成的线性码. 我们这里考虑 $p=3$ 的情况并计算码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的维数和最小重量.

表 4.1 码 $\mathcal{C}(2m,p)$ 的重量分布

重量	重数
0	1
$p^{2m-1}(p-1)-p^{m-1}$	$p^{2m}(p^m-1)(p-1)$
$p^{2m-1}(p-1)$	$p(p^{2m}-1)$
$(p^{2m-1}+p^{m-1})(p-1)$	$p^{2m}(p^m-1)$
p^{2m}	$p-1$

注 4.1 文献[13] 所处理的由域 $\mathbb{F}_3$ 上的二次函数 $\mathrm{Tr}_{2m}(at^2+bt)+h$ 所定义的三元线性码有参数 $[3^{2m},4m+1,2(3^{2m-1}-3^{m-1})]$. 由 $\mathbb{F}_3$ 上的 Hermitian 函数 $\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h$ 所定义的三元线性码具有参数 $[n,k,d]=[3^{2m},3m+1,2\cdot 3^{2m-1}-3^{m-1}]$. 由此可知, 这两种函数所定义的码具有不同的维数, 所以它们是不等价的.

为了简化符号, 我们在后面的篇幅中等价表示函数 $f(t)$ 和向量 $(f(t))_{t\in\mathbb{F}_{3^{2m}}}$. 下面我们列出本章的主要结论, 这些结论的证明我们将在后面的第 4.1.6节给出.

定理 4.9 对任意的整数 $m \geq 2$, 域 $\mathbb{F}_3$ 上的线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 是由下列的向量生成的

$$\left\{\begin{array}{c}\mathrm{Tr}_{2m}(bt), \mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't), \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt),\\ \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1}), \mathrm{Tr}_{2m}(at^{3^m+1}), 1 \ : \ a,a'\in\mathbb{F}_{3^m}, b,b'\in\mathbb{F}_{3^{2m}}\end{array}\right\}.$$

定理 4.10 对任意的整数 $m \geq 2$, 线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 由如下向量给定

$$\left\{\begin{array}{c}\sum_{i=0}^{m-1}\mathrm{Tr}_{2m}(b_it^{(3^m+1)3^i+1}) + \sum_{i=0}^{2m-1}\mathrm{Tr}_{2m}(b_i't^{3^i+1})\\ +\sum_{i=0}^{m-1}\mathrm{Tr}_m(a_it^{(3^m+1)(3^i+1)}) + \mathrm{Tr}_{2m}(bt) + h : b, b_i, b_i'\in\mathbb{F}_{3^{2m}}, a_i\in\mathbb{F}_{3^m}, h\in\mathbb{F}_3\end{array}\right\},$$

并且该码中存在 2-设计.

定理 4.11 对任意的整数 $m \geq 1$, 线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 长度为 $n = p^{2m}$, 维数为 $k = \frac{9m^2+7m}{2} + 1$ 以及最小重量的下界是 3^{2m-2}.

例 4.1 当 $m = 1, 2$ 时, 线性码 $\mathcal{C}(2m,3)$ 和 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的参数如下:

m	$\mathcal{C}(2m,3)$	$\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$
1	$[9,4,5]$	$[9,9,1]$
2	$[81,7,51]$	$[81,26,21]$.

线性码 $\mathcal{C}(4,3)$ 的重量分布为

$$1 + 1296z^{51} + 240z^{54} + 648z^{60} + 2z^{81}.$$

线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(4,3)))$ 的重量分布为

$$\begin{array}{lll}1 & +648z^{21} & +240z^{27} & +38880z^{28}\\ & +25920z^{29} & +104976z^{30} & +373248z^{31}\\ & +678780z^{32} & +2491560z^{33} & +9305280z^{34}\\ & +12791520z^{35} & +52067880z^{36} & +167585760z^{37}\\ & +193771440z^{38} & +633582000z^{39} & +1789957440z^{40}\\ & +1784204820z^{41} & +5114657520z^{42} & +12311494560z^{43}\\ & +10655818920z^{44} & +26240268600z^{45} & +54869931360z^{46}\\ & +40818498480z^{47} & +86821798860z^{48} & +155822087880z^{49}\\ & +99765111888z^{50} & +181835828208z^{51} & +279785262240z^{52}\\ & +153082363320z^{53} & +238171803600z^{54} & +311801503680z^{55}\\ & +144740601000z^{56} & +190453223160z^{57} & +210148421760z^{58}\\ & +81951931440z^{59} & +90132625584z^{60} & +82728913248z^{61}\\ & +26672379840z^{62} & +24134094720z^{63} & +18117430380z^{64}\\ & +4739847840z^{65} & +3450820320z^{66} & +2053913760z^{67}\\ & +424174320z^{68} & +238097880z^{69} & +109483488z^{70}\\ & +16715808z^{71} & +7076700z^{72} & +2442960z^{73}\\ & +116640z^{74} & +58320z^{75} & +38880z^{77}\\ & +6480z^{78} & +2106z^{80} & +2186z^{81}.\end{array}$$

4.1.6 主要结论的证明

在这一节中, 我们证明了定理 4.9, 4.10和 4.11. 我们首先给出了设计 $\mathbb{D}_d(\mathcal{C}(2m,3))$ 的关联矩阵的行的具体表达形式, 并将结论列在了定理 4.9中. 接着, 简化了定理 4.9中的向量, 并给出了定理 4.10的证明. 由定理 4.10 的结论, 可知线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 是 4 阶广义 Reed-Muller 码的子码. 在此基础上, 可以计算码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的最小重量的下界. 最后, 我们通过计算式子 (4.14) 定义的码 $\mathcal{C}$ 的定义集的大小, 得到了码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的维数, 并将结论列在了定理 4.11中.

我们根据第 4.1.5节关于码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的定义可以得到如下引理.

引理 4.2 假设 $m \geq 2$ 是一个正整数. 线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 是由下面集合中的向量在域 $\mathbb{F}_3$ 上生成的:

$$\{(\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h)^2 \,:\, a\in\mathbb{F}_{3^m}^*, b\in\mathbb{F}_{3^{2m}}, h\in\mathbb{F}_3\setminus\{\mathrm{Tr}_{2m}(b)\}\}.$$

利用引理 4.2, 对任意的 $a\in\mathbb{F}_{3^m}^*, b\in\mathbb{F}_{3^{2m}}$ 和 $h\in\mathbb{F}_3\setminus\{\mathrm{Tr}_{2m}(b)\}$, 可得

$$\begin{aligned}(\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h)^2 &= \mathrm{Tr}_{2m}(at^{3^m+1}+bt)^2+2h\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h^2\\ &= \mathrm{Tr}_{2m}(at^{3^m+1})^2+2\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt)+\mathrm{Tr}_{2m}(bt)^2\\ &\quad +2h\mathrm{Tr}_{2m}(at^{3^m+1})+2h\mathrm{Tr}_{2m}(bt)+h^2 \ \in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))),\end{aligned} \tag{4.3}$$

$$\begin{aligned}(\mathrm{Tr}_{2m}(at^{3^m+1}-bt)+h)^2 &= \mathrm{Tr}_{2m}(at^{3^m+1}-bt)^2+2h\mathrm{Tr}_{2m}(at^{3^m+1}-bt)+h^2\\ &= \mathrm{Tr}_{2m}(at^{3^m+1})^2-2\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt)+\mathrm{Tr}_{2m}(bt)^2\\ &\quad +2h\mathrm{Tr}_{2m}(at^{3^m+1})-2h\mathrm{Tr}_{2m}(bt)+h^2 \ \in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).\end{aligned} \tag{4.4}$$

将式子 (4.3) 减去式子 (4.4), 可得

$$\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt)+h\mathrm{Tr}_{2m}(bt) \ \in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \tag{4.5}$$

将式子 (4.3) 加上式子 (4.4), 可得

$$2\mathrm{Tr}_{2m}(at^{3^m+1})^2+2\mathrm{Tr}_{2m}(bt)^2+h\mathrm{Tr}_{2m}(at^{3^m+1})+2h^2 \ \in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \tag{4.6}$$

我们接下来证明式子 (4.3) 中的每一项均在码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 中.

引理 4.3 假设 $a\in\mathbb{F}_{3^m}$ 和 $b\in\mathbb{F}_{3^{2m}}$. 于是 $\{\mathrm{Tr}_{2m}(bt), \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt)\}\subseteq\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.

证明 对任意的 $a\in\mathbb{F}_{3^m}^*, b\in\mathbb{F}_{3^{2m}}$ 和 $h_1\neq h_2\in\mathbb{F}_3\setminus\{\mathrm{Tr}_{2m}(b)\}$, 根据 (4.5), 可得

$$\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt)+h_1\mathrm{Tr}_{2m}(bt) \ \in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))), \tag{4.7}$$

$$\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt)+h_2\mathrm{Tr}_{2m}(bt)\ \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \tag{4.8}$$

于是我们通过将式子 (4.7) 和式子 (4.8) 相减就可得到该引理中的结论.

引理 4.4 对任意的 $t\in\mathbb{F}_{3^{2m}}$, 下列式子成立:

(1) $\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_{2m}(at^{3^m+1})^2=0.$

(2) $\sum_{b\in\mathbb{F}_{3^{2m}}^*}\mathrm{Tr}_{2m}(bt)^2=0.$

(3) $\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_{2m}(at^{3^m+1})=0.$

证明 当 $t=0$ 时, 结论显然成立. 我们现在考虑 $t\neq 0$. 对任意的 $t\in\mathbb{F}_{3^{2m}}^*$, 方程 $(t^{3^m+1})^{3^m}=t^{3^m+1}$ 成立意味着 $t^{3^m+1}\in\mathbb{F}_{3^m}^*$. 注意到, 对任意的 $a\in\mathbb{F}_{3^m}$, 都有 $\mathrm{Tr}_{2m}(a)=2\mathrm{Tr}_m(a)$.

首先, 我们有

$$\begin{aligned}\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_{2m}(at^{3^m+1})^2&=\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_m(a)^2\\&=|\{a\in\mathbb{F}_{3^m}|\mathrm{Tr}_m(a)\neq 0\}|\pmod 3\\&=3^m-|\{a\in\mathbb{F}_{3^m}|\mathrm{Tr}_m(a)=0\}|\pmod 3\\&=3^m-3^{m-1}\pmod 3\\&=0.\end{aligned}$$

接着, 计算

$$\begin{aligned}\sum_{b\in\mathbb{F}_{3^{2m}}^*}\mathrm{Tr}_{2m}(bt)^2&=\sum_{b\in\mathbb{F}_{3^{2m}}}\mathrm{Tr}_{2m}(b)^2\\&=|\{b\in\mathbb{F}_{3^{2m}}|\mathrm{Tr}_{2m}(b)\neq 0\}|\pmod 3\\&=3^{2m}-3^{2m-1}\pmod 3\\&=0.\end{aligned}$$

最后, 可以得到

$$\begin{aligned}\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_{2m}(at^{3^m+1})&=2\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_m(a)\\&=2\mathrm{Tr}_m(\sum_{a\in\mathbb{F}_{3^m}^*}a)\\&=0.\end{aligned}$$

引理 4.5 常值码字 $1\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.

证明 对任意的 $a \in \mathbb{F}_{3^m}^*$ 和 $b \in \mathbb{F}_{3^{2m}}$, 选取 $h_b = \mathrm{Tr}_{2m}(b) + 1$. 根据引理 4.4和式子 (4.6), 可得

$$\begin{aligned}
&\sum_{b\in\mathbb{F}_{3^{2m}}^*}\sum_{a\in\mathbb{F}_{3^m}^*}(\mathrm{Tr}_{2m}(at^{3^m+1})^2+\mathrm{Tr}_{2m}(bt)^2+2h_b\mathrm{Tr}_{2m}(at^{3^m+1})+h_b^2)\\
&\quad=2\sum_{b\in\mathbb{F}_{3^{2m}}^*}(\mathrm{Tr}_{2m}(b)+1)^2\\
&\quad=\sum_{b\in\mathbb{F}_{3^{2m}}^*}(\mathrm{Tr}_{2m}(b)+2)\\
&\quad=1\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).
\end{aligned}$$

引理 4.6 对任意的 $b, b' \in \mathbb{F}_{3^{2m}}$, $\mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.

证明 假设 $b_1 = \frac{b+b'}{2}, b_2 = \frac{b'-b}{2} \in \mathbb{F}_{3^{2m}}$. 将 b_1 和 b_2 代入到式子 (4.6) 中, 我们得到

$$2\mathrm{Tr}_{2m}(at^{3^m+1})^2+2\mathrm{Tr}_{2m}(b_1t)^2+h_1\mathrm{Tr}_{2m}(at^{3^m+1})+2h_1^2\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))), \tag{4.9}$$

$$2\mathrm{Tr}_{2m}(at^{3^m+1})^2+2\mathrm{Tr}_{2m}(b_2t)^2+h_2\mathrm{Tr}_{2m}(at^{3^m+1})+2h_2^2\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))), \tag{4.10}$$

其中 $h_1 \in \mathbb{F}_3\backslash\{\mathrm{Tr}(b_1)\}$ 以及 $h_2 \in \mathbb{F}_3\backslash\{\mathrm{Tr}(b_2)\}$. 设定 $h_1 = h_2 = h$, 其中 h 是 $\mathbb{F}_3\backslash\{\mathrm{Tr}_{2m}(b_1), \mathrm{Tr}_{2m}(b_2)\}$ 中的一个元素. 通过将式子 (4.10) 和式子 (4.9) 相减, 我们得到

$$2\mathrm{Tr}_{2m}((b_1-b_2)t)\mathrm{Tr}_{2m}((b_1+b_2)t)\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).$$

因此, $\mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.

引理 4.7 对任意的 $a, a' \in \mathbb{F}_{3^m}$,

$$\{\mathrm{Tr}_{2m}(at^{3^m+1}), \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1})\}\subseteq\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).$$

证明 由引理 4.5, 引理 4.6和式子 (4.6), 我们有

$$\mathrm{Tr}_{2m}(at^{3^m+1})^2+2h\mathrm{Tr}_{2m}(at^{3^m+1})\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \tag{4.11}$$

可以选取 $h_1 \neq h_2 \in \mathbb{F}_3 \setminus \{\mathrm{Tr}_{2m}(b)\}$, 并将 h_1, h_2 代入到式子 (4.11) 中, 于是可以得到

$$\mathrm{Tr}_{2m}(at^{3^m+1})^2+2h_1\mathrm{Tr}_{2m}(at^{3^m+1})\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))), \tag{4.12}$$

$$\mathrm{Tr}_{2m}(at^{3^m+1})^2+2h_2\mathrm{Tr}_{2m}(at^{3^m+1})\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \tag{4.13}$$

将式子 (4.13) 和式子 (4.12) 相减, 可得

$$2(h_1-h_2)\mathrm{Tr}_{2m}(at^{3^m+1})\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).$$

因为 $h_1 \neq h_2$, 所以 $\mathrm{Tr}_{2m}(at^{3^m+1}), \mathrm{Tr}_{2m}(at^{3^m+1})^2 \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. 假设 $a_1 = \frac{a+a'}{2}$, $a_2 = \frac{a-a'}{2} \in \mathbb{F}_{3^m}$. 注意到 $\mathrm{Tr}_{2m}(a_1t^{3^m+1})^2, \mathrm{Tr}_{2m}(a_2t^{3^m+1})^2 \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. 所以有

$$\begin{aligned}\mathrm{Tr}_{2m}(a_1t^{3^m+1})^2 - \mathrm{Tr}_{2m}(a_2t^{3^m+1})^2 &= \mathrm{Tr}_{2m}((a_1+a_2)t^{3^m+1})\mathrm{Tr}_{2m}((a_1-a_2)t^{3^m+1}) \\ &= \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).\end{aligned}$$

证明 (定理 4.9) 根据以上的结论和式子 (4.3), 我们容易得到该结论.

引理 4.8 [文献[73], 推论 8.4] 假设 p 是一个素数, n 是一个正整数. 假设 $t_1, \cdots, t_n \in \mathbb{F}_{p^n}$. 那么 $\{t_1, \cdots, t_n\}$ 是 $\mathbb{F}_{p^n}$ 中关于 $\mathbb{F}_p$ 的一组基当且仅当

$$\begin{vmatrix} t_1 & t_2 & \cdots & t_n \\ t_1^p & t_2^p & \cdots & t_n^p \\ \vdots & \vdots & \cdots & \vdots \\ t_1^{p^{n-1}} & t_2^{p^{n-1}} & \cdots & t_n^{p^{n-1}} \end{vmatrix} \neq 0.$$

引理 4.9 对任意的正整数 $m \geq 2$，我们有

$$\langle \mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't) \ : \ b, b' \in \mathbb{F}_{3^{2m}} \rangle = \langle \sum_{i=0}^{2m-1} \mathrm{Tr}_{2m}(b_it^{3^i+1}) \ : \ b_i \in \mathbb{F}_{3^{2m}} \rangle.$$

证明 对 $\mathbb{F}_{3^{2m}}$ 中任意的两个元素 b, b',

$$\begin{aligned}\mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't) &= \sum_{i=0}^{2m-1}\sum_{j=0}^{2m-1} b^{3^i}b'^{3^j}t^{3^i+3^j} = \sum_{i=0}^{2m-1} b^{3^i}(\sum_{j=0}^{2m-1} b'^{3^{j-i}}t^{1+3^{j-i}})^{3^i} \\ &= \sum_{i=0}^{2m-1} b^{3^i}(\sum_{j=0}^{2m-1} b'^{3^j}t^{1+3^j})^{3^i} = \sum_{j=0}^{2m-1} \mathrm{Tr}_{2m}(bb'^{3^j}t^{1+3^j}).\end{aligned}$$

假设 γ 是 $\mathbb{F}_{3^{2m}}$ 中的一个本原元. 易知 $\{\gamma, \gamma^3, \cdots, \gamma^{3^{2m-1}}\}$ 是 $\mathbb{F}_{3^{2m}}$ 关于 $\mathbb{F}_3$ 的一组正规基. 通过引理 4.8, 下面集合中的元素在域 $\mathbb{F}_3$ 上是线性无关的,

$$\{(b', b'^3, \cdots, b'^{3^{2m-1}}) \ : \ b' = \gamma^{3^i}, 0 \leq i \leq 2m-1\}.$$

这意味着它们组成 $\mathbb{F}_{3^{2m}}^{2m}$ 关于 $\mathbb{F}_{3^{2m}}$ 的一组基. 因此 $\langle \sum_{j=0}^{2m-1} \mathrm{Tr}_{2m}(bb'^{3^j}t^{3^j+1}) \ : \ b, b' \in \mathbb{F}_{3^{2m}} \rangle = \langle \sum_{i=0}^{2m-1} \mathrm{Tr}_{2m}(b_it^{3^i+1}) \ : \ b_i \in \mathbb{F}_{3^{2m}} \rangle$.

引理 4.10 对任意的正整数 $m \geq 2$,

$$\langle \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) \ : \ a \in \mathbb{F}_{3^m}, b \in \mathbb{F}_{3^{2m}} \rangle = \langle \sum_{i=0}^{m-1} \mathrm{Tr}_{2m}(b_it^{(3^m+1)3^i+1}) \ : \ b_i \in \mathbb{F}_{3^{2m}} \rangle.$$

证明 对任意的 $a \in \mathbb{F}_{3^m}$ 和 $b \in \mathbb{F}_{3^{2m}}$,

$$\begin{aligned}\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) &= 2\sum_{i=0}^{m-1}(at^{3^m+1})^{3^i}\sum_{j=0}^{2m-1}(bt)^{3^j} = 2\sum_{j=0}^{2m-1}(bt)^{3^j}\sum_{i=0}^{m-1}(at^{3^m+1})^{3^{i+j}} \\ &= 2\sum_{j=0}^{2m-1}(bt\sum_{i=0}^{m-1}(at^{3^m+1})^{3^i})^{3^j} = 2\sum_{i=0}^{m-1}\mathrm{Tr}_{2m}(ba^{3^i}t^{(3^m+1)3^i+1}).\end{aligned}$$

通过引理 4.8, 可知下面集合中的元素在 $\mathbb{F}_3$ 上是线性无关的,

$$\{(a, a^3, \cdots, a^{3^{m-1}}) : a = \gamma^{(3^m+1)3^i}, 0 \le i \le m-1\}.$$

这意味着它们组成了 $\mathbb{F}_{3^{2m}}^m$ 关于 $\mathbb{F}_{3^{2m}}$ 的一组基. 因此 $\langle 2\sum_{i=0}^{m-1}\mathrm{Tr}_{2m}(ba^{3^i}t^{(3^m+1)3^i+1}) : a \in \mathbb{F}_{3^m}, b \in \mathbb{F}_{3^{2m}}\rangle = \langle \sum_{i=0}^{m-1}\mathrm{Tr}_{2m}(b_i t^{(3^m+1)3^i+1}) : b_i \in \mathbb{F}_{3^{2m}}\rangle$.

引理 4.11 对任意的正整数 $m \ge 2$,

$$\langle \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1}) : a, a' \in \mathbb{F}_{3^m}\rangle = \langle \sum_{i=0}^{m-1}\mathrm{Tr}_m(a_i t^{(3^m+1)(3^i+1)}) : a_i \in \mathbb{F}_{3^m}\rangle.$$

证明 对任意 $\mathbb{F}_{3^m}$ 中的元素 a 和 a',

$$\begin{aligned}\mathrm{Tr}_{2m}(a't^{3^m+1})\mathrm{Tr}_{2m}(at^{3^m+1}) &= \sum_{i=0}^{2m-1}(a't^{3^m+1})^{3^i}\sum_{j=0}^{2m-1}(at^{3^m+1})^{3^j} \\ &= \sum_{i=0}^{2m-1}((a't^{3^m+1})\sum_{j=0}^{2m-1}(at^{3^m+1})^{3^{j-i}})^{3^i} \\ &= \sum_{i=0}^{2m-1}((a't^{3^m+1})\sum_{j=0}^{2m-1}(at^{3^m+1})^{3^j})^{3^i} \\ &= \sum_{i=0}^{2m-1}(\sum_{j=0}^{2m-1}a'a^{3^j}t^{(3^m+1)(3^j+1)})^{3^i} \\ &= \sum_{j=0}^{2m-1}\mathrm{Tr}_{2m}(a'a^{3^j}t^{(3^m+1)(3^j+1)}) \\ &= \sum_{j=0}^{m-1}\mathrm{Tr}_m(a'a^{3^j}t^{(3^m+1)(3^j+1)}).\end{aligned}$$

类似于引理 4.10中的证明, 我们得到了该引理中的结论.

证明 (定理 4.10) 定理中的第一部分可由定理 4.9和引理 4.9–4.11得到.

现在我们证明线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 是仿射不变的, 由此可根据定理 4.8得到该码中存在 2-设计. 对任意的 $\sigma_{s_1,s_2} \in \mathrm{GA}_1(\mathbb{F}_{3^{2m}})$, 其中 $s_1 \in \mathbb{F}_{3^{2m}}^*$ 以及 $s_2 \in \mathbb{F}_{3^{2m}}$, 我们只需要证

明 $\mathrm{Tr}_{2m}(b\sigma_{s_1,s_2}(t)+b'(\sigma_{s_1,s_2}(t))^{3^i+1}+b''(\sigma_{s_1,s_2}(t))^{(3^m+1)3^j+1}+c(\sigma_{s_1,s_2}(t))^{(3^m+1)(3^k+1)})+h\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 对所有的 $0\le i\le 2m-1, 0\le j,k\le m-1, b,b',b''\in\mathbb{F}_{3^{2m}}, c\in\mathbb{F}_{3^m}$ 和 $h\in\mathbb{F}_3$ 均成立. 容易验证 $\mathrm{Tr}_{2m}(b(s_1t+s_2)+b'(s_1t+s_2)^{3^i+1})+h\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. 可得

$$\begin{aligned}
&\mathrm{Tr}_{2m}(b''(s_1t+s_2)^{(3^m+1)3^j+1})\\
&=\mathrm{Tr}_{2m}(b''(s_1^{3^{m+j}}t^{3^{m+j}}+s_2^{3^{m+j}})(s_1^{3^j}t^{3^j}+s_2^{3^j})(s_1t+s_2))\\
&=\mathrm{Tr}_{2m}(b''(s_1t)^{3^{m+j}+3^j+1}+b''(s_1t)^{3^{m+j}+1}s_2^{3^j})\\
&+\mathrm{Tr}_{2m}(b''(s_1t)^{3^j+1}s_2^{3^{m+j}}+b''s_1ts_2^{3^{m+j}+3^j}+b''(s_1t)^{3^m+1}s_2^{3^{-j}})\\
&+\mathrm{Tr}_{2m}(b''s_1ts_2^{3^m+3^{m-j}}+b''s_1ts_2^{3^m+3^{-j}}+b''s_2^{3^{m+j}+3^j+1})\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).
\end{aligned}$$

类似地, 我们有 $\mathrm{Tr}_{2m}(c(s_1t+s_2)^{(3^m+1)(3^k+1)})\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. 于是结论成立.

在继续接下来的计算之前, 我们先介绍一些符号. 假设 γ 是 $\mathbb{F}_{3^{2m}}$ 的本原元. 对任意的 $0\le k\le 2$ 和 $0\le j\le 2m-1$, 定义下面的线性码:

$$\begin{aligned}
\mathcal{C}_{\gamma_{kj}}&=\{\sum_{i=0}^{3^{2m}-2}\mathrm{Tr}_{2m}(a_i\gamma_{kj}^i)x^i\ :\ a_i\in\mathbb{F}_{3^{2m}}\},\\
\mathcal{C}_{\gamma_{3j}}&=\{\sum_{i=0}^{3^{2m}-2}\mathrm{Tr}_{2m}(a_i\gamma_{3j}^i)x^i\ :\ a_i\in\mathbb{F}_{3^m}\},
\end{aligned}$$

其中 $\gamma_{0j}=\gamma, \gamma_{1j}=\gamma^{(3^m+1)3^j+1}, \gamma_{2j}=\gamma^{3^j+1}$ 以及 $\gamma_{3j}=\gamma^{(3^j+1)(3^m+1)}$. 我们定义线性码

$$\mathcal{C}=\left\langle x\ :\ x\in\mathcal{C}_{\gamma_{kj}}, 0\le k\le 3, 0\le j\le 2m-1\right\rangle_{\mathbb{F}_3}. \tag{4.14}$$

对于 $0\le j\le 2m-1$, 我们设定

$$\begin{aligned}
S_{0j}&=\{-3^i\ :\ 0\le i\le 2m-1\},\\
S_{1j}&=\{-3^i(3^j(3^m+1)+1)\ :\ 0\le i\le 2m-1\},\\
S_{2j}&=\{-3^i(3^j+1)\ :\ 0\le i\le 2m-1\},\\
S_{3j}&=\{-3^i(3^j+1)(3^m+1)\ :\ 0\le i\le 2m-1\}.
\end{aligned} \tag{4.15}$$

注 4.2 通过定理 4.10, 可知码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 置换等价于码 $\overline{\mathcal{C}^\perp}^\perp$, 其中 $\mathcal{C}$ 是式子 (4.14) 中定义的线性码. 通过定理 4.2, 可知每个码 $\mathcal{C}_{\gamma_{kj}}(0\le k\le 3, 0\le j\le 2m-1)$ 的定义集为 $T_{kj}=\mathbb{F}_{3^{2m}}^*\setminus S_{jk}$. 于是根据性质 4.1, 线性码 $\mathcal{C}$ 有定义集 $T=\cap_{k=0}^3\cap_{j=0}^{2m-1}T_{kj}$. 假设 $S_k=\cup_{j=0}^{2m-1}S_{kj}$, $0\le k\le 3$. 可以直接验证得到定义集

$$T=\cap_{k=0}^3\cap_{j=0}^{2m-1}(\mathbb{F}_{3^{2m}}^*\setminus S_{kj})=\cap_{k=0}^3(\mathbb{F}_{3^{2m}}^*\setminus(\cup_{j=0}^{2m-1}S_{kj}))=\mathbb{F}_{3^{2m}}^*\setminus(\cup_{k=0}^3S_k).$$

容易验证, 对任意的 $0 \le i \ne j \le 3, S_i \cap S_j = \varnothing$. 现在我们计算 $S_i, 0 \le i \le 3$, 中元素的个数. 注意到 $|S_0| = 2m$.

引理 4.12 假设 $S_{1j}(0 \le j \le 2m-1)$ 是如式子 (4.15) 中所定义的集合. 我们有如下结论:

(1) 对任意的 $0 \le i_1, i_2, j_1, j_2 \le 2m-1$, $-3^{i_1}(3^{j_1}(3^m+1)+1) \equiv -3^{i_2}(3^{j_2}(3^m+1)+1) \pmod{(3^{2m}-1)}$ 当且仅当 $i_1 = i_2$ 以及 $j_1 = j_2$ 或 $j_1 + m \equiv j_2 \pmod{2m}$.

(2) 对任意的 $0 \le i \ne j \le 2m-1, |S_{1i}| = 2m$ 以及

$$\begin{cases} S_{1i} = S_{1j} & \text{如果} i + m \equiv j \pmod{2m}, \\ S_{1i} \cap S_{1j} = \varnothing & \text{如果} i + m \not\equiv j \pmod{2m}. \end{cases}$$

(3) $|S_1| = 2m^2$.

证明 (1) 不失一般性, 假设 $i_2 \ge i_1$. 如果 $-3^{i_1}(3^{j_1}(3^m+1)+1) \equiv -3^{i_2}(3^{j_2}(3^m+1)+1) \pmod{(3^{2m}-1)}$, 就有

$$3^{i_2-i_1+j_2+m} + 3^{i_2-i_1+j_2} + 3^{i_2-i_1} - 3^{j_1+m} - 3^{j_1} - 1 \equiv 0 \pmod{(3^{2m}-1)}. \tag{4.16}$$

假设 a_1, a_2, a_3 是满足如下条件的整数

$$\begin{cases} 0 \le i_2 - i_1 + j_2 + m - 2a_1 m \le 2m-1, \\ 0 \le i_2 - i_1 + j_2 - 2a_2 m \le 2m-1, \\ 0 \le j_1 + m - 2a_3 m \le 2m-1. \end{cases}$$

上述式子意味着 $0 \le a_1 \le 2, 0 \le a_2 \le 1$ 和 $0 \le a_3 \le 1$. 记

$$\begin{cases} s_1 = i_2 - i_1 + j_2 + m - 2a_1 m, \\ s_2 = i_2 - i_1 + j_2 - 2a_2 m, \\ s_3 = i_2 - i_1, \\ t_1 = j_1 + m - 2a_3 m, \\ t_2 = j_1. \end{cases}$$

因为 $2 - 2 \cdot 3^{2m-1} \le 3^{s_1} + 3^{s_2} + 3^{s_3} - 3^{t_1} - 3^{t_2} - 1 \le 3^{2m} - 3$, 所以由式子 (4.16) 得到 $3^{s_1} + 3^{s_2} + 3^{s_3} - 3^{t_1} - 3^{t_2} - 1 = 0$. 注意到, 集合 $\{s_1, s_2, s_3\}$ 中有至少一个零元. 我们有 $s_2 \equiv s_1 + m \pmod{2m}$, 于是 s_1, s_2 和 s_3 不全为零.

如果集合 $\{s_1, s_2, s_3\}$ 中恰有一个元素等于 0, 那么当 k 取 $\{1, 2, 3\}$ 中不同的值时, 我们有三种情况要考虑: $s_k = 0$, $\min(\{s_1, s_2, s_3\} \setminus \{s_k\}) = \min\{t_1, t_2\}$ 并且 $\max(\{s_1, s_2, s_3\} \setminus \{s_k\}) = \max\{t_1, t_2\}$. 因此可得 $i_1 = i_2$ 和

$$\begin{cases} j_1 = 0, j_2 = m \text{ 或 } j_1 = j_2 = m & \text{如果 } k = 1, \\ j_1 = j_2 = 0 \text{ 或 } j_1 = m, j_2 = 0 & \text{如果 } k = 2, \\ j_1 = j_2 \text{ 或 } j_2 \equiv j_1 + m \pmod{2m} & \text{如果 } k = 3. \end{cases}$$

如果集合 $\{s_1, s_2, s_3\}$ 中恰有两个元素等于 0, 就有 $1+3^s = 3^{t_1}+3^{t_2}$, 其中 s 是集合 $\{s_1, s_2, s_3\}$ 中的非零元. 这意味着 $\min\{t_1, t_2\} = \min\{s, 0\} = 0$ 以及 $\max\{t_1, t_2\} = \max\{s, 0\} = s$. 因为 $s_1 = 0$ 和 $s_2 = 0$ 不同时成立, 所以 $s_3 = 0$, 也就是说, $i_1 = i_2$. 并且我们有下面四种情况:

$$\begin{cases} j_1 = 0, j_2 = m & \text{如果 } s_1 = 0, s_2 = t_1, t_2 = 0, \\ j_1 = j_2 = m & \text{如果 } s_1 = 0, s_2 = t_2, t_1 = 0, \\ j_1 = j_2 = 0 & \text{如果 } s_2 = 0, s_1 = t_1, t_2 = 0, \\ j_1 = m, j_2 = 0 & \text{如果 } s_2 = 0, s_1 = t_2, t_1 = 0. \end{cases}$$

结合以上计算所得到的结论, 我们证明了式子 (4.16) 成立当且仅当 $i_1 = i_2$ 以及 $j_1 = j_2$ 或 $j_1 + m \equiv j_2 \pmod{2m}$.

(2) 通过结论 (1), 可知 $-3^{i_1}(3^j(3^m + 1) + 1) \equiv -3^{i_2}(3^j(3^m + 1) + 1) \pmod{(3^{2m} - 1)}$ 当且仅当 $i_1 = i_2$. 因此对任意的 $0 \le i \le 2m - 1$, $|S_{1i}| = 2m$. 假设 $0 \le i \ne j \le 2m - 1$. 再次使用 (1) 中的结论得到, 如果 $i + m \equiv j \pmod{2m}$, 就有 $S_{1i} = S_{1j}$. 如果 $i + m \not\equiv j \pmod{2m}$, 就有 $S_{1i} \cap S_{1j} = \varnothing$.

(3) 通过结论 (2), $S_1 = \cup_{i=0}^{m-1} S_{1i}$. 因此 $|S_1| = \sum_{i=0}^{m-1} |S_{1i}| = 2m^2$.

引理 4.13 假设 $S_{2j}, 0 \le j \le 2m - 1$, 是定义在式子 (4.15) 中的集合. 我们有如下结论:

(1) 对任意的 $0 \le i_1, i_2, j_1, j_2 \le 2m - 1$, $-3^{i_1}(3^{j_1} + 1) \equiv -3^{i_2}(3^{j_2} + 1)(\bmod (3^{2m} - 1))$ 当且仅当 $j_1 = j_2$ 和 $i_1 = i_2$ 或 $j_1 \equiv -j_2 \pmod{2m}$ 和 $i_1 \equiv i_2 + j_2 \pmod{2m}$.

(2) 对任意的 $0 \le i \ne j \le 2m - 1$

$$|S_{2i}| = \begin{cases} m & \text{如果 } i = m, \\ 2m & \text{否则}, \end{cases}$$

并且

$$\begin{cases} S_{2i} = S_{2j} & \text{如果 } i \equiv -j \pmod{2m}, \\ S_{2i} \cap S_{2j} = \varnothing & \text{如果 } i \not\equiv -j \pmod{2m}. \end{cases}$$

(3) $|S_2| = (2m+1)m$.

证明 (1) 假设 $i_2 \geq i_1$. 如果 $3^{i_1}(3^{j_1}+1) \equiv 3^{i_2}(3^{j_2}+1) \pmod{(3^{2m}-1)}$, 就有

$$3^{i_2-i_1+j_2} + 3^{i_2-i_1} - 3^{j_1} - 1 \equiv 0 \pmod{(3^{2m}-1)}. \tag{4.17}$$

假设 a 是一个整数, 满足 $0 \leq i_2 - i_1 + j_2 - 2am \leq 2m-1$. 注意到 $0 \leq a \leq 1$. 定义

$$\begin{cases} s_1 = i_2 - i_1 + j_2 - 2am, \\ s_2 = i_2 - i_1, \\ t = j_1. \end{cases}$$

因为 $1 - 3^{2m-1} \leq 3^{s_1} + 3^{s_2} - 3^t - 1 \leq 2 \cdot 3^{2m-1} - 2$, 由式子 (4.18), 可得 $3^{s_1} + 3^{s_2} - 3^t - 1 = 0$. 因为 $\min\{s_1, s_2\} = \min\{t, 0\} = 0$, 易知集合 $\{s_1, s_2\}$ 中至少有一个元素等于 0.

如果集合 $\{s_1, s_2\}$ 恰好有一个元素等于 0, 就可得如下两种情况:

$$\begin{cases} j_1 + j_2 \equiv 0 \pmod{2m}, i_2 - i_1 = j_1 & \text{如果 } s_1 = 0, s_2 = t, \\ j_1 = j_2, i_1 = i_2 & \text{如果 } s_2 = 0, s_1 = t. \end{cases}$$

如果 $s_1 = s_2 = 0$, 就有 $t = 0$. 由此可得 $j_1 = j_2 = 0$ 和 $i_1 = i_2$.

那么我们根据以上讨论, 可以知道式子 (4.18) 成立当且仅当 $j_1 = j_2$ 和 $i_1 = i_2$ 或 $j_1 + j_2 \equiv 0 \pmod{2m}$ 和 $i_1 \equiv i_2 + j_2 \pmod{2m}$.

(2) 由结论 (1), $-3^{i_1}(3^j+1) \equiv -3^{i_2}(3^j+1) \pmod{(3^{2m}-1)}$ 当且仅当

$$\begin{cases} i_1 = i_2 & \text{如果 } j \neq m, \\ i_1 = i_2 \text{ 或 } i_1 \equiv i_2 + m \pmod{2m} & \text{如果 } j = m. \end{cases}$$

如果 $j = m$, 就有 $|S_{2j}| = m$. 否则, $|S_{2j}| = 2m$. 设 $0 \leq i \neq j \leq 2m-1$. 通过结论 (1) 的证明, 如果 $i + j \equiv 0 \pmod{2m}$, 就有 $S_{2i} = S_{2j}$. 如果 $i + j \not\equiv 0 \pmod{2m}$, 就有 $S_{2i} \cap S_{2j} = \varnothing$.

(3) 由结论 (2), 我们有 $S_2 = \cup_{i=0}^{m} S_{2i}$. 因此 $|S_2| = \sum_{i=0}^{m-1} |S_{2i}| + |S_{2,m}| = 2m^2 + m = (2m+1)m$.

引理 4.14 设 $S_{3j}, 0 \leq j \leq 2m-1$, 是定义在式子 (4.15) 中的集合. 我们有如下结论:

(1) 对任意的 $0 \leq i_1, i_2, j_1, j_2 \leq 2m-1$, $-3^{i_1}(3^{j_1}+1) \equiv -3^{i_2}(3^{j_2}+1) \pmod{(3^m-1)}$ 当且仅当 $j_1 \equiv j_2 \pmod{m}$ 和 $i_1 \equiv i_2 \pmod{m}$ 或 $j_1 \equiv -j_2 \pmod{m}$ 和 $i_1 \equiv i_2 + j_2 \pmod{m}$.

(2) 对任意的 $0 \leq i \neq j \leq 2m-1$,

$$|S_{3i}| = \begin{cases} \frac{m}{2} & \text{如果 } m \text{ 是偶数且 } i = \frac{m}{2} \text{ 或 } \frac{3m}{2}, \\ m & \text{否则.} \end{cases}$$

并且

$$\begin{cases} S_{3i} = S_{3j}, & \text{如果 } i \equiv \pm j \pmod{m}, \\ S_{3i} \cap S_{3j} = \varnothing, & \text{如果 } i \not\equiv \pm j \pmod{m}. \end{cases}$$

(3) $|S_3| = \frac{m(m+1)}{2}$.

证明 (1) 不失一般性, 假设 $i_2 \geq i_1$. 如果 $3^{i_1}(3^{j_1}+1) \equiv 3^{i_2}(3^{j_2}+1) \pmod{(3^m-1)}$, 就有

$$3^{i_2-i_1+j_2} + 3^{i_2-i_1} - 3^{j_1} - 1 \equiv 0 \pmod{(3^m-1)}. \tag{4.18}$$

设 a_1, a_2, a_3 为正整数, 使得

$$\begin{cases} 0 \leq i_1 - i_2 + j_2 - a_1 m \leq m-1, \\ 0 \leq i_2 - i_1 - a_2 m \leq m-1, \\ 0 \leq j_1 - a_3 m \leq m-1. \end{cases}$$

这意味着 $0 \leq a_1 \leq 3, 0 \leq a_2 \leq 1$ 以及 $0 \leq a_3 \leq 1$. 记

$$\begin{cases} s_1 = i_2 - i_1 + j_2 - a_1 m, \\ s_2 = i_2 - i_1 - a_2 m, \\ t = j_1 - a_3 m. \end{cases}$$

因为 $1 - 3^{m-1} \leq 3^{s_1} + 3^{s_2} - 3^t - 1 \leq 2 \cdot 3^{m-1} - 2$, 由式子 (4.18) 得到 $3^{s_1} + 3^{s_2} - 3^t - 1 = 0$. 由于 $\min\{s_1, s_2\} = \min\{t, 0\} = 0$, 集合 $\{s_1, s_2\}$ 包含了至少一个零元.

如果集合 $\{s_1, s_2\}$ 恰好有一个元素等于 0, 就有如下两种情况:

$$\begin{cases} j_1 \equiv -j_2 \pmod{m}, i_1 \equiv i_2 + j_2 \pmod{m} & \text{如果 } s_1 = 0, s_2 = t, \\ j_1 \equiv j_2 \pmod{m}, i_1 \equiv i_2 \pmod{m} & \text{如果 } s_2 = 0, s_1 = t. \end{cases}$$

如果 $s_1 = s_2 = 0$, 就有 $t = 0$. 由此得到 $j_1 \equiv j_2 \equiv 0 \pmod{m}$ 和 $i_1 \equiv i_2 \pmod{m}$.

结合上面的讨论, 我们得到式子 (4.18) 成立当且仅当 $j_1 \equiv j_2 \pmod{m}, i_1 \equiv i_2 \pmod{m}$ 或 $j_1 \equiv -j_2 \pmod{m}, i_1 \equiv i_2 + j_2 \pmod{m}$.

(2) 由结论 (1), 可得 $-3^{i_1}(3^j+1) \equiv -3^{i_2}(3^j+1) \pmod{(3^m-1)}$ 当且仅当

$$\begin{cases} i_1 \equiv i_2 \pmod{m} \text{ 或 } i_1 \equiv i_2 + \frac{m}{2} \pmod{m} & \text{如果 } m \text{ 是偶数并且 } j = \frac{m}{2} \text{ 或 } \frac{3m}{2}, \\ i_1 \equiv i_2 \pmod{m} & \text{否则}. \end{cases}$$

因此, 如果 m 是偶数, 对任意的 $0 \leq i \leq 2m-1$ 和 $i \neq \frac{m}{2}, \frac{3m}{2}$, $|S_{3,\frac{m}{2}}| = |S_{3,\frac{3m}{2}}| = \frac{m}{2}$ 和 $|S_{3i}| = m$. 如果 m 是奇数, 对任意的 $0 \leq i \leq 2m-1$, $|S_{3i}| = m$. 另外, 当 $i \equiv \pm j \pmod{m}$ 时, $S_{3i} = S_{3j}$. 当 $i \not\equiv \pm j \pmod{m}$ 时, $S_{3i} \cap S_{3j} = \varnothing$.

(3) 由结论 (2), 如果 m 是偶数, 那么 $|S_3| = \sum_{i=0}^{\frac{m}{2}-1} |S_{3i}| + |S_{3,\frac{m}{2}}| = \frac{m^2}{2} + \frac{m}{2} = \frac{m(m+1)}{2}$. 如果 m 是奇数, 那么 $|S_3| = \sum_{i=0}^{\frac{m-1}{2}} |S_{3i}| = \frac{m(m+1)}{2}$. 因此对任意的整数 $m \geq 2$, $|S_3| = \frac{m(m+1)}{2}$.

证明 (定理 4.11) 通过引理 4.12, 引理 4.13和引理 4.14, 可知 $|S| = \sum_{i=0}^{3} |S_i| = 2m+2m^2+(2m+1)m + \frac{m(m+1)}{2} = \frac{9m^2+7m}{2}$. 现在我们有 $\dim(\mathcal{C}) = n - |T| = n - (n - |S|) = \frac{9m^2+7m}{2}$. 那么

$$\dim(\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))) = \dim(\overline{\mathcal{C}^{\perp}}^{\perp}) = \dim(\mathcal{C}) + 1 = \frac{9m^2+7m}{2} + 1.$$

线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 是 4 阶广义 Reed-Muller 码 $\mathcal{R}_3(4,2m)$ 的子码. 另外根据定理 4.9和定理 4.6可知码 $\mathcal{R}_3(4,2m)$ 的最小重量为 3^{2m-2}. 于是码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的最小重量的下界为 3^{2m-2}.

注 4.3 由定理 4.6, 4 阶广义 Reed-Muller 码 $\mathcal{R}_3(4,2m)$ 的维数

$$\begin{aligned} k &= \binom{2m+3}{4} + \binom{2m+2}{3} - \frac{(2m-1)2m}{2} + 1 \\ &> \frac{9m^2+7m}{2} + 1 \\ &= \dim(\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))). \end{aligned}$$

4.2 本章小结

本章计算了线性码 $\mathcal{C}(2m,3)$ 的最小重量码字所对应的支撑 2-设计的关联矩阵. 在 $m \geq 2$ 的情况下, 由关联矩阵的行生成的线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 包含了 $\mathcal{C}(2m,3)$, 并且其有许多仿射不变子码. 这意味着线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的结构较之前的更加丰富. 我们证明了线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 是四阶广义 Reed-Muller 码的子码, 并给出了 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的最小重量的下界. 最后我们通过计算定义在式子 (4.14) 中的码 $\mathcal{C}$ 的定义集确定了 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ 的维数.

5 总结与展望

在本文的第二章中, 我们构造了 Davis-Xiang 图和 RT2 图的指数为 4, 8, 16 以及幂零类数为 2, 3, 4 和 6 的非交换正则自同构群. 这些正则自同构群产生了无定形非交换凯莱结合方案, 这些群包含与 Davis-Xiang 图和 RT2 图相同参数集的偏差集. 由于检验两个 2-群是否同构是一个困难的问题, 在所有正则子群中考虑同构群似乎是困难的. 于是我们通过计算一些群的理论不变量将这些群做一个简单的区分. 本章的结果表明, 通过已知的强正则图和已知的无定形凯莱结合方案的正则子群构造包含非平凡偏差集和无定形凯莱结合方案的非交换群是一个可取的办法. 目前对非交换 p-群上的偏差集的构造依然很欠缺, 所以在接下来的工作中, 我们可以通过研究 p 为奇数时交换 p-群上的强正则图的正则自同构群, 试图得到 p 为奇数时的非交换 p-群上的偏差集. 另外, 在一些结构比较清晰的非交换 p-群上构造新的偏差集也将会是一个有趣的工作.

在本文的第三章中, 我们在由局部环所形成的加法群上构造了部分和族. 通过这种构造, 得到了一类新的有向强正则 m-凯莱图, 其中 $m \geq 2$. 本章所构造的一些有向强正则 m-凯莱图具有大量的新参数, 这意味着部分和族是用来构造有向强正则图非常有用的一种工具. 此外, 推论 3.1表明, 我们亦可以在 $s = 1$ 的情况下通过定理 3.1中的构造得到一类新的一致部分和族. 在目前看来, 关于如何在不同的群上构造带有新参数的有向强正则凯莱图依然是一个比较热门的研究课题. 除此之外, 有关于部分和族的研究和构造还比较欠缺, 在未来的工作中, 我们可以进一步研究部分和族以及一致部分和族的更多性质.

在本文的第四章中, 我们计算了码 $\mathcal{C}(2m, 3)$ 的最小重量码字所对应的支撑 2-设计的关联矩阵. 对任意的整数 $m \geq 2$, 由关联矩阵的行所生成的线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 包含码 $\mathcal{C}(2m, 3)$ 为子码. 这意味着所得到的线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 拥有比码 $\mathcal{C}(2m, 3)$ 更丰富的结构. 我们证明了线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 是 4 阶广义 Reed-Muller 码的子码, 并由此得到了码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 的最小重量的下界. 在这章节的最后我们通过计算式子 (4.14) 中定义的码 $\mathcal{C}$ 的定义集中的元素个数确定了线性码 $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ 的维数. 我们也可以尝试利用其他的线性码, 研究其支撑 t-设计的关联矩阵所生成的线性码, 试图得到性质优良的码. 从大方向看来, 许多有意思的组合结构和码之间的关系还有很大的研究空间, 在接下来的工作我们可以朝着这方面努力.

参考文献

[1] A. Araluze, K. Kutnar, L. Martínez, and D. Marušič (2011). Edge connectivity in difference graphs and some new constructions of partial sum families. *European J. Combin.*, **32**(3), 352–360.

[2] A. Araluze, I. Kovács, K. Kutnar, L. Martínez, and D. Marušič (2012). Partial sum quadruples and bi-Abelian digraphs. *J. Combin. Theory, Ser. A*, **119**(8), 1811–1831.

[3] A. Brouwer, O. Olmez, and S. Y. Song (2012). Directed strongly regular graphs from $1\frac{1}{2}$-designs. *European J. Combin.*, **33**(6), 1174–1177.

[4] A. Duval (1988). A directed graph version of strongly regular graphs. *J. Combin. Theory, Ser. A*, **47**(1), 71–100.

[5] A. E. Brouwer, and W. H. Haemers (2012). Spectra of Graphs. *Universitext*.

[6] A. E. Brouwer, and J. H. van Lint(1984). Strongly regular graphs and partial geometries. *Enumeration and Designs*, **85**, 122.

[7] A. E. Brouwer, and S. A. Hobart. Parameters of directed strongly regular graphs. https://homepages.cwi.nl/∼aeb/math/dsrg/dsrg.html.

[8] A. Kohnert (2007). Constructing two-weight codes with prescribed groups of automorphisms. *Discrete Appl. Math.*, **155**(11), 1451–1457.

[9] A. M. Duval, and D. Iourinski (2003). Semidirect product constructions of directed strongly regular graphs. *J. Combin. Theory, Ser. A*, **104**(1), 157–167.

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

[11] A. V. Ivanov (1985). Amorphous cell rings. II. *Investigations in the algebraic theory of combinatorial objects*, 39–49.

[12] C. Ding (2018). Designs from Linear Codes. *World Scientific*.

[13] C. Ding, C. Tang, and D. Tonchev (2020). Linear codes of 2-designs associated with subcodes of the ternary generalized Reed-Muller codes. *Des. Codes Cryptogr.*, **88**(5), 625–641.

[14] C. Ding, and C. Tang(2020). Infinite families of near MDS codes holding t-designs. *IEEE Trans. Inf. Theory*, **66**(9), 5419–5428.

[15] C. Ding (2018). Infinite families of 3-designs from a type of five-weight code. *Des. Codes Cryptogr.*, **86**(3), 703–719.

[16] C. Ding, and C. Li (2017). Infinite families of 2-designs and 3-designs from linear codes. *Discrete Math.*, **340**(10), 2415–2431.

[17] C. Tang, and C. Ding (2021). An infinite family of linear codes supporting 4-designs. *IEEE Trans. Inf. Theory*, **67**, 244–254. doi: 10.1109/TIT.2020.3032600.

[18] D. Ghinelli (2012). Characterization of some 4-gonal configurations of Ahrens-Szekeres type. *European J. Combin.*, **33**(7), 1557–1573.

[19] E. R. van Dam (2003). Strongly regular decompositions of the complete graph. *J. Algebr. Combin.*, **17**(2), 181–201.

[20] E. Swartz (2015). A construction of a partial difference set in the extraspecial groups of order p^3 with exponent p^2. *Des. Codes Cryptogr.*, **75**(2), 237–242.

[21] F. Adams, A. Gendreau, O. Olmez, and S. Y. Song (2013). Construction of directed strongly regular graphs using block matrices. arXiv preprint, arXiv:1311.0494.

[22] F. Fiedler, M. H. Klin, and M. Muzychuk (2002). Small vertex-transitive directed strongly regular graphs. *Discrete Math.*, **255**(1), 87–115.

[23] F. Fiedler, M. Klin, and C. Pech (1999). Directed strongly regular graphs as elements of coherent algebras. *General Algebra and Discrete Mathematics, Shaker Verlag, Aachen*, 69–87.

[24] I. Bouyukliev, V. Fack, W. Willems, and J. Winne (2006). Projective two-weight codes with small parameters and their corresponding graphs. *Des. Codes Cryptogr.*, **41**(1), 59–78.

[25] J. A. Davis (1994). Partial difference sets in p-groups. *Arch. Math.*, **63**(2), 103–110.

[26] J. A. Davis, and Q. Xiang (2000). A family of partial difference sets with Denniston parameters in nonelementary abelian 2-groups. *European J. Combin.*, **21**(8), 981–988.

[27] J. A. Davis, and Q. Xiang (2004). Negative Latin square type partial difference sets in nonelementary abelian 2-groups. *J. London Math. Soc. (2)*, **70**(1), 125–141.

[28] J. B. Polhill (2008). Generalizations of partial difference sets from cyclotomy to nonelementary abelian p-groups. *Electron. J. Combin.*, **15**(15), 125.

[29] J. B. Polhill (2009). Paley type partial difference sets in non p-groups. *Des. Codes Cryptogr.*, **52**(2), 163–169.

[30] J. B. Polhill (2009). Negative Latin square type partial difference sets and amorphic association schemes with Galois rings. *J. Combin. Des.*, **17**(3), 266–282.

[31] J. B. Polhill, J. A. Davis and K. Smith (2013). A new product construction for partial difference sets. *Des. Codes Cryptogr.*, **68**(1), 15–161.

[32] J. B. Polhill (2002). Constructions of nested partial difference sets with Galois rings. *Designs, Codes and Cryptography*, **25**(3), 299–309.

[33] Jr. E. F. Assmus, and J. D. Key (1998). Polynomial codes and finite geometries. *The Handbook of Coding Theory*, **2**(2), 1269–1343.

[34] Jr. E. F. Assmus, and J. D. Key (1994). Designs and Their Codes. *Cambridge University Press*.

[35] Jr. E. F. Assmus, and Jr. H. F. Mattson (1969). New 5-designs. *J. Combin. Theory(A)*, **6**(2), 122–151.

[36] J. J. Seidel (1979). Strongly regular graphs. *Surveys in Combinatorics*, **38**, 157–180.

[37] K. H. Leung, and S. L. Ma (1995). Partial difference sets with Paley parameters. *Bull. Lond. Math. Soc.*, **27**(6), 553–564.

[38] K. H. Leung, and S. L. Ma (1996). A construction of partial difference sets in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \cdots \mathbb{Z}_{p^2}$. *Des. Codes Cryptogr.*, **8**(1), 167–172.

[39] K. H. Leung, and S. L. Ma (1990). Constructions of partial difference sets and relative difference sets on p-groups. *Bull. London Math. Soc.*, **22**(6), 533–539.

[40] K. H. Leung, and S. L. Ma (1993). Partial difference triples. *J. Algebraic Combin.*, **2**(4), 397–409.

[41] K. Kutnar, D. Marušič, Š. Miklavič, and P. Šparl (2009). Strongly regular tri-Cayley graphs. *European J. Combin.*, **30**(4), 822–832.

[42] K. W. Smith (1995). Non-abelian Hadamard difference sets. *J. Combin. Theory Ser. A*, **70**(1), 144–156.

[43] L. K. Jørgensen (2001). Directed strongly regular graphs with $\mu = \lambda$. *Discrete Math.*, **231**(1), 289–293.

[44] L. Martínez, and A. Araluze (2010). New tools for the construction of directed strongly regular graphs: Difference digraphs and partial sum families. *J. Combin. Theory, Ser. B*, **99**(6), 720–728.

[45] M. J. de Resmini, and D. Jungnickel (1992). Strongly regular semi-Cayley digraphs. *J. Algebraic Combin.*, **1**(2), 171–195.

[46] M. Klin, A. Munemasa, M. Muzychuk, and P. H. Zieschang (2004). Directed strongly regular graphs obtain from coherent algebras. *Linear Algebra Appl.*, **377**(1), 83–109.

[47] N. Hamilton (2002). Strongly regular graphs from differences of quadrics. *Discrete Math.*, **256**(1), 465–469.

[48] O. Olmez, and S. Y. Song (2014). Some families of directed strongly regular graphs obtained from certain finite incidence structures. *Graphs Combin.*, **30**(6), 1529–1549.

[49] P. J. Cameron (2004). Strongly regular graphs. *Topics in Algebraic Graph Theory*, **102**, 203–221.

[50] P. J. Cameron, and J. H. van Lint (1991). Designs, Graphs, Codes and Their Links. *Cambridge: Cambridge University Press*, **22**.

[51] R. C. Bose (1963). Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math.*, **13**(2), 389–419.

[52] R. Wang, X. Du, and C. Fan (2019). Infinite families of 2-designs from a class of non-binary Kasami cyclic codes. *Adv. Math. Commun.*, doi: 10.3934/amc.2020088.

[53] S. A. Hobart, and T. J. Shaw (1999). A note on a family of directed strongly regular graphs. *European J. Combin.*, **20**(8), 819–820.

[54] S. Dodunekov, and I. Landgev (1995). On near-MDS codes. *J. Geometry*, **54**(1), 30–43.

[55] S. Gyürki (2016). Infinite families of directed strongly regular graphs using equitable partitions. *Discrete Math.*, **339**(12), 2970–2986.

[56] S. L. Ma (1994). A survey of partial difference sets. *Des. Codes Cryptogr.*, **4**(4), 221–261.

[57] T. Feng, B. Wen, Q. Xiang, and J. Yin (2013). Partial difference sets from quadratic forms and p-ary weakly regular bent functions. *Adv. Lect. Math. (ALM)*, **27**, 25–40.

[58] T. Ito, A. Munemasa, and M. Yamada (1991). Amorphous association schemes over the Galois rings of characteristic 4. *European J. Combin.*, **12**(6), 513–526.

[59] U. Ott (2016). Some new families of partial difference sets in finite fields. *J. Geom.*, **107**(2), 267–278.

[60] W. C. Huffman, and V. Pless (2010). Fundamentals of Error Correcting Codes. *Cambridge University Press*.

[61] X. D. Hou (2000). Bent functions, partial difference sets, and quasi-Frobenius local rings. *Des. Codes Cryptogr.*, **20**(3), 251–268.

[62] X. D. Hou (2002). New partial difference sets in p-groups. *J. Combin. Des.*, **10**(6), 394–402.

[63] X. D. Hou (2003). Rings and constructions of partial difference sets. *Discrete Math.*, **270**(1), 149–176.

[64] X. D. Hou, K. H. Leung, and Q. Xiang (2001). New partial difference sets in $\mathbb{Z}_{p^2}^t$ and a related problem about Galois ring. *Finite Fields Appl.*, **7**(1), 165–188.

[65] X. D. Hou, and A. A. Nechaev (2007). Construction of finite Frobenius rings and its application to partial difference sets. *J. Algebra*, **309**(1), 1–9.

[66] X. Du, R. Wang, C. Tang, and Q. Wang (2020). Infinite families of 2-designs from two classes of binary cyclic codes with three nonzeros. *Adv. Math. Commun.*, doi: 10.3934/amc.2020106.

[67] X. Du, R. Wang, and C. Fan(2019). Infinite families of 2-designs from a class of cyclic codes with two non-zeros. arXiv:1904.04242 [math.CO].

[68] X. L. Hubaut (1975). Strongly regular graphs. *Discrete Math.*, **13**(4), 357–381.

[69] Y. M. Chee, Y. Tan, and X. D. Zhang (2011). Strongly regular graphs constructed from p-ary bent functions. *J. Algebraic Combin.*, **34**, 251–266.

[70] Y. Q. Chen, and J. B. Polhill (2013). Partial difference sets and amorphic group schemes from pseudo-quadratic bent functions. *J. Algebraic Combin.*, **37**(1), 11–26.

[71] Y. Q. Chen, D. K. Ray-Chaudhuri, and Q. Xiang (1996). Constructions of partial difference sets and relative difference sets using Galois rings II. *J. Combin. Theory, Ser. A*, **76**(2), 179–196.

[72] Y. Tan, Alexander. Pott, and T. Feng (2010). Strongly regular graphs associated with ternary bent functions. *J. Combin. Theory Ser. A*, **117**(6), 668–682.

[73] Z. Wan (2011). Finite Fields and Galois Rings. *World Scientific*.

作者简历

何智文, 女, 1994 年, 汉族, 湖南长沙人. 2012 年考入东北林业大学理学院 (数学与应用数学专业), 2016 年本科毕业, 获得理学学士学位. 2016 年进入浙江大学数学科学学院应用数学专业研究生学习至今.

1. 攻读学位期间发表的论文

- Feng, T., He, Z. W., Chen, Y. Q., Partial difference sets and amorphic Cayley schemes in non-abelian 2-groups, *J. Combin. Des.*, **28** (2019) 273-293.
- Zhou, J., He, Z. W., Chai, Z., Two kinds of constructions of directed strongly regular graphs, *Des. Codes Cryptogr.*, **89** (2021) 255−268.
- He, Z. W., Wen, J. J., Linear codes of 2-designs as subcodes of the generalized Reed-Muller codes, *Cryptogr. Commun.*, (2021).

2. 联系方式

- 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
- 联系方式: zhiwenhe94@163.com